Forum of Mathematics, Sigma (2022), **Vol. 10**:e46 1–46
doi:10.1017/fms.2022.40

CAMBRIDGE
UNIVERSITY PRESS

RESEARCH ARTICLE

The 8-rank of the narrow class group and the negative Pell equation

Stephanie Chan[1], Peter Koymans[2], Djordjo Milovic[3] and Carlo Pagano[4]

[1]University of Michigan, 530 Church Street, Ann Arbor, MI 48109, United States of America; E-mail: ytchan@umich.edu.
[2]University of Michigan, 530 Church Street, Ann Arbor, MI 48109, United States of America; E-mail: koymans@umich.edu.
[3]University College London, 25 Gordon Street, London, WC1E 6BT, United Kingdom.
[4]University of Glasgow, University Place, Glasgow, G12 8SQ, United Kingdom; E-mail: carlein90@gmail.com.

Received: 11 July 2021; **Revised:** 27 April 2022; **Accepted:** 17 May 2022

Keywords: Class groups, negative Pell

2020 Mathematics subject classification: *Primary* – 11N45, 11R29, 11R45, 11R65; *Secondary* – 11R11, 11R37

Abstract

Using a recent breakthrough of Smith [18], we improve the results of Fouvry and Klüners [4, 5] on the solubility of the negative Pell equation. Let $\mathcal{D}$ denote the set of positive squarefree integers having no prime factors congruent to 3 modulo 4. Stevenhagen [19] conjectured that the density of d in $\mathcal{D}$ such that the negative Pell equation $x^2 - dy^2 = -1$ is solvable with $x, y \in \mathbb{Z}$ is 58.1%, to the nearest tenth of a percent. By studying the distribution of the 8-rank of narrow class groups $\mathrm{Cl}^+(d)$ of $\mathbb{Q}(\sqrt{d})$, we prove that the infimum of this density is at least 53.8%.

Contents

1. Introduction

In recent years, much progress has been made in the study of the distribution of 2-parts of class groups of quadratic number fields, most notably by Fouvry and Klüners [4, 5] and Smith [18]. One way to test the robustness of new methods in this subject is to study their applications to a conjecture of Stevenhagen [19] concerning the solvability over $\mathbb{Z}$ of the negative Pell equation

$$x^2 - dy^2 = -1. \tag{1.1}$$

Here and henceforth, we take d to be a positive squarefree integer. Equation (1.1) is solvable over $\mathbb{Z}$ if and only if the ordinary and narrow class groups of the quadratic field $\mathbb{Q}(\sqrt{d})$, denoted by $\mathrm{Cl}(d)$ and $\mathrm{Cl}^+(d)$, respectively, coincide. As the odd parts of $\mathrm{Cl}(d)$ and $\mathrm{Cl}^+(d)$ are isomorphic, the frequency of solvability of equation (1.1) is intimately related to the joint distribution of the 2-primary parts of $\mathrm{Cl}(d)$ and $\mathrm{Cl}^+(d)$. We note that $\mathrm{Cl}(d)/2\,\mathrm{Cl}(d) \cong \mathrm{Cl}^+(d)/2\,\mathrm{Cl}^+(d)$ if and only if d is in the set

$$\mathcal{D} = \{d \text{ positive squarefree integer} : p \mid d \implies p \not\equiv 3 \bmod 4\},$$

which we occasionally refer to as the *Pell family*. As $\mathcal{D}$ has natural density 0 in the set of all squarefree integers, it is more meaningful to study density questions concerning the solvability of equation (1.1) relative to $\mathcal{D}$ than relative to the set of all squarefree integers.

One of the main conjectures in [19] is that

$$\lim_{X\to\infty} \frac{|\mathcal{D}^-(X)|}{|\mathcal{D}(X)|} = 1 - \alpha = 0.58057\ldots,$$

where

$$\mathcal{D}(X) = \{d \in \mathcal{D} : d \leq X\},$$

$$\mathcal{D}^-(X) = \{d \in \mathcal{D}(X) : (1.1) \text{ is solvable over } \mathbb{Z}\},$$

and

$$\alpha = \prod_{j \text{ odd}} (1 - 2^{-j}) = \prod_{j=1}^{\infty} (1 + 2^{-j})^{-1} = 0.41942\ldots.$$

We remark that the constant α already appears in the work of Cremona–Odoni [3], namely as the constant λ_∞. These authors studied the negative Pell equation when the number of prime divisors is fixed, which is traditionally viewed as a simpler problem.

Until now, the best bounds in the direction of Stevenhagen's conjecture are due to Fouvry and Klüners [6, 7], who used the methods they developed in [5] to prove that

$$\frac{5}{4}\alpha \leq \liminf_{X\to\infty} \frac{|\mathcal{D}^-(X)|}{|\mathcal{D}(X)|} \leq \limsup_{X\to\infty} \frac{|\mathcal{D}^-(X)|}{|\mathcal{D}(X)|} \leq \frac{2}{3}. \tag{1.2}$$

By incorporating the methods developed by Smith [18], we can improve the lower bound.

Theorem 1.1. *With $\mathcal{D}(X)$, $\mathcal{D}^-(X)$ and α defined as above, we have*

$$\liminf_{X\to\infty} \frac{|\mathcal{D}^-(X)|}{|\mathcal{D}(X)|} \geq \alpha\beta,$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

where

$$\beta = \sum_{n=0}^{\infty} 2^{-n(n+3)/2} = 1.28326\dots.$$

We note that $\beta > 5/4$. To the nearest tenth of a percent, Stevenhagen's conjecture states that the density of $d \in \mathcal{D}$ for which (1.1) is solvable over $\mathbb{Z}$ is 58.1%. Fouvry and Klüners proved that the lower density is at least 52.4%, and we prove that the lower density is at least 53.8%.

For a finite abelian group G and an integer $k \geq 1$, we let $\operatorname{rk}_{2^k} G = \dim_{\mathbb{F}_2}(2^{k-1}G/2^kG)$; this is called the 2^k-rank of G. The nonincreasing sequence of nonnegative integers $\{\operatorname{rk}_{2^k} G\}_k$ determines the isomorphism class of the 2-primary part of G. Hence

$$(1.1) \text{ is solvable} \iff \operatorname{rk}_{2^k} \operatorname{Cl}(d) = \operatorname{rk}_{2^k} \operatorname{Cl}^+(d) \text{ for all integers } k \geq 1.$$

The lower bound in (1.2) comes from proving that the density of $d \in \mathcal{D}$ such that

$$\operatorname{rk}_4 \operatorname{Cl}^+(d) = 0$$

is equal to α and the density of $d \in \mathcal{D}$ such that

$$\operatorname{rk}_4 \operatorname{Cl}(d) = \operatorname{rk}_4 \operatorname{Cl}^+(d) = 1 \text{ and } \operatorname{rk}_8 \operatorname{Cl}^+(d) = 0$$

is equal to $\alpha/4$. We obtain our lower bound by proving that the density of $d \in \mathcal{D}$ such that

$$\operatorname{rk}_4 \operatorname{Cl}(d) = \operatorname{rk}_4 \operatorname{Cl}^+(d) = n \text{ and } \operatorname{rk}_8 \operatorname{Cl}^+(d) = 0$$

is equal to $2^{-n(n+3)/2}\alpha$. In fact, we will prove more. Define $P(r|n)$ to be the probability that a uniformly chosen r by r symmetric matrix with coefficients in $\mathbb{F}_2$ has rank $r - n$ and define $Q(n|m)$ to be the probability that a uniformly chosen $(n+1)\times n$ matrix with coefficients in $\mathbb{F}_2$ has a bottom row consisting of all zeroes and rank $n - m$.

Theorem 1.2. *Let $\mathcal{D}(X)$ and α be as above, and, for integers $n \geq m \geq 0$, let*

$$\mathcal{D}_{n,m}(X) = \{d \in \mathcal{D}(X) : \operatorname{rk}_4 \operatorname{Cl}(d) = \operatorname{rk}_4 \operatorname{Cl}^+(d) = n \text{ and } \operatorname{rk}_8 \operatorname{Cl}^+(d) = m\}.$$

Then

$$\lim_{X\to\infty} \frac{|\mathcal{D}_{n,m}(X)|}{|\mathcal{D}(X)|} = Q(n|m) \cdot \lim_{r\to\infty} P(r|n) = \alpha \cdot 2^{-n(n+1)} \frac{\prod_{j=m+1}^{n}(2^n - 2^{n-j})}{\prod_{k=1}^{m}(2^k - 1)\prod_{l=1}^{n-m}(2^l - 1)}.$$

It is the first equality that we shall prove in Section 6. The second equality is a straightforward computation but has the nice feature that it makes immediately visible how Theorem 1.2 implies Theorem 1.1. We note that our proof of Theorem 1.2 gives an alternative proof of [5, Theorem 2] and [7, Theorem 2].

The major novel difficulty with working in the Pell family is that the integers $d \in \mathcal{D}$ have the remarkable property that the sets

$$\{a \mid d : a > 0,\ a \text{ squarefree}, (a, -d/a) = 1\}$$

and

$$\{b \mid d : b > 0,\ b \text{ squarefree}, (b, d/b) = 1\}$$

coincide, where $(\cdot,\cdot)$ denotes the Hilbert symbol. However, for Smith's method to work, it is essential that these spaces typically intersect trivially. For instance, this is used in [18, p.76] to argue that most

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

assignments a are generic. This is not the case for the Pell family, and all the integers $d \in \mathcal{D}$ end up in the error term in Smith's proof. It is therefore of utmost importance to extend Smith's algebraic results.

We introduce a different notion of genericity in equations (6.1) and (6.2) to circumvent this. This necessitates new algebraic results, which can be found in Section 2. These algebraic results essentially rely on the fact that we are working with the 8-rank, which brings manipulations with Rédei symbols into play; see [20] for an extensive treatment of Rédei symbols. Note that this approach is inspired by Smith's first paper [17]. However, the result in [17] assumes GRH, which we avoid by borrowing from the ideas that Smith introduced in his breakthrough paper [18].

In Section 4, we give more direct proofs of the results that appear in [18, Section 5] and concern the typical distribution of prime divisors of a squarefree integer. Of course, we once again adapt these results to d coming from the Pell family $\mathcal{D}$.

2. Algebraic results

We start this section by introducing the Rédei symbol, which will play a prominent role throughout the paper. Then we prove several identities on the sum of four Rédei symbols, which serve as the algebraic input for our analytic machinery.

2.1. Rédei symbols

We shall review the fundamental properties of Rédei symbols. Our main reference is Stevenhagen's recent work [20]. Fix a separable closure $\mathbb{Q}^{\text{sep}}$ of $\mathbb{Q}$. All our number fields are implicitly taken inside this fixed separable closure. If K is a number field, we write $G_K := \text{Gal}(\mathbb{Q}^{\text{sep}}/K)$ for its absolute Galois group.

Definition 2.1. Write Ω for the collection of the places of $\mathbb{Q}$. For a place v in Ω, we write $(-,-)_v$ for the Hilbert symbol. If $K/\mathbb{Q}$ is a finite extension, write Δ_K for the discriminant of $K/\mathbb{Q}$.

Definition 2.2. Let $a, b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$. If a is nontrivial, write χ_a for the unique character $\chi_a : G_{\mathbb{Q}} \to \mathbb{F}_2$ with kernel $G_{\mathbb{Q}(\sqrt{a})}$. We say that (a, b) is acceptable if we have that $(a, b)_v = 1$ for each $v \in \Omega$.

In case one of a, b is trivial, then (a, b) is clearly acceptable. Now suppose a and b are both nontrivial. Then (a, b) is acceptable if and only if there exists a Galois extension $L/\mathbb{Q}$ containing $\mathbb{Q}(\sqrt{a}, \sqrt{b})$, with $\text{Gal}(L/\mathbb{Q}(\sqrt{ab}))$ cyclic of order 4, and such that every element $\sigma \in \text{Gal}(L/\mathbb{Q})$ with $\chi_a(\sigma) \neq \chi_b(\sigma)$ must be an involution: that is, $\sigma^2 = \text{id}$.

If $a = b$, we are simply requiring $L/\mathbb{Q}$ to be a cyclic extension of degree 4 of $\mathbb{Q}$ containing $\mathbb{Q}(\sqrt{a})$. If $a \neq b$, we are requiring $L/\mathbb{Q}$ to be dihedral of degree 8 with $\text{Gal}(L/\mathbb{Q}(\sqrt{ab}))$ cyclic of order 4. When a, b are both nontrivial and (a, b) is acceptable, denote by $\mathcal{F}_{a,b}$ the collection of fields $L/\mathbb{Q}$ described above.

Write $\Gamma_{\mathbb{F}_2}(\mathbb{Q}) := \text{Hom}_{\text{top.gr.}}(G_{\mathbb{Q}}, \mathbb{F}_2)$. For $\chi \in \Gamma_{\mathbb{F}_2}(\mathbb{Q})$, write $\mathbb{Q}(\chi) := (\mathbb{Q}^{\text{sep}})^{\ker(\chi)}$. We put $\Gamma_{\mathbb{F}_2}(\mathbb{Q}, \{a, b\}) := \frac{\Gamma_{\mathbb{F}_2}(\mathbb{Q})}{\langle\{\chi_a, \chi_b\}\rangle}$. Note that the set $\mathcal{F}_{a,b}$ is equipped with a *difference*, which is a map $- : \mathcal{F}_{a,b} \times \mathcal{F}_{a,b} \to \Gamma_{\mathbb{F}_2}(\mathbb{Q}, \{a, b\})$ such that for all $L_1, L_2, L_3 \in \mathcal{F}_{a,b}$,

$$(L_3 - L_2) + (L_2 - L_1) = L_3 - L_1$$

and $L_2 - L_1 = 0$ if and only if $L_1 = L_2$. Indeed, for $L_1, L_2 \in \mathcal{F}_{a,b}$, we define $L_2 - L_1$ to be the unique $\chi \in \Gamma_{\mathbb{F}_2}(\mathbb{Q}, \{a, b\})$ such that $\mathbb{Q}(\chi) \cdot L_2 \supseteq L_1$.

Therefore each $L \in \mathcal{F}_{a,b}$ induces an explicit bijection between $\mathcal{F}_{a,b}$ and $\Gamma_{\mathbb{F}_2}(\mathbb{Q}, \{a, b\})$. For any subgroup $H \leq \Gamma_{\mathbb{F}_2}(\mathbb{Q}, \{a, b\})$, we say that $S \subseteq \mathcal{F}_{a,b}$ is a H-coset if there exists some $s_0 \in S$ such that $S = \{s \in \mathcal{F}_{a,b} : s - s_0 \in H\}$.

Now let (a, b) be an acceptable pair such that a and b are not divisible by any prime congruent to 3 modulo 4. Write $a = t_a \prod_{l|a} l$ and $b = t_b \prod_{l'|b} l'$, where the products run over all odd primes

$l \mid a$ and $l' \mid b$. Define $\Gamma^{\mathrm{unr}}_{\mathbb{F}_2}(\mathbb{Q}, \{a, b\})$ to be the subgroup of $\Gamma_{\mathbb{F}_2}(\mathbb{Q}, \{a, b\})$ generated by the set $\{\chi_p : p \mid a\} \cup \{\chi_p : p \mid b\} \cup \{\chi_{t_a}, \chi_{t_b}\}$. One calls an element $L \in \mathcal{F}_{a,b}$ *minimally ramified* (see [20, Definition 7.4]) if

- $L/\mathbb{Q}(\sqrt{a}, \sqrt{b})$ does not ramify above any odd, finite place $v \nmid \gcd(\Delta_{\mathbb{Q}(\sqrt{a})}, \Delta_{\mathbb{Q}(\sqrt{b})})$;
- $L/\mathbb{Q}(\sqrt{a}, \sqrt{b})$ is unramified at 2 if $\Delta_{\mathbb{Q}(\sqrt{a})}\Delta_{\mathbb{Q}(\sqrt{b})}$ is odd or if one of the discriminants is 1 modulo 8;
- if $\{\Delta_{\mathbb{Q}(\sqrt{a})}, \Delta_{\mathbb{Q}(\sqrt{b})}\}$ is the set $\{4, 5\}$ modulo 8, then we ask that $L/\mathbb{Q}(\sqrt{ab})$ is 2-minimally ramified; see [20, Definition 7.3].

We denote by $\mathcal{F}^{\mathrm{unr}}_{a,b}$ the subset of $\mathcal{F}_{a,b}$ consisting of minimally ramified elements. As it is shown in [20, Lemma 7.5], the set $\mathcal{F}^{\mathrm{unr}}_{a,b}$ is a $\Gamma^{\mathrm{unr}}(\mathbb{Q}, \{a, b\})$-coset (which in particular implies that it is nonempty).

Definition 2.3. Let (a, b, c) be a triple with $a, b, c \in (\mathbb{Q}^*)/(\mathbb{Q}^*)^2$. We say that (a, b, c) is jointly unramified if

$$\gcd(\Delta_{\mathbb{Q}(\sqrt{a})}, \Delta_{\mathbb{Q}(\sqrt{b})}, \Delta_{\mathbb{Q}(\sqrt{c})}) = 1.$$

We say that (a, b, c) is admissible if all $(a, b), (a, c), (b, c)$ are acceptable pairs; a, b and c are not divisible by any prime congruent to 3 modulo 4; and (a, b, c) is jointly unramified.

Observe that if a triple is admissible, then so is any permutation of it.

Definition 2.4. For any admissible triple (a, b, c), define the Rédei symbol $[a, b, c] \in \mathbb{F}_2$ as follows.[1] If any of a, b, c is trivial, set $[a, b, c] := 0$. Assuming a, b, c are all nontrivial, choose $L \in \mathcal{F}^{\mathrm{unr}}_{a,b}$ and $\mathfrak{c}$ an integral ideal of norm $|c|$ in the ring of integers of $\mathbb{Q}(\sqrt{ab})$; existence of $\mathfrak{c}$ follows from admissibility of (a, b, c). Define

$$[a, b, c] := \begin{cases} \left[\frac{L/\mathbb{Q}(\sqrt{ab})}{\mathfrak{c}}\right] & \text{if } c > 0 \\ \left[\frac{L/\mathbb{Q}(\sqrt{ab})}{\mathfrak{c}\tilde{\infty}}\right] & \text{if } c < 0, \end{cases}$$

where $\tilde{\infty}$ is any choice of infinite prime in $\mathbb{Q}(\sqrt{ab})$. We identify the Artin symbol with its image under the isomorphism $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{a}, \sqrt{b})) \cong \mathbb{F}_2$.

A priori, the resulting symbol would depend on the choices of L and $\mathfrak{c}$, so the notation should reflect this dependency. However, the following theorem shows in particular that the symbol does not depend on any of the choices. For a proof, see [20, Theorem 7.7].

Theorem 2.5 (Rédei reciprocity). *Let (a, b, c) be an admissible triple. Then $[a, b, c]$ does not depend on the choice of L and $\mathfrak{c}$. Furthermore,*

$$[a, b, c] = [a, c, b]. \tag{2.1}$$

As a consequence of Rédei reciprocity, the following proposition shows that the Rédei symbol is linear in every entry.

Proposition 2.6. *Let (a, b, c), (a, b', c) be two admissible triples. Then (a, bb', c) is also an admissible triple, and furthermore,*

$$[a, b, c] + [a, b', c] = [a, bb', c].$$

Since admissibility and the Rédei symbol do not depend on the order of a, b, c in the triple, the corresponding statements hold for all three entries.

[1] We use, in contrast to [20], the convention that Rédei symbols take their values in $\mathbb{F}_2$, since this shall be notationally more convenient in the rest of the paper.

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

Proof. It follows from $(a,b)_v = (a,b')_v = 1$ for all $v \in \Omega$ and the bilinearity of Hilbert symbols that $(a,bb')_v = 1$ for all $v \in \Omega$. Therefore (a,bb') is acceptable, and similarly (bb',c). Since (a,b,c) or (a,b',c) are jointly ramified, we have

$$\gcd(\Delta_{\mathbb{Q}(\sqrt{a})}, \Delta_{\mathbb{Q}(\sqrt{b})}\Delta_{\mathbb{Q}(\sqrt{b'})}, \Delta_{\mathbb{Q}(\sqrt{c})}) = \\ \gcd(\Delta_{\mathbb{Q}(\sqrt{a})}, \Delta_{\mathbb{Q}(\sqrt{b})}, \Delta_{\mathbb{Q}(\sqrt{c})}) \gcd(\Delta_{\mathbb{Q}(\sqrt{a})}, \Delta_{\mathbb{Q}(\sqrt{b'})}, \Delta_{\mathbb{Q}(\sqrt{c})}) = 1.$$

Observe that $\Delta_{\mathbb{Q}(\sqrt{bb'})} \mid \Delta_{\mathbb{Q}(\sqrt{b})}\Delta_{\mathbb{Q}(\sqrt{b'})}$. Hence (a,bb',c) is jointly unramified. It follows that (a,bb',c) is an admissible triple.

Now the desired identity follows from Theorem 2.5 and the linearity of the last entry. □

We need a final fact that will be crucial in the proof of Theorem 2.10. We thank Professor Stevenhagen for showing us this fact.

Proposition 2.7. *Let (a,b,c) be an admissible triple such that $a,b > 0$ and*

$$\gcd(\Delta_{\mathbb{Q}(\sqrt{a})}, \Delta_{\mathbb{Q}(\sqrt{b})}) = 1.$$

Then $(a,b,-abc)$ is also admissible and

$$[a,b,c] = [a,b,-abc].$$

Proof. Assume that a,b are both nontrivial; otherwise, the statement is immediate.

We first show that $(a,b,-ab)$ is admissible. The condition of being jointly unramified follows immediately from the assumption that $\Delta_{\mathbb{Q}(\sqrt{a})}$ and $\Delta_{\mathbb{Q}(\sqrt{b})}$ are coprime. Since $(a,-a)$ and $(b,-b)$ are always acceptable and (a,b) is acceptable by assumption, we conclude that $(a,b,-ab)$ is admissible.

