SPECTRALLY INDISTINGUISHABLE PSEUDORANDOM GRAPHS

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

Abstract. We construct explicit families of graphs whose eigenvalues are asymptotically distributed according to Wigner's semicircle law; in other words, that are spectrally indistinguishable from random graphs. However, in other respects they are strikingly dissimilar from random graphs; for example, they are $\mathrm{K}_{2,3}$-free graphs with almost the maximum possible edge density.

1. Introduction

One of the most important developments in the last half-century of combinatorics and many related fields has been the notion of *pseudorandomness*. Loosely, one says that a discrete object (say, a graph) is pseudorandom if it satisfies some *deterministic* property that is also shared, with high probability, by a randomly chosen object.

In graph theory, the best-known and most studied notion[1] of pseudorandomness is often called *spectral pseudorandomness*. Loosely speaking, one says that a graph is spectrally pseudorandom if all of its non-trivial eigenvalues[2] are much smaller in absolute value than its average degree. The *expander mixing lemma* of Alon and Chung [2] states that such a condition implies a fairly uniform distribution of edges among all large sets in the graph, as one would expect in a random graph. Of particular importance are *(near-)Ramanujan graphs*, where all the non-trivial eigenvalues are at most roughly the square root of the degree, as these give essentially optimal control on the distribution of edges. For an in-depth introduction to spectrally pseudorandom graphs, we refer the reader to the excellent survey [37] of Krivelevich and Sudakov.

Our focus in this paper is on the construction of explicit graphs that are "even more spectrally pseudorandom". More precisely, Wigner's semicircle law [59] implies that, upon appropriate scaling, the spectrum of an Erdős–Rényi random graph at any[3] edge density converges to the semicircle distribution (see, e.g., the paper [56, §1.2] of Tran, Vu and Wang for the precise statement). Moreover, as is common in probability, Wigner's result exhibits universality, and it is now known that many other models of random graphs, such as random regular graphs and power-law graphs, also exhibit a semicircular spectrum; see the papers [10, 56] of Chung–Lu–Vu and Tran–Vu–Wang for details.

2020 *Mathematics Subject Classification.* 11T23, 05C35, 05C50.

[1]For dense graphs, the seminal works of Thomason [55] and Chung–Graham–Wilson [11] imply that essentially all notions of pseudorandomness are roughly equivalent. However, this is known to be false for sparse graphs (see, e.g., the paper [47] of Sah, Sawhney, Tidor and Zhao and the discussion therein).

[2]As usual, when referring to the eigenvalues of a graph, we mean the eigenvalues of its adjacency matrix.

[3]To be exact, one must impose the weak (and necessary) assumption that pn and $(1-p)n$ both tend to infinity, where n is the number of vertices and $p = p(n)$ the edge probability.

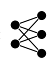
By contrast, the explicit pseudorandom graphs that we are aware of (such as those in [37, §3]) have a spectral distribution that is very far from semicircular. In fact, these constructions have a very "spiky" spectrum, where a small number of eigenvalues appear with extremely large multiplicity. As such, the spectral distribution does not converge to *any* absolutely continuous distribution, but rather to a finitely-supported atomic measure. For example, Paley graphs and many graphs arising from finite geometries are *strongly regular*, implying that they only have two non-trivial eigenvalues, both of which occur with multiplicity linear in the number of vertices.

Our main result in this paper is an explicit construction of graphs that turn out not only to be spectrally pseudorandom in the strongest possible sense (they are nearly Ramanujan graphs), but also to have the property that their empirical spectral distribution converges to the semicircle distribution. However, in other respects, they are highly unlike random graphs, as exhibited by the avoidance of certain small subgraphs.

Theorem 1.1. *Let k be a finite field. Set*[4]

$$\mathrm{K}(k) = \{(x,y) \in k \times k \mid xy = 1\} \quad \textit{and} \quad \mathrm{B}(k) = \{(x,y) \in k \times k \mid y = x^3\}.$$

Define graphs $\Gamma_{\mathrm{K}}(k)$ and $\Gamma_{\mathrm{B}}(k)$ with vertex set $k \times k$ in both cases and with edges joining x and y if and only if $x + y \in \mathrm{K}(k)$ or $x + y \in \mathrm{B}(k)$, respectively. These are regular graphs of degree $|k| - 1$ and $|k|$, respectively, and satisfy the following additional properties:

(1) *The complete bipartite graph $\mathrm{K}_{2,3} =$*  *is not a subgraph of $\Gamma_{\mathrm{K}}(k)$.*
(2) *All the non-trivial eigenvalues λ of the adjacency matrix of $\Gamma_{\mathrm{K}}(k)$ satisfy*

$$|\lambda| \leqslant 2|k|^{1/2}.$$

(3) *As the size of k tends to infinity, the numbers*

$$\Big\{\frac{\lambda}{\sqrt{|\mathrm{K}(k)|}} \mid \lambda \textit{ an eigenvalue of } \Gamma_{\mathrm{K}}(k)\Big\}$$

converge in distribution to the semicircle distribution

$$\mu_{\mathrm{sc}} = \frac{1}{\pi}\sqrt{1 - \frac{x^2}{4}}dx \tag{1.1}$$

on $[-2, 2]$. In other words, for all $-2 \leqslant a < b \leqslant 2$, we have

$$\frac{1}{|k|^2}\Big|\Big\{\lambda \textit{ an eigenvalue of } \Gamma_{\mathrm{K}}(k) \mid \frac{\lambda}{\sqrt{|\mathrm{K}(k)|}} \in [a,b]\Big\}\Big| \to \frac{1}{\pi}\int_a^b \sqrt{1 - \frac{x^2}{4}}dx$$

as $|k| \to +\infty$. In fact, we have the estimate

$$\mathrm{W}_1\Big(\frac{1}{|k|^2 - 1}\sum_{\lambda \neq |k|-1} \delta_{\lambda/\sqrt{|\mathrm{K}(k)|}}, \mu_{\mathrm{sc}}\Big) = \mathrm{O}(|k|^{-1/3}), \tag{1.2}$$

where δ_t denotes a Dirac mass at t and W_1 denotes the Wasserstein distance for probability measures and the sum is over the non-trivial eigenvalues of the graph $\Gamma_{\mathrm{K}}(k)$.
(4) *The same properties hold for the graphs $\Gamma_{\mathrm{B}}(k)$, provided k has characteristic $\geqslant 7$.*

[4] The letters K and B stand for "Kloosterman" and "Birch" respectively, for reasons that will be clear in the course of the proof in Section 3.

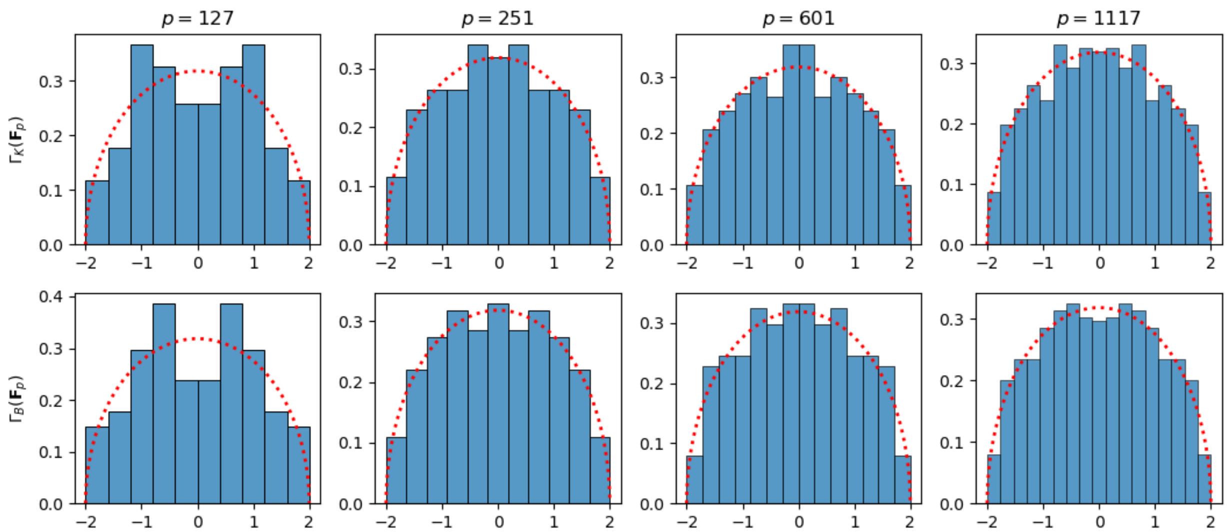


FIGURE 1. The normalized spectrum of the graphs $\Gamma_{\mathrm{K}}(k)$ (first row) and $\Gamma_{\mathrm{B}}(k)$ (second row), for $k = \mathbf{F}_{127}, \mathbf{F}_{251}, \mathbf{F}_{601}, \mathbf{F}_{1117}$. The dashed red curve is the density function of μ_{sc}, the semicircle distribution.

Remark 1.2. We now make a few remarks about the statement of Theorem 1.1.

(1) As is often the case in explicit constructions of pseudorandom graphs, both $\Gamma_{\mathrm{K}}(k)$ and $\Gamma_{\mathrm{B}}(k)$ may have up to d vertices with loops (where d is the degree). One can delete these loops and obtain graphs with essentially the same properties, but as is standard, it is more convenient for the analysis to include them.

(2) The bound $|\lambda| \leqslant 2\sqrt{|k|} = (2+o(1))\sqrt{d}$ means that these graphs are near-Ramanujan graphs, and hence they enjoy essentially optimal pseudorandomness in the traditional sense; see, e.g., the survey of Krivelevich and Sudakov [37, p. 19].

(3) The fact that these graphs do not contain a copy of $\mathrm{K}_{2,3}$ is quite surprising. Indeed, the Kővári–Sós–Turán theorem [34] 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 it was shown by Füredi [22] that this bound is asymptotically sharp. That is, up to the constant factor $\sqrt{2}$, the graphs $\Gamma_{\mathrm{K}}(k)$ and $\Gamma_{\mathrm{B}}(k)$ are as dense as possible among all $\mathrm{K}_{2,3}$-free graphs, and in this sense extremely atypical among all graphs of the same edge density.

In fact, 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 $d = \sqrt{n}$.

(4) The restriction to characteristic $\geqslant 7$ is necessary for the statement concerning the spectrum of the graphs $\Gamma_{\mathrm{B}}(k)$. Indeed, if the characteristic of k is 2 or 5, then the limiting spectrum of $\Gamma_{\mathrm{B}}(k)$ is a finitely-supported atomic measure (see Remark 4.4 for details). On the other hand, these graphs are still $\mathrm{K}_{2,3}$-free.

