JACOBIAN GRAPHS

ARTHUR FOREY, JAVIER FRESÁN, EMMANUEL KOWALSKI, AND YUVAL WIGDERSON

Abstract. We introduce *jacobian graphs*, which are explicit families of regular graphs that are spectrally indistinguishable from random graphs, but whose local structure is very different from that of random graphs. The construction relies on the geometric properties of generalized jacobians of curves and on general equidistribution theorems for character sums over finite fields.

Contents

1. Introduction

In the companion paper [15], we constructed explicit families of graphs which have very strong spectral pseudorandomness properties, and yet differ strikingly from random graphs by the fact that they do not contain either $K_{2,3}$ or C_4 as subgraphs. These graphs are parameterized by a finite field k, and their properties relied on two facts: (1) that certain explicit subsets of $k \times k$ are Sidon sets (or close relatives of Sidon sets); (2) that certain deep equidistribution theorems due to Katz and Deligne for families of exponential sums over finite fields imply that the empirical spectral distribution is close to the semicircle distribution. These are rather remarkable properties: as we discuss in much greater detail in [15], the latter property implies that our graphs are "spectrally indistinguishable" from random graphs of the same density, whereas the former property is strikingly different from the behavior of random graphs of the same density.

The starting point of the current paper is the fact that both (1) and (2) can be generalized considerably. This allows us in this paper to construct many new examples of graphs with properties similar to those defined in [15]. On the other hand, in doing so we have to rely on more advanced techniques from algebraic and arithmetic geometry. This means that the resulting graphs, which we call *jacobian graphs*, are rather less transparent to the broader

combinatorics community. However, we view these as interesting test cases for many extremal combinatorial problems, in view of the richness of the underlying geometry.

Our goal in this paper is not "merely" to generalize the construction in [15]. The constructions we gave in [15] are rather special: we were only able to construct graphs on p^{2k} vertices, where p is a prime, and gave at most two non-isomorphic graphs of that order. By contrast, the constructions in the present paper are much more varied, in a number of ways: we can construct a graph satisfying (1) and (2) on nearly every number n of vertices (see Section 3), and moreover the number of "genuinely different constructions" is rather large. More precisely, our graphs are defined in terms of curves of genus 1 or 2 over finite fields, and these are parameterized by moduli spaces of dimension 1 and 3, respectively. This means that, rather than arising as "sporadic" examples as in [15], the construction of jacobian graphs in the present paper is much more "robust". We are hopeful that this extra flexibility will manifest itself as further applications; concretely, it may be possible to prove the existence of a jacobian graph with additional desirable properties without explicitly constructing it, by instead averaging over the large family of different jacobian graphs (see Remark 1.6).

This paper will mostly be written with an audience familiar with the language of algebraic geometry, although we provide an appendix with concrete descriptions of some of the basic objects (and we emphasize that these are indeed concrete enough to allow us to compute fully explicitly the graphs that we describe).

A jacobian graph is associated to the following data:

- a field k;
- a smooth projective geometrically connected algebraic curve C defined over k;
- a k-rational effective divisor $\mathfrak{m}$ on C, called a *modulus*;
- a k-rational divisor δ of degree 1 on C.

Given these data, one can define:

- the generalized jacobian $\mathrm{J}_\mathfrak{m}$, which is a connected algebraic group defined over k, of dimension $\dim(\mathrm{J}_\mathfrak{m}) = g + \max(\deg(\mathfrak{m}) - 1, 0)$, where g is the genus of C;
- an Abel–Jacobi map $i_\delta \colon \mathrm{C} - \mathfrak{m} \to \mathrm{J}_\mathfrak{m}$, which is a closed immersion if $\dim(\mathrm{J}_\mathfrak{m}) \geqslant 2$.

Definition 1.1. The corresponding *jacobian graph*[1] $\Gamma(\mathrm{C}, \mathfrak{m}; k)$ is the graph[2] with vertex set $\mathrm{J}_\mathfrak{m}(k)$ and with an edge joining x to y if and only if $x + y \in i_\delta(\mathrm{C} - \mathfrak{m})(k)$.

We will be particularly interested in the case where the dimension of $\mathrm{J}_\mathfrak{m}$ is 2 and $g \geqslant 1$, which implies that $g = 1$ or 2. In this case, it was proved in [13] that the image $\mathrm{S}(k)$ of the k-points of $\mathrm{C} - \mathfrak{m}$ in $\mathrm{J}_\mathfrak{m}(k)$ is a *symmetric Sidon set*, i.e., that there exists an element a_0 of $\mathrm{J}_\mathfrak{m}(k)$, called the *center*, such that $\mathrm{S}(k) = a_0 - \mathrm{S}(k)$, and furthermore the equation

$$a + b = c + d$$

with (a, b, c, d) in $\mathrm{S}(k)$ has only the solutions where $a \in \{c, d\}$ and where $b = a_0 - a$.

[1] We omit δ from the notation.

[2] In this paper, graphs are undirected, without multiple edges, but may have loops.

Theorem 1.2. *With notation as above, assume that k is a finite field. For $n \geqslant 1$, denote by k_n the extension of degree n of k in a fixed algebraic closure $\bar{k}$ of k. Denote further*

$$\Gamma_n(\mathrm{C}, \mathfrak{m}) = \Gamma(\mathrm{C}, \mathfrak{m}; k_n).$$

Assume that $\dim(\mathrm{J}_{\mathfrak{m}}) = 2$ *and the genus of* C *is either* 1 *or* 2.

(1) *The graph $\Gamma_n(\mathrm{C}, \mathfrak{m})$ is a finite graph, d_n-regular with $d_n = |i_\delta(\mathrm{C} - \mathfrak{m})(k_n)|$, and contains no subgraph* $\mathrm{K}_{2,3} =$  .

(2) *The non-trivial spectrum*[3] *of $\Gamma_n(\mathrm{C}, \mathfrak{m})$ is contained in an interval*

$$\Big[-\frac{2}{\sqrt{|k_n|}} + \mathrm{O}(|k_n|^{-1}), \frac{2}{\sqrt{|k_n|}} + \mathrm{O}(|k_n|^{-1})\Big]$$

for all $n \geqslant 1$.

(3) *If* C *is* ordinary, *then there exists a sequence of values of n of positive density such that $\Gamma_n(\mathrm{C}, \mathfrak{m})$ is a Ramanujan graph, i.e., such that the non-trivial spectrum of $\Gamma_n(\mathrm{C}, \mathfrak{m})$ is contained in the interval*

$$\Big[-\frac{2\sqrt{d_n - 1}}{d_n}, \frac{2\sqrt{d_n - 1}}{d_n}\Big].$$

(4) *Suppose that the center of the symmetric Sidon set $i_\delta((\mathrm{C} - \mathfrak{m})(k_n))$ belongs to $2\mathrm{J}_{\mathfrak{m}}(k)$ and that one of the following conditions holds:*

(i) $g = 2$.

(ii) $g = 1$, $\mathfrak{m}$ *is a double point and the integer $a_{\mathrm{C}}(k)$ defined by $|\mathrm{C}(k)| = |k|+1-a_{\mathrm{C}}(k)$ is either* 0 *or has multiplicative order at least* 5 *in $k^\times$.*

(iii) $g = 1$ *and, for some prime ℓ invertible in k, the set of unramified characters for the object $i_{\delta,*}\overline{\mathbf{Q}}_\ell[1](1/2)$ on $\mathrm{J}_{\mathfrak{m}}$, in the sense of Forey–Fresán–Kowalski [14], coincides with the set of characters which are trivial on the kernel of the natural projection $\mathrm{J}_{\mathfrak{m}} \to \mathrm{C}$.*

Then, as $n \to +\infty$, the numbers

$$\lambda \frac{d_n}{\sqrt{d_n - 1}},$$

where λ ranges over the non-trivial eigenvalues of $\Gamma_n(\mathrm{C}, \mathfrak{m})$, counted with multiplicity, become equidistributed according to the semicircle law

$$\mu_{\mathrm{sc}} = \frac{1}{\pi}\sqrt{1 - \frac{x^2}{4}}dx$$

supported on the interval $[-2, 2]$.

(5) *More precisely, for $n \geqslant 1$, the estimate*

$$\mathrm{W}_1\Big(\frac{1}{|\mathrm{J}_{\mathfrak{m}}(k_n)| - 1} \sum_{\substack{\lambda \in \mathrm{Sp}(\Gamma_n(\mathrm{C},\mathfrak{m})) \\ \lambda \neq 1}} \delta_{\lambda d_n/\sqrt{d_n - 1}}, \mu_{\mathrm{sc}}\Big) \ll \frac{1}{n}, \tag{1.1}$$

[3] The spectrum refers to that of the Markov averaging operator of the graph, i.e., to that of $d_n^{-1}\mathrm{A}$, where A is the adjacency matrix. The eigenvalue 1 is called the *trivial* eigenvalue.

holds, where the sum over the spectrum is performed with multiplicity and W_1 *denotes the* 1*-Wasserstein distance between measures on* $\mathbf{R}$.

These properties are similar to those of the graphs described in [15], and we refer the reader to the introduction and discussion in [15] for comments on the context and combinatorial background, as well as motivation for such constructions.

These properties suggest that it would be interesting to understand further invariants of jacobian graphs. In fact, the answer to the following question could have remarkable consequences in Ramsey theory, as we discuss in [15, § 2.3].

Question 1.3. What is the independence number[4] of jacobian graphs? In particular, does there exist $\delta > 0$ such that the independence number of a jacobian graph with n vertices is $\mathrm{O}(n^{3/4-\delta})$? Even if this is not the case for all jacobian graphs, is it true for some infinite sequence of jacobian graphs?

Remark 1.4. Here are some remarks concerning Theorem 1.2.

(1) The proof of this theorem relies on deep tools of algebraic geometry; besides our earlier construction in [15], a useful and fair[5] comparison is the construction of the original Ramanujan graphs [29], which also depends essentially on the Riemann hypothesis over finite fields (as well as on the relation between Hecke eigenvalues of modular forms and varieties over finite fields, due to Eichler, Igusa and Shimura).

(2) The jacobian graphs are "explicit", and can be efficiently constructed once the data that define them is given (Figure 1 below demonstrates this by giving the numerical data in one more or less random example). On the other hand, it is not necessarily straightforward to construct such a graph with n vertices for a given integer n. However, it is easy to find one with $(1+o(1))n$ vertices, at least using a probabilistic algorithm, even if one wishes to have a true Ramanujan graph (see Proposition 3.2).

(3) It is noteworthy that the general jacobian graphs vary in "continuous" families, as explained in Remark 1.6. This is an unusual feature for "extremal" constructions based on algebraic or geometric objects, including those from [15], and we are intrigued by the possibility of exploiting these degrees of freedom in some applications (see Remark 1.6).

(4) Another contrasting feature is that, whereas all non-trivial eigenvalues of the graphs in [15] have large multiplicity (about the square root of the number of vertices), we expect that very few eigenvalues of jacobian graphs should have any multiplicity. This is confirmed experimentally. See [15, § 2.1] for more details about eigenvalue multiplicity and its relation to the phenomenon of eigenvalue repulsion in the study of random matrices.

[4] Recall that this is the largest order of a subset I of vertices such that no $x \neq y$ in I are joined by an edge. If the graph contains loops, we ignore them when considering independent sets.

[5] However, we stress that in our setting, the degree tends to infinity with the order of the graph. In this regime, it is much easier to construct Ramanujan graphs, and proving that certain explicit sequences of graphs (e.g. Paley graphs) are Ramanujan can be done using purely elementary arguments.

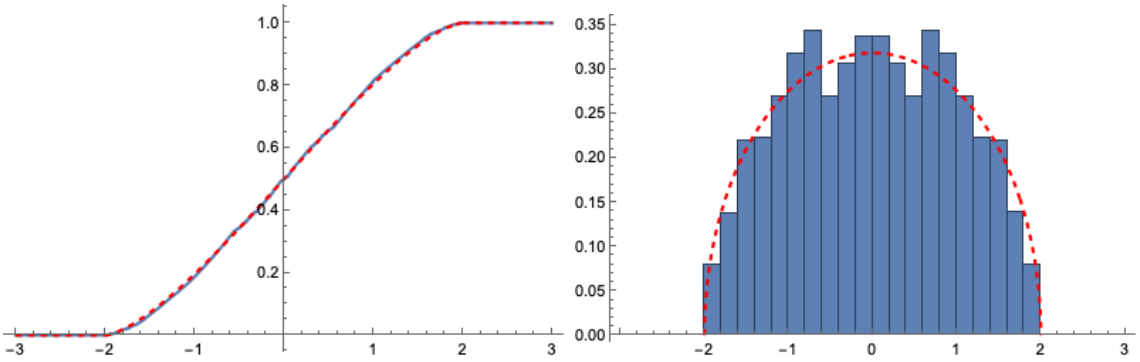

FIGURE 1. Numerical data for the spectrum of the jacobian graph associated to the genus 2 curve defined by $y^2 = x^5 - x^4 + 2x^3 + 2$ over $\mathbf{F}_{53}$ and the trivial modulus. The graph has 2660 vertices. In both charts, the blue data are the spectrum of the graph, and the red curve is the semicircle distribution; the first chart shows the cumulative distribution function, and the second shows a histogram of the probability density function.

(5) The condition that $\Gamma_n(\mathrm{C}, \mathfrak{m})$ is a Ramanujan graph in Theorem 1.2(3) means in particular that it enjoys essentially optimal spectral pseudorandomness properties; see, e.g., the survey of Krivelevich and Sudakov [27, page 19].

(6) For comparison, the graphs constructed in [15] arise in a similar way, but with the underlying group $\mathrm{J}_{\mathfrak{m}}(k_n)$ replaced with the additive group $k_n \times k_n$ and the image of the Abel–Jacobi map replaced by either the graph of the restriction of $x \mapsto x^{-1}$ to $k_n^\times$ or the graph of the cube map $x \mapsto x^3$ (the latter if the characteristic of k is $\geqslant 7$).

(7) As in [15], the fact that our jacobian graphs do not contain a copy of $\mathrm{K}_{2,3}$ is quite striking. Indeed, the Kővári–Sós–Turán theorem [22] implies that *every* n-vertex graph with average degree at least $(\sqrt{2}+o(1))\sqrt{n}$ contains a copy of $\mathrm{K}_{2,3}$, and work of Füredi [16] shows that this is asymptotically best possible (including the factor $\sqrt{2}$). Thus, up to a small multiplicative factor, our jacobian graphs are as dense as possible among all $\mathrm{K}_{2,3}$-free graphs, and therefore highly atypical among all graphs of the same edge density. In particular, an Erdős–Rényi random graph at the same density contains a copy of $\mathrm{K}_{2,3}$ asymptotically almost surely (in fact, it has on the order of n^2 such copies). The same holds in other natural random graph models at the same density, such as random regular graphs with degree $d = \sqrt{n}$.

(8) Condition (iii) in part (4) of the theorem is somewhat technical and will be discussed in more detail when we give the proof. It is related to the finer aspects of the equidistribution theorem of [14]. Although we expect that it should be true in all cases, we do not currently know how to check it concretely in any given case. On the other hand, we will see that the second condition is not very restrictive at all, and can be checked easily for a concrete curve.

Remark 1.5. (1) The Wasserstein (or Monge–Kontorovich or Rubinstein–Kontorovich) distance $\mathrm{W}_1(\mu_1, \mu_2)$ between probability measures on a compact metric space X (in our case,

the interval $[-2,2]$) can be defined as

$$\mathrm{W}_1(\mu_1,\mu_2) = \sup_{f \text{ 1-Lipschitz}} \Big| \int_{\mathrm{X}} f d\mu_1 - \int_{\mathrm{X}} f d\mu_2 \Big|,$$

where f runs over 1-Lipschitz functions $\mathrm{X} \to \mathbf{C}$ (see [26] for an introduction to Wasserstein metrics from the point of view of equidistribution).