We claim that $[a,b,-ab] = 0$. Let us pick L in $\mathcal{F}^{\mathrm{unr}}_{a,b}$. Since $\gcd(\Delta_{\mathbb{Q}(\sqrt{a})}, \Delta_{\mathbb{Q}(\sqrt{b})}) = 1$, it follows that $L/\mathbb{Q}(\sqrt{ab})$ is unramified at all odd, finite places. At the prime 2, we use that $a > 0$ and admissibility to deduce that $\Delta_{\mathbb{Q}(\sqrt{a})}$ is never 4 modulo 8. Then we see that $2 \mid \Delta_{\mathbb{Q}(\sqrt{a})}$ implies that $\Delta_{\mathbb{Q}(\sqrt{b})}$ is odd by our coprimality condition and hence 1 modulo 8, since otherwise (a,b) is not acceptable. We conclude that we are always in the second case in the definition of minimally ramified, and we conclude that $L/\mathbb{Q}(\sqrt{ab})$ is also unramified at 2.

Furthermore, $L/\mathbb{Q}(\sqrt{ab})$ is a cyclic degree 4 extension. On the other hand, the principal ideal $(\sqrt{ab})$ generates the kernel of the natural surjection $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{ab})) \twoheadrightarrow \mathrm{Cl}(\mathbb{Q}(\sqrt{ab}))$. The extension $L/\mathbb{Q}(\sqrt{ab})$ is totally real if and only if this kernel acts trivially on L via the Artin map. Therefore

$$\left[\frac{L/\mathbb{Q}(\sqrt{ab})}{(\sqrt{ab})}\right] = \left[\frac{L/\mathbb{Q}(\sqrt{ab})}{\tilde{\infty}}\right].$$

Hence $[a,b,-ab] = 0$. By Proposition 2.6, we have that $(a,b,-abc)$ is also admissible and

$$[a,b,c] = [a,b,c] + [a,b,-ab] = [a,b,-abc]$$

as desired. □

2.2. *Reflection principles*

We begin by recalling the connection between Rédei symbols and 8-rank pairings. Throughout this subsection, D is a positive squarefree integer with no prime divisors 3 modulo 4.

Recall that $\mathrm{Cl}^+(D)[2]$ is generated by the primes above the rational primes ramifying in $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$. For each positive $b \mid D$, we define $\mathfrak{B}_D(b)$ to be the unique integral ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ having norm equal to b. If $b < 0$, we instead put $\mathfrak{B}_D(b) := \mathfrak{B}_D(|b|) \cdot (\sqrt{D})$. Recall that $\mathfrak{B}_D(b) \in 2\,\mathrm{Cl}^+(D)[4]$ if and only if (b,D) forms an acceptable pair: that is, $(b,D)_v = 1$ for all $v \in \Omega$.

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

We now define the dual class group $\mathrm{Cl}^+(D)^\vee = \mathrm{Hom}(\mathrm{Cl}^+(D), \mathbb{Q}/\mathbb{Z})$. Then recall that $\mathrm{Cl}^+(D)^\vee[2]$ is generated by the characters χ_p with p a prime dividing D. There is precisely one relation among these characters, which comes from the fact that χ_D is the trivial character when restricted to $\mathbb{Q}(\sqrt{D})$. For a positive divisor $a \mid D$, we have that $\chi_a \in 2\,\mathrm{Cl}^+(D)^\vee[4]$ if and only if $(a, -D)$ is an acceptable pair: that is, $(a, -D)_v = 1$ for all $v \in \Omega$.

Since D is not divisible by any primes congruent to 3 mod 4, we have for any positive $a \mid D$ that $(a, D)_v = (a, -D)_v$. In particular, we have for any positive $a \mid D$

$$\chi_a \in 2\,\mathrm{Cl}^+(D)^\vee[4] \quad \text{if and only if} \quad \mathfrak{B}_D(a) \in 2\,\mathrm{Cl}^+(D)[4]. \tag{2.2}$$

Now let $a, b \mid \Delta_{\mathbb{Q}(\sqrt{D})}$ such that $\chi_a \in 2\,\mathrm{Cl}^+(D)^\vee[4]$ and $\mathfrak{B}_D(b) \in 2\,\mathrm{Cl}^+(D)[4]$. Then for all cyclic degree 4 extensions $L/\mathbb{Q}(\sqrt{D})$ unramified at all finite places and containing $\mathbb{Q}(\sqrt{a}, \sqrt{D})$, the Artin symbol $\left[\frac{L/\mathbb{Q}(\sqrt{D})}{\mathfrak{B}_D(b)}\right]$ always lands in the unique cyclic subgroup of order 2 of $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{D}))$, since $\mathfrak{B}_D(b) \in \mathrm{Cl}^+(D)[2]$. Furthermore, for a fixed a, the value of the symbol does not depend on the choice of L, since $\mathfrak{B}_D(b) \in 2\,\mathrm{Cl}^+(D)[4]$. In this statement, we are implicitly identifying any two groups of size 2 in the unique possible way. The value of this symbol is by definition

$$\langle \chi_a, b \rangle_D,$$

and we shall refer to it as the *Artin pairing* between χ_a and b. The two crucial features of this pairing are that it can be computed using Rédei symbols and that it determines $4\,\mathrm{Cl}^+(D)[8]$ and $4\,\mathrm{Cl}^+(D)^\vee[8]$ (namely, they are respectively the right and the left kernel of the pairing).

Proposition 2.8. *Let (a, b) be a pair with $a, b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ and such that $\Delta_{\mathbb{Q}(\sqrt{a})}, \Delta_{\mathbb{Q}(\sqrt{b})}$ are coprime. Furthermore, assume that $a, b > 0$ are not divisible by any prime congruent to 3 modulo 4. Let c be a squarefree divisor of $\Delta_{\mathbb{Q}(\sqrt{ab})}$, not necessarily positive. Assume that $\chi_a \in 2\,\mathrm{Cl}^+(ab)^\vee[4]$ and $\mathfrak{B}_{ab}(c) \in 2\,\mathrm{Cl}^+(ab)[4]$. Then the triple (a, b, c) is admissible, and we have that*

$$\langle \chi_a, c \rangle_{ab} = [a, b, c].$$

Proof. Observe that (a, b) and (ab, c) are acceptable since $\chi_a \in 2\,\mathrm{Cl}^+(ab)^\vee[4]$ and $\mathfrak{B}_{ab}(c) \in 2\,\mathrm{Cl}^+(ab)[4]$.

We claim that (a, c) is acceptable. A similar argument shows that (b, c) is acceptable. Firstly, $a > 0$ implies $(a, c)_\infty = 1$. Now we check that $(a, c)_v = 1$ for all $v \in \Omega$ finite and odd. If $v \nmid ac$, we trivially have $(a, c)_v = 1$. If v divides only a but not c, we have that $(a, c)_v = (ab, c)_v = 1$. If v divides only c but not a, we have that $(a, c)_v = (a, ab)_v = 1$. Now assume that v divides both a and c. Since $\Delta_{\mathbb{Q}(\sqrt{a})}, \Delta_{\mathbb{Q}(\sqrt{b})}$ are coprime, we must have $v \nmid b$. Also, by assumption, v^2 cannot divide a or c, so $(b, ac)_v = 1$. Therefore

$$(a, c)_v = (a, ac)_v = (ab, ac)_v.$$

Since (a, b) and (ab, c) are acceptable, we have

$$(a, ab)_v = (a, b)_v = (ab, c)_v = 1,$$

so $(ab, ac)_v = 1$, as required. The remaining case $v = 2$ follows from Hilbert reciprocity. This shows that (a, c) and similarly (b, c) are acceptable pairs.

Since a, b are coprime and not divisible by any prime congruent to 3 mod 4, we conclude that $\gcd(\Delta_{\mathbb{Q}(\sqrt{a})}, \Delta_{\mathbb{Q}(\sqrt{b})}, \Delta_{\mathbb{Q}(\sqrt{c})}) = 1$. Therefore the triple (a, b, c) is admissible. Now observe that any

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

$L \in \mathcal{F}^{\mathrm{unr}}_{a,b}$ gives a cyclic degree 4 extension of $\mathbb{Q}(\sqrt{ab})$ that is unramified at all finite places and contains $\mathbb{Q}(\sqrt{a}, \sqrt{b})$. Therefore

$$\langle \chi_a, c \rangle_{ab} = \left[\frac{L/\mathbb{Q}(\sqrt{ab})}{\mathfrak{B}_{ab}(c)} \right] = [a, b, c]$$

as was to be shown. □

We are now ready to prove our main algebraic results.

Theorem 2.9. *Let $d \in \mathcal{D}$. Let p_1, p_2, q_1, q_2 be primes that are 1 modulo 4 and coprime to d. Let a be a positive divisor of d, and let b be any (possibly negative) divisor of d. Assume that*

$$\mathfrak{B}_{p_i q_j d}(b) \in 2\,\mathrm{Cl}^+(p_i q_j d)[4] \text{ for all } i, j \in \{1, 2\}.$$

1. *Suppose*

$$\chi_a \in 2\,\mathrm{Cl}^+(p_i q_j d)^\vee[4] \text{ for all } (i, j) \in i, j \in \{1, 2\}.$$

Then

$$\langle \chi_a, b \rangle_{p_1 q_1 d} + \langle \chi_a, b \rangle_{p_1 q_2 d} + \langle \chi_a, b \rangle_{p_2 q_1 d} + \langle \chi_a, b \rangle_{p_2 q_2 d} = 0. \tag{2.3}$$

2. *Suppose instead*

$$\chi_{p_i a} \in 2\,\mathrm{Cl}^+(p_i q_j d)^\vee[4] \text{ for all } (i, j) \in i, j \in \{1, 2\}.$$

Then the triple $(p_1 p_2, q_1 q_2, b)$ is admissible and

$$\langle \chi_{p_1 a}, b \rangle_{p_1 q_1 d} + \langle \chi_{p_1 a}, b \rangle_{p_1 q_2 d} + \langle \chi_{p_2 a}, b \rangle_{p_2 q_1 d} + \langle \chi_{p_2 a}, b \rangle_{p_2 q_2 d} = [p_1 p_2, q_1 q_2, b]. \tag{2.4}$$

Proof. (i) By Proposition 2.8, we obtain that the four triples $(a, p_1 q_1 \frac{d}{a}, b)$, $(a, p_1 q_2 \frac{d}{a}, b)$, $(a, p_2 q_1 \frac{d}{a}, b)$ and $(a, p_2 q_2 \frac{d}{a}, b)$ are all admissible and the left-hand side of (2.3) equals

$$\left[a, p_1 q_1 \frac{d}{a}, b\right] + \left[a, p_1 q_2 \frac{d}{a}, b\right] + \left[a, p_2 q_1 \frac{d}{a}, b\right] + \left[a, p_2 q_2 \frac{d}{a}, b\right].$$

By Proposition 2.6, this sum equals

$$[a, q_1 q_2, b] + [a, q_1 q_2, b] = 0.$$

(ii) By Proposition 2.8, we know that the triples $(p_1 a, q_1 \frac{d}{a}, b), (p_1 a, q_2 \frac{d}{a}, b), (p_2 a, q_1 \frac{d}{a}, b)$ and $(p_2 a, q_2 \frac{d}{a}, b)$ are all admissible and that the left-hand side of (2.4) equals

$$\left[p_1 a, q_1 \frac{d}{a}, b\right] + \left[p_1 a, q_2 \frac{d}{a}, b\right] + \left[p_2 a, q_1 \frac{d}{a}, b\right] + \left[p_2 a, q_2 \frac{d}{a}, b\right].$$

Applying Proposition 2.6, we find that $(p_1 a, q_1 q_2, b)$ and $(p_2 a, q_1 q_2, b)$ are also admissible and this sum equals

$$[p_1 a, q_1 q_2, b] + [p_2 a, q_1 q_2, b].$$

Another application of Proposition 2.6 shows that $(p_1 p_2, q_1 q_2, b)$ is admissible and the above sum is $[p_1 p_2, q_1 q_2, b]$, completing the proof. □

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

We remark that it is possible to prove Proposition 2.6 without using Rédei reciprocity. It is precisely this approach that works in the generality of [18, Theorem 2.8]. The resulting argument is substantially more involved, so for brevity, we opted to use the proofs with Rédei reciprocity. Note that Theorem 2.10, Theorem 2.11 and Theorem 2.12 have no analogues in [18].

Theorem 2.10. *Let $d \in \mathcal{D}$. Take primes p_1, p_2, q_1, q_2 that are 1 modulo 4 and coprime to d. Let a be a positive divisor of d. We assume that*

$$\mathfrak{B}_{p_iq_jd}(p_ia) \in 2\,\mathrm{Cl}^+(p_iq_jd)[4] \text{ for all } i, j \in \{1, 2\}.$$

Then we have

$$\chi_{p_ia} \in 2\,\mathrm{Cl}^+(p_iq_jd)^\vee[4] \text{ for all } i, j \in \{1, 2\}.$$

Moreover, the triple (p_1p_2, q_1q_2, p_1p_2) is admissible and

$$\langle \chi_{p_1a}, p_1a\rangle_{p_1q_1d} + \langle \chi_{p_1a}, p_1a\rangle_{p_1q_2d} + \langle \chi_{p_2a}, p_2a\rangle_{p_2q_1d} + \langle \chi_{p_2a}, p_2a\rangle_{p_2q_2d} = [p_1p_2, q_1q_2, p_1p_2]. \tag{2.5}$$

Proof. By equation (2.2), $\mathfrak{B}_{p_iq_jd}(p_ia) \in 2\,\mathrm{Cl}^+(p_iq_jd)[4]$ implies that $\chi_{p_ia} \in 2\,\mathrm{Cl}^+(p_iq_jd)^\vee[4]$ for each $i, j \in \{1, 2\}$.

By Proposition 2.8, we conclude that $(p_1a, q_1\frac{d}{a}, p_1a)$, $(p_1a, q_2\frac{d}{a}, p_1a)$, $(p_2a, q_1\frac{d}{a}, p_2a)$ and $(p_2a, q_2\frac{d}{a}, p_2a)$ are all admissible, and furthermore that the left-hand side of (2.5) is

$$\left[p_1a, q_1\frac{d}{a}, p_1a\right] + \left[p_1a, q_2\frac{d}{a}, p_1a\right] + \left[p_2a, q_1\frac{d}{a}, p_2a\right] + \left[p_2a, q_2\frac{d}{a}, p_2a\right].$$

Using Proposition 2.6, we have that (p_1a, q_1q_2, p_1a) and (p_2a, q_1q_2, p_2a) are admissible triples, and the sum becomes

$$[p_1a, q_1q_2, p_1a] + [p_2a, q_1q_2, p_2a].$$

Next, since p_1a, q_1q_2 are coprime and p_2a, q_1q_2 are coprime, Proposition 2.7 implies that $(p_1a, q_1q_2, -q_1q_2)$ and $(p_2a, q_1q_2, -q_1q_2)$ are admissible, and the above sum is

$$[p_1a, q_1q_2, -q_1q_2] + [p_2a, q_1q_2, -q_1q_2].$$

By Proposition 2.6, $(p_1p_2, q_1q_2, -q_1q_2)$ is admissible, and the above sum is

$$[p_1p_2, q_1q_2, -q_1q_2].$$

Since p_1p_2, q_1q_2 are coprime, applying Proposition 2.7 again shows that (p_1p_2, q_1q_2, p_1p_2) is admissible and

$$[p_1p_2, q_1q_2, -q_1q_2] = [p_1p_2, q_1q_2, p_1p_2],$$

which gives the desired result. □

Theorem 2.11. *Let $d \in \mathcal{D}$. Let p_1, p_2, q_1, q_2 be distinct primes that are 1 modulo 4 and coprime to d. Let a, b be a positive divisors of d. We assume that*

$$\mathfrak{B}_{p_iq_jd}(b), \mathfrak{B}_{p_iq_jd}(p_ia) \in 2\,\mathrm{Cl}^+(p_iq_jd)[4] \text{ for all } i, j \in \{1, 2\}.$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

Then we have that

$$\chi_b, \chi_{p_i a} \in 2\,\mathrm{Cl}^+(p_i q_j d)^\vee[4] \text{ for all } i, j \in \{1, 2\}.$$

Furthermore, we have that

$$\sum_{i,j\in\{1,2\}} \langle \chi_{p_i a}, b\rangle_{p_i q_j d} + \langle \chi_b, p_i a\rangle_{p_i q_j d} = 0.$$

Proof. The first assertion follows from equation (2.2). By Proposition 2.8, $(p_i a, \frac{d}{a} q_j, b)$ and $(b, \frac{d}{b} p_i q_j, a p_i)$ are admissible for all choices of i, j in $\{1, 2\}$. Therefore the sum of the pairings in this proposition can be rewritten as

$$\sum_{i,j\in\{1,2\}} \left[p_i a, \frac{d}{a} q_j, b\right] + \left[b, \frac{d}{b} p_i q_j, a p_i\right].$$

Applying Proposition 2.6, we can rewrite this as

$$[p_1 a, q_1 q_2, b] + [p_2 a, q_1 q_2, b] + [b, q_1 q_2, a p_1] + [b, q_1 q_2, a p_2] = [p_1 p_2, q_1 q_2, b] + [b, q_1 q_2, p_1 p_2] = 0.$$

The first equality follows from Proposition 2.6, and the last equality follows from applying Theorem 2.5. □

Theorem 2.12. *Let $d \in \mathcal{D}$. Let p_1, p_2, q_1, q_2 be distinct primes that are 1 modulo 4 and coprime to d. Let a, b be positive divisors of d. We assume that*

$$\mathfrak{B}_{p_i q_j d}(q_j b), \mathfrak{B}_{p_i q_j d}(p_i a) \in 2\,\mathrm{Cl}^+(p_i q_j d)[4] \textit{ for all } i, j \in \{1, 2\}.$$

Then we have that

$$\chi_{q_j b}, \chi_{p_i a} \in 2\,\mathrm{Cl}^+(p_i q_j d)^\vee[4] \textit{ for all } i, j \in \{1, 2\}.$$

In addition, the triple $(p_1 p_2, q_1 q_2, -1)$ is admissible and

$$\sum_{i,j\in\{1,2\}} \langle \chi_{p_i a}, q_j b\rangle_{p_i q_j d} + \langle \chi_{q_j b}, p_i a\rangle_{p_i q_j d} = [p_1 p_2, q_1 q_2, -1]. \tag{2.6}$$

Proof. The first assertion follows as usual. By Proposition 2.8, we have that the triples $(p_i a, \frac{d}{a} q_j, q_j b), (q_j b, \frac{d}{b} p_i, p_i a)$ are admissible for each choice of i, j in $\{1, 2\}$, and the left-hand side of equation (2.6) equals

$$\sum_{i,j\in\{1,2\}} \left[p_i a, \frac{d}{a} q_j, q_j b\right] + \left[q_j b, \frac{d}{b} p_i, p_i a\right].$$

By Proposition 2.6, we can rewrite this sum of Rédei symbols as

$$\left[p_1 p_2, \frac{d}{a} q_1, b q_1\right] + \left[p_1 p_2, \frac{d}{a} q_2, b q_2\right] + \left[q_1 q_2, \frac{d}{b} p_1, a p_1\right] + \left[q_1 q_2, \frac{d}{b} p_2, a p_2\right].$$

One readily checks that $p_i \frac{d}{b}$ is coprime to $q_1 q_2$ and $q_j \frac{d}{a}$ is coprime to $p_1 p_2$. Therefore, we can apply Proposition 2.7 to each of the terms in the above sum to obtain

$$\left[p_1 p_2, \frac{d}{a} q_1, -dabp_1 p_2\right] + \left[p_1 p_2, \frac{d}{a} q_2, -dabp_1 p_2\right] + \left[q_1 q_2, \frac{d}{b} p_1, -dabq_1 q_2\right] + \left[q_1 q_2, \frac{d}{b} p_2, -dabq_1 q_2\right].$$

Applying Proposition 2.6, we can further simplify this and get

$$[p_1 p_2, q_1 q_2, -dabp_1 p_2] + [p_1 p_2, q_1 q_2, -dabq_1 q_2] = [p_1 p_2, q_1 q_2, p_1 p_2 q_1 q_2].$$

Since $p_1 p_2$ and $q_1 q_2$ are coprime, we can apply Proposition 2.7 and get that $(p_1 p_2, q_1 q_2, -1)$ is admissible and the above Rédei symbol equals $[p_1 p_2, q_1 q_2, -1]$ as required. □

3. A combinatorial result

Let $X_1, \ldots, X_m$ be finite, nonempty sets, and let $X := X_1 \times \ldots \times X_m$. Put

$$V := \{F : X \longrightarrow \mathbb{F}_2\}, \quad W := \{g : X \times X \longrightarrow \mathbb{F}_2\}.$$

Given two elements $x_1, x_2 \in X$ and $\mathbf{v} \in \{1, 2\}^m$, we define $\mathbf{v}(x_1, x_2)$ to be the unique element $y \in X$ such that $\pi_j(y) = \pi_j(x_{\pi_j(\mathbf{v})})$. Let $d : V \longrightarrow W$ be the linear map given by

$$dF(x_1, x_2) = \sum_{\mathbf{v} \in \{1,2\}^m} F(\mathbf{v}(x_1, x_2)).$$

We define $\mathcal{A}(X) := \operatorname{im}(d)$.

Lemma 3.1. *We have that*

$$\dim_{\mathbb{F}_2} \mathcal{A}(X) = \prod_{i=1}^{m} (|X_i| - 1).$$

Proof. See Proposition 9.3 of Koymans and Pagano [13]. □

Definition 3.2. Let $\epsilon > 0$ be given. We say that F is ϵ-bad if

$$\left| F^{-1}(0) - \frac{|X|}{2} \right| \geq \epsilon |X|.$$

We say that $g \in \mathcal{A}(X)$ is ϵ-bad if there is ϵ-bad F such that $dF = g$.

In our application, we shall be able to prove distributional properties of g by using the Chebotarev density theorem. However, we have no direct control over F itself. Nevertheless, the following theorem will allow us to prove the desired equidistribution for F. Note the similarity to Proposition 4.3 in Smith [18]. Since we are dealing with the 8-rank, we shall not need the more complicated Proposition 4.4 in Smith [18].

