Max-Planck-Institut für Mathematik Bonn

On Stevenhagen's conjecture
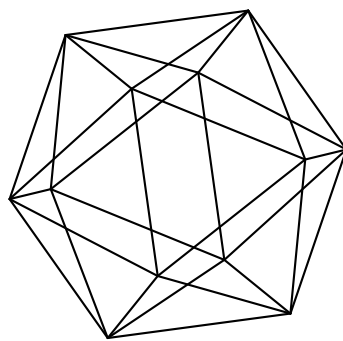
by

Peter Koymans
Carlo Pagano

On Stevenhagen's conjecture

by

Peter Koymans
Carlo Pagano

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Department of Mathematics
University of Michigan
Ann Arbor, MI 48109
USA

School of Mathematics and Statistics
University of Glasgow
University Place
Glasgow G12 8SQ
UK

On Stevenhagen's conjecture

Peter Koymans[*1] and Carlo Pagano[†2]

[1]University of Michigan
[2]University of Glasgow

August 7, 2022

Abstract

We generalize a classical reciprocity law due to Rédei using our recently developed description of the 2-torsion of class groups of multiquadratic fields. This result is then used to prove a variety of new reflection principles for class groups, one of which involves a symbol similar to the spin symbol as defined in work of Friedlander, Iwaniec, Mazur and Rubin. With these reflection principles we overcome a well-known impasse faced by the most recent techniques available in class groups. As a first application, we prove Stevenhagen's conjecture on the solubility of the negative Pell equation.

1 Introduction

Integral points on conics are a classical topic of study going back to at least the ancient Greeks. For fixed squarefree $d > 0$, the equation

$$x^2 - dy^2 = 1 \text{ to be solved in } x, y \in \mathbb{Z}$$

is known as Pell's equation and features in Archimedes' cattle problem. This equation was extensively studied by the Indian mathematicians Brahmagupta and Bhaskara II, who gave an algorithm to find a non-trivial solution of the equation for a given value of d.

Unbeknownst of the work of these Indian mathematicians, its study began in Europe with Pierre de Fermat who challenged several English mathematicians to solve it for various values of d with $d = 61$ being particularly notorious (the smallest non-trivial solution being $x = 1766319049$ and $y = 226153980$). Inspired by Fermat's inquiries, William Brouncker and John Wallis also found an algorithm to solve Pell's equation. Euler then misattributed their work to John Pell and named the equation in his honor.

In this paper we shall focus on the equation

$$x^2 - dy^2 = -1 \text{ to be solved in } x, y \in \mathbb{Z}, \tag{1.1}$$

which is known as the negative Pell equation. Unlike Pell's equation, it is not true that there is always a solution to equation (1.1). Indeed, for equation (1.1) to be soluble it must certainly be soluble with $x, y \in \mathbb{Q}$. The Hasse–Minkowski theorem then shows that equation (1.1) is soluble with $x, y \in \mathbb{Q}$ if and only if $p \mid d$ implies $p \equiv 1, 2 \bmod 4$.

---

[*]Department of Mathematics, Ann Arbor, MI 48109, USA, koymans@umich.edu
[†]School of Mathematics and Statistics, University Place, Glasgow G12 8SQ, UK, carlein90@gmail.com

Inspired by this, we define $\mathcal{D}$ to be the set of squarefree integers $d > 0$ such that $p \mid d$ implies $p \equiv 1, 2 \bmod 4$ and we define $\mathcal{D}^-$ to be the set of squarefree integers d for which equation (1.1) is soluble. Dirichlet [14] proved that every prime number $p \equiv 1 \bmod 4$ lies in $\mathcal{D}^-$. In particular, $\mathcal{D}^-$ is an infinite set. It is well-known, see [18, Lemma 1], that $d \in \mathcal{D}^-$ if and only if the 2-Sylow subgroup of the ordinary class group of $\mathbb{Q}(\sqrt{d})$ coincides with the 2-Sylow subgroup of the narrow class group. We define $\mathcal{D}(X)$ and $\mathcal{D}^-(X)$ to be those d that further satisfy $d < X$. We are interested in the quantity