If the characteristic of k is 3, then one can check that $\Gamma_{\mathrm{B}}(k)$ is a disjoint union of $(|k|-1)/2$ copies of the complete bipartite graph $\mathrm{K}_{|k|,|k|}$, as well as one copy of the complete graph $\mathrm{K}_{|k|}$, and hence none of the properties above hold in this case.

(5) In Theorem 1.1, we define the graphs $\Gamma_{\mathrm{B}}(k)$ and $\Gamma_{\mathrm{K}}(k)$ to be Cayley sum graphs. However, every statement in Theorem 1.1 would remain true if, instead, we defined them as Cayley graphs of the same groups with the same generating sets. However, for the remainder of the paper we work with Cayley sum graphs, because some of the variant constructions we consider later in Section 5 are defined in terms of non-symmetric generating sets, and hence do not naturally have (undirected) Cayley graphs. By working with Cayley sum graphs throughout, we can avoid having to worry about the symmetry of the generating set.

(6) The Wasserstein (also called Monge–Kontorovich or Rubinstein–Kontorovich) distance $\mathrm{W}_1(\mu_1,\mu_2)$ between probability measures μ_1,μ_2 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 [36] for an introduction to Wasserstein metrics from the point of view of equidistribution).

(7) In a companion paper [20], we will describe other classes of examples of graphs with properties similar to those of $\Gamma_{\mathrm{K}}(k)$ and $\Gamma_{\mathrm{B}}(k)$. These are constructed using jacobians (and generalized jacobians) of algebraic curves over finite fields, and will show that there are very rich families of high-density $\mathrm{K}_{2,3}$-free graphs with semicircular spectral distribution. The proofs of these will however require more sophisticated results in algebraic and arithmetic geometry.

The remainder of this paper is organized as follows. In Section 2, we discuss our motivation for proving Theorem 1.1, and why we consider it interesting and surprising. In Section 3, we prove Theorem 1.1; our proof is quite short, since the $\mathrm{K}_{2,3}$-freeness of the graphs $\Gamma_{\mathrm{K}}(k)$ and $\Gamma_{\mathrm{B}}(k)$ is quite elementary to prove, and the remaining properties follow rather quickly from known, but very deep, results in number theory and algebraic geometry. In Section 4, we give an alternative, and more self-contained, proof that the spectrum of $\Gamma_{\mathrm{K}}(k)$ is given by the semicircular distribution. Notably, this proof exhibits a surprising connection between the spectral distribution and the $\mathrm{K}_{2,3}$-freeness of $\Gamma_{\mathrm{K}}(k)$; this $\mathrm{K}_{2,3}$-freeness is critical to allow us to apply a group-theoretic tool called *Larsen's alternative*, which is itself the main tool towards identifying the semicircle distribution as the limiting spectral distribution. Finally, in Section 5, we discuss a few variants of our construction; in particular, we can similarly construct C_4-free graphs of nearly optimal density, whose limiting spectral distributions are no longer semicircular, but are specific measures that we can describe and analyze.

Acknowledgments. We thank H. T. Pham for pointing out to us the paper of Soloveychik, Xiang and Tarokh, and T. Tokieda for his help in finding the paper of Sunada. We also thank T. Schramm for insights on the relationship between semicircular spectra, small subgraph counts and computational indistinguishability.

This project has received funding from 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. Discussion and historical background

2.1. **Why should we care?** Why should one care about explicit graphs with semicircular spectrum? From the perspective of extremal graph theory, it is not clear that such graphs provide much advantage over other known constructions of spectrally pseudorandom graphs. Indeed, we are aware of very few applications where the knowledge of the full spectrum is meaningfully more powerful than simply bounding the largest and smallest non-trivial eigenvalues (although we return to this point in § 2.3).

One reason why we should care is purely philosophical: since almost all graphs (at any edge density) have a semicircular spectrum, it is very natural to look for explicit examples with the same property. This is very similar to the search for explicit normal numbers, for explicit Ramsey graphs, for pseudorandom generators in computer science, and for other instances of "finding hay in a haystack".

Beyond its inherent appeal, this question is also closely related to important notions in computational complexity theory and cryptography, especially that of computational indistinguishability, introduced by Goldwasser and Micali in [23]. Roughly speaking, one says that two probability distributions are *computationally indistinguishable* if no efficient algorithm can distinguish samples from them (see [57, §7.3.1] for a more thorough introduction). As such, one way of formalizing pseudorandomness, which is very influential in theoretical computer science, is to say that a construction is pseudorandom if it is computationally indistinguishable from the uniformly random distribution.

Of course, proving computational indistinguishability amounts to proving limitations on the power of efficient algorithms, and hence is tantamount to proving that $\mathrm{P} \neq \mathrm{NP}$. Nonetheless, there is a great deal of interest in proving that certain restricted types of algorithms cannot distinguish an explicit pseudorandom object from a truly random one. For example, when it comes to distinguishing an explicit graph from a random graph, natural things one can try are to compute the spectrum and to count the number of copies of any constant-sized graph H, as both of these tasks can be easily done in polynomial time. Both of these are special cases of so-called *low-degree tests*, which are those quantities that can be read off from a low-degree polynomial of the input (in this case, the entries of the adjacency matrix). In fact, it is not hard to see that in the setting of graphs, low-degree polynomials are equivalent to *signed* subgraph counts (see, e.g., [4, Th. 2.1]). Moreover, the *low-degree heuristic* (see, e.g., [38, § 4]) roughly states that such low-degree tests capture the entire notion of computational indistinguishability, in that two distributions are indistinguishable if and only if they agree on all low-degree tests.

Our construction gives a family of graphs that are easily distinguishable from random graphs (by checking the presence of $\mathrm{K}_{2,3}$ as a subgraph), and yet are *spectrally indistinguishable*. This implies that if one wants to prove indistinguishability, it is not enough to restrict oneself to spectral algorithms: some graphs that are easily distinguished from random graphs may still have a completely random-like spectrum. One can compare the situation to that of the *planted clique problem*, which has become a cornerstone problem in indistinguishability, where the best known distinguishing algorithm [3] uses only spectral information.

Another way of looking at the same statement is to ask which structural features of a graph are determined by its spectrum. For example, the fact that the counts of short cycles determine the moments of the spectral distribution implies that if two graphs have asymptotically equal spectra, then they have roughly equal numbers of all short cycles. One could ask if something stronger is true: are the counts of all small subgraphs controlled by the spectrum? Our result shows that the answer is negative: our graphs are spectrally indistinguishable from a random graph of the same density, yet have very different numbers of copies of $\mathrm{K}_{2,3}$.

In the study of random matrices, semicircular limiting distributions often come with other desirable properties, including *eigenvector delocalization* and *eigenvalue repulsion*. For a detailed introduction to these topics, see the survey [54] of Tao and Vu. Our graphs $\Gamma_{\mathrm{K}}(k)$ and $\Gamma_{\mathrm{B}}(k)$ exhibit essentially optimal eigenvector delocalization, meaning that the ℓ^∞ norm of every (ℓ^2-normalized) eigenvector is $\mathrm{O}(n^{-1/2})$, where n is the number of vertices of the graph. This follows immediately from the algebraic structure of the graph; Proposition 3.3 below shows that the eigenvectors of $\Gamma_{\mathrm{K}}(k)$ and $\Gamma_{\mathrm{B}}(k)$ are linear combinations of at most 2 characters of the abelian group $k \times k$, which immediately implies that every entry of the eigenvector is at most $\mathrm{O}(n^{-1/2})$ in absolute value. On the other hand, our graphs are extremely far from exhibiting eigenvalue repulsion; it again follows immediately from Proposition 3.3 below, as well as the symmetry properties $\mathrm{K}(a,b;k) = \mathrm{K}(a\alpha, b\alpha^{-1};k)$ and $\mathrm{B}(a,b;k) = \mathrm{B}(a\alpha, b\alpha^3;k)$ of Kloosterman and Birch sums (for α non-zero), that every non-trivial eigenvalue of $\Gamma_{\mathrm{K}}(k)$ and $\Gamma_{\mathrm{B}}(k)$ appears with very high multiplicity, namely multiplicity at least $|k| - 1 = (1 + o(1))\sqrt{n}$ (in the case of $\Gamma_{\mathrm{K}}(k)$). Again, these facts raise interesting questions about how much the phenomena of eigenvector delocalization and eigenvalue repulsion have to do with the limiting distribution itself.

2.2. **History.** Despite its natural appeal, there seems to have been very little prior work on this question, and we are only aware of a few prior results.

(1) First, McKay [41] determined the limiting spectral distribution for *any* sequence of d-regular graphs, so long as d is fixed and the girth[5] of the graphs tends to infinity. Indeed, under such assumptions, one can explicitly compute the moments of the spectrum, as this boils down to counting rooted trees by the girth condition. The limiting distribution is the so-called *Kesten–McKay distribution*, given by the density function[6]
$$\frac{d(d-1)\sqrt{4-x^2}}{2\pi(d^2-(d-1)x^2)}$$
for $x \in [-2, 2]$. As $d \to \infty$, this density function approaches that of the semicircle distribution. As a consequence, if we have a sequence of regular graphs whose girth

[5] In fact, he proved that it suffices that the number of short cycles is not too large.

[6] This is not the most standard form of the Kesten–McKay distribution which appears in the literature; here we are renormalizing by $\sqrt{d-1}$ so that all of our limiting distributions are supported on $[-2, 2]$. As pointed out by Serre [49, p. 80] in a similar context, in the case where $d = p + 1$ for some prime number p, this distribution is related to the Plancherel measure for the group $\mathbf{PGL}_2(\mathbf{Q}_p)$.

tends to infinity and whose degrees tend to infinity sufficiently slowly, then the limiting spectral distribution will be semicircular. Explicit estimates on the required relations between the order, degree and girth of the graphs are given by Sunada [52] (also quoted in [42, Th. 4]) and Dumitriu–Pal[7] [14, Th. 1].

A natural family of explicit graphs satisfying (essentially) these conditions are certain Cayley graphs of the symmetric group S_n, namely those generated by the transpositions $\{(12), (13), \ldots, (1n)\}$. The fact that the spectrum of this family converges to the semicircle distribution was first obtained by Biane [5], by computing the moments and (implicitly) using the fact that these Cayley graphs have few short cycles. For an exposition of the proof, as well as more on the spectrum of these graphs and their history, see the note of Chapuy and Féray [9].