(2) We expect that the bound (1.1) could be improved to

$$\mathrm{W}_1\Big(\frac{1}{|\mathrm{J}_{\mathfrak{m}}(k_n)|-1} \sum_{\substack{\lambda \in \mathrm{Sp}(\Gamma_n(\mathrm{C},\mathfrak{m})) \\ \lambda \neq 1}} \delta_{\lambda d_n/\sqrt{d_n-1}}, \mu_{\mathrm{sc}} \Big) \ll \frac{1}{|k_n|^{\gamma}},$$

for some $\gamma > 0$.

Remark 1.6. As we already stated in Remark 1.4, one feature of jacobian graphs is that they depend on "continuous" parameters. More precisely, recall that for any genus g and field k, there exists an algebraic variety $\mathscr{M}_g$ defined over k whose points in any extension k' of k correspond naturally to isomorphism classes of curves of genus g over k'; this is called the coarse moduli space of curves of genus g. The dimension of $\mathscr{M}_g$ is $3g-3$ for $g \geqslant 2$. In particular, for jacobian graphs associated to a curve of genus 2, we have a 3-parameter family of examples over k.

More concretely, some interesting one-parameter families can be obtained, e.g., by looking at the (smooth projective model of the) family of curves

$$y^2 = f(x)(x-t)$$

for a fixed squarefree polynomial $f \in k[\mathrm{X}]$ of degree 4, with t varying among the elements of k which are not roots of f.

One potential application of these continuous families has to do with averaging over many different jacobian graphs. For example, returning to Question 1.3, we expect it to be very difficult to bound the independence number of an arbitrary jacobian graph, but it is not inconceivable that one could instead bound the independence number of an average jacobian graph, using the fact that we have a rich family of these parameterized by $\mathscr{M}_2$. In closely related contexts, such averaging arguments were used by Ruzsa [37] and Pach–Zakharov [36] to study variants of Sidon sets; in both cases, the key input is that abelian groups such as $k \times k$ contain a rich "continuous" family of Sidon sets, and hence one can prove the existence of one with desirable properties by averaging over the whole family. In another closely related context, there is a major line of work that proves that many groups have Cayley graphs and Cayley sum graphs with desirable properties (in particular, small independence number, as in Question 1.3), by averaging over all possible generating sets; see the papers by Conlon–Fox–Pham–Yepremyan [6] and Alon–Pham [1], as well as the references therein, for more details.

Notation. Given complex-valued functions f and g defined on a set S, we write synonymously $f = \mathrm{O}(g)$ or $f \ll g$ if there exists a real number $\mathrm{C} \geqslant 0$ (called an "implicit constant") such that the inequality $|f(s)| \leqslant \mathrm{C}|g(s)|$ holds for all $s \in \mathrm{S}$. We write $f \asymp g$ if $f \ll g$ and $g \ll f$ hold. If f and g are defined on some infinite subset of positive integers, we write $f \sim g$ if $\lim_{n\to\infty} f(n)/g(n) = 1$.

Acknowledgements. We thank K. Soundararajan and J. Merikoski for discussions related to analytic properties of elliptic curves and D. Loeffler for remarks on elliptic curves modulo primes.

A. F. acknowledges the support of the CDP C2EMPI, together with the French State under the France-2030 programme, the University of Lille, the Initiative of Excellence of the University of Lille, the European Metropolis of Lille for their funding and support of the R-CDP-24-004-C2EMPI project. J. F. is partially supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement no. 101170066). E. K. is partially supported by the SNF grant 219220 and the SNF-ANR "Etiene" grant 10003145. Y. W. is supported by Dr. Max Rössler, the Walter Haefner Foundation and the ETH Zürich Foundation.

2. Sum graphs: basic properties and spectrum

The graphs we consider in this paper are examples of the general construction of sum graphs. We begin by surveying some of their basic properties in general. Let G be a finite abelian group and let S be a subset of G. The *(Cayley) sum graph* $\Gamma(\mathrm{G},\mathrm{S})$ is the graph with vertex set G and with x and y connected by an edge if and only if $x+y\in\mathrm{S}$. This graph is $|\mathrm{S}|$-regular (potentially with loops on at most $|\mathrm{S}|$ vertices), and in particular all operators that can be used to define the spectrum are directly equivalent up to scaling. We will use the Markov averaging operator, which we will denote by $\mathrm{M}_{\mathrm{G,S}}$ (omitting the subscript when no confusion arises). This is defined on functions $f\colon \mathrm{G}\to\mathbf{C}$ by

$$\mathrm{M}_{\mathrm{G,S}}f(y)=\frac{1}{|\mathrm{S}|}\sum_{\substack{x\in\mathrm{G}\\ x+y\in\mathrm{S}}}f(x)=\frac{1}{|\mathrm{S}|}\sum_{s\in\mathrm{S}}f(s-y)$$

for all $y\in\mathrm{G}$. Throughout, the spectrum of a graph $\Gamma(\mathrm{G},\mathrm{S})$ always refers to the spectrum of its Markov operator $\mathrm{M}_{\mathrm{G,S}}$, which is a self-adjoint linear map on the space of complex-valued functions on G. It is classical that one can compute this spectrum using characters of G (this already appears, somewhat implicitly, in the work of Chung [5]). We state this formally now, with a minor additional property. We denote by $\widehat{\mathrm{G}}$ the group of characters of G, i.e., the group (under pointwise multiplication) of group homomorphisms from G to $\mathbf{C}^\times$.

Proposition 2.1. *Let* G *be a finite abelian group and* $\mathrm{S}\subset\mathrm{G}$ *a non-empty subset.*

(1) *The spectrum of the graph* $\Gamma(\mathrm{G},\mathrm{S})$ *consists of the numbers*

$$\frac{1}{|\mathrm{S}|}\sum_{y\in\mathrm{S}}\chi(y)$$

for all characters $\chi\in\widehat{\mathrm{G}}$ *such that* $\chi^2=1$ *and of the numbers*

$$-\Big|\frac{1}{|\mathrm{S}|}\sum_{y\in\mathrm{S}}\chi(y)\Big|,\qquad \Big|\frac{1}{|\mathrm{S}|}\sum_{y\in\mathrm{S}}\chi(y)\Big|$$

for all pairs $(\chi,\bar\chi)$ *of non-real characters.*

(2) *For any* $a\in\mathrm{G}$*, the graphs* $\Gamma(\mathrm{G},\mathrm{S})$ *and* $\Gamma(\mathrm{G},a+\mathrm{S})$ *have the same eigenvalues, with multiplicity, associated to pairs of non-real characters.*

The statement is to be understood as follows: if some of the sums coincide for different choices of χ, then the corresponding eigenvalue occurs with multiplicity equal to the number of characters that give rise to it.

Remark 2.2. Many readers will also be aware of Cayley graphs, which are defined similarly to sum graphs, but where we insist that the set S be symmetric (i.e., satisfies $S = -S$), and then join x and y by an edge if and only if $x - y \in S$. Most of our results immediately carry through for Cayley graphs, since their spectra are given by the same character sums above (without taking absolute values). However, we work with Cayley sum graphs because they are defined for all $S \subset G$, rather than only symmetric subsets. Another difference, which may be relevant to certain applications, is that whereas Cayley graphs are highly symmetric (the group G acts transitively on the vertices), this is usually not the case for sum graphs.

The short proof of Proposition 2.1 is given in [15, Prop. 3.3]. We repeat it in a more general context, considering general linear operators on compact abelian groups with additive kernel, since it is no more difficult, and it might be useful for other purposes.

Let G be a compact abelian group. We denote by dx the unique probability Haar measure on G (so it is the normalized counting measure if G is a finite group). Let $t\colon G \to \mathbf{C}$ be a bounded measurable function on G, and let T be the integral operator with kernel $(x, y) \mapsto t(x + y)$, acting on the Hilbert space $L^2(G)$. That is,

$$Tf(y) = \int_G t(x + y)f(x)dx$$

for $f \in L^2(G)$ and $y \in G$. We will generalize Proposition 2.1 by finding a "spectral decomposition" of T (note that T is not always diagonalizable).

For the compact group G, the dual group $\widehat{G}$ is the group of continuous group morphisms $G \to \mathbf{C}^\times$; since G is compact, every such character takes values in the unit circle.

For every character $\chi \in \widehat{G}$ and any $y \in G$, we get

$$T\chi(y) = \int_G t(x + y)\chi(x)dx = \overline{\chi(y)}\,\widehat{t}(\chi),$$

where $\widehat{t}$ is the Fourier transform of t on G, defined as

$$\widehat{t}(\chi) = \int_G t(x)\chi(x)dx$$

for $\chi \in \widehat{G}$ (for convenience, we use here the "probabilistic" normalization of the Fourier transform, instead of the more usual analytic one involving $\overline{\chi(x)}$). Hence, we get the equation

$$T\chi = \widehat{t}(\chi)\overline{\chi}.$$

There are now two cases.

Case 1. If $\chi^2 = 1$, then $\chi = \overline{\chi}$ is an eigenvector with eigenvalue $\widehat{t}(\chi)$.

Case 2. If $\chi^2 \neq 1$, then χ and $\overline{\chi}$ span a 2-dimensional subspace E_χ of $L^2(G)$ satisfying $T(E_\chi) \subset E_\chi$ (by linear independence of characters, or simply because $\overline{\chi} = \alpha\chi$ implies $\alpha = 1$

by evaluating at 1). In the basis $(\chi, \overline{\chi})$, the matrix of the linear map induced by T on E_χ is

$$\begin{pmatrix} 0 & \widehat{t}(\overline{\chi}) \\ \widehat{t}(\chi) & 0 \end{pmatrix}.$$

We now appeal to a simple lemma from linear algebra.

Lemma 2.3. *Let α and β be complex numbers and $\mathrm{A}_{\alpha,\beta} = \begin{pmatrix} 0 & \beta \\ \alpha & 0 \end{pmatrix}$.*

1. *The spectrum of $\mathrm{A}_{\alpha,\beta}$ is $\{\sqrt{\alpha\beta}, -\sqrt{\alpha\beta}\}$, where the choice of the square root is irrelevant if the product $\alpha\beta$ is not a positive real number.*
2. *The matrix $\mathrm{A}_{\alpha,\beta}$ is diagonalizable unless exactly one of α and β is zero.*
3. *Let us endow $\mathbf{C}^2$ with the standard inner product. Then the matrix $\mathrm{A}_{\alpha,\beta}$ is normal if and only if $|\alpha| = |\beta|$, it is self-adjoint if and only if $\beta = \overline{\alpha}$, and it is unitary if and only if $|\alpha| = |\beta| = 1$.*

Proof. The characteristic polynomial $\det(\mathrm{X} - \mathrm{A}_{\alpha,\beta})$ is $\mathrm{X}^2 - \alpha\beta$, and the adjoint (for the standard inner product) is $\mathrm{A}_{\bar{\beta},\bar{\alpha}}$, so all these facts follow from elementary linear algebra. □

This lemma implies that the spectrum of the linear operator T consists of the numbers $\widehat{t}(\chi)$ for χ of order 2, and the numbers

$$\sqrt{\widehat{t}(\chi)\widehat{t}(\overline{\chi})}, \qquad -\sqrt{\widehat{t}(\chi)\widehat{t}(\overline{\chi})}$$

for each pair $(\chi, \overline{\chi})$ with $\chi^2 \neq 1$. Moreover, T is normal if and only if the two-by-two blocks are all normal, meaning if and only if $|\widehat{t}(\chi)| = |\widehat{t}(\overline{\chi})|$ for all χ with $\chi^2 \neq 1$ (or for all χ, since this condition is automatic for $\chi^2 = 1$). Similarly, the operator T is self-adjoint if and only if $\overline{\widehat{t}(\chi)} = \widehat{t}(\overline{\chi})$ for all χ. Since

$$\overline{\widehat{t}(\chi)} = \int_{\mathrm{G}} \overline{t(x)\chi(x)}dx, \qquad \widehat{t}(\overline{\chi}) = \int_{\mathrm{G}} t(x)\overline{\chi(x)}dx,$$

this is the case if and only if t is real-valued. In this case, the operator T is diagonalizable; its spectrum consists of $\widehat{t}(\chi)$ for $\chi^2 = 1$ and

$$|\widehat{t}(\chi)|, \qquad -|\widehat{t}(\chi)|$$

for pairs $(\chi, \overline{\chi})$ with $\chi^2 \neq 1$, with multiplicity taken into account.

We now specialize this discussion to prove Proposition 2.1. We consider therefore a finite group G, a non-empty subset $\mathrm{S} \subset \mathrm{G}$, and t of the form

$$t = \frac{\mathbf{1}_{\mathrm{S}}}{|\mathrm{S}|},$$

where $\mathbf{1}_{\mathrm{S}}$ denotes the characteristic function of S. Then the operator T is the Markov operator $\mathrm{M}_{\mathrm{G},\mathrm{S}}$ of the graph $\Gamma(\mathrm{G}, \mathrm{S})$, and the previous discussion establishes the first two statements of Proposition 2.1.

For the last statement, observe that for any character χ of G, we have

$$\frac{1}{|\mathrm{S}|}\sum_{y \in a+\mathrm{S}} \chi(y) = \frac{\overline{\chi(a)}}{|\mathrm{S}|}\sum_{y \in \mathrm{S}} \chi(y),$$

and thus the two sums have the same modulus for any non-real character.

3. Jacobian graphs: basic properties

Let k be a finite field. We now consider the data $(k, \mathrm{C}, \mathfrak{m})$ which is used to define the jacobian graphs $\Gamma_n(\mathrm{C}, \mathfrak{m})$. For simplicity, we will assume that all components of the modulus $\mathfrak{m}$ are k-rational points. For each $n \geqslant 1$, we abbreviate

$$\mathrm{S}_n = i_\delta((\mathrm{C} - \mathfrak{m})(k_n)) \subset \mathrm{J}_\mathfrak{m}(k_n).$$

From the Riemann hypothesis for curves over finite fields, due to Weil, and the structure of the generalized jacobians, it follows that $|\mathrm{J}_\mathfrak{m}(k_n)| \sim |k_n|^{\dim(\mathrm{J}_\mathfrak{m})}$ and $|\mathrm{S}_n| \sim |k_n|$ as $n \to +\infty$ (see, for instance, [13, § 3] for precise bounds and references for these facts; for curves and for the case $\mathfrak{m} = \emptyset$, see also [33, Th. 19.1] and [34, Th. 11.1]). Thus, the degree d and the number of vertices $|\mathrm{V}|$ of $\Gamma_n(\mathrm{C}, \mathfrak{m})$ are related by $d \sim |\mathrm{V}|^{1/\dim(\mathrm{J}_\mathfrak{m})}$.

From Proposition 2.1 applied to $\Gamma_n(\mathrm{C}, \mathfrak{m})$, it follows that the spectrum of $\Gamma_n(\mathrm{C}, \mathfrak{m})$ is determined by the exponential sums

$$\sum_{x \in \mathrm{S}_n} \chi(x) = \sum_{x \in (\mathrm{C} - \mathfrak{m})(k_n)} \chi(i_\delta(x))$$

for $\chi \in \widehat{\mathrm{G}}_n$. We deduce the following spectral bound.

Proposition 3.1. *Let $(\mathrm{C}, \mathfrak{m})$ be as above. There exists a constant $c \geqslant 0$ with the following property: if $n \geqslant 1$ satisfies*

$$|(\mathrm{C} - \mathfrak{m})(k_n)| > c|k_n|^{1/2},$$

then the graph $\Gamma_n(\mathrm{C}, \mathfrak{m})$ is connected, so $\lambda = 1$ is an eigenvalue with multiplicity 1, and any eigenvalue $\lambda \neq 1$ of the Markov operator of $\Gamma_n(\mathrm{C}, \mathfrak{m})$ satisfies

$$|\lambda| \leqslant c\frac{|k_n|^{1/2}}{|(\mathrm{C} - \mathfrak{m})(k_n)|} = \mathrm{O}(1/|k_n|^{1/2}).$$

Proof. We first recall that a graph is connected if and only if 1 is an eigenvalue with multiplicity 1.