$$\lim_{X \to \infty} \frac{|\mathcal{D}^-(X)|}{|\mathcal{D}(X)|}.$$

Nagell [37] conjectured that the limit exists and lies in the interval $(0, 1)$. Stevenhagen developed a heuristical model to predict the value of the above limit[1]. Based on this model, he [43] conjectured that

$$\lim_{X \to \infty} \frac{|\mathcal{D}^-(X)|}{|\mathcal{D}(X)|} = 1 - \alpha, \quad \alpha = \prod_{j \text{ odd}} (1 - 2^{-j}) \approx 0.41942.$$

Cremona–Odoni [11] studied the analogous problem in case the number of prime divisors is equal to a fixed integer $t \geq 1$, which is traditionally viewed as an easier problem[2]. Their main theorem shows that, in this setting, the lim inf is bounded below by some number λ_t satisfying $\lambda_t \geq \alpha$. Their method is similar to the one used by Gerth [21] to deal with the 4-rank of class groups. Blomer [4] showed that

$$\mathcal{D}^-(X) \gg \frac{X}{(\log X)^{0.62}},$$

which is a small logarithmic power off (namely 0.12) from the correct order of magnitude. Fouvry and Klüners [18] were the first to make substantial progress towards Stevenhagen's conjecture. They showed that

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

One important feature of their work is that the number of prime factors is no longer treated as fixed. The lower bound was further improved by Fouvry and Klüners [19], and later by joint work of Chan–Koymans–Milovic–Pagano [8], who extended [41] to the family $\mathcal{D}$. These works proceeded by studying the 4-torsion and 8-torsion of the narrow class group for which the algebraic foundations were laid by Rédei and Reichardt [38, 39, 40]. Recently, the upper bound was further improved by the authors [29] with the main tool being a generalization of the Rédei reciprocity law. In this paper we shall prove Stevenhagen's conjecture.

Theorem 1.1. *We have*
$$\lim_{X \to \infty} \frac{|\mathcal{D}^-(X)|}{|\mathcal{D}(X)|} = 1 - \alpha.$$

---

[1]Strictly speaking, this is not true, since Stevenhagen orders the real quadratic fields by discriminants instead of radicands. However, both the heuristic model and our proofs work for both orderings.

[2]In retrospect, this might in fact be the harder problem. At the time of writing the authors are unable to prove the analogue of Stevenhagen's conjecture when the number of prime divisors is fixed.

Using an argument similar to [42, Corollary 7.2], one can use Theorem 8.1 to give an explicit error term for the rate of convergence in Theorem 1.1. The implied constant is effectively computable.

We remark that the Galois module structure of the unit group of a real quadratic field is precisely determined by the solubility of the negative Pell equation. From this standpoint, Theorem 1.1 can be interpreted as giving an asymptotic formula for the occurrence of a certain Galois module structure, namely $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ with the action that sends $(1, 0)$ to $(-1, 1)$ and fixes $(0, 1)$. It is also worth mentioning that some interesting conjectures have recently been proposed for the Galois module structure of the unit group of odd degree abelian extensions of $\mathbb{Q}$, see [7].

Since classical techniques in analytic number theory give an asymptotic formula for $|\mathcal{D}(X)|$, Theorem 1.1 implies an asymptotic formula for $|\mathcal{D}^-(X)|$. From now on we will write $\mathrm{Cl}(K)$ for the narrow class group of a number field K. Our proof proceeds by studying the distribution of $2\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$ for $d \in \mathcal{D}$. In outstanding work, Smith [42] recently proved Gerth's [21] extension fo the Cohen–Lenstra heuristics [9], that is

$$\frac{|\{K \text{ im. quadr.} : |D_K| \leq X, 2\mathrm{Cl}(K)[2^\infty] \cong A\}|}{|\{K \text{ im. quadr.} : |D_K| \leq X\}|} = \frac{\prod_{i=1}^\infty (1 - 2^{-i})}{|\mathrm{Aut}(A)|} \tag{1.2}$$