For another example, the famous Ramanujan graphs of Lubotzky, Phillips and Sarnak [40] give an explicit family of d-regular graphs (for $d = p + 1$, where p is a prime number) whose girth tends to infinity with the order of the graph. As such, an appropriately chosen sequence of such Ramanujan graphs would yield an explicit sequence of graphs whose limiting spectral distribution is semicircular. However, note that in both of these examples, the degree of the graphs grows very slowly with their order, and this appears to be necessary to use such an approach (e.g., in [14, Th. 1], the degree d_n must be $n^{o(1)}$, for a graph with n vertices). By contrast, our Theorem 1.1 gives a degree that grows as fast as $\sqrt{n}$.

(2) At the other extreme, this question was considered for graphs of *linear* degree by Soloveychik, Xiang and Tarokh [51], in the equivalent guise of constructing explicit symmetric matrices with ± 1 entries whose limiting spectrum is semicircular. In our language, they construct, for all $n = 2^m - 1$, a family $\mathscr{G}_n$ of n explicit graphs with n vertices, with the property that if one samples a graph Γ_n from $\mathscr{G}_n$ uniformly at random, then almost surely the sequence (Γ_n) has the semicircular distribution as its limiting spectral distribution. Due to this random sampling, their construction is not fully explicit, although they conjecture that their result can be strengthened so that it holds for all choices of $\Gamma_n \in \mathscr{G}_n$ (and hence would give an explicit construction).

In both of these examples, the convergence to the semicircular distribution is proved using the method of moments: the moments of the spectrum can be explicitly computed in terms of combinatorial counts of closed walks in the graphs, and one can prove that these moments converge to those of the semicircle law.

By contrast, our technique is completely different, and uses the fact that the semicircular distribution appears in an entirely unrelated setting. Namely, if one picks a matrix in $\mathbf{SU}_2(\mathbf{C})$ at random according to the Haar probability measure, then its trace is distributed according to the semicircle law (this follows from the Weyl integration formula; see, e.g., [7, p. 339, Example]). This distribution arises this way very naturally in number theory, where it is called the *Sato–Tate distribution* associated to $\mathbf{SU}_2(\mathbf{C})$ (see Sutherland's survey [53] for an introduction to this topic). To the best of our knowledge, there is no direct connection between the spectrum of Wigner matrices and the traces of $\mathbf{SU}_2(\mathbf{C})$-random matrices, apart from the fact that they both happen to have the same distribution.

[7] While [14, Th. 1] is only stated for *random* regular graphs, their proof uses nothing more than the control on the number of short cycles in these graphs.

We prove that the spectrum of our graphs converges to the semicircular distribution by exploiting this coincidence. Specifically, we use Deligne's *equidistribution theorem* [13, § 3.5], which allows us to relate the spectrum of the graphs to the traces of certain matrices, which behave like Haar-distributed random matrices, and results of Katz [28] which show that these matrices are in $\mathbf{SU}_2(\mathbf{C})$.

2.3. **The independence number.** Recall that given two graphs H_1 and H_2, the *Ramsey number*[8] $r(H_1, H_2)$ is the smallest integer N such that, for any partition of the edges of the complete graph K_N on N vertices in two parts E_1 and E_2, there is either a copy of H_1 in E_1 or one of H_2 in E_2. In particular, if $H_2 = K_t$ for some integer $t \geqslant 2$, then it follows elementarily that an integer n is less than $r(H_1, K_t)$ if and only if there is a graph with n vertices without any copy of H_1 and with independence number less than t. (We recall that the *independence number* $\alpha(\Gamma)$ of a graph Γ is the maximum size of a set of vertices containing no edges.)

Let C_4 denote the 4-cycle. One of the central open problems in graph Ramsey theory is the estimation of the Ramsey number $r(C_4, K_t)$, which is therefore equivalent to asking for the smallest independence number among all n-vertex C_4-free graphs. As an n-vertex C_4-free graph has $O(n^{3/2})$ edges by the Kővári–Sós–Turán theorem [34], one immediately finds (see, e.g., [1]) that it must have independence number at least $c\sqrt{n}$, for some absolute constant $c > 0$. An infamous conjecture of Erdős [17], reiterated many times, posits that in fact there should exist some absolute constant $\delta > 0$ such that $\alpha(\Gamma) \geqslant \delta n^{\frac{1}{2}+\delta}$ for every n-vertex C_4-free graph Γ. To date, the best known lower bound is $\alpha(\Gamma) \geqslant c\sqrt{n}\log n$ for some constant $c > 0$, which follows immediately from the classical Ajtai–Komlós–Szemerédi [1] bound on the independence number of graphs with few triangles (note that in a C_4-free graph, every edge lies on at most one triangle).

In the other direction, the best known upper bound for $\alpha(\Gamma)$ is $O((n\log n)^{\frac{2}{3}})$, which follows from work of Bohman–Keevash [6] on the random C_4-free process (see also [43] for a very different construction of Mubayi and Verstraëte achieving the same bound). The main difficulty in closing the gap between the lower and the upper bound seems to be the following: any truly "random-like" C_4-free graph cannot have average degree much greater than $n^{\frac{1}{3}}$, and hence cannot have independence number much smaller than $n^{\frac{2}{3}}$. While there do exist a plethora of constructions of denser C_4-free graphs, of average degree as large as $\sqrt{n}$, all known constructions have a much larger independence number, namely on the order of $n^{\frac{3}{4}}$, than what we would expect in a random graph of the same density.

Why $n^{\frac{3}{4}}$? It follows immediately from the expander mixing lemma (see (2.1) below) that if an n-vertex d-regular graph has all of its non-trivial eigenvalues bounded by λ, then the bound $\alpha(\Gamma) \leqslant n\lambda/d$ holds; a slightly more precise bound is given by Hoffman's ratio bound (see the account by Haemers [24]). Known constructions of dense C_4-free graphs are optimally spectrally pseudorandom, thus satisfying $\lambda = O(\sqrt{d}) = O(n^{\frac{1}{4}})$. This immediately implies that their independence number is at most $O(n^{\frac{3}{4}})$; however, while there is no reason to expect this spectral bound to be tight in general, it turns out to be so for all known examples of dense C_4-free graphs (see the work of Mubayi and Williford [44]).

[8]For an introduction to Ramsey theory, see the survey of Conlon, Fox and Sudakov [12] or the lecture notes of Wigderson [58].

In principle, more detailed knowledge of the whole spectrum, rather than simply a bound on the magnitude of the non-trivial eigenvalues, should allow one to obtain tighter control on the independence number. Indeed, let Γ be an n-vertex d-regular graph, let A be its adjacency matrix, and let $\mathrm{A} = \sum_{i=1}^{n} \lambda_i v_i v_i^t$ be the spectral decomposition of A, where $\lambda_1 = d$ and $v_1 = (\frac{1}{\sqrt{n}}, \ldots, \frac{1}{\sqrt{n}})$. If I is any independent set in Γ, then its indicator vector $\mathbf{1}_{\mathrm{I}}$ satisfies

$$0 = \langle \mathbf{1}_{\mathrm{I}}, \mathrm{A}\mathbf{1}_{\mathrm{I}} \rangle = \sum_{i=1}^{n} \lambda_i \langle \mathbf{1}_{\mathrm{I}}, v_i \rangle^2 = \frac{d\,|\mathrm{I}|^2}{n} + \sum_{i=2}^{n} \lambda_i \langle \mathbf{1}_{\mathrm{I}}, v_i \rangle^2. \tag{2.1}$$

By plugging in the bound $|\lambda_i| \leqslant \lambda$ and the formula $\sum_{i=1}^{n} \langle \mathbf{1}_{\mathrm{I}}, v_i \rangle^2 = |\mathrm{I}|$, one immediately obtains the bound $|\mathrm{I}| \leqslant n\lambda/d$ mentioned above. However, this is in principle quite wasteful: we may expect to have a great deal of cancellation in the sum $\sum \lambda_i \langle \mathbf{1}_{\mathrm{I}}, v_i \rangle^2$, which could yield a much stronger bound. Concretely, if the bound $\alpha(\Gamma) \leqslant n\lambda/d$ is essentially tight, it means that a largest independent set in Γ must correlate very strongly with the eigenvectors corresponding to the most negative eigenvalues of Γ.

In some instances, one can use such an idea to slightly improve on this simple bound (see, e.g., Newman's thesis [45, §6.11]), and there are a few other examples (e.g. the paper [16] of Elphick, Tang and Zhang) of using the entire spectrum to bound the independence number. Moreover, it is very tempting to believe that such ideas may be relevant for the case of C_4-free graphs: the classical constructions of dense C_4-free graphs are strongly regular, and thus their most negative eigenvalue has enormous multiplicity (roughly $n/2$). It is thus relatively easy to construct an indicator vector of a set that correlates very strongly with these eigenvectors.

This brings us back to our graphs. Since their limiting spectral distribution is continuous, we are hopeful that their independence number is substantially smaller than that of the classical constructions: we believe that this continuous spectrum should yield strong cancellation in (2.1). That said, proving this is likely to be quite difficult: even proving that sets of the form $\mathrm{I} \times \mathrm{J}$, where $\mathrm{I}, \mathrm{J} \subset \mathbf{F}_p$ are intervals, are not independent in $\Gamma_{\mathrm{K}}(\mathbf{F}_p)$ if $|\mathrm{I}|\,|\mathrm{J}| \geqslant p^{\frac{3}{2}-\delta}$ is a difficult open problem (see Theorem 13 and the subsequent discussion in the survey of Shparlinski [50]). While our graphs are not C_4-free, they "almost" are. Moreover, we can extract well-behaved C_4-free subgraphs of them in such a way that the limiting spectral distribution remains an explicit distribution with continuous density (although it is not semicircular anymore; see Section 5). Alternatively, one can simply study $r(\mathrm{K}_{2,3}, \mathrm{K}_t)$, or equivalently the minimum independence number of $\mathrm{K}_{2,3}$-free graphs, a problem with a great deal of similarities with the C_4-free problem discussed above, and where our graphs can be directly applied (see, e.g., the paper [8] of Caro, Li, Rousseau and Zhang).

3. Proof of Theorem 1.1

Although our proof will be quite short, the spectral information relies on very deep results of algebraic geometry, namely *Deligne's equidistribution theorem*, and on Katz's concrete versions of this result for the specific case of Kloosterman sums and Birch sums.