Theorem 3.3. *Let $\epsilon > 0$ be given. Then we have*

$$\frac{|\{g \in \mathcal{A}(X) : g \text{ is } \epsilon\text{−bad}\}|}{|\mathcal{A}(X)|} \leq 2^{1+|X| - \prod_{i=1}^{m}(|X_i|-1)} \cdot \exp(-2\epsilon^2 |X|).$$

Proof. Hoeffding's inequality shows that the proportion of F that are ϵ-bad is at most

$$\frac{|\{F \in V : F \text{ is } \epsilon\text{−bad}\}|}{|V|} \leq 2 \exp(-2\epsilon^2 |X|). \tag{3.1}$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

Define

$$a := |X| - \prod_{i=1}^{m}(|X_i| - 1).$$

By Lemma 3.1, we see that the kernel of d is an a-dimensional vector space. Combining this with equation (3.1), we infer that

$$\frac{|\{g \in \mathcal{A}(X) : g \text{ is } \epsilon\text{−bad}\}|}{|\mathcal{A}(X)|} \le \frac{|\{F \in V : F \text{ is } \epsilon\text{−bad}\}|}{|\mathcal{A}(X)|} \le 2^{a+1} \cdot \exp(-2\epsilon^2|X|),$$

which is the theorem. □

4. Prime divisors

In [18, Section 5], Smith proved that several properties pertaining to the spacing of prime divisors of integers in the set $\{1 \le n \le N : \omega(n) = r, \ p \mid n \Rightarrow p > D\}$ occur frequently. Using different methods, we will obtain similar results on squarefree integers with no prime factor congruent to 3 mod 4.

Define $S(N) := \{1 \le n < N : p \mid n \Rightarrow p \not\equiv 3 \bmod 4, \ n \text{ squarefree}\}$, $S_r(N) := \{n \in S(N) : \omega(n) = r\}$ and $\mu := \frac{1}{2}\log\log N$. A classical result by Landau [14] shows that

$$\Phi(N) := |S(N)| = \frac{CN}{\sqrt{\log N}} + o\left(\frac{N}{\sqrt{\log N}}\right)$$

for some constant $C > 0$. We recall the prime number theorem for arithmetic progressions

$$|\{p \le N : p \equiv 1 \bmod 4\}| = \frac{1}{2}\operatorname{Li}(N) + O\left(N\exp\left(-c\sqrt{\log N}\right)\right).$$

Write $\Phi_r(N) := |S_r(N)|$. Then following the proof of the Sathé–Selberg theorem [16], one can deduce that there exists a constant $A > 0$ such that for all $r < 10\mu$ and all $N \ge A$,

$$\frac{A^{-1}N}{\log N}\frac{\left(\frac{1}{2}\log\log N\right)^{r-1}}{(r-1)!} \le \Phi_r(N) \le \frac{AN}{\log N}\frac{\left(\frac{1}{2}\log\log N\right)^{r-1}}{(r-1)!}. \tag{4.1}$$

We can easily bound the number of integers with more than, say, 10μ prime divisors by computing the average number of divisors. Then by standard bounds for the tail of the Poisson distribution, it follows that

$$\frac{|\{n \in S(N) : |\omega(n) - \mu| > \mu^{2/3}\}|}{|S(N)|} \ll \exp\left(-\frac{1}{3}\mu^{1/3}\right). \tag{4.2}$$

In the following, for any $n \in S(N)$, write $r = \omega(n)$ and list the distinct prime factors of n as $p_1 < p_2 < \cdots < p_r$. We will prove that almost all $n \in S_r(N)$ have three particular types of spacing.

Theorem 4.1. *Let $\epsilon > 0$. Take $y_1 > 3$ and $\eta > 1$. Assume*

$$|r - \mu| < \mu^{2/3}. \tag{4.3}$$

Then

1. *other than $\ll_\epsilon \Phi_r(N)\left((\log y_1)^{-1} + (\log x)^{-1/2+\epsilon}\right)$ exceptions, all $n \in S_r(N)$ are comfortably spaced above y_1: $2y_1 < p_i < p_{i+1}/2$ for any $p_i > y_1$;*

2. *other than* $\ll \Phi_r(N)\exp(-k\eta)$ *exceptions, where* k *is an absolute constant, all* $n \in S_r(N)$ *are* η*-regularly spaced:*

$$\left|\frac{1}{2}\log\log p_i - i\right| < \eta^{1/5}\max\{i,\eta\}^{4/5} \text{ for all } i < \frac{1}{3}r;$$

3. *other than* $\ll_\epsilon \Phi_r(N)\exp\bigl(-(\log\log\log N)^{1/3-\epsilon}\bigr)$ *exceptions, all* $n \in S_r(N)$ *are extravagantly spaced:*

$$\log p_i \ge (\log\log p_i)^2 \cdot \log\log\log N \cdot \sum_{j=1}^{i-1}\log p_j \text{ for some } \frac{1}{2}r^{1/2} < i < \frac{1}{2}r.$$

4.1. Some estimates

4.1.1. Upper bound for rough numbers

Mertens' theorem shows that there exist constants $c, M > 0$ such that for any $N > 2$,

$$\sum_{\substack{p \le N \\ p \not\equiv 3 \bmod 4}} \frac{1}{p} = \frac{1}{2}\log\log N + M + O\Bigl(\exp\Bigl(-c\sqrt{\log N}\Bigr)\Bigr).$$

Fixing some large enough absolute constant $B_1 > 0$, we have for any $N > 2$

$$\frac{1}{2}\log\log N - B_1 \le \sum_{\substack{p \le N \\ p \not\equiv 3 \bmod 4}} \frac{1}{p} \le \frac{1}{2}\log\log N + B_1.$$

For any set of primes E, define

$$E(N) := \sum_{\substack{p \le N \\ p \in E}} \frac{1}{p}.$$

We also define $\omega_E(n)$ to be the number of prime divisors of n that are in E. We will apply the following theorem by Tudesq [21, Theorem 2].

Theorem 4.2. *There exists an absolute constant* $B_2 > 0$ *such that*

$$|\{n \le N : \omega_{E_j}(n) = k_j \text{ for } 0 \le j \le l\}| \ll N\exp\left(-\sum_{j=0}^{l} E_j(N)\right)\prod_{j=0}^{l}\frac{(E_j(N)+B_2)^{k_j}}{k_j!}$$

for all $N \ge 1$, $l \ge 0$, E_j *pairwise disjoint sets of primes,* $k_j \ge 0$.

In our application, we will take E_0 to be the set of primes congruent to 3 mod 4 and $E_0, E_1, \ldots, E_l$ to be pairwise disjoint sets of primes so that $\cup_{j=0}^{l} E_j$ contains all primes. Also take $k_0 = 0$ and $k_1 + \cdots + k_l = r$. Then

$$|\{n \in S_r(N) : \omega_{E_j}(n) = k_j,\ 1 \le j \le l\}| \ll \frac{N}{\log N}\prod_{j=1}^{l}\frac{(E_j(N)+B_2)^{k_j}}{k_j!}.$$

We set $B := \max(B_1 + B_2, 100)$, where B_2 is the absolute constant from Theorem 4.2.

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

4.1.2. Upper bound for smooth numbers

Define

$$\Psi_r(N,y) := \{n \in S_r(N) : \ p \mid n \Rightarrow p < y\},$$

so that $|\Psi_r(N,y)|$ is the size of the set of y-smooth numbers in $S_r(N)$.

We will need an upper bound for smooth numbers for small $u := \log N/\log y$. There are works treating the number of prime factors of smooth numbers [1, 10, 11], but none of them explicitly give a formula for the range of small u we are interested in. We prove an upper bound here that is sufficient for our application, although more work could be done to obtain a more precise estimate.

Lemma 4.3. *Fix some $\epsilon \in (0,1)$. There exists some large enough $A > 0$ such that the following holds. Take $N > y > 2$ and some integer $k \geq 1$ such that $\frac{1}{2}k < \frac{1}{2}\log\log y < 2k$ and $u := \frac{\log N}{\log y} < (\log N)^{1-\epsilon}$, and assume $u > A$. Then*

$$\Psi_k(N,y) \leq \frac{u^{-u}N}{\log y} \cdot \frac{(\frac{1}{2}\log\log y)^{k-1}}{(k-1)!}.$$

Proof. We have

$$(\log N)\Psi_k(N,y) = \sum_{n\in\Psi_k(N,y)} \log n + \sum_{n\in\Psi_k(N,y)} \log\frac{N}{n}. \tag{4.4}$$

We first treat the first term, which is the main contribution. Factoring each $n \in \Psi_k(N,y)$ gives

$$\sum_{n\in\Psi_k(N,y)} \log n \leq \sum_{m\in\Psi_{k-1}(N,y)} \sum_{\substack{p<\min\{\frac{N}{m},y\} \\ p\not\equiv 3 \bmod 4}} \log p. \tag{4.5}$$

Indeed, for every $n \in \Psi_k(N,y)$ and every prime divisor p of n, we see that the pair $(n/p, p)$ contributes $\log p$ to the sum on the RHS of equation (4.5) so that the total contribution of n is $\log n$. Now, taking any $0 < \sigma < 1$, we have

$$\sum_{\substack{p<\min\{\frac{N}{m},y\} \\ p\not\equiv 3 \bmod 4}} \log p \ll \min\left\{\frac{N}{m}, y\right\} \leq \left(\frac{N}{m}\right)^{\sigma} y^{1-\sigma}.$$

Then, writing $\frac{1}{m} = \prod_{p|m}\frac{1}{p}$, equation (4.5) becomes

$$\sum_{n\in\Psi_k(N,y)} \log n \ll N^{\sigma}y^{1-\sigma} \sum_{m\in\Psi_{k-1}(N,y)} \frac{1}{m^{\sigma}} \ll \frac{N^{\sigma}y^{1-\sigma}}{(k-1)!}\left(\sum_{\substack{p<y \\ p\not\equiv 3 \bmod 4}} \frac{1}{p^{\sigma}}\right)^{k-1}.$$

Take $\sigma = 1 - \frac{\log(u\log u)}{\log y}$, which is positive and tends to 1 since $u < (\log N)^{1-\epsilon}$. Then $N^{\sigma} = \frac{N}{(u\log u)^u}$ and $y^{1-\sigma} = u\log u$. Noting that $\mathrm{Li}(t) = \frac{t}{\log t} + O(\frac{t}{(\log t)^2})$ and $\mathrm{Ei}(1/t) = -\log t + O(1)$ as $t \to \infty$, we have

$$\int_{e<t<y} \frac{dt}{t^{\sigma}\log t} = \mathrm{Li}(u\log u) - \mathrm{Ei}\left(\frac{\log(u\log u)}{\log y}\right) = \log\log y + u\left(1 + O\left(\frac{\log\log u}{\log u}\right)\right).$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

Therefore, evaluating the Stieltjes integral $\int_{t<y} \frac{d\pi(t)}{2t^\sigma}$ gives

$$\sum_{\substack{p<y\\ p\not\equiv 3 \bmod 4}} \frac{1}{p^\sigma} = \frac{1}{2}\log\log y + \frac{1}{2}u\left(1+O\left(\frac{\log\log u}{\log u}\right)\right).$$

Putting the above together, we obtain

$$\sum_{n\in\Psi_k(N,y)} \log n \ll \frac{N}{(u\log u)^{u-1}} \cdot \frac{\left(\frac{1}{2}\log\log y + \frac{1}{2}u\left(1+O\left(\frac{\log\log u}{\log u}\right)\right)\right)^{k-1}}{(k-1)!}.$$

The second sum in equation (4.4) is at most

$$\frac{N^\sigma}{\sigma}\sum_{n\in\Psi_k(N,y)}\frac{1}{n^\sigma} \le \frac{N^\sigma}{\sigma\cdot k!}\left(\sum_{\substack{p<y\\ p\not\equiv 3 \bmod 4}}\frac{1}{p^\sigma}\right)^k \ll \frac{N}{(u\log u)^u}\cdot\frac{\left(\frac{1}{2}\log\log y + \frac{1}{2}u\left(1+O\left(\frac{\log\log u}{\log u}\right)\right)\right)^{k}}{k!}.$$

Since $\log\log y/2k$ is bounded, putting back in equation (4.4) yields

$$\Psi_k(N,y) \ll \frac{1}{(u\log u)^{u-1}}\cdot\frac{N}{\log N}\cdot\frac{\left(\frac{1}{2}\log\log y + \frac{1}{2}u\left(1+O\left(\frac{\log\log u}{\log u}\right)\right)\right)^{k-1}}{(k-1)!}.$$

We have

$$\left(\frac{1}{2}\log\log y + \frac{1}{2}u\left(1+O\left(\frac{\log\log u}{\log u}\right)\right)\right)^{k-1} = \left(\frac{1}{2}\log\log y\right)^{k-1}\cdot\left(1+\frac{u}{\log\log y}\left(1+O\left(\frac{\log\log u}{\log u}\right)\right)\right)^{k-1}.$$

Since $k < \log\log y$, we get that this is at most

$$\left(1+\frac{u}{\log\log y}\left(1+O\left(\frac{\log\log u}{\log u}\right)\right)\right)^{\log\log y} \le e^{u\left(1+O\left(\frac{\log\log u}{\log u}\right)\right)}.$$

Because

$$\frac{e^{u\left(1+O\left(\frac{\log\log u}{\log u}\right)\right)}}{(u\log u)^{u-1}} \ll u^{-u+1} = u^{-u}\cdot\frac{\log N}{\log y}$$

for sufficiently large u, this implies that

$$\Psi_k(N,y) \ll u^{-u}\cdot\frac{N}{\log y}\cdot\frac{\left(\frac{1}{2}\log\log y\right)^{k-1}}{(k-1)!}$$

as desired. □

4.2. Proof of Theorem 4.1

4.2.1. Proof of Theorem 4.11

The number of $n \in S_r(N)$ for which

$$y_1 < p < 2y_1 \text{ for some } p \mid n \text{ or } y_1 < q < p < 2q \text{ for some } pq \mid n$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

is bounded by

$$\sum_{\substack{y_1<p_i<2y_1\\ p\equiv 1 \bmod 4}} \Phi_{r-1}\left(\frac{N}{p}\right) + \sum_{\substack{y_1<q<\sqrt{N}\\ q\equiv 1 \bmod 4}} \sum_{\substack{q<p<2q\\ p\equiv 1 \bmod 4}} \Phi_{r-2}\left(\frac{N}{pq}\right).$$

Split the sum into the cases $p < N^{1/4}$ and $p > N^{1/4}$. First, bound the sum $p < N^{1/4}$ and assume $y_1 < N^{1/4}$; otherwise the sum is zero. Using equation (4.1), we see that the sum is bounded by

$$\ll \Phi_r(N) \sum_{\substack{y_1<p<2y_1\\ p\equiv 1 \bmod 4}} \frac{1}{p} + \Phi_r(N) \sum_{\substack{y_1<q<\sqrt{N}\\ q\equiv 1 \bmod 4}} \sum_{\substack{q<p<2q\\ p\equiv 1 \bmod 4}} \frac{1}{pq} \ll \frac{\Phi_r(N)}{\log y_1}.$$

The sum $p > N^{1/4}$ is similarly bounded by

$$N \sum_{\substack{y_1<p<2y_1\\ p>N^{1/4}\\ p\equiv 1 \bmod 4}} \frac{1}{p} + N \sum_{\substack{y_1<q<\sqrt{N}\\ q\equiv 1 \bmod 4}} \sum_{\substack{q<p<2q\\ p>N^{1/4}\\ p\equiv 1 \bmod 4}} \frac{1}{pq} \ll \frac{N}{\log N} \ll_\epsilon \frac{\Phi_r(N)}{(\log N)^{1/2-\epsilon}},$$

completing the proof of part (i).

4.2.2. Proof of Theorem 4.12

Recall that $B = \max(B_1 + B_2, 100)$.

Lemma 4.4. *Then there exist some $A > 0$ such that the following holds. Assume r satisfies equation (4.3), and take $1 \le i \le \frac{1}{2}r$. Let $\max\{200B, i^{4/5}\} \le \lambda < \frac{1}{3}r$. For all $N > A$,*

$$\left|\left\{n \in S_r(N) : \left|\frac{1}{2}\log\log p_i - i\right| > \lambda\right\}\right| \ll \Phi_r(N)\exp\left(-\frac{\lambda^2}{100(i+\lambda)}\right).$$

Proof. We apply Theorem 4.2 with E_0 the set of primes that are 3 modulo 4, E_1 the set of primes p with $\frac{1}{2}\log\log p < i+\lambda$ and E_2 the set of primes p with $i+\lambda \le \frac{1}{2}\log\log p \le \mu$. We take $k_0 = 0$, $k_1 < i$ and $k_1 + k_2 = r$. Then the number of $n \in S_r(N)$ such that $\frac{1}{2}\log\log p_i > i+\lambda$ is at most

$$\frac{N}{\log N}\sum_{l=0}^{i-1}\frac{(i+\lambda+B)^l}{l!}\frac{(\mu-(i+\lambda)+B)^{r-l}}{(r-l)!} \ll \Phi_r(N)\sum_{l=0}^{i-1}\binom{r}{l}\left(\frac{i+\lambda}{\mu}\right)^l\left(1-\frac{i+\lambda}{\mu}\right)^{r-l}, \tag{4.6}$$

where the second inequality uses equation (4.1) and the inequality

$$\left(1+\frac{B}{i+\lambda}\right)^l\left(1+\frac{B}{\mu-(i+\lambda)}\right)^{r-l} \le \exp\left(\frac{iB}{i+\lambda}+\frac{rB}{\mu-(i+\lambda)}\right) \le \exp(7B).$$

Let $X_1,\ldots,X_n$ be independent random variables taking values in $\{0,1\}$. If X denotes their sum and $M = \mathbb{E}[X]$, then the lower tail Chernoff bound states that for any $0 \le \delta \le 1$,

$$\mathbb{P}(X \le (1-\delta)M) \le e^{-\delta^2 M/2}.$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

See [2, Theorem A.1.13] for a reference in a slightly different form. We warn the reader that the X there corresponds to our $X - M$. Then we bound equation (4.6) as

$$\begin{aligned}\Phi_r(N)\exp\left(-\frac{r\mu}{2(i+\lambda)}\left(\frac{i+\lambda}{\mu}-\frac{i}{r}\right)^2\right) &\le \Phi_r(N)\exp\left(-\frac{1-\mu^{-1/3}}{2(i+\lambda)}\left(i+\lambda-\frac{i}{1-\mu^{-1/3}}\right)^2\right)\\ &\le \Phi_r(N)\exp\left(-\frac{1-\mu^{-1/3}}{2(i+\lambda)}\left(\lambda-i^{2/3}\right)^2\right)\\ &\le \Phi_r(N)\exp\left(-\frac{\lambda^2}{4(i+\lambda)}\right).\end{aligned}$$

If $n \in S_r(N)$ satisfies $\frac{1}{2}\log\log p_i < i - \lambda$, then certainly $\lambda < i$. Another application of Theorem 4.2 yields the bound

$$\frac{N}{\log N}\sum_{l=i}^{r}\frac{(i-\lambda+B)^l}{l!}\frac{(\mu-(i-\lambda)+B)^{r-l}}{(r-l)!} \ll \Phi_r(N)\sum_{l=i}^{r}\binom{r}{l}\left(\frac{i-\lambda+B}{\mu}\right)^l\left(1-\frac{i-\lambda+B}{\mu}\right)^{r-l},$$

where the last inequality uses that

$$\left(\frac{\mu-i+\lambda+B}{\mu-i+\lambda-B}\right)^{r-l} = \left(1+\frac{2B}{\mu-(i-\lambda)-B}\right)^{r-l} \le \exp\left(\frac{2B(r-l)}{\mu-i+\lambda-B}\right) \le \exp(4B).$$

We now apply the upper tail Chernoff bound

$$\mathbb{P}(X \ge (1+\delta)M) \le e^{-\delta^2 M/(2+\delta)}$$

with $(1+\delta)M = i$. In case $\delta \le 1$, the computation proceeds among the same lines as before. If instead $\delta > 1$, we use that

$$\frac{\delta^2}{2+\delta} \ge \frac{1+\delta}{6}$$

so we have $\exp(-i/6)$. Since $\delta > 1$ implies that $\lambda > \frac{i}{3}$, this finishes the proof. □

We are now ready to prove part (ii). The theorem is trivial when $\eta > 2r$, so assume $\eta < 2r$. Take $\tilde{\eta} = \frac{1}{6}\eta$ so that $\tilde{\eta} < \frac{1}{3}r$, and apply Lemma 4.4 with $\lambda = \tilde{\eta}^{1/5}\max\{i,\tilde{\eta}\}^{4/5}$ for every i between 1 to $\frac{1}{3}r$. We get that the number of $n \in S_r(N)$ such that

$$\left|\frac{1}{2}\log\log p_i - i\right| > \eta^{1/5}\max\{i,\eta\}^{4/5} > \tilde{\eta}^{1/5}\max\{i,\tilde{\eta}\}^{4/5} \text{ for some } i < \frac{1}{3}r$$

is bounded by

$$\begin{aligned}\Phi_r(N)\sum_{i=1}^{\lfloor\frac{1}{3}r\rfloor}\exp\left(-\frac{\tilde{\eta}^{2/5}\max\{i,\tilde{\eta}\}^{8/5}}{100(i+\tilde{\eta}^{1/5}\max\{i,\tilde{\eta}\}^{4/5})}\right) &\ll \Phi_r(N)\exp\left(-\frac{\tilde{\eta}}{200}\right)\\ &= \Phi_r(N)\exp\left(-\frac{\eta}{1200}\right)\end{aligned}$$

when $\tilde{\eta} > 200B$.