The statements follow from the Riemann hypothesis over finite fields, but in the most general form proved by Deligne [9]. More precisely, the latter implies (see [14, Ch. 11], or compare with the beginning of the proof of Theorem 4.1 below) that there exists a constant $c \geqslant 0$ such that

$$\Big|\frac{1}{|k_n|^{1/2}} \sum_{x \in (\mathrm{C} - \mathfrak{m})(k_n)} \chi(i_\delta(x))\Big| \leqslant c$$

for any non-trivial character $\chi \colon \mathrm{J}_\mathfrak{m}(k_n) \to \mathbf{C}^\times$.

If a character $\chi \neq 1$ gives rise to the eigenvalue 1 of the Markov operator, then the corresponding sum must be equal to

$$\Big|\frac{1}{|k_n|^{1/2}} \sum_{x \in (\mathrm{C} - \mathfrak{m})(k_n)} \chi(i_\delta(x))\Big| = \frac{|(\mathrm{C} - \mathfrak{m})(k_n)|}{|k_n|^{1/2}},$$

and hence the following inequality holds:

$$\frac{|(\mathrm{C}-\mathfrak{m})(k_n)|}{|k_n|^{1/2}} \leqslant c.$$

Therefore, for all n for which the above inequality fails (in particular for all large n, since $|(\mathrm{C}-\mathfrak{m})(k_n)| \sim |k_n|$ as $n \to +\infty$), we deduce that 1 is an eigenvalue with multiplicity 1, and that the other eigenvalues satisfy

$$|\lambda| = \Big|\frac{1}{|\mathrm{S}_n|}\sum_{x\in \mathrm{S}_n}\chi(x)\Big| = \frac{|k_n|^{1/2}}{|\mathrm{S}_n|}\Big|\frac{1}{|k_n|^{1/2}}\sum_{x\in(\mathrm{C}-\mathfrak{m})(k_n)}\chi(i_\delta(x))\Big| \leqslant c\frac{|k_n|^{1/2}}{|\mathrm{S}_n|},$$

for some character χ. □

In the remainder of this paper, we will restrict our attention to pairs $(\mathrm{C},\mathfrak{m})$ such that the graphs have maximal possible edge density and C has genus $g \geqslant 1$. As explained in [13, § 3], this occurs when $g = 1$ and $\mathfrak{m}$ has degree 2, or $g = 2$ and $\mathfrak{m}$ is trivial, and the image of $\mathrm{C}-\mathfrak{m}$ in $\mathrm{J}_\mathfrak{m}$ is then a symmetric Sidon set.

We will now describe the three possible cases of data $(\mathrm{C},\mathfrak{m})$ that satisfy these conditions. We first recall that in the case $g = 1$, since k is a finite field, there exists a k-rational point which can be taken as the origin to define an abelian group law on C, which becomes an elliptic curve. We always assume that this is done.

(1) If $g = 1$ and $\mathfrak{m}$ is the sum of two distinct k-rational points, then the group $\mathrm{J}_\mathfrak{m}(k_n)$ sits for all $n \geqslant 1$ in an exact sequence

$$1 \to k_n^\times \to \mathrm{J}_\mathfrak{m}(k_n) \to \mathrm{C}(k_n) \to 1. \tag{3.1}$$

(2) If $g = 1$ and $\mathfrak{m}$ is a single k-rational point with multiplicity two, then the group $\mathrm{J}_\mathfrak{m}(k_n)$ sits for all $n \geqslant 1$ in an exact sequence

$$1 \to k_n \to \mathrm{J}_\mathfrak{m}(k_n) \to \mathrm{C}(k_n) \to 1. \tag{3.2}$$

(3) If $g = 2$ and $\mathfrak{m}$ is zero, then $\mathrm{J}_\mathfrak{m}$ is the classical two-dimensional jacobian variety of the smooth curve C. We then write J instead of $\mathrm{J}_\mathfrak{m}$.

We now use this information to address the question of which integers arise as the number of vertices for jacobian graphs satisfying the assumptions of Theorem 1.2. Readers mostly interested in the proof of the theorem for an individual curve may skip to the next section.

Proposition 3.2. *Let $x \geqslant 2$ be a real number. Let $\mathrm{N}(x)$ (resp. $\mathrm{M}(x)$) be the number of positive integers $m \leqslant x$ for which there exist a prime p and an ordinary curve of genus 2 over $\mathbf{F}_p$ such that $\mathrm{J}(\mathbf{F}_p)$ has m points (resp. the number $m \leqslant x$ for which such a curve exists for which the center of the symmetric Sidon set is in $2\mathrm{J}(\mathbf{F}_p)$).*

We then have

$$\mathrm{N}(x) = x + \mathrm{O}(x^{5/6}), \qquad \mathrm{M}(x) \geqslant \frac{x}{2} + \mathrm{O}(x^{5/6}).$$

Proof. The second statement follows from the first by simply considering the odd integers counted by $\mathrm{N}(x)$. Indeed, if $\mathrm{J}(\mathbf{F}_p)$ has odd cardinality, then the multiplication by 2 map is an isomorphism of $\mathrm{J}(\mathbf{F}_p)$, so the center of the symmetric Sidon set is in its image.

Let $\mathrm{N}'(x)$ be the number of positive integers $m \leqslant x$ for which there exists an *ordinary abelian surface* over a finite field $\mathbf{F}_p$ with $p > 7$ having m rational points. It was proved by Bröker, Howe, Lauter and Stevenhagen [4, Th. 3.1] that $\mathrm{N}'(x)$ satisfies[6]

$$\mathrm{N}'(x) = x + \mathrm{O}(x^{5/6})$$

(to be precise, the fact that the surfaces are ordinary is not formally stated, but is mentioned in the first paragraph of the proof of [4, Lemma 3.2]).

A criterion of Howe, Nart and Ritzenthaler [20, Th. 1.2] determines which isogeny classes of abelian surfaces over finite fields contain the jacobian of a genus 2 curve. Since isogenous abelian varieties over finite fields have the same number of rational points, it suffices therefore to prove that the abelian surfaces constructed in [4, Lemma 3.2] satisfy these conditions except possibly for $\ll x^{5/6}$ values of m.

For a given m, let A be the ordinary abelian surface constructed in [4, Proof of Lemma 3.2]. Recall, for instance from [33, Th. 19.1], that the size of $\mathrm{A}(\mathbf{F}_p)$ is the value $f(1)$ of the so-called Weil polynomial of A. The Weil polynomials for the abelian surface constructed in [4] are expressed in the form

$$f = \mathrm{X}^4 - a\mathrm{X}^3 + (b + 2p)\mathrm{X}^2 - ap\mathrm{X} + p^2$$

for some integers a and b (see [4, (3.1)]). On the other hand, the criterion of [20] concerns a Weil polynomial of the form

$$f = \mathrm{X}^4 + a_1\mathrm{X}^3 + b_1\mathrm{X}^2 + a_1p\mathrm{X} + p^2$$

for integers a_1 and b_1.

Suppose that the isogeny class of A does *not* contain a jacobian. Then [20, Th. 1.2] proves that one of the following two situations occurs.

Case 1. *The abelian surface splits (up to isogeny) as a product of two elliptic curves.* Then, by [20, Th. 1.2], the associated Weil polynomials are of the form

$$(\mathrm{X}^2 - s\mathrm{X} + p)(\mathrm{X}^2 - t\mathrm{X} + p)$$

for some integers s and t, and we have either $|s - t| = 1$ or $s = t$ (see [20, table 1], noting that the ordinary case corresponds to p-rank equal to 2).

If $s = t$, then $m = (p - s + 1)^2$ is a square, so this can only occur for $\ll x^{1/2}$ values of m. If $s - t = 1$ (and symmetrically if $s - t = -1$), then

$$m = (p - (t + 1) + 1)(p - t + 1) = (p - t + 1)^2 - (p - t + 1)$$

is of the form $u^2 - u$ for some integer u, and this can only occur for $\ll x^{1/2}$ values of m.

Case 2. *The abelian surface is simple.* Then by [20, table 2], we first see that $b_1 < 0$ (this is part of the information from the first three lines of this table). However, the construction in [4, Lemma 3.2] for primes $p > 7$ provides polynomials with $b \geqslant -2p - 2$, and hence $b_1 = b + 2p \geqslant -2$. Thus, the only possibilities would be $b_1 = -1$ or $b_1 = -2$. The second case is not possible for $p > 7$, because from [20, table 2], we have either $b_1 = 1 - 2p \leqslant -13$, or $b_1 = 2 - 2p \leqslant -12$, or all primes dividing b_1 are $\equiv 1 \pmod 3$. In the first case, from [20, table 2], we see that $a_1^2 = p + b_1 = p - 1$. Thus, the prime p must be of the form $s^2 + 1$

[6] A key analytic input is a theorem of Matomäki [30] concerning the average size of "large" gaps between primes; using a more recent result of Heath-Brown [19], we would obtain an error term of size $x^{4/5}$.

for some integer $s \geqslant 1$, and for such a prime, the Weil polynomial of A can only be one of the two polynomials

$$\mathrm{X}^4 + s\mathrm{X}^3 - \mathrm{X}^2 + ps\mathrm{X} + p^2, \qquad \mathrm{X}^4 - s\mathrm{X}^3 - \mathrm{X}^2 - ps\mathrm{X} + p^2.$$

Note that p is of size $\mathrm{O}(m^{1/2})$ by the estimate $|\mathrm{A}(\mathbf{F}_p)| \sim |\mathbf{F}_p|^{\dim(\mathrm{A})}$; the number of primes p of the form s^2+1 that are of this size is $\mathrm{O}(m^{1/4})$ (just counting all integers which can be of the form s^2+1), and each prime leads to at most two excluded values of $m = f(1)$. Hence, the number of $m \leqslant x$ where this second case may occur is $\mathrm{O}(x^{1/4})$. □

Remark 3.3. (1) We note that standard conjectures on gaps between primes suggest strongly that *all* positive integers (except maybe squares or integers of the form $r(r \pm 1)$ and finitely many exceptions) should arise as the size of a jacobian graph.

(2) Here are some comments on values of the orders of jacobian graphs in genus 1. For simplicity, we focus on the cases where the base field is $\mathbf{F}_p$ for some prime p.

(1) If $g = 1$ and $\mathfrak{m}$ is a double point, then from the exact sequence (3.2), we see that the number of vertices is $p|\mathrm{C}(\mathbf{F}_p)|$, while the degree is $|\mathrm{C}(\mathbf{F}_p)| - 1$. It follows from the Hasse bound that $|\mathrm{C}(\mathbf{F}_p)| = p + 1 - a_{\mathrm{C}}$, with $|a_{\mathrm{C}}| \leqslant 2\sqrt{p}$, and from the work of Deuring and Honda–Tate that every integer a satisfying this condition occurs for some suitable curve C (see, for instance, the accounts by Waterhouse in [42, Th. 4.1] and by Serre in [40, § 2.6]). So the integers we obtain for these jacobian graphs are very special, since they are those of the form pn for some prime p and some integer n satisfying $|n - 1 - p| \leqslant 2\sqrt{p}$, whereas it is well-known that most integers do not have a prime factor of size close to their square root.

(2) If $g = 1$ and $\mathfrak{m}$ is a sum of two distinct points, from the exact sequence (3.1) we see that the number of vertices is $(p-1)|\mathrm{C}(\mathbf{F}_p)|$, while the degree is $|\mathrm{C}(\mathbf{F}_p)| - 2$. So we again have very special integers, those of the form nm with $n+1$ prime and $|n + 2 - m| \leqslant 2\sqrt{n+1}$.

Finally, we conclude this section by commenting on the issue of the "effectivity" of our construction. There are a number of aspects:

(1) Given a prime number p, it is straightforward to "write down" a curve C over $\mathbf{F}_p$ of genus 1 or 2, using equations of the form $y^2 = f(x)$, and to find rational points to describe a modulus $\mathfrak{m}$ (in the genus 1 case). Because curves of genus 2 and their jacobians are extensively used in cryptography, there are many well-developed algorithms to work with them, and thus to construct the corresponding jacobian graphs efficiently. The case of generalized jacobians is less developed, but Déchène's thesis [8, § 5.3] provides all basic algorithms for this purpose. Given the size of p, the number of vertices of the jacobian graph associated to C is well-understood by the Riemann hypothesis over finite fields, and is of order $p^2 + \mathrm{O}(p^{3/2})$.

(2) One might also be interested in constructing a jacobian graph with a *given* number n of vertices. If n can be factored and has the form given in Remark 3.3 (2), this can be done efficiently using elliptic curves (see the references in [4, § 2]). On the other hand, the work of Bröker, Howe, Lauter and Stevenhagen [4, Th. 1.1, § 3] indicates that the corresponding problem for genus 2 is more difficult.

Remark 3.4. The case $g = 0$ and $\deg(\mathfrak{m}) = 3$ also gives graphs with $\dim(\mathrm{J}_{\mathfrak{m}}) = 2$, which do have some interest, but these are in fact classical. Indeed, as shown in [13], the sets S_n then correspond to the five known infinite families of "densest" Sidon sets (see, for instance, the discussion of Eberhard and Manners [11]), and moreover, their spectrum is much simpler, consisting of only a bounded number of eigenvalues as n varies. More precisely, one can show the following (see previous discussions, e.g., in [27, 35]): the spectrum of $\Gamma_n(\mathrm{C}, \mathfrak{m})$ in this case consists of

(1) the eigenvalue 1 with multiplicity 1;

(2) two eigenvalues of size asymptotic to $-1/|k_n|^{1/2}$ and $1/|k_n|^{1/2}$ with multiplicity $\sim |k_n|^2/2$;

(3) a single eigenvalue of size $\mathrm{O}(1/|k_n|)$ with multiplicity $\sim |k_n|$.

In terms of exponential sums, using the descriptions of the sets S_n in [13], this boils down to the fact that the sums

$$\sum_{\substack{x\in k_n^\times \\ x\neq 1}} \chi_1(x)\chi_2(1-x), \qquad \sum_{x\in k^\times} \chi(x)\psi(ax), \qquad \sum_{x\in k_n} \psi(ax+bx^2),$$

(where χ, χ_1, χ_2 are multiplicative characters of k_n, ψ is a non-trivial additive character of k_n, and $(a, b) \in k_n^2$) are all "generically" of modulus exactly $\sqrt{|k_n|}$ (these are, respectively, Jacobi sums, Gauss sums and quadratic additive Gauss sums).

In this case, there is no further interesting information to be gathered from the distribution of the spectrum, which is very rigid: multiplying the non-trivial eigenvalues by $\sqrt{|k_n|}$, the limit of the empirical spectral measures is simply the atomic measure $\frac{1}{2}(\delta_{-1} + \delta_1)$.

4. Jacobian graphs: semicircular spectrum

We use the basic notation from the previous section. We recall here the main equidistribution result of [14, Ch. 4], as applied to the situation corresponding to the jacobian graphs we consider (this is partly sketched at the end of [14, § 11.1]). The outcome of the general theory, combined with some specific analysis of the current situation, is the following equidistribution property. For $n \geqslant 1$ and $\chi \in \widehat{\mathrm{J}}_{\mathfrak{m}}(k_n)$, we denote

$$\mathrm{U}_n(\chi) = \frac{1}{|k_n|^{1/2}} \sum_{x\in(\mathrm{C}-\mathfrak{m})(k_n)} \chi(i_\delta(x))$$

Except for the normalization, these are the exponential sums that determine the spectrum of $\Gamma_n(\mathrm{C}, \mathfrak{m})$ by Proposition 2.1.