On the other hand, the fact that $\Gamma_{\mathrm{K}}(k)$ and $\Gamma_{\mathrm{B}}(k)$ do not contain $\mathrm{K}_{2,3}$ is straightforward.

More generally, let G be an abelian group and S a subset of G. We define the *Cayley sum graph* $\Gamma(\mathrm{G}, \mathrm{S})$ to have vertex set G and and edge joining x to y if and only if $x + y \in \mathrm{S}$. We recall that a subset $\mathrm{S} \subset \mathrm{G}$ is called a *Sidon set* if the equation

$$\alpha + \beta = \gamma + \delta, \qquad (\alpha, \beta, \gamma, \delta) \in \mathrm{S}^4, \tag{3.1}$$

only has solutions with $\alpha \in \{\gamma, \delta\}$. Moreover, we say that S is a *partial symmetric Sidon set*, with center some element $a_0 \in \mathrm{S}$, if the equation (3.1) has only solutions with $\alpha \in \{\gamma, \delta\}$ or $\alpha + \beta = \gamma + \delta = a_0$ (in which case $\{\alpha, \gamma\} \subset \mathrm{S} \cap (a_0 - \mathrm{S})$). If the set S also satisfies $\mathrm{S} = a_0 - \mathrm{S}$, then we say that S is a *symmetric Sidon set* with center a_0 (as in [18]).

We then have the following simple result, variants of which are well-known in the literature.

Proposition 3.1. *Let* G *be an abelian group and* S *a subset of* G*.*

(1) *If* S *is a Sidon set in* G*, then* $\mathrm{C}_4 \not\subset \Gamma(\mathrm{G}, \mathrm{S})$*.*
(2) *If* S *is a partial symmetric Sidon set in* G*, then* $\mathrm{K}_{2,3} \not\subset \Gamma(\mathrm{G}, \mathrm{S})$*.*

Proof. Let (w, x, y, z) be the vertices of a four-cycle in $\Gamma(\mathrm{G}, \mathrm{S})$. We define $\alpha = w + x$, $\gamma = x + y$, $\beta = y + z$ and $\delta = z + w$, and note that these are elements of S such that

$$\alpha + \beta = \gamma + \delta.$$

(1) If S is a Sidon set, then we have either $\alpha = \gamma$, and hence $w = y$, or $\alpha = \delta$, and hence $x = z$; both of these are impossible.

(2) If S is a partial symmetric Sidon set with center $a_0 \in \mathrm{G}$, then the only remaining option is that $\alpha + \beta = \gamma + \delta = a_0$ with $\alpha,\ \gamma \in \mathrm{S} \cap (a_0 - \mathrm{S})$. Given the values of $w \in \mathrm{G}$ and $(\alpha, \gamma) \in \mathrm{S}^2$, this gives *at most one* 4-cycle of the form

$$(w, \alpha - w, \gamma - \alpha + w, a_0 - \gamma - w)$$

with opposite vertices w and $y = \gamma - \alpha + w$. We conclude that there is no copy of $\mathrm{K}_{2,3}$, either because every pair of vertices (w, y) are joined by at most two distinct paths of length 2, or because $\mathrm{K}_{2,3}$ contains two different 4-cycles with opposite vertices. ∎

Thus, the first statement of Theorem 1.1 follows from the elementary observation that $\mathrm{K}(k)$ and $\mathrm{B}(k)$ (the latter for a field k of characteristic different from 3) are symmetric Sidon sets with center 0 in $k \times k$, as stated in the following proposition.

Proposition 3.2. *For every finite field* k*, the set* $\mathrm{K}(k)$ *is a symmetric Sidon set in* $k \times k$ *(with center* 0*). If the characteristic of* k *is* $\neq 3$*, then the same property holds for* $\mathrm{B}(k)$*.*

We remark that these facts appear implicitly in several places in the literature, e.g. both in the paper [46, p. 349–350] of Ruzsa, in a paper [29, p. 118] of Katz for $\mathrm{B}(k)$, and in Kloosterman's work [33, p. 425] for $\mathrm{K}(k)$, but as far as we are aware, not explicitly, although they are related to many of the known constructions of Sidon sets (see, e.g., [15]).

Proof of Proposition 3.2. Let us fix some $(u, v) \in k \times k$. We wish to count the number of solutions to $(x, 1/x) + (y, 1/y) = (u, v)$ for $(x, 1/x), (y, 1/y) \in \mathrm{K}(k)$; it suffices to show that if $(u, v) \neq (0, 0)$, then there is at most one solution up to ordering. If $v = 0$, then we have $1/x = -1/y$, hence $x = -y$, and hence $u = 0$ as well, so we may assume that $v \neq 0$. The equation $1/x + 1/y = v$ is equivalent to $x + y = vxy$, which in turn implies that $xy = u/v$ using that $x + y = u$. That is, from the equation $(x, 1/x) + (y, 1/y) = (u, v)$, we have deduced that $x + y = u$ and $xy = u/v$. But we now know the sum and product of x and y, which means that x, y are unique up to ordering, as claimed. This proves the statement for $\mathrm{K}(k)$.

We now assume that k has characteristic $\neq 3$, and prove the claim for $\mathrm{B}(k)$. Again, given $(u,v) \in k \times k$, we wish to determine the solutions to $(x,x^3)+(y,y^3) = (u,v)$. As before, if $u = 0$ then $v = 0$ as well, so we may assume $u \neq 0$. Plugging $y = u - x$ into the equation $x^3+y^3 = v$, we find that $x^3+(u-x)^3 = v$, or equivalently that $3ux^2-3u^2x+u^3 = v$. This is a quadratic equation in x with non-zero leading coefficient (by the assumptions), and hence there are at most two values of x satisfying this equation. Given x, the value of $y = u-x$ is uniquely determined (and is in fact the other root of the quadratic equation), which completes the proof. $\square$

To prove the remainder of the theorem, we require the next property, which is also well-known. We denote here by $\widehat{\mathrm{G}}$ the character group of a finite group G.

Proposition 3.3. *Let G be a finite abelian group and $\mathrm{S} \subset \mathrm{G}$ a non-empty subset.*

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

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

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

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

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

If some of the sums appearing in these statement coincide, for different choices of χ, then the corresponding eigenvalue occurs with multiplicity equal to the number of characters that give rise to it.

Proof. If A denotes the adjacency matrix, viewed as a linear map acting on the space $\mathscr{C}$ of complex-valued functions on G, we simply observe that by direct computation, we have

$$\mathrm{A}(\chi) = \mathrm{S}(\chi)\bar{\chi}$$

for any character χ of G, where

$$\mathrm{S}(\chi) = \sum_{y\in\mathrm{S}} \chi(y).$$

It follows that any real character χ is an eigenvector of A with eigenvalue $\mathrm{S}(\chi)$, and that any pair $(\chi,\bar{\chi})$ of distinct non-real characters spans a 2-dimensional invariant subspace on which A acts according to the matrix

$$\begin{pmatrix} 0 & \mathrm{S}(\bar{\chi}) \\ \mathrm{S}(\chi) & 0 \end{pmatrix}.$$

The characteristic polynomial of this matrix is $\mathrm{X}^2 - |\mathrm{S}(\chi)|^2$, and hence its eigenvalues are the numbers $|\mathrm{S}(\chi)|$ and $-|\mathrm{S}(\chi)|$. $\square$

Proof of Theorem 1.1. We first assume that the characteristic of k is not 2. We apply Proposition 3.3 to $\mathrm{G} = k \times k$ and $\mathrm{S} = \mathrm{K}(k)$ or $\mathrm{B}(k)$. Fixing a non-trivial additive character ψ of k, the characters of $k \times k$ are of the form

$$(x,y) \mapsto \psi(ax+by)$$

for $(a,b)\in k\times k$, and none of them is a real character, with the exception of the trivial one. Thus the eigenvalues of the Cayley sum graphs $\Gamma_{\mathrm{K}}(k)$ and $\Gamma_{\mathrm{B}}(k)$ are, on the one hand the trivial eigenvalue, equal to the degree $|\mathrm{K}(k)|$ or $|\mathrm{B}(k)|$ of the graph, and on the other hand the quantities

$$|\mathrm{K}(a,b;k)| \quad\text{and}\quad -|\mathrm{K}(a,b;k)|, \qquad\text{or}\qquad |\mathrm{B}(a,b;k)| \quad\text{and}\quad -|\mathrm{B}(a,b;k)|,$$

in terms of the exponential sums

$$\mathrm{K}(a,b;k)=\sum_{x\in k^{\times}}\psi(ax+bx^{-1}),\qquad \mathrm{B}(a,b;k)=\sum_{x\in k}\psi(ax+bx^{3}).$$

In the number theory literature, these are known as *Kloosterman sums* or *Birch sums*, respectively. They are real numbers, so that

$$\mathrm{K}(-a,-b;k)=\mathrm{K}(a,b;k)\quad\text{and}\quad \mathrm{B}(-a,-b;k)=\mathrm{B}(a,b;k).$$

A well-known application of the Riemann hypothesis for curves over finite fields, due to Weil, implies the bounds

$$|\mathrm{K}(a,b;k)|\leqslant 2\sqrt{|k|},\qquad |\mathrm{B}(a,b;k)|\leqslant 2\sqrt{|k|},$$

if $(a,b)\neq(0,0)$ (see, e.g., [26, § 11.7] for an elementary proof using Stepanov's method, in the case of Kloosterman sums), thus proving the second statement of Theorem 1.1.

The final and deepest statement (for which no fully elementary proof is known) is provided by work of Katz. In the case of Kloosterman sums, Katz proved in [28, Th. 11.1, Th.11.4] that the normalized Kloosterman sums $\mathrm{K}(a,1;k)/\sqrt{|k|}$ for $a\in k^{\times}$ become equidistributed according to the semicircle distribution as $|k|\to+\infty$. The relation

$$\mathrm{K}(a,b;k)=\mathrm{K}(ab,1;k)$$

for $(a,b)\in k^{\times}\times k^{\times}$ implies that the distribution of $\mathrm{K}(a,b;k)/\sqrt{|k|}$ (as a measure on $\mathbf{R}$) is the same as that of $\mathrm{K}(a,1;k)/\sqrt{|k|}$. Moreover, since $\mathrm{K}(a,0;k)=\mathrm{K}(0,b;k)=-1$ for $ab\neq 0$, the contribution of the eigenvalues with $a=0$ or $b=0$ (but not both) to the limiting distribution vanishes.