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

4.2.3. Proof of Theorem 4.13

Fix $\kappa > \frac{2}{3}$. We will show that other than $\ll_\epsilon \Phi_r(N)\exp\big(-(\log\mu)^{1-\kappa(1+\epsilon)}\big)$ exceptions, we have

$$\max_{\frac{1}{2}\sqrt{r}<i<\frac{1}{2}r} \log\log p_i - \log\left(\sum_{j=1}^{i-1}\log p_j\right) - 2\log\log\log p_i > (3\kappa-1)\log\log\mu - 2.$$

First, remove $n \in S_r(N)$ for which

$$\left|\frac{1}{2}\log\log p_i - i\right| > i^{4/5} \text{ for some } \frac{1}{2}\sqrt{r} < i < \frac{1}{2}r.$$

For each i with $\frac{1}{2}\sqrt{r} < i < \frac{1}{2}r$, we apply Lemma 4.4 with $\lambda = i^{4/5}$ to deduce that there are at most $\Phi_r(N)\exp\Big(-\frac{1}{200}i^{3/5}\Big)$ such n. Summing over $\frac{1}{2}\sqrt{r} < i < \frac{1}{2}r$ gives

$$\ll \Phi_r(N)\exp\left(-\frac{1}{400}\mu^{3/10}\right).$$

The remaining $n \in S_r(N)$ satisfy

$$\left|\frac{1}{2}\log\log p_i - i\right| < i^{4/5} \text{ for every } \frac{1}{2}\sqrt{r} < i < \frac{1}{2}r. \tag{4.7}$$

Let $m = \lceil \frac{1}{2}\sqrt{r}\rceil - 1$ and $k = \lfloor \frac{1}{2}r\rfloor - 1$, so $p_1\cdots p_k \le \sqrt{N}$. We first bound the number of $n \in S_r(N)$ for which $p_i < p_{i+1} \le p_i^{a_i}$ for all $m \le i < k$, where $a_i = (i+1)^2(\log\mu)^{2\kappa}$. Apply Theorem 4.2 with the set E_1 containing the primes less than p_m and E_2 containing the primes greater than p_k and on numbers up to $\frac{N}{p_m\cdot\ldots\cdot p_k}$. We let $\mathcal{T}$ be the set of tuples $(p_m,\ldots,p_k)$ all consisting of primes not congruent to 3 modulo 4 such that $p_i < p_{i+1} \le p_i^{a_i}$ for all $m \le i < k$. Then the number of $n \in S_r(N)$ for which $p_i < p_{i+1} \le p_i^{a_i}$ for all $m \le i < k$ is at most

$$\ll \frac{N}{\log N}\sum_{(p_m,\ldots,p_k)\in\mathcal{T}}\frac{1}{p_m\cdots p_k}\cdot\frac{\Big(\mu-\frac{1}{2}\log\log p_k + B\Big)^{r-k}}{(r-k)!}\cdot\frac{\Big(\frac{1}{2}\log\log p_m + B\Big)^{m-1}}{(m-1)!}.$$

Now, fixing some $m \le i < k$, we obtain by partial summation on $\frac{1}{p_{i+1}}$ and the prime number theorem that

$$\sum_{\substack{p_i<p_{i+1}\le p_i^{a_i}\\ p_{i+1}\not\equiv 3 \bmod 4}}\frac{1}{p_{i+1}}\frac{\Big(\frac{1}{2}\log\log p_{i+1}\Big)^{r-i-1}}{(r-i-1)!}$$
$$= \frac{\Big(\frac{1}{2}\log\log p_i + \frac{1}{2}\log a_i\Big)^{r-i}}{(r-i)!} - \frac{\Big(\frac{1}{2}\log\log p_i\Big)^{r-i}}{(r-i)!} + O\Big(\exp(-c\sqrt{\log p_i})\Big).$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

Hence we deduce

$$\begin{aligned}
&\sum_{\substack{p_i<p_{i+1}\le p_i^{a_i}\\ p_{i+1}\not\equiv 3 \bmod 4}} \frac{1}{p_{i+1}} \frac{\left(\mu-\frac{1}{2}\log\log p_{i+1}+B\right)^{r-i-1}}{(r-i-1)!}\\
&=\frac{\left(\mu-\frac{1}{2}\log\log p_i+B\right)^{r-i}}{(r-i)!}-\frac{\left(\mu-\frac{1}{2}\log\log p_i-\frac{1}{2}\log a_i+B\right)^{r-i}}{(r-i)!}+O\Big(\exp(-c\sqrt{\log p_i})\Big)\\
&=\frac{\left(\mu-\frac{1}{2}\log\log p_i+B\right)^{r-i}}{(r-i)!}\left(1-\left(1-\frac{\frac{1}{2}\log a_i}{\mu-\frac{1}{2}\log\log p_i+B}\right)^{r-i}\right)+O\Big(\exp(-c\sqrt{\log p_i})\Big).
\end{aligned}$$

Furthermore, we have the lower bound

$$\left(1-\frac{\frac{1}{2}\log a_i}{\mu-\frac{1}{2}\log\log p_i+B}\right)^{r-i}\ge a_i^{-\frac{1}{2}-2\mu^{-1/5}}.$$

Applying this repeatedly for $i=k-1,k-2,\dots,m$, we obtain the upper bound

$$\Phi_r(N)\prod_{m\le i<k}\left(1-\frac{1}{((i+1)\cdot(\log\mu)^{\kappa})^{1+4\mu^{-1/5}}}\right)\ll_\epsilon \Phi_r(N)\exp\Big(-(\log\mu)^{1-\kappa(1+\epsilon)}\Big).$$

It follows that other than $\ll_\epsilon \Phi_r(N)\exp\big(-(\log\mu)^{1-\kappa(1+\epsilon)}\big)$ exceptions, we have

$$p_{i-1}^{i^2(\log\mu)^{2\kappa}}<p_i \text{ for some } \frac{1}{2}\sqrt{r}<i<\frac{1}{2}r. \tag{4.8}$$

For the remaining $n\in S_r(N)$, we have equations (4.7) and (4.8), which implies

$$\max_{\frac{1}{2}\sqrt{r}<i<\frac{1}{2}r}\log\log p_i-\log\log p_{i-1}-2\log\log\log p_i>2\kappa\log\log\mu-2.$$

It remains to remove $n\in S_r(N)$ for which there exists some $\frac{1}{2}\sqrt{r}\le i<\frac{1}{2}r$ such that $p_i^{a_i}<p_{i+1}$ and

$$\sum_{j=1}^{i}\log p_j>(\log\mu)^{1-\kappa}\log p_i.$$

Rewrite the second condition as $p_i^u<p_1\cdots p_{i-1}$, where $u:=(\log\mu)^{1-\kappa}-1$. We wish to bound

$$\begin{aligned}
&\sum_{\substack{p_i\equiv 1 \bmod 4\\ (4.7)}}\ \sum_{\substack{p_1<\cdots<p_i\\ p_1\cdots p_{i-1}>p_i^u\\ p_j\not\equiv 3 \bmod 4}}\ \sum_{\substack{p_i^{a_i}<p_{i+1}<\cdots<p_r\\ p_{i+1}\cdots p_r<\frac{N}{p_1\cdots p_i}\\ p_j\not\equiv 3 \bmod 4}} 1\\
&\qquad\ll\frac{N}{\log N}\sum_{\substack{p_i\equiv 1 \bmod 4\\ (4.7)}}\frac{\left(\mu-\frac{1}{2}\log\log p_i-\frac{1}{2}\log a_i+B\right)^{r-i}}{p_i(r-i)!}\sum_{\substack{p_1<\cdots<p_i\\ p_1\cdots p_{i-1}>p_i^u\\ p_j\not\equiv 3 \bmod 4}}\frac{1}{p_1\cdots p_{i-1}}.
\end{aligned} \tag{4.9}$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

Fix a given p_i with $\left|\frac{1}{2}\log\log p_i - i\right| < i^{4/5}$, and fix x with $p_i^u < x < \min\{p_i^{i-1}, N\}$. By Lemma 4.3, we have

$$\sum_{\substack{p_1<\cdots<p_{i-1}<p_i\\ x<p_1\cdots p_{i-1}\le 2x\\ p_j\not\equiv 3 \bmod 4}} \frac{1}{p_1\cdots p_{i-1}} \le \frac{1}{x}|\Psi_{i-1}(2x,p_i)| \ll \frac{v^{-v}}{\log p_i}\cdot\frac{(\frac{1}{2}\log\log p_i)^{i-1}}{(i-1)!},$$

where $v := \log x/\log p_i$. To deal with final part of the sum in equation (4.9), split (p_i^u, p_i^{i-1}) into dyadic intervals of the form $(x, 2x]$; then

$$\sum_{\substack{p_1<\cdots<p_i\\ p_1\cdots p_{i-1}>p_i^u\\ p_j\not\equiv 3 \bmod 4}} \frac{1}{p_1\cdots p_{i-1}} \ll \frac{1}{\log p_i}\cdot\frac{(\frac{1}{2}\log\log p_i)^{i-1}}{(i-1)!}\sum_{\substack{k\ge 0\\ x=2^k p_i^u}} v^{-v}$$

$$\ll \frac{(\frac{1}{2}\log\log p_i)^{i-1}}{(i-1)!}\int_{v>u} v^{-v}\,dv \ll u^{-u}\frac{\left(\frac{1}{2}\log\log p_i\right)^{i-1}}{(i-1)!}.$$

Therefore, equation (4.9) becomes

$$\ll \frac{Nu^{-u}}{\log N}\sum_{\substack{p_i\equiv 1 \bmod 4\\ (4.7)}}\frac{1}{p_i}\cdot\frac{\left(\mu-\frac{1}{2}\log\log p_i\right)^{r-i}}{(r-i)!}\cdot\frac{(\frac{1}{2}\log\log p_i)^{i-1}}{(i-1)!}\left(1-\frac{\frac{1}{2}\log a_i}{\mu-\frac{1}{2}\log\log p_i+B}\right)^{r-i}$$

$$\ll \frac{N}{\log N}\cdot\frac{u^{-u}}{a_i^{1/2+2\mu^{-1/5}}}\sum_{\substack{p_i\equiv 1 \bmod 4\\ (4.7)}}\frac{1}{p_i}\cdot\frac{\left(\mu-\frac{1}{2}\log\log p_i\right)^{r-i}}{(r-i)!}\cdot\frac{(\frac{1}{2}\log\log p_i)^{i-1}}{(i-1)!} \ll \frac{u^{-u}\Phi_r(N)}{a_i^{1/2+2\mu^{-1/5}}}.$$

Summing over $\frac{1}{2}\sqrt{r} < i < \frac{1}{2}r$, the total number of such n is

$$\ll \Phi_r(N)\exp\left(-2(\log\mu)^{1-\kappa}\right)\sum_{\frac{1}{2}r^{1/2}<i<\frac{1}{2}r}\frac{1}{i} \ll \Phi_r(N)\exp\left(-(\log\mu)^{1-\kappa}\right),$$

which completes the proof of the theorem.

5. Equidistribution of Legendre symbol matrices

We will use the two following propositions from Section 6 of Smith [18].

Proposition 5.1. *Suppose $L/\mathbb{Q}$ is Galois of degree d and $K/\mathbb{Q}$ is an elementary abelian extension, and $\gcd(\Delta_L, \Delta_K) = 1$. Let K_0 be a quadratic subfield of K with maximal discriminant $|\Delta_{K_0}|$. Let $G := \mathrm{Gal}(KL/\mathbb{Q})$ be a 2-group. Take $F : G \to [-1, 1]$ to be a class function with average 0 over G. Then there exists an absolute constant $c > 0$ such that*

$$\sum_{p\le x} F\left(\left(\frac{KL/\mathbb{Q}}{p}\right)\right)\log p \ll x^{\beta}|G| + x|G|(d^2\log|x\Delta_{K_0}\Delta_L|)^4\exp\left(\frac{-cd^{-4}\log x}{\sqrt{\log x}+3d\log|\Delta_{K_0}\Delta_L|}\right)$$

for $x \ge 3$, where β is the maximal real zero of any Artin L-function defined for G.

Proof. This follows from the Chebotarev density theorem; see [18, Proposition 6.5]. □

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

Proposition 5.2. *Let X_1 and X_2 be disjoint sets of odd primes with its elements bounded by t_1 and t_2, respectively. Then for any $\epsilon > 0$, we have*

$$\sum_{x_1 \in X_1} \left| \sum_{x_2 \in X_2} \left(\frac{x_1}{x_2} \right) \right| \ll_\epsilon t_1 t_2^{3/4+\epsilon} + t_2 t_1^{3/4+\epsilon}.$$

Proof. This is an easy consequence of the large sieve inequality stated in the work of Jutila [12, Lemma 3]; see Proposition 6.6 in Smith [18]. □

We shall not work with all squarefree integers simultaneously but instead work with more restricted sets of squarefree integers that have extra combinatorial structure. In our next definition, we define this combinatorial structure, which we call preboxes.

Definition 5.3. Take a sequence of real numbers

$$0 < s_1 < t_1 < s_2 < t_2 < \cdots < s_r < t_r.$$

Take $P, X_1, \ldots, X_r$ to be disjoint sets of primes not congruent to 3 mod 4 so that $X_i \subset (s_i, t_i)$. Define $X := X_1 \times \cdots \times X_r$. We call the pair (X, P) a prebox.

The goal of this section is to prove a weak equidistribution statement regarding matrices of Jacobi symbols associated to each $x \in X$. To make sense of this, we first need to define how we attach a matrix of Jacobi symbols to each $x \in X$, which we shall do now. We will often implicitly identify $\mathbb{F}_2$ with $\{\pm 1\}$ in this section. We use $\sqcup$ to denote disjoint union and $[r]$ to denote the set $\{1, \ldots, r\}$.

Definition 5.4. Let (X, P) be a prebox. Take $\mathcal{M} \subseteq \{(i, j) : 1 \le i < j \le r\}$ and $\mathcal{N} \subseteq P \times [r]$. Define $M : X \to \mathbb{F}_2^{\mathcal{M} \sqcup \mathcal{N}}$ as follows:

$$M(x_1, \ldots, x_r) : \mathcal{M} \sqcup \mathcal{N} \to \{\pm 1\} \qquad M(x_1, \ldots, x_r)(\mathbf{m}) = \begin{cases} \left(\frac{x_i}{x_j} \right) & \text{if } \mathbf{m} = (i, j) \in \mathcal{M} \\ \left(\frac{p}{x_j} \right) & \text{if } \mathbf{m} = (p, j) \in \mathcal{N}. \end{cases}$$

Denote $\mathcal{N}_j := \{(p, j) \in \mathcal{N} : p \in P\}$. Let $M_j : X_j \to \mathbb{F}_2^{\mathcal{N}_j}$ be the function defined by

$$M_j(x_j) : \mathcal{N}_j \to \{\pm 1\} \qquad M_j(x_j)(p, j) = \left(\frac{p}{x_j} \right).$$

For any $a : \mathcal{M} \sqcup \mathcal{N} \to \{\pm 1\}$, define

$$X(a) := \{x \in X : M(x) = a\}$$

and $X_j(a, P) := \{x_j \in X_j : M_j(x_j) = a \restriction_{\mathcal{N}_j}\}$, where $\restriction$ is restriction of functions. Let $Y \subseteq X$ be a subset, let $S \subseteq [r]$, and let $Q \in \prod_{i \in S} X_i$. We put

$$Y(Q) := \{y \in Y : \pi_S(y) = Q\}.$$

We shall slightly abuse notation by writing $X(a, Q)$ for $X(a)(Q)$.

Ideally, we would like to prove that $X(a)$ is of the expected size: that is,

$$|X(a)| = \frac{|X|}{2^{|\mathcal{M}| + |\mathcal{N}|}}.$$

Instead, we shall prove a weaker equidistribution statement that allows for permutations of the first few rows and columns.

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

Definition 5.5. Let $\mathcal{P}(r)$ denote the set of permutations of $[r]$. For any $\sigma \in \mathcal{P}(r)$, any prebox (X, P) and any $a : \mathcal{M} \sqcup \mathcal{N} \to \{\pm 1\}$, define

$$X(\sigma, a) = \{x \in X : M(\sigma(x)) = a\},$$

where $\sigma(x) = \sigma(x_1, \ldots, x_r) = (x_{\sigma(1)}, \ldots, x_{\sigma(r)})$.

Finally, there is the well-known problem of Siegel zeroes that we need to take care of. This prompts the following definition.

Definition 5.6. For $c > 0$, take $\mathcal{S}(c)$ to be the set of (possibly negative) squarefree integers d so that

$$L(s, \chi_d) = 0 \text{ for some } 1 - \frac{c}{\log(|d| + 4)} \le s \le 1.$$

List the elements in $\mathcal{S}(c)$ as $|d_1| \le |d_2| \le \cdots$. By Landau's theorem, fix an absolute c sufficiently small so that $d_i^2 \le |d_{i+1}|$ for all $i \ge 1$. We say that a prebox (X, P) is Siegel-less above t if

$$\left\{ \epsilon \prod_{i \in S} \pi_i(x) \prod_{p \in \tilde{P}} p : x \in X, \epsilon \in \{\pm 1\}, \tilde{P} \subseteq P, S \subseteq [r], \left| \epsilon \prod_{i \in S} \pi_i(x) \prod_{p \in \tilde{P}} p \right| > t \right\} \cap \mathcal{S}(c) = \varnothing.$$

We are now ready to prove our first proposition, which shows that $X(a)$ is of the expected size for sufficiently regular preboxes (X, P) and sufficiently nice $\mathcal{M}$ and $\mathcal{N}$. It is directly based on Proposition 6.3 in Smith [18].

Proposition 5.7. *Fix positive constants $c_1, \ldots, c_6$ such that $c_2c_3 + 2c_4 + c_5 < \frac{1}{4}$ and $c_6 > 3$. Take $\delta > 0$ satisfying $2\delta < \frac{1}{4} - c_2c_3 - 2c_4 - c_5$; then the following holds for any large enough D_1. Let (X, P) be a prebox with parameters $D_1 < s_1 < t_1 < s_2 < t_2 < \cdots < s_r < t_r$. Take $1 \le k \le r$. Let $\mathcal{M} \subseteq \{(i, j) : 1 \le i < j \le r\}$ and $\mathcal{N} \subseteq P \times \{k + 1, \ldots, r\}$. Suppose that*

$$X_j := \{x_j \in (s_j, t_j) \text{ prime } : x_j \equiv 1 \bmod 4,\ M_j(x_j) = a \restriction_{\mathcal{N}_j}\} \quad \text{if } j > k.$$

Assume

1. *(X, P) is Siegel-less above D_1;*
2. *$|P| \le \log t_i - i$ for all $1 \le i \le r$ and $p \in P$ implies $p < s_1$;*
3. *$\log t_{k+1} > \max\{(\log t_1)^{c_6}, D_1^{c_1}\}$ if $k < r$, and $\log t_k < t_1^{c_2}$;*
4. *$|X_i| \ge e^i t_i (\log t_i)^{-c_3}$ for all $1 \le i \le r$;*
5. *$r < t_1^{c_4}$;*
6. *for each $1 \le i \le r$, $j_i := 1 + i + \lfloor c_5 \log t_i \rfloor$ satisfy $j_1 > k$, and $\log t_{j_i} > (\log t_i)^{c_6}$ if $j_i \le r$.*

Then for all $a : \mathcal{M} \sqcup \mathcal{N} \to \{\pm 1\}$,

$$\left| |X(a)| - 2^{-|\mathcal{M}|}|X| \right| \le t_1^{-\delta} \cdot 2^{-|\mathcal{M}|}|X|.$$

Proof. Let $\kappa := c_4 + \delta$. Since $r < t_1^{c_4}$, it suffices to show that

$$\left| |X(a)| - 2^{-|\mathcal{M}|}|X| \right| \le r t_1^{-\kappa} \cdot 2^{-|\mathcal{M}|}|X|.$$

We proceed by induction on r. Define

$$X_j(a, x_1) := \left\{ x_j \in X_j : \left(\frac{x_1}{x_j} \right) = a(1, j) \text{ if } (1, j) \in \mathcal{M} \right\}.$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

First consider $(1, j) \in \mathcal{M}$, where $j > k$. Apply Proposition 5.1 to

$$K = \mathbb{Q}(\sqrt{-1}, \sqrt{p} : p \in P), \quad L = \mathbb{Q}(\sqrt{x_1})$$

and

$$F : \sigma \mapsto \begin{cases} 1 - 2^{-|P|-2} & \text{if } \sigma = \left(\frac{KL/\mathbb{Q}}{x_j}\right) \text{ for some } x_j \in X_j(a, x_1), \\ -2^{-|P|-2} & \text{otherwise.} \end{cases}$$

Notice that $\left(\frac{KL/\mathbb{Q}}{x_j}\right)$ is independent of the choice $x_j \in X_j(a, x_1)$. By Siegel's theorem, for D_1 sufficiently large, we have $1 - \beta > D_1^{-c_1/6}$ if β is an exceptional real zero of $L(s, \chi_d)$ with $|d| < D_1$. Then

$$t_j^\beta < t_j \exp\left(-(\log t_j)^{5/6}\right).$$

We have the bounds

$$\log |\Delta_{K_0}\Delta_L| \ll |P| \log t_1 \leq (\log t_1)^2 \ll (\log t_j)^{\frac{2}{c_6}}$$

and

$$|\operatorname{Gal}(KL/\mathbb{Q})| = 2^{|P|+2} \leq 2^{1+\log t_1} < t_1 < \exp\left((\log t_j)^{\frac{1}{c_6}}\right).$$

Since $c_6 > 3$, we have by a double application of Proposition 5.1 and partial summation

$$\left| \sum_{s_j < p < t_j} F\left(\left(\frac{KL/\mathbb{Q}}{p}\right)\right) \right| \leq t_j \exp\left(-(\log t_j)^{1/3}\right)$$

for sufficiently large D_1. Repeating this for the field $K/\mathbb{Q}$, we get after possibly enlarging D_1

$$\left| |X_j(a, x_1)| - \frac{1}{2}|X_j| \right| \leq 2t_j \exp\left(-(\log t_j)^{1/3}\right) < t_1^{-1}|X_j|.$$

Next consider $(1, j) \in \mathcal{M}$, where $j \leq k$. Note that $\frac{1}{4} - c_2c_3 - c_5 - 2\kappa > 0$ by assumption, so we can fix a positive constant ϵ such that $2\epsilon < \frac{1}{4} - c_2c_3 - c_5 - 2\kappa$. The large sieve in Proposition 5.2 gives

$$\sum_{x_1 \in X_1} \left| \sum_{x_j \in X_j} \left(\frac{x_1}{x_j}\right) \right| \ll_\epsilon t_j t_1^{3/4+\epsilon}.$$

From the identity

$$|X_j(a, x_1)| = \frac{1}{2} \sum_{x_j \in X_j} \left(a(1, j)\left(\frac{x_1}{x_j}\right) + 1 \right) = \frac{a(1, j)}{2} \sum_{x_j \in X_j} \left(\frac{x_1}{x_j}\right) + \frac{1}{2}|X_j|,$$

we deduce that for sufficiently large D_1,

$$\sum_{x_1 \in X_1} \left| |X_j(a, x_1)| - \frac{1}{2}|X_j| \right| = \frac{1}{2} \sum_{x_1 \in X_1} \left| \sum_{x_j \in X_j} \left(\frac{x_1}{x_j}\right) \right| \leq t_1^{-\frac{1}{4}+c_2c_3+\epsilon} |X_1||X_j|.$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

Let $B_1 := c_5 + \kappa$ and $B_2 := \kappa + \epsilon$; then $B_1 + B_2 < \frac{1}{4} - c_2c_3 - \epsilon$. We conclude that

$$\left| |X_j(a, x_1)| - \frac{1}{2}|X_j| \right| < t_1^{-B_2}|X_j| \text{ for all } (1, j) \in \mathcal{M} \text{ and } j \le k$$

holds with at most $kt_1^{-B_1}|X_1|$ exceptions $x_1 \in X$. Call the set of exceptions $X_1^{\mathrm{bad}}(a)$.