Theorem 4.1. *Let $(\mathrm{C}, \mathfrak{m})$ be such that $\dim(\mathrm{J}_{\mathfrak{m}}) = 2$ and $g = 1$ or 2. Assume that the center of the symmetric Sidon set $i_\delta(\mathrm{C} - \mathfrak{m})$ is $0 \in \mathrm{J}_{\mathfrak{m}}$. If $g = 1$ and $\mathfrak{m}$ is a double point, assume further that the characteristic of k is $\geqslant 5$.*

There exist two compact Lie groups K^g and K^a, contained in $\mathbf{SU}_2(\mathbf{C})$, with K^g a normal subgroup of K^a, such that the following properties hold:

(1) *For any continuous and bounded function* $f\colon \mathbf{C}\to\mathbf{C}$*, we have*

$$\lim_{\mathrm{N}\to+\infty}\frac{1}{\mathrm{N}}\sum_{1\leqslant n\leqslant \mathrm{N}}\frac{1}{|\mathrm{J}_{\mathfrak{m}}(k_n)|}\sum_{\chi\in\widehat{\mathrm{J}}_{\mathfrak{m}}(k_n)} f(\mathrm{U}_n(\chi))=\int_{\mathrm{K}^a} f(\mathrm{Tr}(x))dx.$$

(2) *If* $\mathrm{K}^a=\mathrm{K}^g$*, then for any continuous and bounded function* $f\colon \mathbf{C}\to\mathbf{C}$*, we have*

$$\lim_{n\to+\infty}\frac{1}{|\mathrm{J}_{\mathfrak{m}}(k_n)|}\sum_{\chi\in\widehat{\mathrm{J}}_{\mathfrak{m}}(k_n)} f(\mathrm{U}_n(\chi))=\int_{\mathrm{K}^a} f(\mathrm{Tr}(x))dx.$$

(3) *Furthermore, either* $\mathrm{K}^a=\mathrm{K}^g=\mathbf{SU}_2(\mathbf{C})$ *or* K^a *is a finite subgroup of* $\mathbf{SU}_2(\mathbf{C})$ *isomorphic to one of* $\mathbf{SL}_2(\mathbf{F}_3)$*,* $\mathbf{GL}_2(\mathbf{F}_3)$ *or* $\mathbf{SL}_2(\mathbf{F}_5)$ *embedded in* $\mathbf{SU}_2(\mathbf{C})$ *by an irreducible representation.*

In these statements, dx denotes the unique probability Haar measure on the group K^a*.*

Proof. The *a priori* equidistribution (i.e., the existence of compact Lie groups K^a and K^g, with K^g a normal subgroup of K^a and $\mathrm{K}^a\subset\mathbf{U}_r(\mathbf{C})$ for some integer $r\geqslant 0$ for which (1) holds) is one of the main results of [14], specifically of Theorem 4.8 of loc. cit., applied to the object $\mathrm{M}=i_{\delta *}\overline{\mathbf{Q}}_\ell[1](1/2)$ of (the derived category of constructible sheaves on) $\mathrm{J}_{\mathfrak{m}}$ whose trace function is the (normalized) characteristic function of the image of i_δ. If $\mathrm{K}^a=\mathrm{K}^g$, we get the similar *a priori* statement (2) from Theorem 4.15 of loc. cit.

To conclude the proof of the theorem, we first check that the integer r here is equal to 2. Recall that, for any $n\geqslant 1$ and character $\chi\in\widehat{\mathrm{J}}_{\mathfrak{m}}(k_n)$, there is an associated lisse character sheaf $\mathscr{L}_\chi$ on the generalized jacobian $\mathrm{J}_{\mathfrak{m}}$ (over k_n) with trace function given by χ. The theory (see [14, Prop. 3.17]) implies that there exist subsets $\mathscr{X}_n$ of characters of $\widehat{\mathrm{J}}_{\mathfrak{m}}(k_n)$ such that the equality

$$r=\dim \mathrm{H}^0_c(\mathrm{J}_{\mathfrak{m},\bar{k}},\mathrm{M}\otimes\mathscr{L}_\chi)=\dim \mathrm{H}^1_c((\mathrm{C}-\mathfrak{m})_{\bar{k}},\mathscr{L}_\chi|(\mathrm{C}-\mathfrak{m})),$$

holds for all $\chi\in\mathscr{X}_n$, and $|\mathscr{X}_n|\sim|\mathrm{J}_{\mathfrak{m}}(k_n)|$ as $n\to+\infty$.

Since C is a curve, this dimension can be computed by means of the Grothendieck–Ogg–Shafarevich formula for the Euler–Poincaré characteristic (see, e.g., [14, Th. C.2]): for any character $\chi\neq 1$ in $\mathscr{X}_n$ one has

$$\dim \mathrm{H}^1_c((\mathrm{C}-\mathfrak{m})_{\bar{k}},\mathscr{L}_\chi|(\mathrm{C}-\mathfrak{m}))=(2g-2+|\mathfrak{m}|)+\sum_{x\in\mathrm{supp}(\mathfrak{m})}\mathrm{swan}_x(\mathscr{L}_\chi|(\mathrm{C}-\mathfrak{m}))$$

(this is because both H^0_c and H^2_c vanish if χ is non-trivial, the latter due to the fact that the image of i_δ generates $\mathrm{J}_{\mathfrak{m}}$, and hence $\mathscr{L}_\chi$ cannot be geometrically trivial on the image of i_δ), where the first term arises as the rank of $\mathscr{L}_\chi$, which is 1, multiplied by minus the Euler–Poincaré characteristic of $\mathrm{C}-\mathfrak{m}$.

We now consider separately the different cases of $(g,\mathfrak{m})$ which may occur.

(1) If $g=1$ and the support of $\mathfrak{m}$ consists of two distinct points, then the Swan conductors vanish (because the character sheaf is tame), and hence

$$r=\dim \mathrm{H}^1_c((\mathrm{C}-\mathfrak{m})_{\bar{k}},\mathscr{L}_\chi|(\mathrm{C}-\mathfrak{m}))=(2-2+2)=2$$

for every non-trivial χ.

(2) If $g = 1$ and the support of $\mathfrak{m}$ consists of one double point, say x_0, then the formula

$$\mathrm{swan}_{x_0}(\mathscr{L}_\chi|\mathrm{C} - \{x_0\}) = \begin{cases} 0 & \text{if } \chi \text{ is trivial on the kernel of } \mathrm{J}_\mathfrak{m} \to \mathrm{C}, \\ 1 & \text{if } \chi \text{ is non-trivial on the kernel of } \mathrm{J}_\mathfrak{m} \to \mathrm{C}. \end{cases}$$

holds by Lemma 5.1 below (we use here the assumption that the characteristic is at least 5), and hence

$$\dim \mathrm{H}^1_c((\mathrm{C} - \mathfrak{m})_{\bar{k}}, \mathscr{L}_\chi|(\mathrm{C} - \mathfrak{m})) = (2 - 2 + 1) + 1 = 2,$$

for χ non-trivial on the kernel of the projection, which implies again that $r = 2$ (since there are only $|\mathrm{C}(k_n)|$ characters trivial on the kernel of the projection, so $\mathscr{X}_n$ is not contained in this set for large enough n).

(3) If $g = 2$ and $\mathfrak{m} = \emptyset$, then there is no Swan conductor to consider, and hence

$$r = \dim \mathrm{H}^1_c(\mathrm{C}_{\bar{k}}, \mathscr{L}_\chi|\mathrm{C}) = (4 - 2) = 2.$$

for every non-trivial χ.

Thus, we have shown that $\mathrm{K}^g \subset \mathrm{K}^a \subset \mathbf{U}_2(\mathbf{C})$ in all cases. Furthermore, the assumption that the image of i_δ is a symmetric Sidon set with center 0 implies that K^a is contained in $\mathbf{SU}_2(\mathbf{C})$ (see the proof of [14, Th. 11.1 (2)] for this argument, or note that it implies that the sums $\mathrm{U}_n(\chi)$ are real).

Moreover, because the image of i_δ is a symmetric Sidon set, the fourth moment

$$\mathrm{M}_4 = \int_{\mathrm{K}^a} |\mathrm{Tr}(x)|^4 dx$$

of $\mathrm{K}^a \subset \mathbf{SU}_2(\mathbf{C})$ is equal to 2 (see Proposition 8.9 and the end of the proof of Theorem 11.1 of loc. cit. for this; in particular, note that although one would expect a fourth moment equal to 3 by a naive computation, the contribution of the trivial character means that the actual fourth moment is 2). Larsen's alternative (see [21, Th. 1.1.6] or [14, Th. 8.5]) then implies that either $\mathrm{K}^a = \mathbf{SU}_2(\mathbf{C})$, or K^a is a finite subgroup of $\mathbf{SU}_2(\mathbf{C})$. In the first case, we deduce that $\mathrm{K}^a = \mathrm{K}^g = \mathbf{SU}_2(\mathbf{C})$, because one knows that K^g is a normal subgroup of K^a with abelian quotient (see [14, Prop. 3.41]), and $\mathbf{SU}_2(\mathbf{C})$ has no such subgroup except itself.

If K^a is finite, then Katz has proved [21, Th. 1.3.2] that the condition $\mathrm{M}_4 = 2$ implies that the representation $\mathrm{K}^a \subset \mathbf{SU}_2(\mathbf{C})$ is not induced, which means that K^a is then an irreducible primitive subgroup of $\mathbf{SU}_2(\mathbf{C})$. The classification of these subgroups is classical (it is a variant of the well-known classification of finite subgroups of $\mathbf{SO}_3$). The three possible primitive groups are often called the binary tetrahedral, octahedral and icosahedral groups, but to check that these are indeed the three groups we indicated, it is enough to check that the orders correspond and that $\mathbf{SL}_2(\mathbf{F}_3)$, $\mathbf{GL}_2(\mathbf{F}_3)$ and $\mathbf{SL}_2(\mathbf{F}_5)$ have faithful two-dimensional representations, since we know that $\mathbf{SU}_2(\mathbf{C})$ contains no other finite primitive subgroup; we refer the reader, e.g, to [28, Th. 6.11] for this classification, and the other facts are elementary. Thus the last part of assertion (3) follows. □

Our next step is a conditional deduction of Theorem 1.2 from Theorem 4.1.

Proof of Theorem 1.2, assuming $\mathrm{K}^a = \mathrm{K}^g = \mathbf{SU}_2(\mathbf{C})$ *in Theorem 4.1.*

(1) The property that $\Gamma_n(\mathrm{C},\mathfrak{m})$ does not contain a copy of $\mathrm{K}_{2,3}$ follows immediately from the fact that $i_\delta((\mathrm{C}-\mathfrak{m})(k_n))$ is a symmetric Sidon set (by [13]) and an elementary computation, which is given for instance in [15, Prop. 3.1].

(2) Let χ be a non-trivial character of $\mathrm{J}_\mathfrak{m}(k_n)$. From the fact that the object $i_{\delta*}\overline{\mathbf{Q}}_\ell[1](1/2)$ is mixed of weights $\leqslant 0$, so that $i_{\delta*}\overline{\mathbf{Q}}_\ell[1](1/2)\otimes\mathscr{L}_\chi$ is also mixed of weights $\leqslant 0$ with trace function on $\mathrm{J}_\mathfrak{m}(k_n)$ given by

$$y\mapsto\begin{cases}\chi(i_\delta(x)) & \text{if } y=i_\delta(x) \text{ for some } x\in(\mathrm{C}-\mathfrak{m})(k_n),\\ 0 & \text{otherwise,}\end{cases}$$

and that

$$\mathrm{H}^2_c((\mathrm{C}-\mathfrak{m})_{\bar{k}},\mathscr{L}_\chi|(\mathrm{C}-\mathfrak{m}))=0$$

(because the image of i_δ generates $\mathrm{J}_\mathfrak{m}$), we first deduce the bound

$$\Big|\sum_{x\in(\mathrm{C}-\mathfrak{m})(k_n)}\chi(i_\delta(x))\Big|\leqslant 2\sqrt{|k_n|}$$

so that the constant c of Proposition 3.1 can be taken to be equal to $r=2$. It follows that the largest absolute value of a non-trivial eigenvalue of $\Gamma_n(\mathrm{C},\mathfrak{m})$ is at most $2\frac{\sqrt{|k_n|}}{d_n}$. Since the Riemann hypothesis for curves implies that

$$d_n=|k_n|-|\mathfrak{m}|+\mathrm{O}(|k_n|^{1/2}),$$

we obtain Theorem 1.2(2).

(3) We now prove Theorem 1.2(3). For this, denote again $d_n=|(\mathrm{C}-\mathfrak{m})(k_n)|$. Since we saw that the non-trivial eigenvalues of the Markov operator have absolute value

$$\leqslant\frac{2\sqrt{|k_n|}}{d_n},$$

the graph $\Gamma_n(\mathrm{C},\mathfrak{m})$ is a Ramanujan graph if

$$\frac{2\sqrt{|k_n|}}{d_n}\leqslant 2\frac{\sqrt{d_n-1}}{d_n},$$

i.e. if $d_n\geqslant|k_n|+1$. We write

$$d_n=|\mathrm{C}(k_n)|-|\mathfrak{m}|=|k_n|+1-|\mathfrak{m}|-a_\mathrm{C}(k_n),$$

so that it suffices to have $a_\mathrm{C}(k_n)\leqslant-|\mathfrak{m}|$ to obtain the desired inequality. According to the Riemann hypothesis for counting points on curves over finite fields, we can write

$$a_\mathrm{C}(k_n)=\begin{cases}2|k_n|^{1/2}\cos(2\pi n\theta_1), & \text{if } g=1,\\ 2|k_n|^{1/2}(\cos(2\pi n\theta_1)+\cos(2\pi n\theta_2)), & \text{if } g=2,\end{cases}$$

for some real numbers θ_1 (resp. θ_1 and θ_2) in the interval $[0,\frac{1}{2}]$.

In the case $g=2$, we see that $\Gamma_n(\mathrm{C},\mathfrak{m})$ is a Ramanujan graph if $a_\mathrm{C}(k_n)\leqslant 0$, and for $g=1$, it suffices that $a_\mathrm{C}(k_n)\leqslant-2$. Roughly speaking, this will occur with probability $1/2$ or very close to $1/2$.

More precisely, assume that C is ordinary. We then have $\theta_1\neq 0$ (resp. $\theta_1\neq 0$ and $\theta_2\neq 0$ if $g=2$). Consider the set X in $(\mathbf{R}/\mathbf{Z})^g$ of points $(\{n\theta_i\})_{1\leqslant i\leqslant g}$, where $\{x\}$ denotes the

image in $\mathbf{R}/\mathbf{Z}$ of a real number x. By the Kronecker–Weyl equidistribution theorem (see, e.g., [25, Th. B.6.5]), the set X is equidistributed as $n \to +\infty$ according to the uniform probability measure on its closure $\bar{\mathrm{X}}$, which is a closed subgroup of $(\mathbf{R}/\mathbf{Z})^g$.

The assumption that $\theta_i \neq 0$ implies straightforwardly that

$$\lim_{\mathrm{N}\to+\infty} \frac{1}{\mathrm{N}} \sum_{1\leqslant n\leqslant \mathrm{N}} \frac{a_{\mathrm{C}}(k_n)}{\sqrt{|k_n|}} = 0,$$

and therefore, by equidistribution, the continuous function $f\colon \bar{\mathrm{X}} \to \mathbf{R}$ defined by

$$f(x) = \sum_{i=1}^{g} \cos(2\pi x_i)$$

has integral 0 on $\bar{\mathrm{X}}$. Since there are points (x_i) in $\bar{\mathrm{X}}$ with $f(x) > 0$ (e.g. $x = 0$), it follows that f must also take negative values on a set of positive measure, which means that there exists $c < 0$ such that the measure of the set of $(x_i) \in \bar{\mathrm{X}}$ with $f(x) < c$ is positive. By equidistribution, there is therefore a positive density set of values of n such that

$$a_{\mathrm{C}}(k_n) \leqslant -\frac{c}{2}\sqrt{|k_n|},$$

which is $\leqslant -2$ if $|k_n|$ is large enough.