Since the measure μ_{sc} is symmetric (i.e., invariant under the transformation $x\mapsto -x$ on $[-2,2]$), it follows that the same equidistribution properties hold for the absolute values of the sums and their opposite, which give the non-trivial spectrum of the Cayley sum graphs for odd characteristic. Precisely, the empirical spectral measure for the non-trivial eigenvalues of $\Gamma_{\mathrm{K}}(k)$ is

$$\frac{1}{|k|^2-1}\sum_{\text{pairs }(a,b)}\Bigl(\delta_{\mathrm{K}(a,b;k)/\sqrt{|k|}}+\delta_{-\mathrm{K}(a,b;k)/\sqrt{|k|}}\Bigr),$$

where the sum ranges over pairs $((a,b),(-a-b))$ of non-trivial characters, whereas the empirical measure for Kloosterman sums is

$$\frac{1}{|k|^2-1}\sum_{(a,b)}\delta_{\mathrm{K}(a,b;k)/\sqrt{|k|}}=\frac{2}{|k|^2-1}\sum_{\text{pairs }(a,b)}\delta_{\mathrm{K}(a,b;k)/\sqrt{|k|}},$$

Since the latter converges to μ_{sc} by Katz's work, and since μ_{sc} is symmetric, the same applies to the former.

The analogue of the bound (1.2) is proved in [36, Th. 4.4] (as spelled-out in [36, Example 4.5 (1)]) for the distribution of $\mathrm{K}(a,1;k)/\sqrt{|k|}$ with $a \in k^\times$. By the preceding remarks, this implies (1.2).

In the case of Birch sums, Katz proved the equidistribution in [27, Th. 19, Cor. 20] for $a \mapsto \mathrm{B}(a,b;k)/\sqrt{|k|}$ with a varying in k for any fixed $b \in k^\times$, when k is restricted to fields of characteristic $\geqslant 7$ (the statement of loc. cit. suggests that it requires $p > 7$; however, the result is valid for $p = 7$ by inspection, the point being that the value of n in [27, Th. 9], which is used in the proof of [27, Th. 19], is the rank 2 and not the degree 3 of the polynomial).

Since $\mathrm{B}(a,0;k) = 0$ for $a \in k^\times$, the values which are excluded do not affect the equidistribution, and the remainder of the argument is essentially identical.

In characteristic 2, a case that only occurs for Kloosterman sums, the argument is similar but simpler: all characters are real characters, so the eigenvalues of the adjacency matrix are exactly the Kloosterman sums $\mathrm{K}(a,b;k)$, and we can directly apply the results of Katz. $\square$

Although this gives a complete proof of Theorem 1.1, we explain in the next section an alternate proof of the equidistribution theorem in the case of $\Gamma_{\mathrm{K}}(k)$ which is based on more recent ideas and is more transparent. In fact, this will reveal that the $\mathrm{K}_{2,3}$-freeness of the graphs is closely related to their spectral properties.

4. Larsen's alternative, Sidon sets and equidistribution

For simplicity, we will restrict our argument to the setting where k varies among the extensions of a fixed base finite field. The starting point is Deligne's general *a priori* equidistribution theorem, which relies on Deligne's most general form of the Riemann hypothesis over finite fields. Specialized to the case of Kloosterman sums, this is the following statement (most easily deduced from the version in [19, Th. 4.8]; see also [13, §3.5] for the original statement, and [28, Th. 3.6] for another version).

Theorem 4.1. *Let k be a finite field. There exist an integer $r \geqslant 0$ and two compact Lie groups K^g and K^a, contained in $\mathbf{U}_r(\mathbf{C})$ such that the following properties hold:*

1. *The subgroup K^g is a normal subgroup of K^a with $\mathrm{K}^a/\mathrm{K}^g$ abelian.*
2. *For any continuous and bounded function $f\colon \mathbf{C} \to \mathbf{C}$, we have*
$$\lim_{\mathrm{N}\to+\infty} \frac{1}{\mathrm{N}} \sum_{1\leqslant n\leqslant \mathrm{N}} \frac{1}{|k_n^\times|^2} \sum_{a,b\in k_n^\times} f\Big(\frac{1}{\sqrt{|k_n|}}\mathrm{K}(a,b;k_n)\Big) = \int_{\mathrm{K}^a} f(\mathrm{Tr}(x))dx,$$
where k_n is the extension of degree n of k in an algebraic closure of k, and the character $\psi_n = \psi \circ \mathrm{Tr}_{k_n/k}$ is used to define $\mathrm{K}(a,b;k_n)$.
3. *If $\mathrm{K}^a = \mathrm{K}^g$, then for any continuous and bounded function $f\colon \mathbf{C} \to \mathbf{C}$, we have*
$$\lim_{n\to+\infty} \frac{1}{|k_n^\times|^2} \sum_{a,b\in k_n^\times} f\Big(\frac{1}{\sqrt{|k_n|}}\mathrm{K}(a,b;k_n)\Big) = \int_{\mathrm{K}^a} f(\mathrm{Tr}(x))dx.$$

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

Assuming this deep result, we can deduce the equidistribution theorem of Katz for Kloosterman sums, provided we can show that $r = 2$ and $\mathrm{K}^a = \mathrm{K}^g = \mathbf{SU}_2(\mathbf{C})$. The first assertion that $r = 2$ is a standard consequence of the Grothendieck–Ogg–Shafarevich formula (see, e.g., [28, § 2.3.1]). It corresponds also to the following fundamental property: according to the formalism underlying Deligne's equidistribution theorem, and the constructions of Katz, it is known that for all $(a,b) \in (k^\times)^2$, there exists an element $\theta(a,b;k)$ of $\mathbf{U}_2(\mathbf{C})$ such that

$$\mathrm{Tr}(\theta(a,b;k)) = \frac{1}{\sqrt{k}} \sum_{x \in k^\times} \psi(ax + bx^{-1}).$$

This fact explains in particular the bound $|\mathrm{K}(a,b;k)| \leqslant 2\sqrt{|k|}$, as all elements of $\mathbf{U}_2(\mathbf{C})$ have trace in $[-2,2]$. Moreover, one proves that the characteristic polynomial of $\theta(a,b;k)$ is

$$\mathrm{X}^2 - \frac{\mathrm{K}(a,b;k)}{\sqrt{|k|}}\mathrm{X} + 1,$$

which implies that $\theta(a,b;k) \in \mathbf{SU}_2(\mathbf{C})$, and then one deduces that $\mathrm{K}^a \subset \mathbf{SU}_2(\mathbf{C})$.

Lemma 4.2. *With notation as above, 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 faithful representation.*

Proof. The fact that K^a is contained in $\mathbf{SU}_2(\mathbf{C})$ has been explained above. Next, by equidistribution again, we can compute

$$\mathrm{M}_4 = \int_{\mathrm{K}^a} |\mathrm{Tr}(x)|^4 \, dx = 2$$

using the fact that the sets $\mathrm{K}(k_n)$ are symmetric Sidon sets. More precisely, it follows from equidistribution that

$$\mathrm{M}_4 = \lim_{\mathrm{N}\to+\infty} \frac{1}{\mathrm{N}} \sum_{n \leqslant \mathrm{N}} \frac{1}{|k_n^\times|^2} \sum_{a,b \in k_n^\times} \Big| \frac{1}{\sqrt{|k_n|}} \sum_{x \in k_n^\times} \psi_n(ax + bx^{-1}) \Big|^4.$$

Expanding the fourth power, the average over (a,b) on the right-hand side, for a given $n \geqslant 1$, is equal to

$$\frac{1}{|k_n|^2} \sum_{x_1,\ldots,x_4 \in k_n^\times} \frac{1}{|k_n|^\times} \sum_{a \in k_n^\times} \psi_n(a(x_1 + x_2 - x_4 - x_4)) \frac{1}{|k_n|^\times} \sum_{b \in k_n^\times} \psi_n(b(x_1^{-1} + x_2^{-1} - x_3^{-1} - x_4^{-1})).$$

Writing both sums over a and b as sums over k_n minus the contributions of $a = 0$ and $b = 0$, we obtain four terms. The first one, by orthogonality of characters, is

$$\frac{1}{|k_n|^2} \sum_{\substack{x_1,\ldots,x_4 \in k_n^\times \\ x_1 + x_2 = x_3 + x_4 \\ x_1^{-1} + x_2^{-1} = x_3^{-1} + x_4^{-1}}} 1,$$

which converges to 3 as $n \to +\infty$ because $\mathrm{K}(k_n)$ is a symmetric Sidon set.

Using orthogonality again, the additional contributions are:

$$-\frac{1}{|k_n|^3}\sum_{\substack{x_1,\ldots,x_4\in k_n^\times\\ x_1^{-1}+x_2^{-1}=x_3^{-1}+x_4^{-1}}} 1 \qquad (\text{from } a=0),$$

$$-\frac{1}{|k_n|^3}\sum_{\substack{x_1,\ldots,x_4\in k_n^\times\\ x_1+x_2=x_3+x_4}} 1 \qquad (\text{from } b=0),$$

$$\frac{1}{|k_n|^4}\sum_{x_1,\ldots,x_4\in k_n^\times} 1 \qquad (\text{from } a=b=0).$$

The first two converge to -1 each, and the last converges to 1. Altogether, we obtain

$$\mathrm{M}_4=\lim_{\mathrm{N}\to+\infty}\frac{1}{\mathrm{N}}\sum_{n\leqslant \mathrm{N}}\frac{1}{|k_n^\times|^2}\sum_{a,b\in k_n^\times}\Big|\frac{1}{\sqrt{|k_n|}}\sum_{x\in k_n^\times}\psi_n(ax+bx^{-1})\Big|^4=3-1-1+1=2.$$

By Larsen's alternative (see [30, Th. 1.1.6] or [19, Th. 8.5]), the fact that $\mathrm{M}_4=2$ implies that either $\mathrm{K}^a=\mathbf{SU}_2(\mathbf{C})$, or that K^a is a finite subgroup of $\mathbf{SU}_2(\mathbf{C})$. In the first case, we deduce that in fact $\mathrm{K}^a=\mathrm{K}^g=\mathbf{SU}_2(\mathbf{C})$ because K^g is a normal subgroup of K^a with abelian quotient and $\mathbf{SU}_2(\mathbf{C})$ has no such subgroup except itself.

If K^a is finite, then Katz has proved [30, 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 from a representation of a proper subgroup. This means that K^a is 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 $\mathbf{SO}_3$), and there are three possible groups, often called the binary tetrahedral, binary octahedral and binary icosahedral groups.