We bound the size of the set of exceptions $X^{\mathrm{bad}}(a) = X(a) \cap \pi_1^{-1}(X_1^{\mathrm{bad}}(a))$ in X. First, fix some $x_1 \in X_1$ and move x_1 to P. Apply the induction hypothesis to

$$X_2 \times X_3 \times \cdots \times X_k \times X_{k+1}(a, x_1) \times \cdots \times X_r(a, x_1).$$

Let us briefly explain the value of k to which we apply the induction hypothesis. Let k_{old} be the current value of k, and let k_{new} be the value of k to which we apply the induction hypothesis. We choose k_{new} as the smallest integer satisfying

$$k_{\mathrm{new}} \ge k_{\mathrm{old}} - 1, \quad t_{k_{\mathrm{new}}+2} > \max(e^{(\log t_2)^{c_6}}, e^{D_1^{c_1}}),$$

and we choose $k_{\mathrm{new}} = r - 1$ if there is no such integer.

Since $t_1 > r^{c_4}$ with $c_4 < \frac{1}{8}$, we get

$$|X(a) \cap \pi_1^{-1}(x_1)| \le \left(1 + \frac{2}{t_1}\right)^r \cdot 2^{-|\mathcal{M}|+k} \frac{|X|}{|X_1|} \le 2^{-|\mathcal{M}|+k+1} \frac{|X|}{|X_1|}$$

and hence

$$|X^{\mathrm{bad}}(a)| \le 2^{k+1} k t_1^{-B_1} \cdot 2^{-|\mathcal{M}|}|X| < 2^{j_1+1} j_1 t_1^{-B_1} \cdot 2^{-|\mathcal{M}|}|X| < t_1^{-\kappa} \cdot \frac{|X|}{2^{|\mathcal{M}|+1}}. \tag{5.1}$$

For $x_1 \notin X^{\mathrm{bad}}(a)$, we look at

$$X_2(a, x_1) \times \cdots \times X_r(a, x_1).$$

Then we obtain

$$\begin{aligned} |X(a) \setminus X^{\mathrm{bad}}(a)| &= \sum_{x_1 \in X_1 \setminus X_1^{\mathrm{bad}}(a)} |X(a) \cap \pi_1^{-1}(x_1)| \\ &= \sum_{x_1 \in X_1 \setminus X_1^{\mathrm{bad}}(a)} |(X_2(a, x_1) \times \cdots \times X_r(a, x_1))(a)|, \end{aligned}$$

which lies between

$$\left(1 \pm \frac{2}{t_1}\right)^r \left(1 \pm \frac{2}{t_1^{B_2}}\right)^k (1 \pm (r-1)t_1^{-\kappa}) \cdot 2^{-|\mathcal{M}|}|X|$$

by the induction hypothesis. Since $r < t_1^{c_4} < t_1^{\kappa}$, $1 - c_4 > \kappa$ and $B_2 > \kappa$, we have

$$\begin{aligned} \left(1 + \frac{2}{t_1}\right)^r \left(1 + \frac{2}{t_1^{B_2}}\right)^k \frac{1 + (r-1)t_1^{-\kappa}}{1 + (r - \frac{1}{2})t_1^{-\kappa}} &= \left(1 + \frac{2}{t_1}\right)^r \left(1 + \frac{2}{t_1^{B_2}}\right)^k \left(1 - \frac{\frac{1}{2}t_1^{-\kappa}}{1 + (r - \frac{1}{2})t_1^{-\kappa}}\right) \\ &< \exp\left(2rt_1^{-1} + 2kt_1^{-B_2} - \frac{1}{4}t_1^{-\kappa}\right) < \exp\left(2t_1^{-(1-c_4)} + 2c_5t_1^{-B_2}\log t_1 - \frac{1}{4}t_1^{-\kappa}\right) < 1 \end{aligned}$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

and similarly

$$\left(1-\frac{2}{t_1}\right)^r\left(1-\frac{2}{t_1^{B_2}}\right)^k\frac{1-(r-1)t_1^{-\kappa}}{1-(r-\frac{1}{2})t_1^{-\kappa}}=\left(1-\frac{2}{t_1}\right)^r\left(1-\frac{2}{t_1^{B_2}}\right)^k\left(1+\frac{\frac{1}{2}t_1^{-\kappa}}{1-(r-\frac{1}{2})t_1^{-\kappa}}\right)>1.$$

We conclude that the sum lies between

$$\left(1\pm\left(r-\frac{1}{2}\right)t_1^{-\kappa}\right)\cdot 2^{-|\mathcal{M}|}|X|. \tag{5.2}$$

Adding the contributions from equations (5.1) and (5.2) completes the inductive step. □

The condition $\mathcal{N}\subseteq P\times\{k+1,\ldots,r\}$ in Proposition 5.7 turns out to be too restrictive for us. It is, however, not so straightforward to remove this condition. Hence we shall only prove a weaker equidistribution statement that allows for permutations of the first few columns. This weaker equidistribution statement will fall as a consequence of Proposition 5.7 and the following combinatorial proposition, which is Proposition 6.7 of Smith [18].

Proposition 5.8. *Let (X,P) be a prebox. Let $\mathcal{M}=\{(i,j):1\le i<j\le r\}$ and $\mathcal{N}=P\times[r]$. Take $0\le k_0\le k_1\le k_2\le r$ so that*

$$2^{|P|+k_0+1}k_1^2<k_2.$$

Let $\sigma\in\mathcal{P}(r)$. Define

$$S(\sigma):=\{(i,j)\in\mathcal{M}:(\sigma(i),\sigma(j))\in([k_0]\times[k_1])\cup([k_1]\times[k_0])\}\sqcup\{(p,j)\in\mathcal{N}:\sigma(j)\in[k_1]\}.$$

Let $m:=|S(\sigma)|=k_1|P|+\frac{1}{2}k_0(k_0-1)+k_0(k_1-k_0)$. If $a:\mathcal{M}\sqcup\mathcal{N}\to\{\pm1\}$, we put

$$X_S(\sigma,a):=\left\{x\in X:M(\sigma(x))\restriction_{S(\sigma)}=a\restriction_{S(\sigma)}\right\}.$$

For any $x\in X$, define

$$W(x,a):=\{\sigma\in\mathcal{P}(k_2):x\in X_S(\sigma,a)\}=\{\sigma\in\mathcal{P}(k_2):M(\sigma(x))\restriction_{S(\sigma)}=a\restriction_{S(\sigma)}\}.$$

Then we have

$$\sum_{a\in\mathbb{F}_2^{\mathcal{M}\sqcup\mathcal{N}}}||W(x,a)|-2^{-m}\cdot k_2!|\le\left(\frac{2^{|P|+k_0+1}}{k_2}\right)^{1/2}k_1\cdot 2^{-m+|\mathcal{M}\sqcup\mathcal{N}|}\cdot k_2!.$$

Proof. Fix some $x\in X$, and write $W(a):=W(x,a)$. We will show that

$$\sum_{a\in\mathbb{F}_2^{\mathcal{M}\sqcup\mathcal{N}}}(|W(a)|-2^{-m}\cdot k_2!)^2\le\frac{2^{|P|+k_0+1}k_1^2}{k_2}\cdot 2^{-2m+|\mathcal{M}\sqcup\mathcal{N}|}(k_2!)^2.$$

Then the proposition follows from the Cauchy-Schwarz inequality.

The average of $|W(a)|$ over a is $2^{-m}\cdot k_2!$, since $|\mathcal{P}(k_2)|=k_2!$ and there are m Legendre symbol conditions to satisfy. Now

$$|W(a)|^2=|\{(\sigma_1,\sigma_2)\in\mathcal{P}(k_2)\times\mathcal{P}(k_2):M(\sigma_1(x))\restriction_{S(\sigma_1)}=a\restriction_{S(\sigma_1)},\ M(\sigma_2(x))\restriction_{S(\sigma_2)}=a\restriction_{S(\sigma_2)}\}|.$$

We have $\sum_{a \in \mathbb{F}_2^{\mathcal{M} \sqcup \mathcal{N}}} |W(a)|^2 = \sum_{\sigma_1, \sigma_2 \in \mathcal{P}(k_2)} |W(\sigma_1, \sigma_2)|$, where

$$W(\sigma_1, \sigma_2) := \{a \in \mathbb{F}_2^{\mathcal{M} \sqcup \mathcal{N}} : M(\sigma_1(x)) \restriction_{S(\sigma_1)} = a \restriction_{S(\sigma_1)},\ M(\sigma_2(x)) \restriction_{S(\sigma_2)} = a \restriction_{S(\sigma_2)}\}.$$

We fix some $\sigma_1, \sigma_2 \in \mathcal{P}(k_2)$ and bound $|W(\sigma_1, \sigma_2)|$. Let $d := |\{i \in [k_2] : \sigma_1(i) \leq k_1,\ \sigma_2(i) \leq k_1\}|$. We have

$$\begin{aligned} |S(\sigma_1) \cap S(\sigma_2)| = |\{(i,j) \in \mathcal{M} : (\sigma_1(i), \sigma_1(j)),\ (\sigma_2(i), \sigma_2(j)) \in ([k_0] \times [k_1]) \cup ([k_1] \times [k_0])\}| \\ + |\{(p,j) \in \mathcal{N} : \sigma_1(j),\ \sigma_2(j) \in [k_1]\}| \leq d(|P| + k_0). \end{aligned}$$

Therefore the conditions fix at least $2m - d(|P| + k_0)$ arguments of $a \in W(\sigma_1, \sigma_2)$. Then

$$|W(\sigma_1, \sigma_2)| \leq 2^{-2m + d(|P| + k_0) + |\mathcal{M} \sqcup \mathcal{N}|}.$$

Given some $d \leq k_1$, we bound the number of $(\sigma_1, \sigma_2) \in \mathcal{P}(k_2) \times \mathcal{P}(k_2)$ that gives the same d. There are $\binom{k_2}{d}$ ways to pick the indices that map to $[k_1]$ under σ_1 and σ_2. Then there are at most $(\frac{k_1!}{(k_1-d)!}(k_2 - d)!)^2$ ways to pick a pair of (σ_1, σ_2) in such a way. Hence the total number is bounded by

$$\binom{k_2}{d}\left(\frac{k_1!}{(k_1 - d)!}(k_2 - d)!\right)^2 \leq (k_2!)^2 \left(\frac{k_1!}{(k_1 - d)!}\right)^2 \frac{(k_2 - d)!}{k_2!} \leq (k_2!)^2 \left(\frac{k_1^2}{k_2}\right)^d.$$

The average of $|W(a)|^2$ is bounded by

$$(k_2!)^2 \sum_{d \geq 0} \left(\frac{k_1^2}{k_2}\right)^d \cdot 2^{-2m + d(|P| + k_0)} = \frac{k_2}{k_2 - 2^{|P| + k_0} k_1^2} \cdot 2^{-2m} (k_2!)^2.$$

Then the variance of $|W(a)|$ is bounded by

$$\begin{aligned} \frac{k_2}{k_2 - 2^{|P| + k_0} k_1^2} \cdot 2^{-2m} (k_2!)^2 - (2^{-m} \cdot k_2!)^2 &= \frac{2^{|P| + k_0} k_1^2}{k_2 - 2^{|P| + k_0} k_1^2} \cdot 2^{-2m} (k_2!)^2 \\ &\leq \frac{2^{|P| + k_0 + 1} k_1^2}{k_2} \cdot 2^{-2m} (k_2!)^2. \end{aligned}$$

Multiplying by $2^{|\mathcal{M} \sqcup \mathcal{N}|}$ gives the required estimate. □

We are now ready to prove our weak equidistribution result for $|X(a)|$, which is very similar to Theorem 6.4 in Smith [18]. We define $a(i,j) := a(j,i)$ in case $i > j$.

Theorem 5.9. *Take positive constants $c_1, \ldots, c_8$, where $c_2 c_3 + 2c_4 + c_5 < \frac{1}{4}$, $c_6 > 3$ and $c_8 < c_7 < \frac{1}{2}$. Let (X, P) be a prebox, and suppose that for all $1 \leq j \leq r$,*

$$X_j := \{x_j \in (s_j, t_j) \text{ prime} : x_j \equiv 1 \bmod 4\}.$$

The following holds for any large enough D_1. Choose integers $0 \leq k_0 < k_1 < k_2 \leq r$, and assume $t_{k_0+1} > D_1$ and $k_2 > D_1$. Assume

1. *$\log k_1 < c_8 \log k_2$;*
2. *$(|P| + k_0) \log 2 < (1 - 2c_7) \log k_2$.*

Further assume

1. *(X, P) is Siegel-less above D_1;*
2. *$|P| \leq \log t_i - i$ for all $k_0 < i \leq r$ and $p \in P$ implies $p < s_{k_0+1}$;*

3. *$\log t_{k_1+1} > \max\{(\log t_{k_0+1})^{c_6}, D_1^{c_1}\}$ and $\log t_{k_1} < t_1^{c_2}$;*
4. *$|X_i| \geq 2^{|P|} e^i k_2^{c_7} t_i (\log t_i)^{-c_3}$ for all $k_0 < i \leq r$;*
5. *$r < t_{k_0+1}^{c_4}$;*
6. *for each $k_0 < i \leq r$, $j_i := 1 + i + \lfloor c_5 \log t_i \rfloor$ satisfy $j_{k_0+1} > k_1$, and $\log t_{j_i} > (\log t_i)^{c_6}$ if $j_i \leq r$.*

Take $\delta_1 < c_7 - c_8$ and $2\delta_2 < \frac{1}{4} - c_2 c_3 - 3c_4 - c_5$. Then for any $\mathcal{M}$ and $\mathcal{N}$, we have

$$\sum_{a \in \mathbb{F}_2^{\mathcal{M} \sqcup \mathcal{N}}} \left| 2^{-|\mathcal{M} \sqcup \mathcal{N}|} \cdot k_2! \cdot |X| - \sum_{\sigma \in \mathcal{P}(k_2)} |X(\sigma, a)| \right| \leq (k_2^{-\delta_1} + t_{k_0+1}^{-\delta_2}) \cdot k_2! \cdot |X|.$$

Proof. Without loss of generality, assume that $\mathcal{M} = \{(i,j) : 1 \leq i < j \leq r\}$ and $\mathcal{N} = P \times [r]$, $X_i = \{x_i\}$ for $i \leq k_0$. Let $m := k_1|P| + \frac{1}{2}k_0(k_0 - 1) + k_0(k_1 - k_0)$ as in Proposition 5.8. Apply the triangle inequality to the sum we wish to bound,

$$\begin{aligned} 2^{-|\mathcal{M} \sqcup \mathcal{N}|} \sum_{a \in \mathbb{F}_2^{\mathcal{M} \sqcup \mathcal{N}}} \left| k_2! \cdot |X| - 2^m \sum_{\sigma \in \mathcal{P}(k_2)} |X_S(\sigma, a)| \right| & \\ + 2^{-|\mathcal{M} \sqcup \mathcal{N}| + m} \sum_{\sigma \in \mathcal{P}(k_2)} \sum_{a \in \mathbb{F}_2^{\mathcal{M} \sqcup \mathcal{N}}} \left| |X_S(\sigma, a)| - 2^{|\mathcal{M} \sqcup \mathcal{N}| - m} |X(\sigma, a)| \right|. & \quad (5.3) \end{aligned}$$

For the first sum in equation (5.3), noting that

$$\sum_{x \in X} |W(x, a)| = \sum_{\sigma \in \mathcal{P}(k_2)} |X_S(\sigma, a)|,$$

we obtain by Proposition 5.8 an upper bound

$$\left(\frac{2^{|P| + k_0 + 1}}{k_2} \right)^{1/2} k_1 \cdot k_2! \cdot |X| < k_2^{-\delta_1} \cdot k_2! \cdot |X|.$$

Now consider the second sum of equation (5.3). For each $\sigma \in \mathcal{P}(k_2)$, we can partition X into 2^m sets according to $\tilde{a} : S(\sigma) \to \{\pm 1\}$ as follows:

$$X_S(\sigma, \tilde{a}) = \{x_1\} \times \cdots \times \{x_{k_0}\} \times X_{k_0+1}(\tilde{a}, \tilde{P}) \times \cdots \times X_{k_1}(\tilde{a}, \tilde{P}) \times X_{k_1+1} \times \cdots \times X_r,$$

where $\tilde{P} = \{x_1\} \cup \cdots \cup \{x_{k_0}\} \cup P$ and $X_i(\tilde{a}, \tilde{P})$ is the subset of those $q \in X_i$ satisfying

$$\left(\frac{q}{x_j} \right) = \tilde{a}(\sigma^{-1}(i), \sigma^{-1}(j)) \text{ for } j \in [k_0] \text{ and } \left(\frac{q}{p} \right) = \tilde{a}(p, \sigma^{-1}(i)) \text{ for } p \in P.$$

We first bound the contribution of $\sigma \in \mathcal{P}(k_2)$ with $|X_i(\tilde{a}, \tilde{P})| < 2^{-|\tilde{P}|} k_2^{-c_7} |X_i|$ for some $\tilde{a} : S(\sigma) \to \{\pm 1\}$ and some $k_0 < i \leq k_1$ in the sum. For each $\sigma \in \mathcal{P}(k_2)$ and $k_0 < i \leq k_1$, we have the upper bound

$$\sum_{\tilde{a} : |X_i(\tilde{a}, \tilde{P})| \leq 2^{-|\tilde{P}|} k_2^{-c_7} |X_i|} |X_S(\sigma, \tilde{a})| \leq k_2^{-c_7} |X|.$$

For each $\tilde{a}$, there are $2^{|\mathcal{M}\sqcup\mathcal{N}|-m}$ many a satisfying $a\restriction_{S(\sigma)}=\tilde{a}$, so the contribution of such a is bounded by

$$\sum_{\sigma\in\mathcal{P}(k_2)}\sum_{k_0<i\leq k_1}\sum_{\tilde{a}:|X_i(\tilde{a},\tilde{P})|\leq 2^{-|\tilde{P}|}\cdot k_2^{-c_7}\cdot|X_i|}|X_S(\sigma,\tilde{a})|\leq k_1k_2^{-c_7}\cdot k_2!\cdot|X|<k_2^{-\delta_1}\cdot k_2!\cdot|X|.$$

For the remaining terms, we have $|X_i(\tilde{a},\tilde{P})|\geq 2^{-|\tilde{P}|}k_2^{-c_7}|X_i|$ for all $k_0<i\leq r$. Bound each summand by Proposition 5.7

$$\left||X_S(\sigma,a)|-2^{|\mathcal{M}\sqcup\mathcal{N}|-m}|X(\sigma,a)|\right|\leq t_{k_0+1}^{-\delta_2}|X_S(\sigma,a)|;$$

then summing over σ and a gives the required estimate. □

There is a final technical proposition that will be of key importance in our next section. First we need a definition.

Definition 5.10. Let (X,P) be a prebox, and let $S\subseteq[r]$. If $j\notin S$, we define for a subset $Z\subseteq\prod_{i\in S}X_i$

$$X_j(a,Z):=X_j(a,P)\cap\left\{x\in X_j:\ \text{for all } i\in S, Q\in Z \text{ we have }\left(\frac{x}{\pi_i(Q)}\right)=a(i,j)\right\}.$$

Note that this is a natural generalisation of $X_j(a,P)$ as defined in Definition 5.4.