(5) We now proceed to the proof of Theorem 1.2(4). We first perform a reduction to the case considered in Theorem 4.1. Let $a \in \mathrm{J}_{\mathfrak{m}}(k)$ be the center of the symmetric Sidon set $\mathrm{S} = i_\delta(\mathrm{C} - \mathfrak{m})(k)$. By assumption, there exists $b \in \mathrm{J}_{\mathfrak{m}}(k)$ such that $a = 2b$. Let $\mathrm{S}' = -b + \mathrm{S}$. Since $\mathrm{S} = a - \mathrm{S}$, we have

$$\mathrm{S}' = -b + \mathrm{S} = -b + a - \mathrm{S} = b - \mathrm{S} = -\mathrm{S}',$$

i.e., S' is a symmetric Sidon set with center 0. In fact, it arises as the image of the Abel–Jacobi embedding associated to $\delta' = \delta - b$ (viewing the point b on the generalized jacobian as a divisor of degree 0). By the last part of Proposition 2.1, combined with the fact that $\mathrm{J}_{\mathfrak{m}}(\bar{k})$ has at most $2^{2g} \leqslant 16$ characters of order 2, the equidistribution property (as $n \to +\infty$) for the spectrum of the sum graph associated to $i_\delta(\mathrm{C} - \mathfrak{m})(k_n)$ is equivalent to that for $i_{\delta'}(\mathrm{C} - \mathfrak{m})(k_n)$. Replacing δ with δ', we can therefore assume that $a = 0$ and apply Theorem 4.1.

From this theorem, under our assumption that $\mathrm{K}^a = \mathrm{K}^g = \mathbf{SU}_2(\mathbf{C})$, the sums $\mathrm{U}_n(\chi)$ are equidistributed as $n \to +\infty$ like the image of the Haar measure by the trace map $\mathbf{SU}_2(\mathbf{C}) \to [-2, 2]$. It is classical that this image is none other than the semicircle measure μ_{sc} ([3, p. 58, exemple]).

Next, by Proposition 2.1, an eigenvalue λ in the spectrum of $\Gamma_n(\mathrm{C}, \mathfrak{m})$ may be either

$$\lambda = \frac{|k_n|^{1/2}}{|(\mathrm{C} - \mathfrak{m})(k_n)|}\mathrm{U}_n(\chi)$$

for χ of order 2, or

$$\lambda = \frac{|k_n|^{1/2}}{|(\mathrm{C} - \mathfrak{m})(k_n)|}|\mathrm{U}_n(\chi)|, \quad \text{or} \quad \lambda = -\frac{|k_n|^{1/2}}{|(\mathrm{C} - \mathfrak{m})(k_n)|}|\mathrm{U}_n(\chi)|,$$

for pairs $(\chi, \bar{\chi})$ of non-real characters. But the condition that $i_\delta(\mathrm{C} - \mathfrak{m})$ is a symmetric Sidon set with center 0 implies that the sums $\mathrm{U}_n(\chi)$ are real (and hence $\mathrm{S}_n(\bar{\chi}) = \mathrm{U}_n(\chi)$). Thus

the number $\lambda d_n/\sqrt{d_n-1}$ is of the form

$$\varepsilon\frac{|(\mathrm{C}-\mathfrak{m})(k_n)|}{\sqrt{|k_n|(|(\mathrm{C}-\mathfrak{m})(k_n)|-1)}}|\mathrm{U}_n(\chi)|$$

for $\varepsilon=1$ or $\varepsilon=-1$. Since $|k_n|\sim|(\mathrm{C}-\mathfrak{m})(k_n)|$ as $n\to+\infty$, and since $\mathrm{U}_n(\chi)$ becomes μ_{sc}-equidistributed as seen previously, we obtain the equidistribution of $\lambda d_n/\sqrt{d_n-1}$ to μ_{sc} using the fact that this measure is symmetric (i.e., invariant under $x\mapsto -x$).

(4) Finally, once we know the equidistribution theorem with $\mathrm{K}^a=\mathrm{K}^g=\mathbf{SU}_2(\mathbf{C})$, we obtain the bound (1.1) for the Wasserstein distance by applying the bound of Kowalski and Untrau [26, § 4.3]. □

Thus, the proof of Theorem 1.2 will be concluded by the following result, which establishes the final condition $\mathrm{K}^a=\mathrm{K}^g=\mathbf{SU}_2(\mathbf{C})$ in the situations considered in Theorem 1.2(4).

Theorem 4.2. *Let $(\mathrm{C},\mathfrak{m})$ be such that $\dim(\mathrm{J}_{\mathfrak{m}})=2$ and $g=1$ or 2. The group K^a is infinite, and hence we have $\mathrm{K}^a=\mathrm{K}^g=\mathbf{SU}_2(\mathbf{C})$, under any of the following conditions:*

(i) *$g=2$.*

(ii) *$g=1$, $\mathfrak{m}$ is a double point and $|\mathrm{C}(k)|=|k|+1-a_{\mathrm{C}}(k)$ for some integer $a_{\mathrm{C}}(k)$ which is either 0 or has multiplicative order at least 5 in $k^\times$.*

(iii) *$g=1$ and the set of unramified characters for the object $i_{\delta,*}\overline{\mathbf{Q}}_\ell[1](1/2)$ on $\mathrm{J}_{\mathfrak{m}}$ coincides with the set of characters that are trivial on the kernel of the projection $\mathrm{J}_{\mathfrak{m}}\to\mathrm{C}$.*

This will be proved in the next section, specifically in Proposition 5.2 for conditions (i) and (iii), and Proposition 5.4 for condition (ii).

Remark 4.3. If we construct a sequence (Γ_m) of jacobian graphs associated to genus 2 curves over prime fields $\mathbf{F}_p$ such that Γ_m has an odd number m of vertices, then the equidistribution still holds as $m\to+\infty$, in the sense that the numbers

$$\lambda\frac{d_m}{\sqrt{d_m-1}},$$

where d_m is the degree of Γ_m and λ ranges over the non-trivial eigenvalues of Γ_m, become equidistributed according to the semicircle law.

This follows from the "horizontal" analogue of [14, Th. 4.8] (compare with [14, Th. 4.19]), taking into account that the complexity (in the sense of Sawin's quantitative sheaf theory [38]) of the objects $i_{\delta*}\overline{\mathbf{Q}}_\ell$ on the varying jacobians is uniformly bounded. This, in turn, can be deduced from [38, Prop. 6.19] and the classical fact from algebraic geometry that there exists an integer N such that a curve of genus 2 and its jacobian both admit projective embeddings in a projective space of dimension at most N, with the image given by at most N equations of degree at most N.

5. Complements on generalized jacobians

We prove here the statements used in the previous section concerning some of the properties of the group K^a in the case of generalized jacobians associated to a genus 1 curve. We keep the notation from the previous section.

Lemma 5.1. *Assume that the characteristic of k is $\geqslant 5$. Suppose that* C *has genus* 1 *and the modulus* $\mathfrak{m}$ *is a double point* $2(x_0)$*. Let* $n \geqslant 1$ *be an integer and let* χ *be a character of* $\mathrm{J}_{\mathfrak{m}}(k_n)$ *which is non-trivial on the kernel of the projection* $\pi\colon \mathrm{J}_{\mathfrak{m}} \to \mathrm{C}$*. Then*

$$\mathrm{swan}_{x_0}(\mathscr{L}_\chi | s(\mathrm{C} - \{x_0\})) = 1.$$

Proof. We view the curve C as given by the solutions of a Weierstrass equation

$$y^2 = x^3 + ax + b,$$

together with the point at infinity ∞, which is then the origin of the group law on C as an elliptic curve. Up to translation we may assume (possibly up to a finite extension) that $x_0 \neq \infty$. We have an exact sequence of algebraic groups

$$1 \to \mathbf{G}_a \to \mathrm{J}_{\mathfrak{m}} \xrightarrow{\pi} \mathrm{C} \to 1.$$

The morphism $s\colon \mathrm{C} - \{x_0\} \to \mathrm{J}_{\mathfrak{m}}$ that maps z to the divisor $(z) - (\infty)$ is a partial section of π. There exists also a partial section $\sigma\colon \mathrm{C} - \{\infty\} \to \mathrm{J}_{\mathfrak{m}}$ (see, e.g., the paper [7, § 3.2] of Corvaja, Masser and Zannier; this reference is written with base field $\mathbf{C}$, but the result only depends on the existence of a Weierstrass equation).

We then define a morphism $\Delta\colon \mathrm{C} - \{x_0, \infty\} \to \mathrm{J}_{\mathfrak{m}}$ by

$$\Delta(z) = s(z) - \sigma(z).$$

Since s and σ are both sections of π, the image of Δ is contained in $\mathbf{G}_a$. Thus, we can view Δ as a rational function on C, with poles at most at $\{x_0, \infty\}$.

We claim that Δ has a *simple* pole at x_0. To see this, fix some $w_0 \in \mathrm{C} - \{x_0, \infty\}$ and consider the rational function κ on C defined by

$$\kappa(z) = \Delta(z + w_0) - \Delta(z) - \Delta(w_0).$$

It suffices to prove that κ has a simple pole at x_0. For this we write $\kappa = \kappa_1 - \kappa_2$, where

$$\kappa_1(z) = s(z + w_0) - s(z) - s(w_0),$$
$$\kappa_2(z) = \sigma(z + w_0) - \sigma(z) - \sigma(w_0).$$

The function κ_2 is regular at x_0. As explained in [7, § 3.5, p. 249], the rational function κ_1 can be expressed in Weierstrass coordinates $z = (x, y)$ as a quotient of linear forms in (x, y), where the denominator has a simple pole at x_0.

We can now complete the proof of the lemma. The Swan conductor is a local quantity, so

$$\mathrm{swan}_{x_0}(\mathscr{L}_\chi | s(\mathrm{C} - \{x_0\})) = \mathrm{swan}_{x_0}(\mathscr{L}_\chi | s(\mathrm{C} - \{x_0, \infty\})).$$

Since χ is a character, there is an isomorphism

$$\mathscr{L}_\chi | s(\mathrm{C} - \{x_0, \infty\}) \simeq \mathscr{L}_\chi | \Delta(\mathrm{C} - \{x_0, \infty\}) \otimes \mathscr{L}_\chi | \sigma(\mathrm{C} - \{x_0, \infty\}).$$

Since the function σ is regular at x_0, the sheaf $\mathscr{L}_\chi | \sigma(\mathrm{C} - \{x_0, \infty\})$ is the restriction of the sheaf $\mathscr{L}_\chi | \sigma(\mathrm{C} - \{\infty\})$ which is lisse at x_0, and hence

$$\mathrm{swan}_{x_0}(\mathscr{L}_\chi | s(\mathrm{C} - \{x_0\})) = \mathrm{swan}_{x_0}(\mathscr{L}_\chi | \Delta(\mathrm{C} - \{x_0, \infty\})).$$

By assumption, the restriction of χ to $\mathbf{G}_a$ is a non-trivial additive character, hence

$$\mathrm{swan}_{x_0}(\mathscr{L}_\chi | \Delta(\mathrm{C} - \{x_0, \infty\}))$$

is the Swan conductor on $\mathbf{G}_a$ of the sheaf associated to an additive character of the function Δ with a simple pole at x_0, and it is classical that it is equal to 1. □

We give two results to prove that the group K^a is infinite. The first applies to all curves, although it is conditional when $g = 1$.

Proposition 5.2. *Let $(\mathrm{C}, \mathfrak{m})$ be data defining a jacobian graph with $g \geqslant 1$ and $\dim \mathrm{J}_{\mathfrak{m}} = 2$. Under the following assumptions, the compact group K^a is infinite.*

(1) *If $g = 2$ and the curve C is arbitrary.*
(2) *If $g = 1$ and the set of ramified characters, in the sense of* [14, Def. 3.25]*, coincides with the set of characters which are trivial on the kernel of the projection $\pi\colon \mathrm{J}_{\mathfrak{m}} \to \mathrm{C}$.*

Proof. (1) The case $g = 2$ is treated in [14, Th. 11.1] (this was known to N. Katz around 2012).

(2) We proceed by contradiction. The assumption that K^a is finite implies that the object

$$\mathrm{M} = i_{\delta *}\overline{\mathbf{Q}}_\ell[1](1/2)$$

is generically unramified by [14, Cor. 3.39]. We assume then that the set of ramified characters coincides with the set of characters that are trivial on the kernel of the projection $\mathrm{J}_{\mathfrak{m}} \to \mathrm{C}$. We denote by $\mathscr{X}$ the set of unramified characters.

Let $n \geqslant 1$ and let χ be a character of $\mathrm{J}_{\mathfrak{m}}(k_n)$. From the basic theory (see [14, § 3.9]), if χ is unramified, then the sum

$$\mathrm{U}_n(\chi) = \frac{1}{|k_n|^{1/2}} \sum_{x \in (\mathrm{C}-\mathfrak{m})(k_n)} \chi(i_\delta(x))$$

is the trace of a matrix belonging to K^a. If K^a is finite, it follows that this is a sum of roots of unity, and in particular it is an algebraic integer (in some cyclotomic field).

Let $y_0 \in \mathrm{J}_{\mathfrak{m}}(k_n)$. Using orthogonality of characters, we compute

$$\sum_{\chi \in \mathscr{X}(k_n)} \overline{\chi(y_0)}\mathrm{U}_n(\chi),$$

which is also an algebraic integer. We find

$$\begin{aligned}\sum_{\chi \in \mathscr{X}(k_n)} \overline{\chi(y_0)}\mathrm{U}_n(\chi) &= \frac{1}{|k_n|^{1/2}} \sum_{x \in (\mathrm{C}-\mathfrak{m})(k_n)} \sum_{\chi \in \mathscr{X}(k_n)} \overline{\chi(y_0)}\chi(i_\delta(x)) \\ &= \frac{1}{|k_n|^{1/2}} \Big(|(\mathrm{C}-\mathfrak{m})(k_n)|\delta(y_0) - \sum_{\chi \notin \mathscr{X}(k_n)} \overline{\chi(y_0)}\chi(i_\delta(x)) \Big),\end{aligned}$$

where $\delta(y_0)$ is 1 if y_0 is in $i_\delta(\mathrm{C})(k_n)$ and 0 otherwise. According to our assumption, the condition $\chi \notin \mathscr{X}(k_n)$ is equivalent to saying that χ is of the form $\chi' \circ \pi$ for some (unique) character χ' of the group $\mathrm{C}(k_n)$. So

$$\sum_{\chi \notin \mathscr{X}(k_n)} \overline{\chi(y_0)}\chi(i_\delta(x)) = \sum_{\chi' \in \widehat{\mathrm{C}}(k_n)} \overline{\chi'(\pi(y_0))}\chi'(x).$$

This is equal to 0 unless $x = \pi(y_0)$, in which case it is $|\mathrm{C}(k_n)|$. There is a single x with the second property, so we conclude that

$$\frac{1}{|k_n|^{1/2}}\Big(|(\mathrm{C} - \mathfrak{m})(k_n)|\delta(y_0) - |\mathrm{C}(k_n)|\Big)$$

is an algebraic integer.