To check that these three groups are indeed those 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 [39, Th. 6.11] for this classification, and the other facts are elementary. ∎

The following finishes the proof of the equidistribution of Kloosterman sums for the sequence of fields $(k_n)_{n\geqslant 1}$.

Lemma 4.3. *The group* K^a *associated to Kloosterman sums is infinite.*

Proof. The key point is that the formalism implies that the matrix $\theta(a,b;k)\in\mathbf{SU}_2(\mathbf{C})$ discussed above is in fact in K^a for all $(a,b)\in k^\times\times k^\times$ (and is unique up to conjugacy in K^a). Suppose then that K^a is finite. The trace of $\theta(a,b;k)$, as the trace of a matrix of finite order, is a sum of finitely many roots of unity, and hence is an algebraic integer. However, taking $b=1$ and summing over $a\in k^\times$, we find that

$$\sum_{a\in k^\times}\mathrm{Tr}(\theta(a,1;k))=\sum_{a\in k}\frac{1}{\sqrt{k}}\sum_{x\in k^\times}\psi(ax+x^{-1})-\frac{1}{\sqrt{|k|}}\sum_{x\in k^\times}\psi(x^{-1})=\frac{1}{\sqrt{|k|}}$$

by orthogonality of characters. Since this is not an algebraic integer, we have a contradiction. ∎

Remark 4.4. It seems difficult to find a similarly elementary argument for the case of Birch sums. The reason is that the restriction $p \geqslant 7$ on the characteristic is necessary, and hence any proof must necessarily involve this assumption in some way. More precisely, Katz proved (see [31, 3.8.4] or [32, Th. 4.1, 4.2]) that for the Birch sums associated to fields of characteristic 2 or 5, the group K^a is finite. This is depicted in Figure 2.

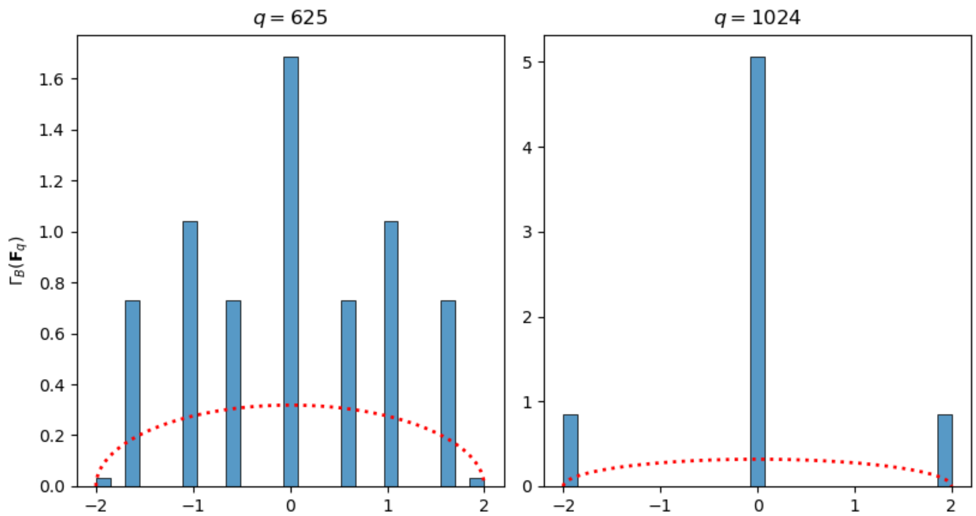


FIGURE 2. The spectrum of the graphs $\Gamma_{\mathrm{B}}(\mathbf{F}_q)$ for $q = 625$ and $q = 1024$. As predicted by Katz's theorem, the limiting spectrum is a finitely-supported atomic measure because the characteristic is less than 7.

5. Variants

We describe here two types of variants, both obtained by considering graphs with edges given by subsets of the hyperbola $\mathrm{K}(k)$. In the first, we present an *uncountable* family of possible limiting spectral distributions for $\mathrm{K}_{2,3}$-free graphs of essentially optimal density, as well as for C_4-free graphs. In the second case, another example of C_4-free graphs is given.

We will use a simple observation in both cases.

Lemma 5.1. *Let* G *be a finite abelian group and* $\mathrm{S} \subset \mathrm{G}$ *a partial symmetric Sidon set with center* 0*. If* $\mathrm{T} \subset \mathrm{G}$ *is a subset such that* $\mathrm{T} \cap (-\mathrm{T}) = \emptyset$*, then* $\mathrm{S} \cap \mathrm{T}$ *is a Sidon set.*

Proof. This is immediate from the definitions. ∎

Given a complex-valued random variable X, we will denote by $\varepsilon|\mathrm{X}|$ the product of $|\mathrm{X}|$ with a random variable ε independent of X and taking values -1 and 1 each with probability $1/2$. We will also use the additive character of $\mathbf{F}_p$ defined by

$$\psi_p(x) = e(x/p), \quad \text{where} \quad e(z) = e^{2i\pi z} \quad \text{for} \quad z \in \mathbf{C}.$$

Our first statement is the following.

Theorem 5.2. *Let t be a real number with $0 < t \leqslant 1$. Let*

$$\mathrm{K}_t(p) = \{(x,y) \in \mathbf{F}_p \times \mathbf{F}_p \mid xy = 1 \text{ and } 1 \leqslant x \leqslant t(p-1)\},$$

where we identify $\mathbf{F}_p$ with the integers $\{0, \ldots, p-1\}$.

(1) *The graph $\Gamma(\mathbf{F}_p \times \mathbf{F}_p, \mathrm{K}_t(p))$ is $\mathrm{K}_{2,3}$-free, and C_4-free if $0 < t \leqslant 1/2$.*
(2) *All the non-trivial eigenvalues λ of the adjacency matrix of $\Gamma(\mathbf{F}_p \times \mathbf{F}_p, \mathrm{K}_t(p))$ satisfy*

$$|\lambda| = \mathrm{O}(p^{1/2} \log p),$$

where the implied constant is absolute, and in particular, independent of t.
(3) *As $p \to +\infty$ among primes, the numbers*

$$\Big\{\frac{\lambda}{\sqrt{|\mathrm{K}_t(p)|}} \mid \lambda \text{ an eigenvalue of } \Gamma(\mathbf{F}_p \times \mathbf{F}_p, \mathrm{K}_t(p))\Big\}$$

converge in distribution to the distribution of

$$\varepsilon\Big|t^{1/2}\mathrm{SC}_0 + \frac{1}{\sqrt{t}} \sum_{\substack{h \in \mathbf{Z}\\ h \neq 0}} \frac{e(ht)-1}{2i\pi h}\mathrm{SC}_h\Big|,$$

where $(\mathrm{SC}_h)_{h \in \mathbf{Z}}$ are independent semicircle-distributed random variables and the random series converges almost surely when taken as a limit of symmetric partial sums.

Proof. The first assertion follows from the fact that $\mathrm{K}_t(p)$ is a partial symmetric Sidon set, and from Lemma 5.1, applied with $\mathrm{G} = \mathbf{F}_p \times \mathbf{F}_p$, $\mathrm{S} = \mathrm{K}_t(p)$ with $0 < t \leqslant 1/2$ and

$$\mathrm{T} = \Big\{(x,y) \in \mathrm{G} \mid 1 \leqslant x \leqslant \frac{p-1}{2}\Big\}.$$

The second statement follows from the completion method for exponential sums (see, e.g., [26, §12.2]), applied to

$$\sum_{1 \leqslant x \leqslant (p-1)t} \psi_p(ax + bx^{-1}).$$

According to a result of Kowalski and Sawin [35, Th. 1.1 (1)], the normalized sums

$$\frac{1}{\sqrt{p}} \sum_{1 \leqslant x \leqslant (p-1)t} \psi_p(ax + bx^{-1})$$

converge in distribution as $p \to +\infty$ to the sum

$$t\mathrm{SC}_0 + \sum_{\substack{h \in \mathbf{Z}\\ h \neq 0}} \frac{e(ht)-1}{2i\pi h}\mathrm{SC}_h,$$

and we deduce the third statement from this and Proposition 3.3, since $|\mathrm{K}_t(p)| \sim (p-1)t$. ☐

The second statement uses a different set T to obtain C_4-free graphs.

Theorem 5.3. *Let p be a prime number with $p \equiv 3 \pmod 4$. Set*

$$\mathrm{K}_+(p) = \{(x,y) \in \mathbf{F}_p \times \mathbf{F}_p \mid xy = 1 \text{ and } \Big(\frac{x}{p}\Big) = 1\},$$

where $(\frac{x}{p})$ is the Legendre symbol.

(1) *The graph* $\Gamma(\mathbf{F}_p\times\mathbf{F}_p,\mathrm{K}_+(p))$ *is a regular graph of degree* $(p-1)/2$*, and it is* C_4*-free.*
(2) *All the non-trivial eigenvalues* λ *of the adjacency matrix of* $\Gamma(\mathbf{F}_p\times\mathbf{F}_p,\mathrm{K}_+(p))$ *satisfy*

$$|\lambda|\leqslant 2p^{1/2}.$$

(3) *As* $p\to+\infty$ *among primes that are* $\equiv 3\,(\mathrm{mod}\,4)$*, the numbers*

$$\Big\{\frac{\lambda}{\sqrt{|\mathrm{K}_+(p)|}}\ \mid\ \lambda \textit{ an eigenvalue of } \Gamma(\mathbf{F}_p\times\mathbf{F}_p,\mathrm{K}_+(p))\Big\}$$

converge in distribution to the distribution of $\varepsilon|\mathrm{SC}+\mathrm{SA}|$*, where* $(\mathrm{SA},\mathrm{SC})$ *are independent random variables such that* SC *is semicircle-distributed and* SA *has distribution*

$$\mu_{\mathrm{sa}}=\frac{1}{2}\delta_0+\frac{1}{2}(x\longmapsto 2i\cos(4\pi x))_*dx,$$

with dx *the Lebesgue measure on* $[0,1]$*.*

Proof. To prove (1), we apply Lemma 5.1 to $\mathrm{G}=\mathbf{F}_p\times\mathbf{F}_p$, $\mathrm{S}=\mathrm{K}_+(p)$ and

$$\mathrm{T}=\{(x,y)\in\mathbf{F}_p\times\mathbf{F}_p\ \mid\ (\tfrac{x}{p})=1\}$$

(using the fact that -1 is not a square modulo p).