Proposition 5.11. *Fix positive constants $c_1,\ldots,c_6$ such that $c_2c_3+2c_4+c_5<\frac{1}{4}$ and $c_6>3$. Take $\delta>0$ satisfying $2\delta<\frac{1}{4}-c_2c_3-2c_4-c_5$; then the following holds for any large enough D_1. Take P to be a set of prime numbers, none of them congruent to 3 modulo 4, and take $1\leq k\leq r$. Suppose $\mathcal{M}=\{(i,j):1\leq i<j\leq r\}$ and $\mathcal{N}=P\times\{k+1,\ldots,r\}$. Let (X,P) be a prebox with parameters $D_1<s_1<t_1<s_2<t_2<\cdots<s_r<t_r$ such that*

$$X_j:=\{x_j\in(s_j,t_j)\text{ prime }:x_j\equiv 1\bmod 4, M_j(x_j)=a\restriction_{\mathcal{N}_j}\}\quad\text{if } j>k.$$

Let $U,V\subseteq[r]$ be disjoint subsets such that $U\cup V=[l]$ for some l. Further assume

1. *(X,P) is Siegel-less above D_1;*
2. *$|P|\leq\log t_i-i$ for all $1\leq i\leq r$ and $p\in P$ implies $p<s_1$;*
3. *$\log t_{k+1}>\max\{(\log t_1)^{c_6},D_1^{c_1}\}$ if $k<r$, and $\log t_k<t_1^{c_2}$;*
4. *$|X_i|\geq e^it_i(\log t_i)^{-c_3}$ for all $1\leq i\leq r$;*
5. *$r<t_1^{c_4}$;*
6. *for each $1\leq i\leq r$, $j_i:=1+i+\lfloor c_5\log t_i\rfloor$ satisfy $j_1>k$ and $\log t_{j_i}>(\log t_i)^{c_6}$ if $j_i\leq r$;*
7. *$c_5\log t_u>r+10$ and $u>k$ for all $u\in U$.*

We say that $Q\in\pi_V(X)$ is poor if there is $u\in U$ such that

$$\left||X_u(a,Q)|-\frac{|X_u|}{2^{|V|}}\right|>t_1^{-c_4-\delta}|V||X_u|.$$

Then for all $a:\mathcal{M}\sqcup\mathcal{N}\to\{\pm1\}$,

$$\sum_{Q\in\pi_V(X)\text{ poor}}|X(a,Q)|\leq r\cdot t_1^{-c_4-\delta}\cdot\frac{|X|}{2^{|\mathcal{M}|}}.$$

Proof. We proceed by induction on $|V|$. The case $|V|=0$ is trivial. Let v be the smallest element in V. Define $\tilde{k}$ to be the k from the proposition if $v=1$, and define $\tilde{k}$ to be r if $v\neq 1$. Fix some $x\in X_v$. Put

$B_1 := c_4 + c_5 + \delta$ and $B_2 := c_4 + \delta$. Following the proof of Proposition 5.7, we get that

$$\left| |X_j(a,x)| - \frac{1}{2}|X_j| \right| < t_1^{-B_2}|X_j| \text{ for all } 1 \le j \le \tilde{k} \text{ with } j \ne v$$

holds for $x \in X_v$ with at most $\tilde{k}t_1^{-B_1}|X_v|$ exceptions, while for $j > \tilde{k}$, we always get

$$\left| |X_j(a,x)| - \frac{1}{2}|X_j| \right| < t_1^{-1}|X_j|.$$

Just as in the proof of Proposition 5.7, define $X_v^{\mathrm{bad}}(a)$ to be the set of exceptions. We split the sum in the proposition as

$$\begin{aligned}\sum_{Q \in \pi_V(X) \text{ poor}} |X(a,Q)| &= \sum_{\substack{Q \in \pi_V(X) \text{ poor} \\ \pi_v(Q) \notin X_v^{\mathrm{bad}}(a)}} |X(a,Q)| + \sum_{\substack{Q \in \pi_V(X) \text{ poor} \\ \pi_v(Q) \in X_v^{\mathrm{bad}}(a)}} |X(a,Q)| \\ &\le \sum_{\substack{Q \in \pi_V(X) \text{ poor} \\ \pi_v(Q) \notin X_v^{\mathrm{bad}}(a)}} |X(a,Q)| + \sum_{\substack{Q \in \pi_V(X) \\ \pi_v(Q) \in X_v^{\mathrm{bad}}(a)}} |X(a,Q)|. \qquad (5.4)\end{aligned}$$

We first treat the latter sum in equation (5.4). In the case $v = 1$, we apply Proposition 5.7 to the prebox

$$(X_2 \times \cdots \times X_k \times X_{k+1}(a,x) \times \cdots \times X_r(a,x), P \cup \{x\})$$

for $x \in X_1^{\mathrm{bad}}(a)$ and the natural restrictions of a, U, V, $\mathcal{M}$ and $\mathcal{N}$. Then the latter sum is bounded by

$$\sum_{\substack{Q \in \pi_V(X) \\ \pi_1(Q) \in X_1^{\mathrm{bad}}(a)}} |X(a,Q)| = \sum_{x \in X_1^{\mathrm{bad}}(a)} |X(a) \cap \pi_1^{-1}(x)| \le |X_1^{\mathrm{bad}}(a)| \cdot 2^{-|\mathcal{M}|+k+1} \frac{|X|}{|X_1|}.$$

A small computation shows that this is at most

$$t_1^{-c_4-\delta} \cdot \frac{|X|}{2^{|\mathcal{M}|+1}}$$

for sufficiently large D_1. Now suppose that $v \ne 1$ so that $1 \in U$. Then apply Proposition 5.7 with $k = r - 1$, the prebox

$$(X_1 \times \cdots \times X_{v-1} \times X_{v+1} \times \cdots \times X_r, \emptyset)$$

and the natural restrictions of a, U, V, $\mathcal{M}$ and $\mathcal{N}$. Crucially, we have that this choice of k satisfies the requirements of Proposition 5.7 for sufficiently large D_1 due to our assumption $c_5 \log t_u > r + 10$ for all $u \in U$. Then a similar computation shows that the latter sum is again at most

$$t_1^{-c_4-\delta} \cdot \frac{|X|}{2^{|\mathcal{M}|+1}}.$$

It remains to bound the former sum in equation (5.4). We first treat the case $v = 1$. Take a poor $Q \in \pi_V(X)$ with $x := \pi_1(Q) \notin X_1^{\mathrm{bad}}(a)$. Then we claim that $\pi_{V-\{1\}}(Q)$ is poor for the prebox

$$(X_2(a,x) \times \cdots \times X_r(a,x), P \cup \{x\}).$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

Suppose that $\pi_{V-\{1\}}(Q)$ is not poor. Then we get for all $u \in U$ that

$$\left| |X_u(a,Q)| - \frac{|X_u(a,x)|}{2^{|V|-1}} \right| \leq t_2^{-B_2}(|V|-1)|X_u|.$$

But from this, we deduce that for all $u \in U$,

$$\begin{aligned}\left| |X_u(a,Q)| - \frac{|X_u|}{2^{|V|}} \right| &\leq \left| |X_u(a,Q)| - \frac{|X_u(a,x)|}{2^{|V|-1}} \right| + \left| \frac{|X_u(a,x)|}{2^{|V|-1}} - \frac{|X_u|}{2^{|V|}} \right| \\ &\leq t_2^{-B_2}(|V|-1)|X_u| + t_1^{-B_2}|X_u| \leq t_1^{-B_2}|V||X_u|,\end{aligned}$$

establishing the claim. Now we can easily bound the former sum in equation (5.4) using the induction hypothesis. Finally, we deal with the case that $v \neq 1$ so that $1 \in U$. In this case, we apply the induction hypothesis to the prebox

$$(X_1(a,x) \times \cdots \times X_{v-1}(a,x) \times X_{v+1}(a,x) \times \cdots \times X_r(a,x), P \cup \{x\})$$

with $k = r - 1$. □

As alluded to earlier, the squarefree integers play a crucial role in our analysis. It turns out to be more convenient to work with squarefree integers with a fixed number of prime divisors, and this naturally leads to the following definition.

We now define special preboxes that we call boxes. These boxes provide a natural way to study distributional properties $S_r(N)$, as we shall see in the coming proposition, which is based on Proposition 6.9 in Smith [18].

Definition 5.12. Suppose $0 \leq k \leq r$. For any $\mathbf{t} = (p_1, \ldots, p_k, s_{k+1}, \ldots, s_r)$ such that

1. $p_1 < p_2 < \cdots < p_k < D_1$ is a sequence of primes not congruent to 3 mod 4,
2. $D_1 < s_{k+1} < t_{k+1} < s_{k+2} < t_{k+2} < \cdots < s_r < t_r$ is a sequence of real numbers where

$$t_i = \left(1 + \frac{1}{e^{i-k}\log D_1}\right)s_i,$$

we define $X(\mathbf{t}) := X_1 \times \cdots \times X_r$ with

$$X_i := \begin{cases} \{p_i\} & \text{if } i \leq k, \\ \{p \in (s_i, t_i) \text{ prime } : p \equiv 1 \bmod 4\} & \text{if } i > k. \end{cases}$$

We call X a box if $X = X(\mathbf{t})$ for some $\mathbf{t}$. There is a bijection from X to a subset of $S_r(\infty)$. By abuse of notation, denote this subset by X.

Theorem 5.13. *Take $N \geq D_1 \geq 3$ with $\log N \geq (\log D_1)^2$. Suppose that r satisfies equation (4.3). Let $W \subseteq S_r(N)$ be a set of comfortably spaced elements above D_1 such that*

$$||W| - \Phi_r(N)| < \epsilon\Phi_r(N)$$

for some constant $\epsilon > 0$. Let $V \subseteq S_r(N)$, and suppose that there exists some constant $\delta > 0$ such that

$$||V \cap X| - \delta|X|| < \epsilon|X|$$

for any box $X \subseteq S_r(N)$ satisfying $X \cap W \neq \varnothing$. Then there exists an absolute constant $C > 0$ such that

$$|V| - \delta\Phi_r(N) \ll \epsilon\Phi_r(N) + \left(\Phi_r(N) - \Phi_r\left(N\left(1 - \frac{C}{\log D_1}\right)\right)\right).$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

Proof. Define $\mathcal{T}_k = \{\mathbf{t} : X(\mathbf{t}) \subseteq S_r(N) \text{ and } X(\mathbf{t}) \cap W \neq \varnothing\}$. Our aim is to estimate $|V|$ in terms of

$$\int_{\mathcal{T}_k} |V \cap X(\mathbf{t})| \frac{dp_1 \cdots dp_k ds_{k+1} \cdots ds_r}{s_{k+1} \cdots s_r},$$

where dp_i is 1 if $p_i \equiv 1 \bmod 4$ is prime and 0 otherwise.

Consider $n = (q_1, \ldots, q_r) \in S_r(N)$ with exactly k prime factors less than D_1. Then $n \in X(\mathbf{t})$ if and only if $q_i = p_i$ for $1 \leq i \leq k$ and

$$s_i < q_i < \left(1 + \frac{1}{e^{i-k} \log D_1}\right) s_i \text{ for } k < i \leq r.$$

If $n \in W$ and

$$n \prod_{i=k+1}^{r} \left(1 + \frac{1}{e^{i-k} \log D_1}\right) < N, \tag{5.5}$$

then

$$\begin{aligned}\int_{\substack{\mathbf{t} \in \mathcal{T}_k: \\ n \in X(\mathbf{t})}} \frac{dp_1 \cdots dp_k ds_{k+1} \cdots ds_r}{s_{k+1} \cdots s_r} &= \int_{q_{k+1}\left(1+\frac{1}{e \log D_1}\right)^{-1}}^{q_{k+1}} \cdots \int_{q_r\left(1+\frac{1}{e^{r-k} \log D_1}\right)^{-1}}^{q_r} \frac{ds_{k+1} \cdots ds_r}{s_{k+1} \ldots s_r} \\ &= \prod_{i=k+1}^{r} \log\left(1 + \frac{1}{e^{i-k} \log D_1}\right).\end{aligned}$$

If equation (5.5) does not hold or $n \notin W$, then

$$\int_{\substack{\mathbf{t} \in \mathcal{T}_k: \\ n \in X(\mathbf{t})}} \frac{dp_1 \cdots dp_k ds_{k+1} \cdots ds_r}{s_{k+1} \cdots s_r} \leq \prod_{i=k+1}^{r} \log\left(1 + \frac{1}{e^{i-k} \log D_1}\right).$$

There exists some constant $C > 0$ such that any n that does not satisfy equation (5.5) lies in

$$N\left(1 - \frac{C}{\log D_1}\right) \leq N \prod_{i=k+1}^{r} \left(1 + \frac{1}{e^{i-k} \log D_1}\right)^{-1} \leq n \leq N,$$

which we bound by

$$\Phi_r(N) - \Phi_r\left(N\left(1 - \frac{C}{\log D_1}\right)\right).$$

Then

$$\sum_{k=0}^{\infty} \prod_{i=k+1}^{r} \log\left(1 + \frac{1}{e^{i-k} \log D_1}\right)^{-1} \int_{\mathcal{T}_k} |V \cap X(\mathbf{t})| \frac{dp_1 \cdots dp_k ds_{k+1} \cdots ds_r}{s_{k+1} \cdots s_r}$$

is bounded above by $|V|$ and below by

$$\begin{aligned}|V \cap W| + O\left(\Phi_r(N) - \Phi_r\left(N\left(1 - \frac{C}{\log D_1}\right)\right)\right) &= \\ |V| + O\left(\Phi_r(N) - \Phi_r\left(N\left(1 - \frac{C}{\log D_1}\right)\right)\right) &+ O(\epsilon \Phi_r(N)).\end{aligned}$$

Similarly,

$$\sum_{k=0}^{\infty}\prod_{i=k+1}^{r}\log\left(1+\frac{1}{e^{i-k}\log D_1}\right)^{-1}\int_{\mathcal{T}_k}|X(\mathbf{t})|\frac{dp_1\cdots dp_k ds_{k+1}\cdots ds_r}{s_{k+1}\cdots s_r}$$
$$=\Phi_r(N)+O\left(\Phi_r(N)-\Phi_r\left(N\left(1-\frac{C}{\log D_1}\right)\right)\right)+O(\epsilon\Phi_r(N)).$$

The result follows from the estimate $|V\cap X(\mathbf{t})|=(\delta+O(\epsilon))|X(\mathbf{t})|$ for $\mathbf{t}\in\mathcal{T}_k$. □

With some extra work, it is possible to prove that

$$\Phi_r(N)-\Phi_r\left(N\left(1-\frac{C}{\log D_1}\right)\right)\ll\frac{\Phi_r(N)}{\log D_1},$$

which ensures that the error term in Theorem 5.13 is smaller than the main term. However, in our applications, we work with all values of r simultaneously so that the trivial bound

$$\sum_r\left(\Phi_r(N)-\Phi_r\left(N\left(1-\frac{C}{\log D_1}\right)\right)\right)\ll\frac{\Phi(N)}{\log D_1}$$

suffices for our purposes. Our next proposition deals with boxes that are not Siegel-less. It is directly based on Proposition 6.10 in Smith [18].

Theorem 5.14. *Let $d_1, d_2, \ldots$ be a sequence of distinct squarefree integers greater than D_1 satisfying $d_i^2 < d_{i+1}$. Take $N \geq D_1 \geq 3$ satisfying $\log N \geq (\log D_1)^4$, and suppose that r satisfies equation (4.3). Define*

$$V_i := \{x\in S_r(N):\ \text{there is a box } X\subseteq S_r(N) \text{ with } x\in X \text{ and there is } x'\in X \text{ with } d_i\mid x'\}.$$

Then

$$|\cup_{i\geq 1}V_i|\ll\frac{\Phi_r(N)}{\log D_1}.$$

Proof. Suppose we have some box $X\subseteq V_i$ and $d_i=p_1\cdots p_m$. For any element $x\in X$, there are prime factors $q_1,\ldots,q_m$ of x such that

$$q_i=p_i \text{ if } p_i<D_1 \quad\text{and}\quad \frac{1}{2}p_i<q_i<2p_i \text{ if } p_i\geq D_1.$$

If $d_i<N^{2/3}$, we deduce from equation (4.1) that there exists some constant $C>0$ with

$$|V_i|\leq\Phi_{r-m}\left(\frac{2^mN}{d_i}\right)\cdot\prod_{p_i\geq D_1}\left|\left\{q_i\text{ prime}:\frac{1}{2}p_i<q_i<2p_i,\ q_i\equiv 1 \bmod 4\right\}\right|$$
$$\leq\Phi_r(N)\cdot\frac{C^m}{d_i}\prod_{p_i\geq D_1}\frac{p_i}{\log p_i}\ll\frac{\Phi_r(N)}{\log d_i}.$$

Notice that $d_i>D_1^{2^{i-1}}$. Then

$$\left|\bigcup_{d_i<N^{2/3}}V_i\right|\ll\Phi_r(N)\sum_{i\geq 1}\frac{1}{2^{i-1}\log D_1}\ll\frac{\Phi_r(N)}{\log D_1}.$$

If $d_i \geq N^{2/3}$, then $d_{i+1} \geq N^{4/3} > N$. Therefore there is at most one i such that $d_i \geq N^{2/3}$ and V_i is not empty. Then for sufficiently large D_1,

$$|V_i| \leq |\{x \in S_r(N) : d_i \mid x\}| \cdot \prod_{p_i \geq D_1} \left|\left\{q_i \text{ prime} : \frac{1}{2}p_i < q_i < 2p_i,\ q_i \equiv 1 \bmod 4\right\}\right|$$
$$\leq \frac{N}{d_i} \prod_{p_i \geq D_1} \frac{2p_i}{\log p_i} \ll \frac{N}{\log d_i} \ll \frac{N}{\log N},$$

which fits into the error bound. □

Definition 5.15. Fix some constants $c_9, c_{10} > 0$. We call a box X of $S_r(N)$ acceptable if it

1. contains a comfortably spaced element above $D_1 = \exp\left(\left(\frac{1}{2}\log\log N\right)^{c_9}\right)$,
2. contains a $(c_{10}\log\log\log N)$-regular element, and
3. is Siegel-less above D_1.

Given any integer $x \in \mathcal{D}$, let $p_1 < \cdots < p_n$ be the distinct prime factors of x, and call the matrix $(c_{ij})_{1 \leq i,j \leq n}$ defined by

$$(-1)^{c_{ij}} = \begin{cases} \left(\frac{p_i}{p_j}\right) & \text{if } i \neq j \\ \prod_{l \neq j}\left(\frac{p_l}{p_j}\right) & \text{if } i = j \end{cases}$$

the Rédei matrix of x. This is a symmetric matrix with column (and row) sum zero due to our assumption $x \in \mathcal{D}$. We are now ready to reprove a well-known result due to Fouvry and Klüners [6]. Note that unlike the work of Fouvry and Klüners, our theorem has the benefit of providing an error term.

Theorem 5.16. *There exists a constant $c > 0$ such that for all integers $k \geq 0$,*

$$\left|\frac{|\{d \in \mathcal{D}(N) : \mathrm{rk}_4 \mathrm{Cl}^+(d) = k\}|}{|\mathcal{D}(N)|} - \lim_{n \to \infty} P(n|k)\right| \ll (\log\log N)^{-c}.$$

Proof. By our Erdős–Kac result – that is, equation (4.2) – it suffices to show that

$$\left|\frac{|\{d \in S_r(N) : \mathrm{rk}_4 \mathrm{Cl}^+(d) = k\}|}{|S_r(N)|} - \lim_{n \to \infty} P(n|k)\right| \ll (\log\log N)^{-c}$$

for any r satisfying equation (4.3). We can find some $W \subseteq S_r(N)$ that is comfortably spaced above D_1 and $(c_{10}\log\log\log N)$-regular by Theorem 4.1 and Siegel-less above D_1 by Proposition 5.14 so that

$$|W| \geq (1 - \epsilon)\Phi_r(N) \text{ with } \epsilon \ll (\log\log N)^{-c}$$

for some absolute constant $c > 0$. Then, applying Theorem 5.13, we see that we can restrict to acceptable boxes by introducing an error $\ll (\log\log N)^{-c}$. In other words, it suffices to show that we have for any acceptable box $X \subseteq S_r(N)$

$$\left|\frac{|\{x \in X : \mathrm{rk}_4 \mathrm{Cl}^+(x) = k\}|}{|X|} - \lim_{n \to \infty} P(n|k)\right| \ll (\log\log N)^{-c}. \tag{5.6}$$

Take X to be an acceptable box. Then one can check that there exist constants that satisfy the requirements in Theorem 5.9 applied to the prebox $(X_1 \times \cdots \times X_r, \varnothing)$. Then Theorem 5.9 shows that the Rédei matrices of $x \in X$ are equidistributed amongst all $r \times r$ symmetric matrices over $\mathbb{F}_2$ with column sum zero, up to reordering some columns and rows, with an error within the statement. Since reordering

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

columns and rows does not change the rank, we can assume that the Rédei matrix is a random $r \times r$ symmetric matrix over $\mathbb{F}_2$ with column sum zero.

Let A be the matrix obtained from the Rédei matrix after removing a column and a row. It is a classical fact that $\mathrm{rk}_4 \, \mathrm{Cl}^+(x)$ is equal to the corank of A. But A is a random $(r-1) \times (r-1)$ symmetric matrix. By [15, Theorem 2], we have for all $n \geq k \geq 0$

$$P(n|k) = \frac{N(n, n-k)}{2^{\frac{n(n+1)}{2}}} = \frac{1}{2^{\frac{n(n+1)}{2}}} \prod_{i=1}^{\frac{n-k}{2}} \frac{2^{2i}}{2^{2i}-1} \cdot \prod_{i=0}^{n-k-1} (2^{n-i}-1)$$
$$= \frac{1}{2^{\frac{k(k+1)}{2}}} \prod_{i=1}^{\frac{n-k}{2}} \frac{2^{2i}}{2^{2i}-1} \cdot \prod_{i=0}^{n-k-1} (1-2^{i-n})$$

if $n - k \equiv 0 \bmod 2$ and

$$P(n|k) = \frac{N(n, n-k)}{2^{\frac{n(n+1)}{2}}} = \frac{1}{2^{\frac{n(n+1)}{2}}} \prod_{i=1}^{\frac{n-k-1}{2}} \frac{2^{2i}}{2^{2i}-1} \cdot \prod_{i=0}^{n-k-1} (2^{n-i}-1)$$
$$= \frac{1}{2^{\frac{k(k+1)}{2}}} \prod_{i=1}^{\frac{n-k-1}{2}} \frac{2^{2i}}{2^{2i}-1} \cdot \prod_{i=0}^{n-k-1} (1-2^{i-n})$$

if $n - k \equiv 1 \bmod 2$, where $N(n, k)$ denotes the number of symmetric $n \times n$-matrices with coefficients in $\mathbb{F}_2$ and rank k. Using this, one directly bounds the difference $P(r-1|k) - \lim_{n\to\infty} P(n|k)$, completing the proof. □

Gerth [8, Theorem 2.2] also studied the difference $P(r-1|k) - \lim_{n\to\infty} P(n|k)$ but without giving a rate of convergence. It is for this reason that we appeal to the work [15] instead.

6. Proof of main theorems

Recall from the introduction that

$$\mathcal{D}_{n,m}(X) = \{D \in \mathcal{D}(X) : \mathrm{rk}_4 \, \mathrm{Cl}(D) = \mathrm{rk}_4 \, \mathrm{Cl}^+(D) = n \text{ and } \mathrm{rk}_8 \, \mathrm{Cl}^+(D) = m\}.$$

We also define

$$\mathcal{D}_n(X) = \{D \in \mathcal{D}(X) : \mathrm{rk}_4 \, \mathrm{Cl}^+(D) = n\}.$$

In this section, we prove the following theorem.

Theorem 6.1. *There are $A, N_0 > 0$ such that for all $N > N_0$ and all integers $n_2 \geq n_3 \geq 0$, we have*

$$\left| |\mathcal{D}_{n_2,n_3}(N)| - Q(n_2|n_3) \cdot |\mathcal{D}_{n_2}(N)| \right| \leq \frac{A|\mathcal{D}(N)|}{\log\log\log\log N}.$$

Theorem 5.16 and Theorem 6.1 together imply Theorem 1.2. Hence it remains to prove Theorem 6.1. Our first step is to reduce to sufficiently nice boxes X. We formalise this in our next definition.

Definition 6.2. Let $r \geq 1$ be an integer, let $X = X_1 \times \ldots \times X_r$ be a box, and let $N \geq 10^{10^{10}}$ be a real number. Put

$$D_1 := e^{(\log\log N)^{1/10}}, \quad \eta := \sqrt{\log\log\log N}.$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

We let W be the maximal subset of $S_r(N)$ that is comfortably spaced above D_1, η-regular and disjoint from the sets V_i in Proposition 5.14. We call X a nice box for N if $X \subseteq S_r(N)$, $X \cap W \neq \varnothing$ and r satisfies equation (4.3).