Assume that y_0 is chosen so that $\delta(y_0) = 0$ (such a y_0 exists at least if n is large enough). Write $|\mathrm{C}(k_n)| = |k_n| + 1 - a_{\mathrm{C}}(k_n)$ for some integer $a_{\mathrm{C}}(k_n)$. Then

$$\sum_{\chi \notin \mathscr{X}(k_n)} \overline{\chi(y_0)}\chi(i_\delta(x)) = -\frac{|\mathrm{C}(k_n)|}{|k_n|^{1/2}} = -\Big(|k_n|^{1/2} - \frac{a_{\mathrm{C}}(k_n) - 1}{|k_n|^{1/2}}\Big)$$

is an algebraic integer, and therefore

$$\beta_n = \frac{a_{\mathrm{C}}(k_n) - 1}{|k_n|^{1/2}}$$

is an algebraic integer. By the Hasse bound, we can write further $a_{\mathrm{C}}(k_n) = |k_n|^{1/2}(\alpha_n + \alpha_n^{-1})$ with $|\alpha_n| = 1$, so that

$$\beta_n = \alpha_n + \alpha_n^{-1} - \frac{1}{|k_n|^{1/2}}.$$

All β_n are algebraic integers. Now observe that if we replace n by $3n$, then the relation

$$\alpha_{3n} + \alpha_{3n}^{-1} = \alpha_n^3 + \alpha_n^{-3} = (\alpha_n + \alpha_n^{-1})^3 - 3(\alpha_n + \alpha_n^{-1})$$

holds, and hence

$$\beta_{3n} = \alpha_{3n} + \alpha_{3n}^{-1} - \frac{1}{|k_n|^{3/2}}$$

is congruent modulo algebraic integers to

$$\frac{1}{|k_n|^{3/2}} - \frac{3}{|k_n|^{1/2}} - \frac{1}{|k_n|^{3/2}} = -\frac{3}{|k_n|^{1/2}},$$

which is not an algebraic integer (even if k has characteristic 3, taking n large enough). Thus, we have a contradiction. □

The assumption concerning ramified characters in part (2) of the proposition seems quite reasonable. Indeed, a slight elaboration of the argument used in the computation of r in the beginning of the proof of Theorem 1.2 shows that it is *exactly* for the characters $\chi \in \widehat{\mathrm{J}}_{\mathfrak{m}}(k_n)$ that are non-trivial on the kernel of $\mathrm{J}_{\mathfrak{m}} \to \mathrm{C}$ that the space $\mathrm{H}^0_c(\mathrm{J}_{\mathfrak{m},\bar{k}}, \mathrm{M} \otimes \mathscr{L}_\chi)$ is two-dimensional and that the action of the Frobenius automorphism is unitary (i.e., pure of weight 0), which are necessary conditions for χ to be unramified. In fact, it should follow from the ongoing PhD thesis of Beat Zurbuchen that this condition is also sufficient, thus proving the result unconditionally.

Independently of these developments, we can prove elementarily that K^a is infinite in many cases when $g = 1$ and $\mathfrak{m}$ consists of a double point. This depends on the following lemma.

Lemma 5.3. *Assume that* C *has genus* 1 *and* $\mathfrak{m}$ *is a double point. If* $|k|$ *is coprime to* $|\mathrm{C}(k)|$, *then the sum*

$$\mathrm{T}(\chi) = \sum_{x \in (\mathrm{C}-\mathfrak{m})(k)} \chi(i_\delta(x))$$

is non-zero for all characters χ of $\mathrm{J}_{\mathfrak{m}}(k)$.

Proof. We denote by p the characteristic of k. We have the exact sequence

$$1 \to k \to \mathrm{J}_{\mathfrak{m}}(k) \xrightarrow{\pi} \mathrm{C}(k) \to 1.$$

As before, we recall that the size of $\mathrm{C}(k)$ is given by the formula

$$|\mathrm{C}(k)| = |k| + 1 - a_{\mathrm{C}}(k),$$

where the integer $a_{\mathrm{C}}(k)$ is of the form

$$a_{\mathrm{C}}(k) = |k|^{1/2}(\alpha + \alpha^{-1})$$

for some algebraic number α with $|\alpha| = 1$.

Since we assume that the order of $\mathrm{C}(k)$ is coprime to $|k|$, the above exact sequence splits, and there exists a (section) homomorphism $\sigma\colon \mathrm{C}(k) \to \mathrm{J}_{\mathfrak{m}}(k)$, defining an isomorphism

$$\mathrm{J}_{\mathfrak{m}}(k) \to k \times \mathrm{C}(k)$$

by $x \mapsto (x - \sigma(\pi(x)), \pi(x))$.

Let χ be a character of $\mathrm{J}_{\mathfrak{m}}(k)$, and denote by χ_1 and χ_2 the characters of k and $\mathrm{C}(k)$ corresponding to χ through this isomorphism; we also view these as characters of $\mathrm{J}_{\mathfrak{m}}(k)$ (e.g., we write $\chi_2(x)$ for $\chi_2(\pi(x))$ when $x \in \mathrm{J}_{\mathfrak{m}}(k)$).

The values of χ_1 are p-th roots of unity. We write

$$\mathrm{T}(\chi) = \sum_{\xi^p=1} \xi \sum_{\substack{x \in (\mathrm{C}-\mathfrak{m})(k) \\ \chi_1(i_\delta(x))=\xi}} \chi_2(i_\delta(x)),$$

where ξ runs over p-th roots of unity in $\mathbf{C}$. For each ξ, the inner sum is a cyclotomic integer and belongs to the field generated by values of χ_2, which are $|\mathrm{C}(k)|$-th roots of unity. Since $p \nmid |\mathrm{C}(k)|$, this field is linearly disjoint from $\mathbf{Q}(e^{2i\pi/p})$, and it follows that $\mathrm{T}(\chi) = 0$ if and only if the cyclotomic integer

$$\sum_{\substack{x \in (\mathrm{C}-\mathfrak{m})(k) \\ \chi_1(i_\delta(x))=\xi}} \chi_2(i_\delta(x)),$$

is *independent* of ξ. If we call this cyclotomic integer β, then we deduce that

$$p\beta = \sum_{\xi^p=1} \sum_{\substack{x \in (\mathrm{C}-\mathfrak{m})(k) \\ \chi_1(i_\delta(x))=\xi}} \chi_2(i_\delta(x)) = \sum_{x \in (\mathrm{C}-\mathfrak{m})(k)} \chi_2(i_\delta(x)) = -\chi_2(i_\delta(x_0)),$$

where $\mathfrak{m} = 2(x_0)$ (since i_δ is a set-theoretic section of π on $\mathrm{C} - \mathfrak{m}$). But this is absurd since the right-hand side is a unit whereas the left-hand side is not, and therefore $\mathrm{T}(\chi) \neq 0$. □

Proposition 5.4. *Let p be the characteristic of k. Suppose that $g = 1$ and that $\mathfrak{m}$ is a double point. Write $|\mathrm{C}(k)| = |k| + 1 - a_{\mathrm{C}}(k)$ for some integer $a_{\mathrm{C}}(k)$. If $a_{\mathrm{C}}(k)$ is zero modulo p or if the multiplicative order $\mathrm{ord}_p(a_{\mathrm{C}}(k))$ of $a_{\mathrm{C}}(k)$ modulo p is $\geqslant 5$, then the group K^a is infinite. In particular, if C is supersingular, so that $p \mid a_{\mathrm{C}}(k)$, then K^a is infinite.*

Proof. We proceed by contradiction. As before, the assumption that K^a is finite implies that the object $\mathrm{M} = i_{\delta,*}\overline{\mathbf{Q}}_\ell[1](1/2)$ is generically unramified by [14, Cor. 3.39].

For any integer $n \geqslant 1$ and any unramified character χ of $\mathrm{J}_{\mathfrak{m}}(k_n)$, the sum $\mathrm{U}_n(\chi)$ coincides with the trace of an element of K^a. Let γ denote the density in K^a of the elements of trace 0. By inspection of the three possible subgroups of $\mathbf{SU}_2(\mathbf{C})$ with fourth moment equal to 2 (see Theorem 4.1(3) and Remark 5.5 for details), the density γ is at least $1/4$.

By equidistribution, the proportion of characters χ such that the sum

$$\mathrm{T}_n(\chi) = |k_n|^{1/2}\mathrm{U}_n(\chi) = \sum_{x \in (\mathrm{C}-\mathfrak{m})(k_n)} \chi(i_\delta(x))$$

vanishes is equal to γ (the proportion is taken in the average limit sense of Theorem 4.1(1)). We now show that this does not happen under the assumptions of the proposition.

Fix again $n \geqslant 1$. By Lemma 5.3, applied to C over k_n instead of k, none of the sums $\mathrm{T}_n(\chi)$ vanish if $|\mathrm{C}(k_n)|$ is coprime to $|k_n|$, or equivalently if $p \nmid |\mathrm{C}(k_n)|$.

Now we claim that $p \mid |\mathrm{C}(k_n)|$ if and only if $a_{\mathrm{C}}^n \equiv 1 \pmod p$, where $a_{\mathrm{C}} = a_{\mathrm{C}}(k)$ is the trace of Frobenius over the base field k. Indeed, we have

$$|\mathrm{C}(k_n)| \equiv 1 - a_{\mathrm{C}}(k_n) \pmod p.$$

Writing $a_{\mathrm{C}} = \alpha + \beta$, where $\alpha\beta = |k|$, we have $a_{\mathrm{C}}(k_n) = \alpha^n + \beta^n$, and therefore

$$a_{\mathrm{C}}^n = (\alpha+\beta)^n = \alpha^n + \alpha\beta \sum_{j=1}^{n-1} \binom{n}{j} \alpha^{j-1}\beta^{n-j-1} + \beta^n \equiv \alpha^n + \beta^n \pmod p,$$

which implies that $|\mathrm{C}(k_n)| \equiv 1 - a_{\mathrm{C}}^n \pmod p$, proving the claim.

Thus $|\mathrm{C}(k_n)|$ is coprime to p unless n is a multiple of $\mathrm{ord}_p(a_{\mathrm{C}})$ modulo p. In particular, the density γ of characters χ with $\mathrm{U}_n(\chi) = 0$ is $\leqslant 1/\mathrm{ord}_p(a_{\mathrm{C}})$, which contradicts the lower-bound $\gamma \geqslant 1/4$ whenever $\mathrm{ord}_p(a_{\mathrm{C}}) \geqslant 5$. □

Remark 5.5. Here is the data for the three possible finite groups from Theorem 4.1. The results were checked with Magma [2], but the groups involved are small and well-understood enough that everything can be done by hand using the list of conjugacy classes and character tables of the groups involved (see, e.g., [24, § 4.6.4]).

(1) $\mathrm{K}^a = \mathbf{SL}_2(\mathbf{F}_3)$: this is a group of order 24; it has three non-isomorphic two-dimensional irreducible representations, which all have fourth moment equal to 2. For each of these, $\mathrm{Tr}(g) = 0$ if and only if g is conjugate to

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

This conjugacy class has size $6 = |\mathbf{SL}_2(\mathbf{F}_3)|/4$, so the density of zero values is $1/4$.

(2) $\mathrm{K}^a = \mathbf{GL}_2(\mathbf{F}_3)$: this is a group of order 48; it has three non-isomorphic two-dimensional irreducible representations, but only two of them have fourth moment equal to 2. For both of these, $\mathrm{Tr}(g) = 0$ if and only if g is conjugate to one of

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}.$$

The conjugacy classes have size respectively 12 and 6, so that the density of zeros is equal to $18/48 > 1/4$.

(3) $\mathrm{K}^a = \mathbf{SL}_2(\mathbf{F}_5)$: this is a group of order 120; it has two non-isomorphic two-dimensional irreducible representations, both of which have fourth moment equal to 2. For each of them, we have $\mathrm{Tr}(g) = 0$ if and only if g is conjugate to

$$\begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix},$$

whose conjugacy class has size $30 = |\mathbf{SL}_2(\mathbf{F}_5)|/4$, with a density of zeros $1/4$.

Remark 5.6. (1) The condition $\mathrm{ord}_p(a_{\mathrm{C}}(k)) \geqslant 5$ can be checked efficiently using polynomial time algorithms to compute $a_{\mathrm{C}}(k)$. It is also a fairly generic condition. Indeed, as already mentioned, it is known by work of Deuring and Honda–Tate theory that the integer $a_{\mathrm{C}}(k)$ parameterizes the isogeny classes of elliptic curves over k; the Hasse bound $|a_{\mathrm{C}}(k)| \leqslant 2\sqrt{|k|}$ implies that the number of such isogeny classes is of order $\sqrt{|k|}$. Since there are only a bounded number of elements of order $\leqslant 4$ modulo p, it follows by periodicity that there are only about

$$\frac{4\sqrt{|k|}}{p} + \mathrm{O}(1)$$

isogeny classes with $\mathrm{ord}_p(a_{\mathrm{C}}(k)) \leqslant 4$. In particular, if $k = \mathbf{F}_p$ for some prime p, at most finitely many isogeny classes are excluded from about $\sqrt{p}$. The cardinality of each isogeny class is a class number of a quadratic order, so that each class contains at most about $\sqrt{|k|}$ isomorphism classes. Hence, there are only about $4|k|/p + \mathrm{O}(\sqrt{|k|})$ isomorphism classes of elliptic curves over k such that $\mathrm{ord}_p(a_{\mathrm{C}}(k)) \leqslant 4$.

(2) If there exists an integer a coprime to p such that $\mathrm{ord}_p(a) \leqslant 4$, then either a is congruent to 1 or -1 modulo p (with order 1 or 2 modulo p), or we must have $p \equiv 1 \pmod 3$ or $p \equiv 1 \pmod 4$. In particular, the only possibility is that $a_{\mathrm{C}}(k)^2 \equiv 1 \pmod p$ for $p \equiv 11 \pmod{12}$; when the base field is $\mathbf{F}_p$, the Hasse bound means that, in that case, only $a_{\mathrm{C}}(\mathbf{F}_p) = 1$ or $a_{\mathrm{C}}(\mathbf{F}_p) = -1$ fail to satisfy $\mathrm{ord}_p(a_{\mathrm{C}}(\mathbf{F}_p)) \geqslant 5$.

The condition $a_{\mathrm{C}}(\mathbf{F}_p) \equiv 1 \pmod p$ appears in the arithmetic of elliptic curves, in the work of Mazur [31], who called these *anomalous primes*. In particular, it was proved by Mazur (see [31, proof of Lemma 8.18]) that if C is an elliptic curve over $\mathbf{Q}$ with a *non-trivial* rational torsion point, then the set of such primes is finite, and in fact is contained in the set of primes that may occur as the order of a torsion point on an elliptic curve over $\mathbf{Q}$, i.e., these are $\leqslant 7$ by another theorem of Mazur [32, Th. 7']. Thus, in this case, we can apply the proposition to prove that K^a is infinite for any prime $p \equiv 11 \pmod{12}$.

(3) We proved elementarily that if C is ordinary, then the degree of the extension of k generated by the coordinates of p-torsion points of C is the same as the multiplicative order of $a_{\mathrm{C}}(k)$ modulo p. As pointed out by D. Loeffler, this can also be understood more geometrically as follows: the p-adic Tate module of C is, in this case, isomorphic to $\mathbf{Z}_p$, with the Frobenius action given by multiplication by the unique root γ of $\mathrm{X}^2 - a_{\mathrm{C}}(k)\mathrm{X} + |k|$, which is a p-adic unit. Looking at the p-torsion points means looking at $\mathbf{Z}/p\mathbf{Z}$ with multiplication by γ modulo p, and since

$$\mathrm{X}^2 - a_{\mathrm{C}}(k)\mathrm{X} + |k| \equiv \mathrm{X}(\mathrm{X} - a_{\mathrm{C}}(k)) \pmod p,$$

we have $\gamma \equiv a_{\mathrm{C}}(k) \pmod{p}$.

Using rather deep results, we can prove furthermore that Proposition 5.4 applies to almost all reductions modulo primes of a fixed elliptic curve over $\mathbf{Q}$.