The characteristic function of $\mathrm{K}_+(p)$ inside $\mathbf{F}_p^\times$ is the function

$$x\longmapsto\frac{1}{2}\Big(1+\Big(\frac{x}{p}\Big)\Big),$$

and therefore the eigenvalues of the adjacency matrix are determined by the sums

$$\frac{1}{2}\sum_{x\in\mathbf{F}_p^\times}\psi_p(ax+bx^{-1})+\frac{1}{2}\sum_{x\in\mathbf{F}_p^\times}\Big(\frac{x}{p}\Big)\psi_p(ax+bx^{-1})=\frac{1}{2}\mathrm{K}(a,b;p)+\frac{1}{2}\mathrm{T}(a,b;p),$$

where the sums $\mathrm{T}(a,b;p)$ are *Salié sums*, and we write $\mathrm{K}(a,b;p)$ instead of $\mathrm{K}(a,b;\mathbf{F}_p)$ for convenience.

As already mentioned, the Kloosterman sums are $\leqslant 2\sqrt{p}$ in absolute value, and the work of Katz (which was already used to prove Theorem 1.1) shows that the (normalized) Kloosterman sums have semicircle limiting distribution.

The case of Salié sums is also known but proceeds somewhat differently, because the "monodromy group" for Salié sums modulo p (which governs the equidistribution properties for extensions of $\mathbf{F}_p$ by Deligne's equidistribution theorem) is a finite group which depends on p, in contrast with Kloosterman sums where it is $\mathbf{SU}_2(\mathbf{C})$ for all p.

We use instead that Salié sums can be evaluated elementarily. Precisely, the formulas

$$\begin{aligned}&\mathrm{T}(a,0;p)=\mathrm{T}(0,b;p)=-1 \text{ if } a,\ b\neq 0,\\ &\mathrm{T}(a,b;p)=\begin{cases}0 & \text{if } (\frac{ab}{p})=-1,\\ 2i\sqrt{p}(\frac{b}{p})\cos(4\pi y/p) & \text{if } ab=y^2\neq 0\end{cases}\end{aligned}\tag{5.1}$$

hold for $p\equiv 3\,(\mathrm{mod}\,4)$ (see, e.g., [25, Lemma 4.9]; the condition $p\equiv 3\,(\mathrm{mod}\,4)$ is used to evaluate the quadratic Gauss sum modulo p).

It follows[9] first that $|\mathrm{T}(a,b;p)| \leqslant 2\sqrt{p}$ for $(a,b) \neq (0,0)$, so that combined with the Weil bound, we conclude that the eigenvalues of the adjacency matrix have modulus $\leqslant 2\sqrt{p}$.

We next claim that the normalized Salié sums $\mathrm{T}(a,b;p)/\sqrt{p}$ become μ_{sa}-equidistributed as $p \to +\infty$ with $p \equiv 3 \pmod 4$. To see this, we write the "empirical measure" for the Salié sums $\mathrm{T}(a,b;p)$ with $(a,b) \neq (0,0)$ in the form

$$\frac{1}{p^2-1} \sum_{(a,b)\neq(0,0)} \delta_{\mathrm{T}(a,b;p)/\sqrt{p}} = \frac{1}{p^2-1} \sum_{ab=0} \delta_{\mathrm{T}(a,b;p)/\sqrt{p}} + \mu_{1,p}.$$

The first term converges weakly to the zero measure as $p \to +\infty$. On the other hand, according to (5.1), we get

$$\mu_{1,p} = \frac{1}{p^2-1}\Big(\sum_{\substack{a,b \\ (ab/p)=-1}} \delta_0 + \sum_{\substack{a,b \\ (ab/p)=1}} \delta_{2i(b/p)\cos(4\pi y/p)} \Big),$$

where y denotes a square root of ab in $\mathbf{F}_p^\times$. The first term in this sum converges to $\frac{1}{2}\delta_0$, since there are $(p-1)^2/2$ values of (a,b) with $(\frac{ab}{p}) = -1$. We express the second as

$$\frac{1}{2(p^2-1)} \sum_{y\in\mathbf{F}_p^\times} \sum_{b\in\mathbf{F}_p^\times} \delta_{2i(b/p)\cos(4\pi y/p)}.$$

Let $f(x) = 2i\cos(4\pi x)$ for $x \in [0,1]$. Since y and b are independent variables, and since the y/p (resp. the Legendre symbols (b/p)) become uniformly distributed on $[0,1]$ (resp. become uniformly distributed on $\{-1,1\}$), the previous expression converges to the measure

$$\frac{1}{2}\Big(\frac{1}{2}f_*dx + \frac{1}{2}(-f)_*dx\Big)$$

as $p \to +\infty$, where dx denotes the Lebesgue measure on $[0,1]$. But the measures f_*dx and $(-f)_*dx$ are equal, and therefore the limit is $\frac{1}{2}f_*dx$. This confirms that the measure μ_{sa} is the limiting measure for Salié sums.

It remains to prove that the sets of pairs

$$\Big(\frac{\mathrm{K}(a,b;p)}{\sqrt{p}}, \frac{\mathrm{T}(a,b;p)}{\sqrt{p}}\Big)$$

of normalized Kloosterman sums and Salié sums converge to a pair of *independent* random variables. This is a problem of a relatively familiar kind, but this case does not seem to have been recorded in the literature.

We restrict our attention to $(a,b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times$, as we may for the same reasons as before. By the method of moments (applicable because all measures here are compactly supported), it then suffices to prove that for all integers $\alpha \geqslant 0$ and $\beta \geqslant 0$, we have the limit

$$\lim_{\substack{p\to+\infty \\ p\equiv 3 \,(\mathrm{mod}\, 4)}} \frac{1}{(p-1)^2} \sum_{a,b\in\mathbf{F}_p^\times} \mathrm{U}_\alpha\Big(\frac{\mathrm{K}(a,b;p)}{\sqrt{p}}\Big)\Big(\frac{\mathrm{T}(a,b;p)}{\sqrt{p}}\Big)^\beta = \mathbf{E}(\mathrm{U}_\alpha(\mathrm{SC}))\mathbf{E}(\mathrm{SA}^\beta), \tag{5.2}$$

[9] This can also be deduced from the general Weil bound.

where U_α is the Chebychev polynomial corresponding to the character of the symmetric α-th power representation of $\mathbf{SU}_2(\mathbf{C})$, so that

$$\mathbf{E}(\mathrm{U}_\alpha(\mathrm{SC})) = \begin{cases} 1 & \text{if } \alpha = 0, \\ 0 & \text{otherwise.} \end{cases}$$

The distribution results of Kloosterman and Salié sums individually show that the formula holds if either $\alpha = 0$ or $\beta = 0$. Thus, we may assume that both α and β are non-zero, and in particular, the limit of the quantity in (5.2) should be 0.

By (5.1), we obtain the expression

$$\sum_{a,b\in\mathbf{F}_p^\times} \mathrm{U}_\alpha\Big(\frac{\mathrm{K}(a,b;p)}{\sqrt{p}}\Big)\Big(\frac{\mathrm{T}(a,b;p)}{\sqrt{p}}\Big)^\beta = (2i)^\beta \sum_{(ab/p)=1} \mathrm{U}_\alpha\Big(\frac{\mathrm{K}(a,b;p)}{\sqrt{p}}\Big)\Big(\frac{b}{p}\Big)^\beta \cos\Big(\frac{4\pi y}{p}\Big)^\beta,$$

where again y denotes one square root of ab modulo p. Using the formula $\mathrm{K}(a,b;p) = \mathrm{K}(ab,1;p)$ and putting $x = ab$, this (up to the factor $(2i)^\beta$) becomes

$$\sum_{(x/p)=1} \mathrm{U}_\alpha\Big(\frac{\mathrm{K}(x,1;p)}{\sqrt{p}}\Big)\cos\Big(\frac{4\pi y}{p}\Big)^\beta \sum_{ab=x}\Big(\frac{b}{p}\Big)^\beta,$$

where y is now a square root of x modulo p. The inner sum vanishes if β is odd, so that the limiting formula certainly holds in this case. We thus assume that β is even, in which case the inner sum is always equal to $p-1$, so that the average in (5.2) is given by

$$\begin{aligned}\frac{1}{(p-1)^2}\sum_{a,b\in\mathbf{F}_p^\times} \mathrm{U}_\alpha\Big(\frac{\mathrm{K}(a,b;p)}{\sqrt{p}}\Big)\Big(\frac{\mathrm{T}(a,b;p)}{\sqrt{p}}\Big)^\beta &= \frac{1}{p-1}\sum_{(x/p)=1} \mathrm{U}_\alpha\Big(\frac{\mathrm{K}(x,1;p)}{\sqrt{p}}\Big)\cos\Big(\frac{4\pi y}{p}\Big)^\beta \\ &= \frac{1}{2(p-1)}\sum_{y\in\mathbf{F}_p^\times} \mathrm{U}_\alpha\Big(\frac{\mathrm{K}(y^2,1;p)}{\sqrt{p}}\Big)\cos\Big(\frac{4\pi y}{p}\Big)^\beta\end{aligned}$$

(where y is a square-root of x in the middle step).

The last transformation is to expand the cosine in complex exponentials, namely

$$\sum_{y\in\mathbf{F}_p^\times} \mathrm{U}_\alpha\Big(\frac{\mathrm{K}(y^2,1;p)}{\sqrt{p}}\Big)\cos\Big(\frac{4\pi y}{p}\Big)^\beta = \frac{1}{2^\beta}\sum_{0\leqslant j\leqslant\beta}\binom{\beta}{j}\sum_{y\in\mathbf{F}_p^\times} \mathrm{U}_\alpha\Big(\frac{\mathrm{K}(y^2,1;p)}{\sqrt{p}}\Big)e\Big(\frac{2(2j-\beta)y}{p}\Big).$$

We are now in a position to simply apply the (by now) fairly standard Lemma 5.4 below to conclude the proof. ☐

Lemma 5.4. *For $\alpha \neq 0$ and for all integers γ, the estimate*

$$\sum_{y\in\mathbf{F}_p^\times} \mathrm{U}_\alpha\Big(\frac{\mathrm{K}(y^2,1;p)}{\sqrt{p}}\Big)e\Big(\frac{\gamma y}{p}\Big) = \mathrm{O}(p^{1/2})$$

holds for all primes p, where the implied constant depends only on α.