Proposition 6.3. *There are $A, N_0 > 0$ such that for all $N > N_0$, all nice boxes X for N and all integers $n_2 \geq n_3 \geq 0$, we have*

$$\left||X \cap \mathcal{D}_{n_2,n_3}(N)| - Q(n_2|n_3) \cdot |X \cap \mathcal{D}_{n_2}(N)|\right| \leq \frac{A|X|}{\log\log\log\log N}.$$

Proof that Proposition 6.3 implies Theorem 6.1. From Erdős—Kac (see equation (4.2)), it follows that we only need to consider r satisfying equation (4.3). For each such r, we apply Proposition 5.13 with W as in Definition 6.2; the required lower bound for $|W|$ follows from the material in Section 4 and Proposition 5.14. □

Given a box X and $a : \mathcal{M} \to \{\pm 1\}$, our next step is to reduce to $X(a)$. However, it turns out that we cannot prove equidistribution for all $a : \mathcal{M} \to \{\pm 1\}$, but only if a is *generic* in the following sense.

Definition 6.4. For a field K and for integers $a, b \geq 0$, we denote by $\mathrm{Mat}(K, a, b)$ the set of $a \times b$-matrices with coefficients in K. Let ι be the unique group isomorphism between $\{\pm 1\}$ and $\mathbb{F}_2$. For the rest of the paper, we will use

$$\mathcal{M} := \{(i, j) : 1 \leq i < j \leq r\}, \quad \mathcal{N} := \varnothing.$$

Given $a : \mathcal{M} \to \{\pm 1\}$, we associate a symmetric matrix $A \in \mathrm{Mat}(\mathbb{F}_2, r, r)$ by setting for all $i < j$

$$A(i, j) = \iota \circ a(i, j), \quad A(j, i) = \iota \circ a(i, j)$$

and finally

$$A(i, i) = \iota \circ \prod_{j=1}^{r} a(i, j).$$

Think of $\mathbb{F}_2^r$ as column vectors. We define the vector space

$$\mathcal{V}_{a,2} = \{v \in \mathbb{F}_2^r : v^T A = 0\} = \{v \in \mathbb{F}_2^r : Av = 0\}.$$

Let $R := (1, \ldots, 1)$ so that $R \in \mathcal{V}_{a,2}$. Put $n_2(a) := -1 + \dim_{\mathbb{F}_2} \mathcal{V}_{a,2}$.

Let N be a large real, and let $X = X_1 \times \ldots \times X_r$ be a nice box for N. Choose an index k_{gap} such that the extravagant spacing of X is between k_{gap} and $k_{\mathrm{gap}} + 1$. Set

$$n_{\max} := \left\lfloor \sqrt{3 \log\log\log\log\log N} \right\rfloor.$$

We say that $a : \mathcal{M} \to \{\pm 1\}$ is generic for X if $n_2(a) \leq n_{\max}$, and furthermore we have for all $S \in \mathcal{V}_{a,2} \setminus \langle R \rangle$ and all $i \in \mathbb{F}_2$ that

$$\left|\left|\left\{j \in [r] : \frac{k_{\mathrm{gap}}}{2} \leq j \leq k_{\mathrm{gap}} \text{ and } \pi_j(S) = i\right\}\right| - \frac{k_{\mathrm{gap}}}{4}\right| \leq 2^{-10n_{\max}} \cdot k_{\mathrm{gap}} \tag{6.1}$$

and

$$\left|\left|\{j \in [r] : k_{\mathrm{gap}} < j \leq 2k_{\mathrm{gap}} \text{ and } \pi_j(S) = i\}\right| - \frac{k_{\mathrm{gap}}}{2}\right| \leq 2^{-10n_{\max}} \cdot k_{\mathrm{gap}}. \tag{6.2}$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

We shall prove that the Artin pairing Art_2 is equidistributed in $X(a)$ under favorable circumstances. For this reason, we make the following definition.

Definition 6.5. We say that a bilinear pairing

$$\mathrm{Art}_2 : \mathcal{V}_{a,2} \times \mathcal{V}_{a,2} \longrightarrow \mathbb{F}_2$$

is valid if the right kernel contains $(1, \dots, 1)$. Fix a basis $w_1, \dots w_{n_2}, R$ for $\mathcal{V}_{a,2}$. Using this basis, we may identify Art_2 with a $(n_2 + 1) \times (n_2 + 1)$ matrix with coefficients in $\mathbb{F}_2$. Since $(1, \dots, 1)$ is in the right kernel, we may also naturally identify Art_2 with a $(n_2 + 1) \times n_2$ matrix. Finally, define for a box X

$$X(a, \mathrm{Art}_2) := \{x \in X(a) : \text{ the Artin pairing of } x \text{ equals } \mathrm{Art}_2\}.$$

Here one defines the Artin pairing of x as follows:

$$\mathrm{Art}_2(x)(i, j) := \left\langle \sum_{a \in [r]} \pi_a(w_j)\chi_{\pi_a(x)}, \prod_{b \in [r]} \pi_b(x)^{\pi_b(w_i)} \right\rangle_x,$$

where w_i and w_j are allowed to be equal to R and $\langle \cdot, \cdot \rangle_x$ is the pairing defined in Section 2. We recall that $\mathrm{rk}_4 \, \mathrm{Cl}(x) = \mathrm{rk}_4 \, \mathrm{Cl}^+(x)$ if and only if $(1, \dots, 1)$ is in the left kernel of $\mathrm{Art}_2(x)$. Furthermore, the dimension of the left kernel of $\mathrm{Art}_2(x)$ is precisely one more than the dimension of $4\,\mathrm{Cl}^+(x)$ [8].

If $X = X_1 \times \cdots \times X_r$ is a box with D_1 sufficiently large, we recall that k is the largest index such that $|X_k| = 1$.

Proposition 6.6. *There are $A, N_0 > 0$ such that for all $N > N_0$, all nice boxes X for N, all integers $n_2 \geq 0$, all generic $a : \mathcal{M} \to \{\pm 1\}$ for X with $n_2(a) = n_2$ and*

$$|X_j(a, (x_1, \dots x_k))| \geq \frac{1}{(\log t_{k+1})^{100}} \cdot |X_j| \tag{6.3}$$

for all $k < j \leq r$, and all valid Artin pairings Art_2*, we have*

$$\Big| |X(a, \mathrm{Art}_2)| - 2^{-n_2(n_2+1)} |X(a)| \Big| \leq \frac{A|X(a)|}{(\log \log \log \log N)^4}.$$

Here we write $x_1, \dots, x_k$ for the unique elements of $X_1, \dots, X_k$.

Proof that Proposition 6.6 implies Proposition 6.3. Take N to be a large integer, and take X to be a nice box for N. If N is sufficiently large and $n_2 > n_{\max}$, we have

$$\lim_{k \to \infty} P(k|n_2) = O\left(\frac{1}{\log \log \log \log N}\right).$$

Then it follows from equation (5.6) that

$$\Big| |X \cap \mathcal{D}_{n_2,n_3}(N)| - Q(n_2|n_3) \cdot |X \cap \mathcal{D}_{n_2}(N)| \Big| \leq 2|X \cap \mathcal{D}_{n_2}(N)| \leq \frac{A|X|}{\log \log \log \log N}$$

for a sufficiently large constant $A > 0$. From now on, suppose that $n_2 \leq n_{\max}$. We deduce from Hoeffding's inequality that the proportion of S in $\mathbb{F}_2^r$ failing equation (6.1) or equation (6.2) is bounded by

$$O\left(\exp\left(-2^{-20n_{\max}^2} \cdot k_{\mathrm{gap}}\right)\right).$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

Given $S \notin \langle R \rangle$, the proportion of $a : \mathcal{M} \to \{\pm 1\}$ with $S \in \mathcal{V}_{a,2}$ is $O(0.5^r)$. Taking the union over all S in $\mathbb{F}_2^r$ failing equation (6.1) or equation (6.2) proves that the proportion of nongeneric a is at most

$$O\Big(\exp\Big(-2^{-20n_{\max}^2} \cdot k_{\mathrm{gap}}\Big)\Big).$$

Put $k_2 := \lfloor 0.25 k_{\mathrm{gap}} \rfloor$. Then we have for all $\sigma \in \mathcal{P}(k_2)$ that $a : \mathcal{M} \to \{\pm 1\}$ is generic if and only if $\sigma(a)$ is generic, where $\sigma(a)$ is defined in the natural way. Theorem 5.9 implies that

$$\sum_{a:\mathcal{M}\to\{\pm 1\}} \left| 2^{-|\mathcal{M}|} \cdot |X| - \frac{1}{k_2!} \sum_{\sigma \in \mathcal{P}(k_2)} |X(\sigma(a))| \right| \le (k_2^{-\delta_1} + t_{k+1}'^{-\delta_2}) \cdot |X|,$$

where δ_1 and δ_2 are small, positive absolute constants. Restricting this sum to the nongeneric a shows that the union of $X(a)$ over all nongeneric a is within the error term of Proposition 6.3. We now deal with the $a : \mathcal{M} \to \{\pm 1\}$ that fail equation (6.3). Let j be an integer satisfying $k < j \le r$. We say that $a, a' : \mathcal{M} \to \{\pm 1\}$ are equivalent at j, which we write as $a \sim_j a'$, if $a(i, j) = a'(i, j)$ for all $1 \le i \le k$. Since our box is η-regular, we see that k is roughly equal to $\log\log D_1$. In particular, if N is sufficiently large, we get

$$k \le 2 \log\log D_1 = \frac{1}{5} \log\log\log N.$$

Then there are at most $2^{\frac{1}{5}\log\log\log N}$ equivalence classes. Furthermore, if $a : \mathcal{M} \to \{\pm 1\}$ is such that equation (6.3) fails for some fixed j, we have that

$$\left| \bigcup_{a' : a \sim_j a'} X(a') \right| \le \frac{1}{(\log t_{k+1})^{100}} \cdot |X|,$$

where the union is over all $a' : \mathcal{M} \to \{\pm 1\}$ equivalent to $a : \mathcal{M} \to \{\pm 1\}$ at j. Summing this over all choices of j and all equivalence classes, we stay within the error term of Proposition 6.3. So far, we have shown

$$\begin{aligned} &\Big| \big| X \cap \mathcal{D}_{n_2,n_3}(N) \big| - Q(n_2|n_3) \cdot \big| X \cap \mathcal{D}_{n_2}(N) \big| \Big| \\ &\qquad \le \sum_{\substack{a \text{ generic} \\ a \text{ sat. eq. } (6.3) \\ n_2(a) = n_2}} \; \sum_{\substack{\mathrm{rk}(\mathrm{Art}_2) = n_2 - n_3 \\ \mathrm{Art}_2 \text{ valid}}} \Big| |X(a, \mathrm{Art}_2)| - 2^{-n_2(n_2+1)} |X(a)| \Big| + \frac{A|X|}{\log\log\log\log N}. \end{aligned}$$

Note that we could have further restricted the sum over Artin pairings to only those with bottom row identically 0. However, the displayed inequality suffices for our purposes. We now apply Proposition 6.6 for every generic $a : \mathcal{M} \to \{\pm 1\}$ for X such that it satisfies equation (6.3) and $n_2(a) = n_2$, and all valid Artin pairings Art_2 with $\mathrm{rk}(\mathrm{Art}_2) = n_2 - n_3$. Since there are at most

$$2^{n_2(n_2+1)} \le 2^{n_{\max}(n_{\max}+1)}$$

valid Artin pairings, we get

$$\sum_{\substack{a \text{ generic} \\ a \text{ sat. eq. } (6.3) \\ n_2(a) = n_2}} \; \sum_{\substack{\mathrm{rk}(\mathrm{Art}_2) = n_2 - n_3 \\ \mathrm{Art}_2 \text{ valid}}} \Big| |X(a, \mathrm{Art}_2)| - 2^{-n_2(n_2+1)} |X(a)| \Big| \le 2^{n_{\max}(n_{\max}+1)} \frac{A|X|}{(\log\log\log\log N)^4}$$

as desired. □

In our next definition, we introduce the notion of variable indices, which are by definition certain subsets S of $[r]$. At the very end of this section, we will reduce to the case where we have chosen one element $x_i \in X_i$ for all $i \in [r] - S$, whence the terminology.

Definition 6.7. Let $a : \mathcal{M} \to \{\pm 1\}$. Recall that we fixed a basis $w_1, \dots w_{n_2}, R$ for $\mathcal{V}_{a,2}$ in Definition 6.5. Let $1 \leq j_1 \leq n_2+1$, and let $1 \leq j_2 \leq n_2$. Let E_{j_1,j_2} be the $(n_2+1)\times n_2$-matrix with $E_{j_1,j_2}(j_1, j_2) = 1$ and 0 otherwise, and let F_{j_1,j_2} be the dual basis. Any nonzero multiplicative character $F : \mathrm{Mat}(\mathbb{F}_2, n_2+1, n_2) \to \{\pm 1\}$ can be written as

$$F = \iota^{-1} \circ \sum_{\substack{1 \leq j_1 \leq n_2+1 \\ 1 \leq j_2 \leq n_2}} c_{j_1,j_2} F_{j_1,j_2}$$

with not all c_{j_1,j_2} zero. A set $S \subseteq [r]$ is called a set of variable indices for F if there are $i_1(F), i_2(F) \in S$ such that

$$\frac{k_{\text{gap}}}{2} \leq i \leq k_{\text{gap}} \text{ for all } i \in S \setminus \{i_2(F)\}, \quad k_{\text{gap}} < i_2(F) \leq 2k_{\text{gap}}$$

and

- ○ if $c_{n_2+1,j_2} = 0$ for all $1 \leq j_2 \leq n_2$ and $c_{j_1,j_1} = 0$ for all $1 \leq j_1 \leq n_2$ and $c_{j_1,j_2} = 0$ implies $c_{j_2,j_1} = 0$ for all $1 \leq j_1, j_2 \leq n_2$, we choose any pair (j_1, j_2) such that $c_{j_1,j_2} = 1$. Furthermore, choose $|S(F)| = 2$,

$$i_1(F) \in \bigcap_{i \neq j_1} \{j \in [r] : \pi_j(w_i) = 0\} \cap \{j \in [r] : \pi_j(w_{j_1}) = 1\}$$

  and

$$i_2(F) \in \bigcap_{i \neq j_2} \{j \in [r] : \pi_j(w_i) = 0\} \cap \{j \in [r] : \pi_j(w_{j_2}) = 1\};$$

- ○ if there are $1 \leq j_1, j_2 \leq n_2$ such that $c_{j_1,j_2} = 1$ and $c_{j_2,j_1} = 0$, choose such a pair (j_1, j_2). Next choose $|S(F)| = 3$ and

$$S(F) \subseteq \bigcap_{i \notin \{j_1,j_2\}} \{j \in [r] : \pi_j(w_i) = 0\}$$

  and

$$S(F) \cap \{j \in [r] : \pi_j(w_{j_1}) = 1, \pi_j(w_{j_2}) = 0\} = \{i_1(F)\}$$

  and

$$S(F) \cap \{j \in [r] : \pi_j(w_{j_2}) = 1, \pi_j(w_{j_1}) = 0\} = \{i_2(F)\}$$

  and

$$S(F) \cap \{j \in [r] : \pi_j(w_{j_1}) = 1, \pi_j(w_{j_2}) = 1\} = \varnothing;$$

- ○ in all other cases, choose a pair (j_2, j_2) such that $c_{j_2,j_2} = 1$ or choose a pair $(n_2 + 1, j_2)$ such that $c_{n_2+1,j_2} = 1$. We pick $|S(F)| = 2$ and

$$i_1(F) \in \bigcap_{i \neq j_2} \{j \in [r] : \pi_j(w_i) = 0\} \cap \{j \in [r] : \pi_j(w_{j_2}) = 1\}$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

and

$$i_2(F) \in \bigcap_{i=1}^{n_2} \{j \in [r] : \pi_j(w_i) = 0\}.$$

If $a : \mathcal{M} \to \{\pm 1\}$ is generic for X, we will now show that one can find variable indices provided that r is sufficiently large. Our essential tool is the following combinatorial lemma.

Lemma 6.8. *Assume that $a : \mathcal{M} \to \{\pm 1\}$ is generic for X. If $w_1, \dots, w_d, R \in \mathcal{V}_{a,2}$ are linearly independent, then we have for all $\mathbf{v} \in \mathbb{F}_2^d$*

$$\left| \left| \left\{ i \in [r] : \frac{k_{\text{gap}}}{2} \leq i \leq k_{\text{gap}} \text{ and } \pi_i(w_j) = \pi_j(\mathbf{v}) \text{ for all } 1 \leq j \leq d \right\} \right| - \frac{k_{\text{gap}}}{2^{d+1}} \right| \leq \frac{3^d \cdot k_{\text{gap}}}{2^{10 n_{\max}}}.$$

Proof. We proceed by induction on d. The base case $d = 1$ follows immediately from equation (6.1). Now suppose that $d > 1$. We define for $\mathbf{w} \in \mathbb{F}_2^d$

$$g(\mathbf{w}) = \left| \left\{ i \in [r] : \frac{k_{\text{gap}}}{2} \leq i \leq k_{\text{gap}} \text{ and } \pi_i(w_j) = \pi_j(\mathbf{w}) \text{ for all } 1 \leq j \leq d \right\} \right|.$$

Let $\mathbf{v} \in \mathbb{F}_2^d$ be given. Let $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ be the three unique pairwise distinct vectors such that $\pi_{d-2}(\mathbf{v}_i) = \pi_{d-2}(\mathbf{v})$ and $\mathbf{v}_i \neq \mathbf{v}$. We have

$$\begin{aligned} 2\left| g(\mathbf{v}) - \frac{k_{\text{gap}}}{2^{d+1}} \right| &\leq \left| 3g(\mathbf{v}) + \sum_{i=1}^{3} g(\mathbf{v}_i) - \frac{3k_{\text{gap}}}{2^d} \right| + \left| \frac{k_{\text{gap}}}{2^{d-1}} - g(\mathbf{v}) - \sum_{i=1}^{3} g(\mathbf{v}_i) \right| \\ &\leq \sum_{i=1}^{3} \left| g(\mathbf{v}) + g(\mathbf{v}_i) - \frac{k_{\text{gap}}}{2^d} \right| + \left| \frac{k_{\text{gap}}}{2^{d-1}} - g(\mathbf{v}) - \sum_{i=1}^{3} g(\mathbf{v}_i) \right|. \end{aligned}$$

Now apply the induction hypothesis. □

With this lemma, it is straightforward to find variable indices provided that a is generic for X and r is sufficiently large. We can now formulate our next reduction step. For a subset $T \subseteq [r]$, a point $P \in \prod_{i \in T} X_i$ and $a : \mathcal{M} \to \{\pm 1\}$, we say that P is consistent with a if

$$\left(\frac{\pi_i(P)}{\pi_j(P)} \right) = a(i, j)$$

for all distinct $i, j \in T$ with $i < j$.

Proposition 6.9. *There are $A, N_0 > 0$ such that for all $N > N_0$, all nice boxes X for N, all integers $n_2 \geq 0$, all generic $a : \mathcal{M} \to \{\pm 1\}$ for X with $n_2(a) = n_2$, all nonzero multiplicative characters F from* $\mathrm{Mat}(\mathbb{F}_2, n_2 + 1, n_2)$ *to $\{\pm 1\}$, all sets of variable indices S for F and all $Q \in \prod_{i \in [k_{\text{gap}}] - S} X_i$ consistent with a such that*

$$|X_j(a, Q)| \geq 4^{-k_{\text{gap}}} \cdot |X_j| \tag{6.4}$$

for all $j \in S$, we have

$$\left| \sum_{x \in X(a,Q)} F(\mathrm{Art}_2(x)) \right| \leq \frac{A|X(a, Q)|}{(\log \log \log \log N)^4}.$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

Proof that Proposition 6.9 implies Proposition 6.6. Let F be a nonzero multiplicative character from $\mathrm{Mat}(\mathbb{F}_2, n_2 + 1, n_2)$ to $\{\pm 1\}$. We claim that there exist absolute constants $A', N_0' > 0$ such that for all $N > N_0'$

$$\left| \sum_{x \in X(a)} F(\mathrm{Art}_2(x)) \right| \leq \frac{A'|X(a)|}{(\log\log\log\log N)^4}. \tag{6.5}$$

Once we establish equation (6.5), Proposition 6.6 follows easily. Take a set of variable indices S for F. We split the sum in equation (6.5) over all $Q \in \prod_{i \in [k_{\mathrm{gap}}] - S} X_i$ consistent with a. If Q satisfies equation (6.4) for all $j \in S$, we apply Proposition 6.9 with this S. It remains to bound

$$\sum_{\substack{Q \in \prod_{i \in [k_{\mathrm{gap}}] - S} X_i \\ Q \text{ consistent with } a \\ Q \text{ fails eq. (6.4)}}} |X(a, Q)|. \tag{6.6}$$

But this follows quickly from an application of Proposition 5.11 with the prebox

$$(X_{k+1}(a, P) \times \cdots \times X_r(a, P), P),$$

where P is the union of $x_1, \ldots, x_k$. Note that we make crucial usage of equation (6.3) to validate the fourth condition of Proposition 5.11. □

It remains to prove Proposition 6.9, which we shall do now.

Proof of Proposition 6.9. Put

$$M := \left\lfloor (\log\log\log\log N)^{20} \right\rfloor, \quad S' := [k_{\mathrm{gap}}] \cap S, \quad m := |S'|.$$

Define

$$X' := \prod_{i \in S'} X_i(a, Q),$$

and

$$Y := \{x \in X' : x \text{ is consistent with } a\}.$$

Also set $R := \lfloor \exp(\exp(0.2 k_{\mathrm{gap}})) \rfloor$. We let $Z_{\mathrm{var}}^1, \ldots, Z_{\mathrm{var}}^t$ be a longest sequence of subsets of X' satisfying

- ○ we have for all $1 \leq s \leq t$ the equality

$$Z_{\mathrm{var}}^s = \prod_{i \in S'} Z_i^s$$

  for some subset Z_i^s of $X_i(a, Q)$ with cardinality M;
- ○ we have $Z_{\mathrm{var}}^s \subseteq Y$ and every $y \in Y$ is in at most R different Z_{var}^s;
- ○ for all distinct $1 \leq s, s' \leq t$, we have $\left| Z_{\mathrm{var}}^s \cap Z_{\mathrm{var}}^{s'} \right| \leq 1$.