Proposition 5.7. *Let* E *be an elliptic curve over* $\mathbf{Q}$. *As* $x \to +\infty$, *the following holds:*

$$|\{p \leqslant x \mid \mathrm{ord}_p(a_{\mathrm{E}}(\mathbf{F}_p)) \geqslant 5\}| \sim \frac{x}{\log x}.$$

Proof. If $\mathrm{ord}_p(a_{\mathrm{E}}(\mathbf{F}_p)) \leqslant 2$, then (for $p \geqslant 7$) we have $a_{\mathrm{E}}(\mathbf{F}_p) = 1$ or -1. Applying Serre's ℓ-adic method for instance, one knows that the number of $p \leqslant x$ with this property is $o(\pi(x))$ as $x \to +\infty$ (see [39, Th. 20] for a more precise estimate; note that this result is stated for curves without complex multiplication, but for the case of values 1 or -1, it extends to the complex multiplication case).

We can handle the possibility that $\mathrm{ord}_p(a_{\mathrm{E}}(\mathbf{F}_p)) = 3$ or 4 in two different ways. Both rely on two facts:

(1) The condition $\mathrm{ord}_p(a_{\mathrm{E}}(\mathbf{F}_p)) = 3$ (resp. $\mathrm{ord}_p(a_{\mathrm{E}}(\mathbf{F}_p)) = 4$) is equivalent to the fact that $x = a_{\mathrm{E}}(\mathbf{F}_p)$ is a root modulo p of a quadratic equation $f(x) = 0$, namely $x^2+x+1 = 0$ for order 3 and $x^2 + 1 = 0$ for order 4.

(2) Because of the Hasse bound $|a_{\mathrm{E}}(\mathbf{F}_p)| \leqslant 2\sqrt{p}$, this root of the equation is "very small".

For the first, more elementary argument, we deduce that $0 \leqslant f(a_{\mathrm{E}}(\mathbf{F}_p)) \leqslant 4p + 2\sqrt{p} + 1$, hence the condition $f(a_{\mathrm{E}}(\mathbf{F}_p)) \equiv 0 \pmod{p}$ means that either

$$a_{\mathrm{E}}(\mathbf{F}_p)^2 + a_{\mathrm{E}}(\mathbf{F}_p) + 1 = jp, \text{ or } a_{\mathrm{E}}(\mathbf{F}_p)^2 + 1 = jp$$

for some integer j with $0 \leqslant j \leqslant 7$. The case $j = 0$ is clearly excluded. For each value of $j \geqslant 1$, an elementary sieve argument implies that there are at most $\mathrm{O}(\sqrt{x}/\log x)$ primes $p \leqslant x$ such that jp is of the form $n^2 + 1$ or $n^2 + n + 1$ (see, e.g., [18, Th. 5.4] for the case $j = 1$). Thus,

$$|\{p \leqslant x \mid \mathrm{ord}_p(a_{\mathrm{E}}(\mathbf{F}_p)) = 3 \text{ or } 4\}| \ll \frac{\sqrt{x}}{\log x}.$$

The second, less elementary argument, deduces from the Hasse bound that the fractional part $\{\frac{a_{\mathrm{E}}(\mathbf{F}_p)}{p}\}$ satisfies

$$0 \leqslant \left\{\frac{a_{\mathrm{E}}(\mathbf{F}_p)}{p}\right\} \leqslant \frac{2}{\sqrt{p}},$$

which cannot happen often because of the result of Duke, Friedlander and Iwaniec [10] which shows that the fractional parts of the roots of these equations are equidistributed modulo primes.

Precisely, let $\varepsilon > 0$ be given. For p large enough, we get

$$|\{p \leqslant x \mid f(a_{\mathrm{E}}(\mathbf{F}_p)) = 0 \pmod{p}\}| \leqslant \left|\left\{(p, \nu) \mid p \leqslant x,\ \nu \in \mathbf{F}_p,\ 0 \leqslant \left\{\frac{\nu}{p}\right\} \leqslant \varepsilon,\ f(\nu) \equiv 0 \pmod{p}\right\}\right|,$$

and hence, by the Duke–Friedlander–Iwaniec theorem,

$$\limsup_{x \to +\infty} \frac{1}{\pi(x)} |\{p \leqslant x \mid f(a_{\mathrm{E}}(\mathbf{F}_p)) = 0 \pmod{p}\}| \leqslant \varepsilon.$$

Since ε is arbitrary, the result follows again. □

Remark 5.8.

(1) This result suggests a variant of Artin's Primitive Root conjecture: given an elliptic curve E over $\mathbf{Q}$, are there infinitely many primes p such that the Frobenius trace $a_{\mathrm{E}}(\mathbf{F}_p)$ is a primitive root modulo p? This can easily be tested numerically, and the results (unsurprisingly) suggest that the answer should be positive, and in fact that the density of these primes should also be positive.

Here is a random example: for the curve

$$y^2 + y = x^3 + x - 1,$$

and for primes $p \leqslant 300\,000$, there are 9 607 primes with $a_{\mathrm{E}}(\mathbf{F}_p)$ a primitive root; for comparison with Artin's Conjecture, there are 9 701 primes in this range for which 2 is a primitive root. Other random choices of elliptic curves display the same behavior; the number of primitive roots is about half of this for complex multiplication curves, as it should be since $a_{\mathrm{E}}(\mathbf{F}_p) = 0$ for about half of the primes in this case. (These computations were performed with PARI/GP [17].)

(2) Continuing with an elliptic curve E over $\mathbf{Q}$, the usual heuristics suggest that there should exist infinitely many primes p for which $a_{\mathrm{E}}(\mathbf{F}_p)$ is of order 4, or 3, but the number of these $\leqslant x$ should grow like $\log\log x$ (because the probability that $a_{\mathrm{E}}(\mathbf{F}_p)^4 = 1 \pmod p$ should be about $1/p$, for instance, and different primes should behave independently). Numerics for random (non-CM) curves are definitely compatible with this, since one finds most commonly 1 or 2 such primes $p \leqslant 300\,000$ and $\log(\log(300\,000)) = 2.53\ldots$.

(3) We do not know how to prove the statement of Proposition 5.7 if the condition $\mathrm{ord}_p(a_{\mathrm{E}}(\mathbf{F}_p)) \geqslant 5$ is replaced by $\mathrm{ord}_p(a_{\mathrm{E}}(\mathbf{F}_p)) \geqslant 6$. Indeed, $a_{\mathrm{E}}(\mathbf{F}_p)$ satisfies then an equation of degree $\geqslant 4$, and there are too many possibilities to apply the elementary sieve argument. And although a solution of (say) $\mathrm{ord}_p(a_{\mathrm{E}}(\mathbf{F}_p)) = 5$ gives a small solution of the equation $\mathrm{X}^4 + \mathrm{X}^3 + \mathrm{X}^2 + \mathrm{X} + 1 = 0$ modulo p, the equidistribution of fractional parts of roots of this equation modulo primes is not known (indeed, *no* irreducible polynomial of degree $\geqslant 3$ is currently known to satisfy the equidistribution property, although it is conjectured to hold).

However, J. Merikoski pointed out that, for any integer $m \geqslant 6$, one can still prove that there is a positive proportion of primes p for which $\mathrm{ord}_p(a_{\mathrm{E}}(\mathbf{F}_p))$ is $\geqslant m$. Indeed, by Dirichlet's theorem on primes in arithmetic progressions, there is a positive proportion of primes p such that $p-1$ is not divisible by any odd prime $< m$ (e.g., primes congruent to 2 modulo the product of the odd primes $< m$). For such primes p, the order of $a_{\mathrm{E}}(\mathbf{F}_p)$ modulo p is either $\leqslant 2$ or $> m$. By the argument at the beginning of the proof of Proposition 5.7, the number of primes $p \leqslant x$ with $\mathrm{ord}_p(a_{\mathrm{E}}(\mathbf{F}_p)) \leqslant 2$ is $o(\pi(x))$, so we obtain the result.

Appendix A. Non-technical overview of generalized jacobians

We give here a quick intuitive overview of the definition of generalized jacobians for non-experts, assuming no background in algebraic geometry (an accessible account can be

found, for instance, in [41, Ch. 1, 2]). The lecture [23] might also be helpful, as well as the more concise description of the construction in [13, § 2].

Let $\mathbf{F}$ be a perfect field, and $\bar{\mathbf{F}}$ an algebraically closed field containing $\mathbf{F}$. An *affine plane algebraic curve* C over $\mathbf{F}$ is defined as the zero set in $\bar{\mathbf{F}}^2$ of a non-constant two-variable polynomial $f \in \mathbf{F}[\mathrm{X}, \mathrm{Y}]$, and the $\mathbf{F}$-*rational points* on the curve are those points $(x, y) \in \mathbf{F}^2$ such that $f(x, y) = 0$; the set of those points is denoted by $\mathrm{C}(\mathbf{F})$.

The curve C is said to be *irreducible* if f is irreducible, and *non-singular* (or smooth) if, for every point $(x, y) \in \bar{\mathbf{F}}^2$ on C, one of the partial derivatives $\partial_x f(x, y)$ or $\partial_y f(x, y)$ is non-zero. An important special case is when f is of the form

$$f(\mathrm{X}, \mathrm{Y}) = \mathrm{Y}^2 - g(\mathrm{X}), \qquad g \in \mathbf{F}[\mathrm{X}], \tag{A.1}$$

and the condition is then that g has simple roots in $\bar{\mathbf{F}}$. (These curves are called *hyperelliptic*.)

Given an irreducible non-singular curve C and a multiset $\mathfrak{m}$ of rational points on C (usually called a *modulus*, or an *effective divisor* on C), there is an associated group called the *generalized jacobian*, and denoted by $\mathrm{J}_{\mathfrak{m}}(\mathrm{C})$. Additionally, except in very special cases, one shows that for a choice of a point $p_0 = (x, y)$ on the curve, there is an associated injective map $i\colon \mathrm{C} \mathbin{-\!\!-} \mathfrak{m} \to \mathrm{J}_{\mathfrak{m}}(\mathrm{C})$, called an *Abel–Jacobi map*; it gives us a natural way of viewing $\mathrm{C} \mathbin{-\!\!-} \mathfrak{m}$ itself as a subset of $\mathrm{J}_{\mathfrak{m}}(\mathrm{C})$. For instance, this holds for hyperelliptic curves if the degree of the polynomial g in (A.1) is greater than or equal to 3.

Quite surprisingly, it was proved in [13] that, under mild assumptions on the curve and the modulus, the image by i of $\mathrm{C} \mathbin{-\!\!-} \mathfrak{m}$ always yields a Sidon or symmetric Sidon subset of the group $\mathrm{J}_{\mathfrak{m}}(\mathrm{C})$. These are infinite sets in infinite groups, but if one starts with a finite field $\mathbf{F}$, one can take the subset of elements invariant under the action of the *Frobenius automorphism* (in the case of C, this means elements with $(x, y) \in \mathbf{F}^2$) to obtain finite sets and finite groups. This is the starting point of our work.

We will now define more precisely the generalized jacobian $\mathrm{J}_{\mathfrak{m}}(\mathrm{C})$ and the Abel–Jacobi maps i, in two concrete special cases, both of which are particularly relevant to our main results: elliptic curves with $\mathfrak{m}$ consisting of two distinct points, and curves of genus 2 with $\mathfrak{m} = \emptyset$. In the spirit of accessibility, we describe these two examples in different languages: for the first, we give a completely explicit description of the group $\mathrm{J}_{\mathfrak{m}}(\mathrm{C})$, whereas for the second we use more abstract language, which extends readily to a complete definition of all generalized jacobians.

Elliptic curves. We begin with the case of elliptic curves. For our purposes,[7] an elliptic curve E is the set of solutions to the polynomial equation $y^2 = x^3 + ax + b$, for some constants $a, b \in \mathbf{F}$, chosen so that the polynomial $x^3 + ax + b$ has simple roots in $\bar{\mathbf{F}}$. It is not hard to see that if a line ℓ passes through two points P, Q of E, then it also passes through a third point; this even holds if $\mathrm{P} = \mathrm{Q}$, so long as we interpret ℓ as the tangent line to E at P.[8] Precisely, the only exceptions to this rule are vertical lines, which pass through only two points of E, but this is corrected by adding to the solutions of the equation a "point at infinity", denoted ∞, which lies on all vertical lines. Given a point $\mathrm{P} = (x, y)$, we denote

[7] As long as the characteristic of $\mathbf{F}$ is not 2 or 3, every elliptic curve can be put into this form, called *Weierstrass form*.

[8] The assumption that the polynomial has simple roots is precisely what is needed to ensure the existence of this tangent line at any point of the curve.

by $-\mathrm{P} = (x, -y)$ the point obtained by reflecting about the x-axis; note that $-\mathrm{P}$ also lies on E, and that $\mathrm{P}, -\mathrm{P}$, and ∞ are collinear. We denote by $\mathrm{E}(\bar{\mathbf{F}})$ the set of points on E, including ∞, and by $\mathrm{E}(\mathbf{F})$ the subset of those with coordinates in $\mathbf{F}$.

The fact above allows us to define a binary operation on $\mathrm{E}(\bar{\mathbf{F}})$, by declaring $\mathrm{P} * \mathrm{Q}$ to be the unique third point lying on the line between P and Q. We then define $\mathrm{P} + \mathrm{Q}$ to be equal to $-(\mathrm{P} * \mathrm{Q})$; that is, $\mathrm{P} + \mathrm{Q}$ is computed by taking the line through P and Q, finding its unique third intersection with E, and reflecting that point about the x-axis. Surprisingly, this rule defines an abelian group on the set $\mathrm{E}(\bar{\mathbf{F}})$ of points of E, in which the identity element is ∞ and the additive inverse of P is $-\mathrm{P}$. Moreover, it is elementary that $\mathrm{E}(\mathbf{F})$ is a subgroup of $\mathrm{E}(\bar{\mathbf{F}})$, which is finite if $\mathbf{F}$ is finite.

Given the group law on $\mathrm{E}(\mathbf{F})$, it is not hard to define the generalized jacobian. In what follows, we rely on work of Déchène [8, § 5.3], who explicitly worked out what the abstract generalized jacobian corresponds to in this special case. Let $\mathrm{M}, \mathrm{N} \in \mathrm{E}(\mathbf{F})$ be two distinct points on E (with coordinates in $\mathbf{F}$), both distinct from ∞, and let $\mathfrak{m}$ consist of M and N, both with multiplicity 1. The set underlying the generalized jacobian $\mathrm{J}_{\mathfrak{m}}(\mathrm{E})$ is $\mathrm{E}(\bar{\mathbf{F}}) \times \bar{\mathbf{F}}^{\times}$, i.e., the elements of the group $\mathrm{J}_{\mathfrak{m}}(\mathrm{E})$ are pairs (P, s), where P is a point on E and $s \in \bar{\mathbf{F}}$ is non-zero. The group operation is not the "obvious" componentwise operation, but is defined (generically) by

$$(\mathrm{P}, s) \cdot (\mathrm{Q}, t) = \left(\mathrm{P} + \mathrm{Q}, s \cdot t \cdot \frac{\ell_{\mathrm{P},\mathrm{Q}}(\mathrm{M})}{\ell_{\mathrm{P}+\mathrm{Q},\infty}(\mathrm{M})} \cdot \frac{\ell_{\mathrm{P}+\mathrm{Q},\infty}(\mathrm{N})}{\ell_{\mathrm{P},\mathrm{Q}}(\mathrm{N})} \right), \tag{A.2}$$

where $\ell_{\mathrm{P}_1,\mathrm{P}_2}$ denotes the equation of the line passing through the points $\mathrm{P}_1, \mathrm{P}_2$. That is, in the first coordinate we simply apply the group law on $\mathrm{E}(\bar{\mathbf{F}})$ described above, whereas the second coordinate multiplies the elements of $\mathbf{F}^{\times}$ together with an additional quantity involving the points P, Q as well as the fixed modulus $\mathfrak{m} = \{\mathrm{M}, \mathrm{N}\}$[9]. The identity element of the group is the pair $(\infty, 1)$. Finally, the Abel–Jacobi map i is defined by $i(\mathrm{P}) = (\mathrm{P}, 1)$. The subgroup of $\mathbf{F}$-rational points is simply the subgroup where $\mathrm{P} \in \mathrm{E}(\mathbf{F})$ and $s \in \mathbf{F}^{\times}$.