Proof. This is a simple special case of the "quasi-orthogonality" interpretation of Deligne's general form of the Riemann Hypothesis over finite fields. For instance, we can use the statement in [21, Lemma 3.5 (2)] with the following data:

– the field k is $\mathbf{F}_p$, the curve X is the multiplicative group and $\mathrm{U} = \mathrm{X}$;

– the sheaf $\mathscr{F}_1$ is the α-th symmetric power of the pullback by $y \mapsto y^2$ of the Kloosterman sheaf of rank 2, so that its trace function is given by

$$t_{\mathscr{F}_1,\mathbf{F}_p}(y) = \mathrm{U}_\alpha\Big(\frac{\mathrm{K}(y^2,1;p)}{\sqrt{p}}\Big)$$

for all $y \in \mathrm{U}(\mathbf{F}_p) = \mathbf{F}_p^\times$;

– the sheaf $\mathscr{F}_2$ is the restriction to U of the Artin–Schreier sheaf $\mathscr{L}_{\psi_p(-\gamma y)}$, with

$$\overline{t_{\mathscr{F}_2,\mathbf{F}_p}(y)} = e\Big(\frac{\gamma y}{p}\Big) \quad \text{for} \quad y \in \mathbf{F}_p^\times.$$

– the constant c is an upper-bound for the conductors of $\mathscr{F}_1$ and $\mathscr{F}_2$, which can be taken to be a suitable constant depending only on α (and not on p) by formal properties of the conductor (although this can be done more elementarily in this case, it is maybe most convenient here to apply [48, Prop. 6.33] and [48, Prop. 7.5], respectively, taking into account [48, Cor. 7.4] to compare the notions of conductors from [21] and [48]).

Katz's study of the Kloosterman sheaf (cf. [28, Th. 4.1.1]) implies that $\mathscr{F}_1$ is lisse, geometrically irreducible of rank $\alpha+1$ and pure of weight 0; the sheaf $\mathscr{F}_2$ is lisse, geometrically irreducible of rank 1 and pure of weight 0 (for essentially tautological reasons). Since $\alpha+1 \geqslant 2$, the two sheaves cannot be geometrically isomorphic, hence by loc. cit., we obtain the result (the key point being that the bound c for the conductors is independent of p). ☐

References

[1] M. Ajtai, J. Komlós, and E. Szemerédi, *A note on Ramsey numbers*, J. Combin. Theory Ser. A **29** (1980), no. 3, 354–360.

[2] N. Alon and F. R. K. Chung, *Explicit construction of linear sized tolerant networks*, Discrete Math. **72** (1988), no. 1–3, 15–19.

[3] N. Alon, M. Krivelevich, and B. Sudakov, *Finding a large hidden clique in a random graph*, Random Structures Algorithms **13** (1998), no. 3–4, 457–466.

[4] K. Bangachev and G. Bresler, *Graph quasirandomness for hypothesis testing of stochastic block models*, 2025. Preprint https://arxiv.org/abs/2504.17202.

[5] P. Biane, *Permutation model for semi-circular systems and quantum random walks*, Pacific J. Math. **171** (1995), no. 2, 373–387.

[6] T. Bohman and P. Keevash, *The early evolution of the* H*-free process*, Invent. math. **181** (2010), no. 2, 291–336.

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

[8] Y. Caro, Y. Li, C. C. Rousseau, and Y. Zhang, *Asymptotic bounds for some bipartite graph: complete graph Ramsey numbers*, Discrete Math. 220 (2000), no. 1-3, **220** (2000), no. 1–3, 51–56.

[9] G. Chapuy and V. Féray, *A note on a Cayley graph of* S_n, 2012. Preprint https://arxiv.org/abs/1202.4976.

[10] F. Chung, L. Lu, and V. Vu, *Spectra of random graphs with given expected degrees*, Proc. Natl. Acad. Sci. USA **100** (2003), no. 11, 6313–6318.

[11] F. R. K. Chung, R. L. Graham, and R. M. Wilson, *Quasi-random graphs*, Combinatorica **9** (1989), no. 4, 345–362.

[12] D. Conlon, J. Fox, and B. Sudakov, *Recent developments in graph Ramsey theory*, Surveys in combinatorics 2015, 2015, pp. 49–118.

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

[14] I. Dumitriu and S. Pal, *Sparse regular random graphs: spectral density and eigenvectors*, Ann. Probab. **40** (2012), no. 5, 2197–2235.

[15] 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.

[16] C. Elphick, Q. Tang, and S. Zhang, *A spectral lower bound on chromatic numbers using p-energy*, 2025. Preprint https://arxiv.org/abs/2504.01295.

[17] P. Erdős, *On the combinatorial problems which i would most like to see solved*, Combinatorica **1** (1981), no. 1, 25–42.

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

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

[20] A. Forey, J. Fresán, E. Kowalski, and Y. Wigderson, *Jacobian graphs*, 2025. In preparation.

[21] E. Fouvry, E. Kowalski, and P. Michel, *Counting sheaves using spherical codes*, Math. Res. Lett. **20** (2013), no. 2, 305–323.

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

[23] S. Goldwasser and S. Micali, *Probabilistic encryption*, J. Comput. System Sci. **28** (1984), no. 2, 270–299.

[24] W. H. Haemers, *Hoffman's ratio bound*, Linear Algebra Appl. **617** (2021), 215–219.

[25] H. Iwaniec, *Topics in classical automorphic forms*, Graduate Studies in Mathematics, vol. 17, American Mathematical Society, Providence, RI, 1997.

[26] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004.

[27] N. M. Katz, *On the monodromy groups attached to certain families of exponential sums*, Duke Math. J. **54** (1987), no. 1, 41–56.

[28] ———, *Gauss sums, Kloosterman sums, and monodromy groups*, Annals of Mathematics Studies, 116., vol. 116, Princeton University Press, Princeton, NJ, 1988.

[29] ———, L*-functions and monodromy: four lectures on Weil II*, Adv. Math. **160** (2001), no. 1, 81–132.

[30] ———, *Larsen's alternative, moments, and the monodromy of Lefschetz pencils*, Contributions to automorphic forms, geometry, and number theory, 2004, pp. 521–560.

[31] ———, *Moments, monodromy, and perversity: a Diophantine perspective*, Annals of Mathematics Studies, vol. 159, Princeton University Press, Princeton, NJ, 2005.

[32] ———, *Rigid local systems on $\mathbf{A}^1$ with finite monodromy*, Mathematika **64** (2018), no. 3, 785–846. With an appendix by Pham Huu Tiep.

[33] H. D. Kloosterman, *On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$*, Acta Math. **49** (1927), no. 3–4, 407–464.

[34] T. Kövari, V. T. Sós, and P. Turán, *On a problem of K. Zarankiewicz*, Colloq. Math. **3** (1954), 50–57.

[35] E. Kowalski and W. F. Sawin, *Kloosterman paths and the shape of exponential sums*, Compos. Math. **152** (2016), no. 7, 1489–1516.

[36] E. Kowalski and T. Untrau, *Wasserstein metrics and quantitative equidistribution of exponential sums over finite fields*, 2025. Preprint https://arxiv.org/abs/2505.22059.

[37] M. Krivelevich and B. Sudakov, *Pseudo-random graphs*, More sets, graphs and numbers, 2006, pp. 199–262.

[38] D. Kunisky, A. S. Wein, and A. S. Bandeira, *Notes on computational hardness of hypothesis testing: predictions using the low-degree likelihood ratio*, Mathematical analysis, its applications and computation, 2022, pp. 1–50.

[39] G. J. Leuschke and R. Wiegand, *Cohen-Macaulay representations*, Mathematical Surveys and Monographs, vol. 181, American Mathematical Society, Providence, RI, 2012.

[40] A. Lubotzky, R. Phillips, and P. Sarnak, *Ramanujan graphs*, Combinatorica **8** (1988), no. 3, 261–277.

[41] B. D. McKay, *The expected eigenvalue distribution of a large regular graph*, Linear Algebra Appl. **40** (1981), 203–216.

[42] Iwao. Mizuno Hirobumi; Sato, *The semicircle law for semiregular bipartite graphs*, J. Combin. Theory Ser. A **101** (2003), no. 2, 174–190.

[43] D. Mubayi and J. Verstraëte, *A note on pseudorandom Ramsey graphs*, J. Eur. Math. Soc. (JEMS) **26** (2024), no. 1, 153–161.

[44] 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.
[45] M. W. Newman, *Independent sets and eigenspaces*, Ph.D. Thesis, 2005.
[46] I. Z. Ruzsa, *Additive and multiplicative Sidon sets*, Acta Math. Hungar. **112** (2006), no. 4, 345–354.
[47] A. Sah, M. Sawhney, J. Tidor, and Y. Zhao, *A counterexample to the Bollobás–Riordan conjectures on sparse graph limits*, Combin. Probab. Comput. **30** (2021), no. 5, 796–799.
[48] W. Sawin, A. Forey, J. Fresán, and E. Kowalski, *Quantitative sheaf theory*, J. Amer. Math. Soc. **36** (2023), no. 3, 653–726.
[49] J-P. Serre, *Répartition asymptotique des valeurs propres de l'opérateur de Hecke* T_p, J. Amer. Math. Soc. **10** (1997), no. 1, 75–102.
[50] I. E. Shparlinski, *Modular hyperbolas*, Jpn. J. Math. **7** (2012), no. 2, 235–294.
[51] I. Soloveychik, Y. Xiang, and V. Tarokh, *Symmetric pseudo-random matrices*, IEEE Trans. Inform. Theory **64** (2018), no. 4, part 2, 3179–3196.
[52] T. Sunada, *The discrete and the continuous (in japanese)*, Sugaku Seminar **40** (2001), no. 10, 48–51.
[53] A. V. Sutherland, *Sato-Tate distributions*, Analytic methods in arithmetic geometry, 2019, pp. 197–248.
[54] T. Tao and V. Vu, *Random matrices: the universality phenomenon for Wigner ensembles*, Modern aspects of random matrix theory, 2014, pp. 121–172.
[55] A. Thomason, *Pseudo-random graphs*, Proceedings of Random Graphs, Poznań 1985, 1987, pp. 307–331.
[56] L. V. Tran, V. H. Vu, and K. Wang, *Sparse random graphs: eigenvalues and eigenvectors*, Random Structures Algorithms **42** (2013), no. 1, 110–134.
[57] A. Wigderson, *Mathematics and computation. A theory revolutionizing technology and science*, Princeton University Press, Princeton, NJ, 2019.
[58] Y. Wigderson, *Ramsey theory—lecture notes*, 2024. Available at https://ywigderson.math.ethz.ch/math/static/RamseyTheory2024LectureNotes.pdf.
[59] E. P. Wigner, *Characteristic vectors of bordered matrices with infinite dimensions*, Ann. of Math. **62** (1955), 548–564.

(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`