Define Y_{bad} as

$$Y_{\mathrm{bad}} := \left\{ y \in Y : \left| \left\{ 1 \leq s \leq t : y \in Z_{\mathrm{var}}^s \right\} \right| < R \right\},$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

and let δ be the density of Y_{bad} in X'. With a greedy algorithm, we can construct a subset W of Y_{bad} of density at least δ/RM^m such that $|W \cap Z_{\text{var}}^s| \leq 1$ for all s. If there were to be subsets $Z_i \subseteq X_i(a, Q)$ for each $i \in S'$ satisfying $|Z_i| = M$ and

$$\prod_{i \in S'} Z_i \subseteq W,$$

we could extend our sequence $Z_{\text{var}}^1, \ldots, Z_{\text{var}}^t$ to a longer sequence. Hence we may apply the contrapositive of Proposition 4.1 of Smith [18] to infer

$$M > \frac{\exp(0.3k_{\text{gap}})}{5\log(RM^m/\delta)},$$

since $|X_i(a, Q)| \geq \exp(\exp(0.3k_{\text{gap}}))$ for sufficiently large N thanks to equation (6.4) and the regular spacing. This yields

$$\delta < \frac{RM^m}{\exp\left(\frac{\exp(0.3k_{\text{gap}})}{5M}\right)} \leq \exp(-0.25\exp(k_{\text{gap}})) \tag{6.7}$$

if N is sufficiently large. An application of the Chebotarev density theorem (see Theorem 5.1) shows that for $i > k_{\text{gap}}$

$$|X_i(a, Q \times Z_{\text{var}}^s)| = \frac{|X_i(a, Q)|}{2^{Mm}}\left(1 + O\left(e^{-2k_{\text{gap}}}\right)\right), \tag{6.8}$$

where we made use of the extravagant spacing of k_{gap}. We can deal with a potential exceptional zero due to our Siegel-less assumption on X and the famous theorem of Heilbronn [9]. Then Proposition 5.7 implies that for each $y \in Y$ the quantity $|X(a, Q \times \{y\})|$ is of the expected size. Hence equation (6.7) implies that

$$\left|\sum_{\substack{x \in X(a,Q) \\ \pi_{S'}(x) \in Y_{\text{bad}}}} F(\text{Art}_2(x))\right| \leq \sum_{\substack{x \in X(a,Q) \\ \pi_{S'}(x) \in Y_{\text{bad}}}} 1$$

is easily within the error of our proposition. Given Z_{var}^s, we define

$$\text{Hull}(Z_{\text{var}}^s) := \{Q\} \times Z_{\text{var}}^s \times \prod_{j \in [r] - [k_{\text{gap}}]} X_j(a, Q \times Z_{\text{var}}^s).$$

For each $x \in X(a, Q)$ with $\pi_{S'}(x) \notin Y_{\text{bad}}$, we define the counting function

$$\Lambda(x) := \left|\left\{1 \leq s \leq t : x \in \text{Hull}(Z_{\text{var}}^s)\right\}\right|.$$

We shall compute the first and second moment of $\Lambda(x)$. Since the second moment will turn out to be approximately the square of the first moment, we see that the value of $\Lambda(x)$ is roughly constant. Then we shall use this to reduce to spaces of the shape $\text{Hull}(Z_{\text{var}}^s) \cap X(a, Q)$.

We start by computing the first moment as follows:

$$\sum_{\substack{x\in X(a,Q)\\ \pi_{S'}(x)\notin Y_{\mathrm{bad}}}} \Lambda(x) = \sum_{y\in Y\setminus Y_{\mathrm{bad}}} \sum_{\substack{x\in X(a,Q)\\ \pi_{S'}(x)=y}} \sum_{1\le s\le t} \mathbf{1}_{x\in \mathrm{Hull}(Z^s_{\mathrm{var}})}$$
$$= \sum_{y\in Y\setminus Y_{\mathrm{bad}}} \sum_{1\le s\le t} \left|X(a,Q)\cap \mathrm{Hull}(Z^s_{\mathrm{var}})\cap \pi_{S'}^{-1}(y)\right|.$$

The last expression is obviously 0 if $y\notin Z^s_{\mathrm{var}}$. If $y\in Z^s_{\mathrm{var}}$, we make an appeal to equation (6.8) and Proposition 5.7 to deduce

$$\left|X(a,Q)\cap \mathrm{Hull}(Z^s_{\mathrm{var}})\cap \pi_{S'}^{-1}(y)\right| = \frac{\left|X(a,Q)\cap \pi_{S'}^{-1}(y)\right|}{2^{(M-1)m\cdot|[r]-[k_{\mathrm{gap}}]|}}\left(1+O\left(e^{-k_{\mathrm{gap}}}\right)\right).$$

Since there are precisely R values of s such that $y\in Z^s_{\mathrm{var}}$, we conclude that the first moment of $\Lambda(x)$ is equal to

$$\frac{R}{2^{(M-1)m\cdot|[r]-[k_{\mathrm{gap}}]|}}\left(1+O\left(e^{-k_{\mathrm{gap}}}\right)\right).$$

To compute the second moment, we expand $\Lambda(x)^2$ as

$$\sum_{\substack{x\in X(a,Q)\\ \pi_{S'}(x)\notin Y_{\mathrm{bad}}}} \Lambda(x)^2 = \sum_{y\in Y\setminus Y_{\mathrm{bad}}} \sum_{\substack{x\in X(a,Q)\\ \pi_{S'}(x)=y}} \sum_{1\le s\le t} \sum_{1\le s'\le t} \mathbf{1}_{x\in \mathrm{Hull}(Z^s_{\mathrm{var}})}\mathbf{1}_{x\in \mathrm{Hull}(Z^{s'}_{\mathrm{var}})},$$

which we split as

$$\sum_{y\in Y\setminus Y_{\mathrm{bad}}} \sum_{\substack{x\in X(a,Q)\\ \pi_{S'}(x)=y}} \sum_{1\le s\le t} \mathbf{1}_{x\in \mathrm{Hull}(Z^s_{\mathrm{var}})} + \sum_{y\in Y\setminus Y_{\mathrm{bad}}} \sum_{\substack{x\in X(a,Q)\\ \pi_{S'}(x)=y}} \sum_{\substack{1\le s,s'\le t\\ s\neq s'}} \mathbf{1}_{x\in \mathrm{Hull}(Z^s_{\mathrm{var}})\cap \mathrm{Hull}(Z^{s'}_{\mathrm{var}})}.$$

We have already seen how to deal with the first sum. To treat the second sum, we first rewrite it as

$$\sum_{y\in Y\setminus Y_{\mathrm{bad}}} \sum_{\substack{1\le s,s'\le t\\ s\neq s'}} \left|X(a,Q)\cap \mathrm{Hull}(Z^s_{\mathrm{var}})\cap \mathrm{Hull}(Z^{s'}_{\mathrm{var}})\cap \pi_{S'}^{-1}(y)\right|.$$

Next observe that the above sum is zero if $y\notin Z^s_{\mathrm{var}}\cap Z^{s'}_{\mathrm{var}}$. If $y\in Z^s_{\mathrm{var}}\cap Z^{s'}_{\mathrm{var}}$, we have, again due to the Chebotarev density theorem and Proposition 5.7, that

$$\left|X(a,Q)\cap \mathrm{Hull}(Z^s_{\mathrm{var}})\cap \mathrm{Hull}(Z^{s'}_{\mathrm{var}})\cap \pi_{S'}^{-1}(y)\right| = \frac{\left|X(a,Q)\cap \pi_{S'}^{-1}(y)\right|}{2^{2(M-1)m\cdot|[r]-[k_{\mathrm{gap}}]|}}\left(1+O\left(e^{-k_{\mathrm{gap}}}\right)\right).$$

There are precisely R^2-R pairs of (s,s') such that $y\in Z^s_{\mathrm{var}}\cap Z^{s'}_{\mathrm{var}}$ and $s\neq s'$. Hence the second moment equals

$$\left(\frac{R^2-R}{2^{2(M-1)m\cdot|[r]-[k_{\mathrm{gap}}]|}}+\frac{R}{2^{(M-1)m\cdot|[r]-[k_{\mathrm{gap}}]|}}\right)\left(1+O\left(e^{-k_{\mathrm{gap}}}\right)\right) = \frac{R^2}{2^{2(M-1)m\cdot|[r]-[k_{\mathrm{gap}}]|}}\left(1+O\left(e^{-k_{\mathrm{gap}}}\right)\right).$$

Having computed the first and second moment, we apply Chebyshev's inequality to deduce that outside a set of density $O\left(e^{-0.5k_{\mathrm{gap}}}\right)$ in the subset of those $x\in X(a,Q)$ satisfying $\pi_{S'}(x)\notin Y_{\mathrm{bad}}$, we have that

$$\left|\Lambda(x)-\frac{R}{2^{(M-1)m\cdot|[r]-[k_{\mathrm{gap}}]|}}\right| \le \frac{Re^{-0.25k_{\mathrm{gap}}}}{2^{(M-1)m\cdot|[r]-[k_{\mathrm{gap}}]|}}.$$

From this, we easily deduce that it suffices to prove that

$$\left|\sum_{x\in X(a,Q)\cap\mathrm{Hull}(Z^s_{\mathrm{var}})} F(\mathrm{Art}_2(x))\right| \leq \frac{A|X(a,Q)\cap\mathrm{Hull}(Z^s_{\mathrm{var}})|}{(\log\log\log\log N)^4}.$$

Since we are only dealing with one Z^s_{var} at a time, we will abbreviate it as Z. If $m = 2$, we will also write $Z = Z_1 \times Z_2$ with $i_1(F) \in Z_1$.

We will now define a field L depending on the shape of F as in Definition 6.7. If we are in the first case, we have $m = 1$, and we set

$$L := \prod_{(p_1,p_2)\in Z\times Z} \phi_{p_1p_2,-1}.$$

Here we construct the fields $\phi_{p_1p_2,-1}$ as follows. First pick $p_1 \in Z$ arbitrary and choose fields $\phi_{p_1p_j,-1}$ in $\mathcal{F}^{\mathrm{unr}}_{p_1p_j,-1}$ for all $p_j \neq p_1$. Then we define $\phi_{p_ip_j,-1}$ to be the unique element of $\mathcal{F}^{\mathrm{unr}}_{p_ip_j,-1}$ contained in the compositum $\phi_{p_1p_i,-1}\phi_{p_1p_j,-1}$. If we are instead in the second case, we have $m = 2$, and we define

$$L := \prod_{(p_1,p_2,q_1,q_2)\in Z_1\times Z_1\times Z_2\times Z_2} \phi_{p_1p_2,q_1q_2}.$$

In this case, we pick $p_1 \in Z_1$, $q_1 \in Z_2$ arbitrary, and we choose fields $\phi_{p_1p_i,q_1q_k}$ in $\mathcal{F}^{\mathrm{unr}}_{p_1p_i,q_1q_k}$ for all $p_i \neq p_1$ and all $q_k \neq q_1$. Then we define $\phi_{p_ip_j,q_kq_l}$ to be the unique element of $\mathcal{F}^{\mathrm{unr}}_{p_ip_j,q_kq_l}$ contained in the compositum $\phi_{p_1p_i,q_1q_k}\phi_{p_1p_j,q_1q_k}\phi_{p_1p_i,q_1q_l}\phi_{p_1p_j,q_1q_l}$.

Finally, if we are in the third case, we have $m = 1$ again, and we put

$$L := \prod_{(p_1,p_2)\in Z\times Z} \phi_{p_1p_2,x},$$

where

$$x := (p_1p_2)^{c_{j_2,j_2}} \cdot (-1)^{c_{n_2+1,j_2}}.$$

Let K be the largest multiquadratic extension of $\mathbb{Q}$ inside L. In each case, we have a natural isomorphism

$$\mathrm{Gal}(L/K) \cong \mathcal{A}(Z). \tag{6.9}$$

In the first case, this isomorphism is given by

$$\sigma \mapsto \big((p_1,p_2) \mapsto \pi_{(p_1,p_2)}(\sigma)\big),$$

where $\pi_{(p_1,p_2)}$ is the natural quotient map $\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(K\phi_{p_1p_2,-1}/K) \cong \mathbb{F}_2$. In the second and third cases, we have similar isomorphisms.

Note that any prime $p \in X_j(a,Q)$ splits completely in K by construction. Given $\sigma \in \mathrm{Gal}(L/K)$, we define $X_j(a, Q\times Z, \sigma)$ be the subset of primes $p \in X_j(a, Q\times Z)$ that map to σ under Frobenius. Then Lemma 3.1 and Proposition 5.1 yield

$$|X_{i_2(F)}(a, Q\times Z,\sigma)| = \frac{|X_{i_2(F)}(a,Q\times Z)|}{2^{(M-1)^m}}\left(1+O\left(e^{-k_{\mathrm{gap}}}\right)\right).$$

Proposition 5.11 shows that for almost all choices of $Q_{\text{gap}} \in \prod_{[r]-[k_{\text{gap}}]-i_2(F)} X_j(a, Q \times Z)$ consistent with a, we have that $|X_{i_2(F)}(a, Q \times Q_{\text{gap}} \times Z)|$ is of the expected size and furthermore

$$|X_{i_2(F)}(a, Q \times Q_{\text{gap}} \times Z, \sigma)| = \frac{|X_{i_2(F)}(a, Q \times Q_{\text{gap}} \times Z)|}{2^{(M-1)^m}} \left(1 + O\left(e^{-k_{\text{gap}}}\right)\right) \tag{6.10}$$

for all $\sigma \in \text{Gal}(L/K)$. By construction, we have that

$$Z_{\text{final}} := \{Q\} \times Z \times \{Q_{\text{gap}}\} \times X_{i_2(F)}(a, Q \times Q_{\text{gap}} \times Z) \subseteq X(a, Q),$$

so it suffices to prove that

$$\left| \sum_{x \in Z_{\text{final}}} F(\text{Art}_2(x)) \right| \leq \frac{A|Z_{\text{final}}|}{(\log\log\log\log N)^4}. \tag{6.11}$$

Now pick

$$\epsilon := \frac{1}{(\log\log\log\log N)^4}.$$

We formally apply Theorem 3.3 to $Z \times [M]$. We see that Theorem 3.3 guarantees the existence of $g_{\text{spec}} \in \mathcal{A}(Z \times [M])$ such that g_{spec} is not ϵ-bad. Now pick any $x_1, \dots, x_M \in X_{i_2(F)}(a, Q \times Q_{\text{gap}} \times Z)$. Then we can define a map $[M] \times [M] \to \text{Gal}(L/K)$ by

$$g(i, j) := \text{Frob}_{L/K}(x_i) + \text{Frob}_{L/K}(x_j),$$

which we can naturally view as a map $[M] \times [M] \to \mathcal{A}(Z)$ due to the isomorphism in equation (6.9). Hence g naturally becomes an element of $\mathcal{A}(Z \times [M])$.

We claim that we can find disjoint ordered subsets $A_1, \dots, A_k$ of $X_{i_2(F)}(a, Q \times Q_{\text{gap}} \times Z)$ whose union is the whole set $X_{i_2(F)}(a, Q \times Q_{\text{gap}} \times Z)$ except for a small remainder such that defining g as above for each $A_1, \dots, A_k$, we get g_{spec} under the natural identifications.

Let $g'_{\text{spec}} : [M] \times [M] \to \text{Gal}(L/K)$ be the map that is sent to g_{spec} under the natural identifications. Suppose that elements $x_1, \dots, x_M \in X_{i_2(F)}(a, Q \times Q_{\text{gap}} \times Z)$ are given. Now look at the equation

$$g'_{\text{spec}}(i, j) := \text{Frob}_{L/K}(x_i) + \text{Frob}_{L/K}(x_j).$$

We see that one can freely choose x_1, and then all the $\text{Frob}_{L/K}(x_j)$ for $j > 1$ are uniquely determined by $g'_{\text{spec}}(i, j)$ and $\text{Frob}_{L/K}(x_1)$. Now an appeal to equation (6.10) finishes the proof of our claim.

Now pick one of the A_i and suppose that $A_i = \{x_1, \dots, x_M\}$. Let $\widetilde{F} : Z_{\text{final}} \to \mathbb{F}_2$ be the map that sends x to $\iota \circ F(\text{Art}_2(x))$. We can restrict $\widetilde{F}$ to A_i and then naturally view $\widetilde{F}$ as a map from $Z \times [M]$ to $\mathbb{F}_2$. Theorem 3.3 then implies equation (6.11) and therefore Proposition 6.9, provided that we can verify the identity $d\widetilde{F} = g'_{\text{spec}}$.

We distinguish three cases depending on the type of F as in Definition 6.7. In the first case, we apply Theorem 2.11 and Theorem 2.12. Let (j_1, j_2) be the entry as chosen in Definition 6.7, so that $c_{j_1,j_2} = c_{j_2,j_1} = 1$. Theorem 2.12 gives

$$d\widetilde{F}_{j_1,j_2} = g'_{\text{spec}},$$

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

where $\widetilde{F}_{j_1,j_2}$ is obtained from F_{j_1,j_2} in the same way as $\widetilde{F}$ was obtained from F. Now consider any (j_3, j_4) not equal to (j_1, j_2), with $1 \leq j_3 \leq n_2 + 1$, $1 \leq j_4 \leq n_2$ and $c_{j_3,j_4} = 1$. Then we have $j_3 \leq n_2$ and $c_{j_4,j_3} = 1$. Hence Theorem 2.11 implies

$$d\widetilde{F}_{j_3,j_4} = 0.$$

Altogether, we conclude that $d\widetilde{F} = g'_{\text{spec}}$.

We now deal with the second case. Once more let (j_1, j_2) be the entry as chosen in Definition 6.7, so that $1 \leq j_1, j_2 \leq n_2$, $c_{j_1,j_2} = 1$ and $c_{j_2,j_1} = 0$. Two applications of part (ii) of Theorem 2.9 show that

$$d\widetilde{F}_{j_1,j_2} = g'_{\text{spec}}.$$

Two applications of Theorem 2.10 show that for all $1 \leq j_2 \leq n_2$,

$$d\widetilde{F}_{j_2,j_2} = 0,$$

while two applications of part (i) of Theorem 2.9 imply

$$d\widetilde{F}_{j_3,j_4} = 0$$

for all $1 \leq j_3 \leq n_2 + 1$, $1 \leq j_4 \leq n_2$ such that $(j_1, j_2) \notin \{(j_3, j_4), (j_4, j_3)\}$ and $j_3 \neq j_4$. This finishes the proof of the second case.

It remains to treat the third case, which follows from an application of Theorem 2.9 and Theorem 2.10. □

Acknowledgements. We would like to thank Andrew Granville for his support throughout this project. We wish to thank Peter Stevenhagen for some very helpful discussions at the beginning of the project. We are grateful to Alexander Smith for answering questions about his paper and for several conversations on the challenges of this project. We are also grateful to Mark Watkins for pointing out a small error in a previous version. We would also like to thank Kevin Ford, Andrew Granville and Sam Porritt for their useful suggestions in writing some of the proofs in Section 4.

Conflicts of Interest. None.

Funding statement. The first and third authors were supported by the European Research Council grant agreement No. 670239. The second and fourth author are grateful to the Max Planck Institute for Mathematics in Bonn for its financial support.

References

[1] K. Alladi. An Erdős-Kac theorem for integers without large prime factors. *Acta Arith.*, **49**(1): 81–105, 1987.

[2] N. Alon and J. H. Spencer. *The probabilistic method*. Wiley Series in Discrete Mathematics and Optimization. John Wiley & Sons, Inc., Hoboken, NJ, fourth edition, 2016.

[3] J. E. Cremona and R. W. K. Odoni. Some Density Results for Negative Pell Equations; an Application of Graph Theory. *J. Lond. Math. Soc. (2)*, **39**(1): 16–28, 1989.

[4] É. Fouvry and J. Klüners. Cohen-Lenstra heuristics of quadratic number fields. *Algorithmic number theory*, 40–55, Lecture Notes in Comput. Sci., **4076**, Springer, Berlin, 2006.

[5] É. Fouvry and J. Klüners. On the 4-rank of class groups of quadratic number fields. *Invent. Math.*, **167**(3): 455–513, 2007.

[6] É. Fouvry and J. Klüners. On the negative Pell equation. *Ann. of Math. (2)*, **172**(3): 2035–2104, 2010.

[7] É. Fouvry and J. Klüners. The parity of the period of the continued fraction of $\sqrt{d}$. *Proc. Lond. Math. Soc. (3)*, **101**(2): 337–391, 2010.

[8] F. Gerth. Limit probabilities for coranks of matrices over $GF(q)$. *Linear and Multilinear Algebra*, **19**:1, 79–93.

[9] H. Heilbronn. On real zeros of Dedekind ζ-functions. *Canadian Journal of Math.*, **25**: 870–873, 1973.

[10] D. Hensley. The distribution of $\Omega(n)$ among numbers with no large prime factors. In *Analytic number theory and Diophantine problems (Stillwater, OK, 1984),* volume **70** of *Progr. Math.,* pages 247–281. Birkhäuser Boston, Boston, MA, 1987.

[11] A. Hildebrand. On the number of prime factors of integers without large prime divisors. *J. Number Theory*, **25**(1): 81–106, 1987.

[12] M. Jutila. On mean values of Dirichlet polynomials with real characters. *Acta Arith.*, **27**: 191–198, 1975.

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press

[13] P. Koymans and C. Pagano. On the distribution of $\mathsf{Cl}(K)[l^\infty]$ for degree l cyclic fields. *J. Eur. Math. Soc*. DOI:10.4171/JEMS/1112

[14] E. Landau. Losung des Lehmer'schen Problems. *Amer. J. Math.*, **31**(1): 86–102, 1909.

[15] J. MacWilliams. Orthogonal matrices over finite fields. *Amer. Math. Monthly*, **76**: 152–164, 1969.

[16] A. Selberg. Note on a paper by L. *G. Sathe. J. Indian Math. Soc. (N.S.)*, **18**: 83–87, 1954.

[17] A. Smith. Governing fields and statistics for 4-Selmer groups and 8-class groups. *arXiv preprint:*1607.07860.

[18] A. Smith. 2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture. *arXiv preprint:*1702.02325.

[19] P. Stevenhagen. The number of real quadratic fields having units of negative norm. *Experiment. Math.*, **2**(2): 121–136, 1993.

[20] P. Stevenhagen. Redei reciprocity, governing fields and negative Pell. *Math. Proc. Camb. Phil. Soc.*, 1–28. DOI:10.1017/S0305004121000335.

[21] C. Tudesq. Majoration de la loi locale de certaines fonctions additives. *Arch. Math. (Basel)*, **67**(6): 465–472, 1996.

https://doi.org/10.1017/fms.2022.40 Published online by Cambridge University Press