We stress that this description of the group law of $\mathrm{J}_{\mathfrak{m}}(\mathrm{E})$ is completely explicit, also in the sense that all expressions arising in it can be efficiently computed.

As an illustration, let us quickly verify that this construction does indeed give a symmetric Sidon set, following the argument of [13, Lemma 7]. As previously stated, this is an infinite subset of $\mathrm{J}_{\mathfrak{m}}(\mathrm{C})$, but taking the points with coordinates in $\mathbf{F}$ gives finite sets and groups when $\mathbf{F}$ is finite.

Proposition A.1. *Let* E *be an elliptic curve over* $\mathbf{F}$*, and let* $\mathfrak{m} = \{\mathrm{M}, \mathrm{N}\}$ *for some distinct points* $\mathrm{M}, \mathrm{N} \in \mathrm{E}(\mathbf{F})$*, both distinct from* ∞*. Then the set* $\mathrm{S} = \{(\mathrm{P}, 1) : \mathrm{P} \in \mathrm{E}(\bar{\mathbf{F}})\}$ *is a symmetric Sidon subset of* $\mathrm{J}_{\mathfrak{m}}(\mathrm{E})$*, with center* $(-(\mathrm{M} + \mathrm{N}), 1) \in \mathrm{S}$.

Proof. Suppose that $\mathrm{P}_1, \mathrm{Q}_1, \mathrm{P}_2, \mathrm{Q}_2 \in \mathrm{E}(\mathbf{F})$ satisfy $(\mathrm{P}_1, 1) \cdot (\mathrm{Q}_1, 1) = (\mathrm{P}_2, 1) \cdot (\mathrm{Q}_2, 1)$; this means, by the group law (A.2), that

$$\mathrm{P}_1 + \mathrm{Q}_1 = \mathrm{P}_2 + \mathrm{Q}_2$$

[9] As written, this group law depends on the choice of which point is M and which is N, rather than on the unordered pair, but it is not hard to see that one obtains an isomorphic group by swapping their roles. More problematically, the expression in (A.2) does not make sense if $\{\mathrm{P}, \mathrm{Q}, \mathrm{P} + \mathrm{Q}\} \cap \{\mathrm{M}, \mathrm{N}\} \neq \emptyset$, as we are then dividing by zero; to define the group operation in this case, one uses an identical formula, simply shifted by some *translation point*; see [8, Prop. 5.5] for details.

and

$$\frac{\ell_{P_1,Q_1}(M)}{\ell_{P_1+Q_1,\infty}(M)} \cdot \frac{\ell_{P_1+Q_1,\infty}(N)}{\ell_{P_1,Q_1}(N)} = \frac{\ell_{P_2,Q_2}(M)}{\ell_{P_2+Q_2,\infty}(M)} \cdot \frac{\ell_{P_2+Q_2,\infty}(N)}{\ell_{P_2,Q_2}(N)}.$$

The second equation can be simplified since $P_1 + Q_1 = P_2 + Q_2$, becoming

$$\frac{\ell_{P_1,Q_1}(M)}{\ell_{P_1,Q_1}(N)} = \frac{\ell_{P_2,Q_2}(M)}{\ell_{P_2,Q_2}(N)} \qquad \Longleftrightarrow \qquad \frac{\ell_{P_1,Q_1}(M)}{\ell_{P_2,Q_2}(M)} = \frac{\ell_{P_1,Q_1}(N)}{\ell_{P_2,Q_2}(N)}.$$

Let $R = -(P_1 + Q_1) = -(P_2 + Q_2)$; this is the intersection point of the lines through P_1, Q_1 and through P_2, Q_2. We are done if $\{P_1, Q_1\} = \{P_2, Q_2\}$, so we may assume this does not happen; the key observation in this case is that the ratio $\ell_{P_1,Q_1}(M)/\ell_{P_2,Q_2}(M)$ determines and is determined by the slope of the line through M and R. As a consequence, we find that the slope of the line through M and R equals the slope of the line through N and R, and hence the points M, N, R are collinear. By the definition of the group law on the elliptic curve, we find that $R = -(M + N)$. But this shows that R is independent of P_1, P_2, Q_1, Q_2; that is, whenever $(P_1, 1) \cdot (Q_1, 1) = (P_2, 1) \cdot (Q_2, 1)$, we either have that $\{P_1, Q_1\} = \{P_2, Q_2\}$, or that $(P_1, 1) \cdot (Q_1, 1) = (-(M + N), 1) = (P_2, 1) \cdot (Q_2, 1)$. As it is straightforward to verify that S is symmetric about $(-(M + N), 1)$, we conclude that S is a symmetric Sidon set. □

Genus 2 curves. We now turn to the second example, which concerns curves of genus 2. For us, such a curve over $\mathbf{F}$ is an algebraic curve given by an equation $y^2 = f(x)$, where f is a polynomial of degree 5 or 6 with no repeated roots in $\bar{\mathbf{F}}$. In this case, we only deal with the case where the modulus $\mathfrak{m}$ is empty; in such instances, the generalized jacobian is nothing more than the "classical" jacobian J(C) of C, which we now define. As in the previous case, we need to add to C some points at infinity to obtain a smooth projective curve; there is only one if $\deg(f) = 5$ and there are two if $\deg(f) = 6$. The notation $C(\bar{\mathbf{F}})$ or $C(\mathbf{F})$ always mean the sets of points including these.

The group J(C) is defined as the quotient of two infinite abelian groups. The first is the group of *degree-zero divisors* on C. Here, a *divisor* is nothing more than a formal linear combination, with integer coefficients, of points on C. The divisors form a group, denoted by Div(C), under the addition of formal linear combinations. In other words, Div(C) is simply the free abelian group generated by the points of $C(\bar{\mathbf{F}})$. It contains the subgroup $\mathrm{Div}^0(C)$ of degree-zero divisors, namely those divisors whose coefficients sum to zero.

A special class of divisors are *principal divisors*, which are those arising from non-zero rational function, that is, from ratios $r(X, Y) = p(X, Y)/q(X, Y)$ of non-zero polynomials in $\bar{\mathbf{F}}[X, Y]$. Namely, each such rational function gives us a divisor $\mathrm{div}(r)$ recording the roots and poles of r. More precisely, $\mathrm{div}(r)$ is defined to be the sum of the points P at which $r(P) = 0$ (counted with multiplicity), minus the sum of the points P at which $r(P) = \infty$ (again with multiplicity). A basic fact of algebraic geometry is that if $\deg p = \deg q$, then $\mathrm{div}(p/q)$ is a degree-zero divisor; this is essentially a restatement of the fact that a degree-d polynomial has exactly d roots, counted with multiplicity, over every algebraically closed field. Since $\mathrm{div}(rr') = \mathrm{div}(r) + \mathrm{div}(r')$, we see that the set of principal divisors forms a subgroup P(C) of $\mathrm{Div}^0(C)$. The *jacobian* is then defined as the quotient $J(C) = \mathrm{Div}^0(C)/P(C)$.

If $\mathbf{F}$ is finite, then the group $J(C)(\mathbf{F})$ of $\mathbf{F}$-rational points of J(C) (which is a finite subgroup of J(C)) is defined as the subgroup of classes of divisors which are invariant under

the Frobenius automorphism σ acting on divisors by the rule

$$\sum_{\mathrm{P}} n_{\mathrm{P}}(\mathrm{P}) \mapsto \sum_{\mathrm{P}} n_{\mathrm{P}}(\sigma(\mathrm{P})).$$

Remark A.2. Being invariant does not necessarily mean that the points P for which $n_{\mathrm{P}} \neq 0$ are in $\mathrm{C}(\mathbf{F})$: for instance, if $\mathrm{P} = (x, y)$ with x and y in the quadratic extension of $\mathbf{F}$ and Q is another point of $\mathrm{C}(\mathbf{F})$, then $(\mathrm{P}) + (\sigma(\mathrm{P})) - 2(\mathrm{Q})$ is in $\mathrm{J}(\mathrm{C})(\mathbf{F})$.

As before, the Abel–Jacobi map is essentially the most natural way one would guess to embed the points of C into J(C). For instance, if one of the points at infinity ∞ is rational, then every point $\mathrm{P} \in \mathrm{C}(\mathbf{F})$ yields a degree-zero divisor $(\mathrm{P}) - (\infty)$, which yields an embedding of the points of C into $\mathrm{Div}^0(\mathrm{C})$. By composing with the quotient map $\mathrm{Div}^0(\mathrm{C}) \to \mathrm{J}(\mathrm{C})$, we obtain the Abel–Jacobi embedding $\mathrm{C}(\mathbf{F}) \to \mathrm{J}(\mathrm{C})$.

Again, it turns out that the image of this map is a symmetric Sidon subset of the group J(C). This is not very hard to prove, but requires some background theory on hyperelliptic curves, so we refer to [13] for details.

Although our description is abstract, there are efficient algorithms to represent points of $\mathrm{J}(\mathrm{C})(\mathbf{F})$ and operate on them (see, for instance, the recent description by Flynn and Khuri-Makdisi [12] of J(C) as a subvariety of $\mathbf{P}^3 \times \mathbf{P}^3$ with an explicit form of the addition map).

References

[1] N. Alon and H. T. Pham, *Random Cayley graphs and random sumsets*, 2025. Preprint https://arxiv.org/abs/2509.02561.

[2] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265.

[3] N. Bourbaki, *Lie groups and Lie algebras. Chapters 7–9*, Elements of Mathematics, Springer, 2005.

[4] R. Bröker, E. W. Howe, K. E. Lauter, and P. Stevenhagen, *Genus-2 curves and Jacobians with a given number of points*, LMS J. Comput. Math. **18** (2015), no. 1, 170–197.

[5] F. R. K. Chung, *Diameters and eigenvalues*, J. Amer. Math. Soc. **2** (1989), no. 2, 187–196.

[6] D. Conlon, J. Fox, H. T. Pham, and L. Yepremyan, *On the clique number of random Cayley graphs and related topics*, 2024. Preprint https://arxiv.org/abs/2412.21194.

[7] P. Corvaja, D. Masser, and U. Zannier, *Sharpening 'Manin-Mumford' for certain algebraic groups of dimension 2*, Enseign. Math. **59** (2013), no. 3–4, 225–269.

[8] I. Déchène, *Generalized jacobians in cryptography*, Ph.D. Thesis, 2005. Available at https://www.math.mcgill.ca/darmon/theses/dechene/thesis.pdf.

[9] P. Deligne, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. **52** (1980), 137–252.

[10] W. Duke, J. B. Friedlander, and H. Iwaniec, *Equidistribution of roots of a quadratic congruence to prime moduli*, Ann. of Math. **141** (1995), no. 2, 423–441.

[11] S. Eberhard and F. Manners, *The apparent structure of dense Sidon sets*, Electron. J. Combin. **30** (2023), no. 1, Paper No. 1.33, 19 pp.

[12] E. V. Flynn and K. Khuri-Makdisi, *An analog of the Edwards model for Jacobians of genus 2 curves*, Res. Number Theory **10** (2024), no. 2, Paper No. 32, 41 pp.

[13] A. Forey, J. Fresán, and E. Kowalski, *Sidon sets in algebraic geometry*, Int. Math. Res. Not. IMRN **8** (2024), 6400–6421.

[14] ———, *Arithmetic Fourier transforms over finite fields: generic vanishing, convolution, and equidistribution*, 2025. Astérisque, to appear.

[15] A. Forey, J. Fresán, E. Kowalski, and Y. Wigderson, *Spectrally indistinguishable pseudorandom graphs*, 2025. Preprint https://arxiv.org/pdf/2511.21351.

[16] Z. Füredi, *New asymptotics for bipartite Turán numbers*, J. Combin. Theory Ser. A **75** (1996), no. 1, 141–144.

[17] The PARI Group, *PARI/GP version 2.14.0*. Université de Bordeaux, 2002, https://pari.math.u-bordeaux.fr.
[18] H. Halberstam and H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs, vol. 4, Academic Press, London-New York, 1974.
[19] R. Heath-Brown, *The differences between consecutive primes, V*, Int. Math. Res. Not. IMRN **22** (2021), 17514–17562.
[20] E. W. Howe, E. Nart, and C. Ritzenthaler, *Jacobians in isogeny classes of abelian surfaces over finite fields*, Ann. Inst. Fourier (Grenoble) **59** (2009), no. 1, 239–289.
[21] N. M. Katz, *Larsen's alternative, moments, and the monodromy of Lefschetz pencils*, Contributions to automorphic forms, geometry, and number theory, Johns Hopkins Univ. Press, Baltimore, MD, 2004, pp. 521–560.
[22] T. Kövari, V. T. Sós, and P. Turán, *On a problem of K. Zarankiewicz*, Colloq. Math. **3** (1954), 50–57.
[23] E. Kowalski, *Sidon sets in algebraic geometry*. Talk at Rényi Institute, February 2023, https://video.renyi.hu/video/emmanuel-kowalski-sidon-sets-in-algebraic-geometry-550.
[24] ———, *An introduction to the representation theory of groups*, Graduate Studies in Mathematics, vol. 155, American Mathematical Society, Providence, RI, 2014.
[25] ———, *An introduction to probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 192, Cambridge University Press, Cambridge, 2021.
[26] E. Kowalski and T. Untrau, *Wasserstein metrics and quantitative equidistribution of exponential sums over finite fields*, 2025. Preprint https://arxiv.org/abs/2505.22059.
[27] M. Krivelevich and B. Sudakov, *Pseudo-random graphs*, More sets, graphs and numbers, 2006, pp. 199–262.
[28] G. J. Leuschke and R. Wiegand, *Cohen–Macaulay representations*, Mathematical Surveys and Monographs, vol. 181, American Mathematical Society, Providence, RI, 2012.
[29] A. Lubotzky, R. Phillips, and P. Sarnak, *Ramanujan graphs*, Combinatorica **8** (1988), no. 3, 261–277.
[30] K. Matomäki, *Large differences between consecutive primes*, Q. J. Math. **58** (2007), no. 4, 489–518.
[31] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. math. **18** (1972), 183–266.
[32] ———, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186.
[33] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.
[34] ———, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 167–212.
[35] D. Mubayi and J. Williford, *On the independence number of the Erdős-Rényi and projective norm graphs and a related hypergraph*, J. Graph Theory **56** (2007), no. 2, 113–127.
[36] J. Pach and D. Zakharov, *Ruzsa's problem on bi-Sidon sets*, Combinatorica **45** (2025), no. 2, Paper No. 26, 9 pp.
[37] I. Z. Ruzsa, *Additive and multiplicative Sidon sets*, Acta Math. Hungar. **112** (2006), no. 4, 345–354.
[38] W. Sawin, A. Forey, J. Fresán, and E. Kowalski, *Quantitative sheaf theory*, J. Amer. Math. Soc. **36** (2023), no. 3, 653–726.
[39] J-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 123–201.
[40] ———, *Rational points on curves over finite fields*, Documents Mathématiques, Société Mathématique de France, Paris, 2020.
[41] J. H. Silverman, *The arithmetic of elliptic curves*, Second edition, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
[42] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. **2** (1969), 521–560.

(A. Forey) Univ. Lille, CNRS, UMR 8524 - Laboratoire Paul Painlevé, F-59000 Lille, France

Email address: arthur.forey@univ-lille.fr

(J. Fresán) Sorbonne Université and Université Paris Cité, CNRS, IMJ-PRG, F-75005 Paris, France

Email address: javier.fresan@imj-prg.fr

(E. Kowalski) D-MATH, ETH Zürich, Rämistrasse 101, 8092 Zürich, Switzerland

Email address: kowalski@math.ethz.ch

(Y. Wigderson) ETH-ITS, Scheuchzerstrasse 70, 8006 Zürich, Switzerland

Email address: yuval.wigderson@eth-its.ethz.ch