for any finite, abelian 2-group A. Here D_K denotes the discriminant of K. Earlier, Fouvry and Klüners [16, 17] found the distribution of $2\mathrm{Cl}(K)[4]$ based on work of Heath-Brown on 2-Selmer groups [22]. Using Smith's ideas, the authors [27] established the analogue of equation (1.2) for cyclic fields of odd prime degree conditional on GRH. This generalizes earlier work of Klys [25] who dealt with the analogous results of Fouvry and Klüners [16, 17] in this setting. Smith recently announced that he has obtained an unconditional generalization of the results in [27] to arbitrary base fields. In the process, he also obtained an excellent error term by developing a flexible version of the large sieve.

In order to prove Theorem 1.1, it is natural to use the ideas introduced by Smith in [42]. However, it is worth emphasizing that the method developed in [42] faces fundamental difficulties when applied to the family $\mathcal{D}$: in fact the entire set $\mathcal{D}$ lands in the error term if one were to follow Smith's methods. In the present work we introduce a number of new techniques that allow us to overcome this impasse. As we outline below, this technological advancement is made possible by several discoveries of independent interest.

Firstly, we establish two new types of reciprocity laws. The first reciprocity law generalizes quadratic reciprocity and Rédei's reciprocity law to arbitrarily high nilpotency class (a substantially weaker version of this result can be found in [29]). The second reciprocity law is intimately related to spins of prime ideals as defined in [20], and proves that a certain spin symbol vanishes. At this point we make essential use of the fact that we are working with the set $\mathcal{D}$. An important guide in the proof of these laws has been our finding of a genus theory in arbitrarily high nilpotency class [28], which generalizes the classical genus theory of Gauss for quadratic extensions.

Secondly, we use these new reciprocity laws to deduce novel reflection principles, in which one compares the class group structure of various fields. We expect that these new tools allow one to attack a large number of well-known conjectures, with an articulated list at the end of this introduction.

We now describe the four fundamental obstacles that one faces from a more technical perspective. To explain the issues, we write $\langle b, \chi_a \rangle_{k, \mathbb{Q}(\sqrt{d})}$ for the pairing $\mathrm{Art}_{k, \mathbb{Q}(\sqrt{d})}$ (see

Subsection 2.3 for the definition) between the character $\chi_a : G_{\mathbb{Q}} \to \mathbb{F}_2$, corresponding to the field $\mathbb{Q}(\sqrt{a})$, and the unique ideal of $\mathbb{Q}(\sqrt{d})$ of norm b. Let

$$C = \{d_0\} \times \{p_{1,1}, p_{1,2}\} \times \cdots \times \{p_{k,1}, p_{k,2}\}$$

be a product space, thought of as squarefree integers by multiplying out the coordinates. Given divisors a and b of d_0, Smith's main algebraic result is a reflection principle of the shape

$$\sum_{d \in C} \langle b\pi_k(d), \chi_a + \chi_{\pi_1(d)} \rangle_{k-1, \mathbb{Q}(\sqrt{d})} = \mathrm{Frob}_{K_{p_{1,1}, p_{1,2}, \ldots, p_{k-1,1}, p_{k-1,2}}/\mathbb{Q}}(p_{k,1}) +$$

$$\mathrm{Frob}_{K_{p_{1,1}, p_{1,2}, \ldots, p_{k-1,1}, p_{k-1,2}}/\mathbb{Q}}(p_{k,2}), \quad (1.3)$$

where π_i denotes the natural projection map, $K_{p_{1,1}, p_{1,2}, \ldots, p_{k-1,1}, p_{k-1,2}}$ is an explicit number field depending on $p_{1,1}, p_{1,2}, \ldots, p_{k-1,1}, p_{k-1,2}$ and $\mathrm{Frob}(p_{k,i})$ lands in

$$Z(\mathrm{Gal}(K_{p_{1,1}, p_{1,2}, \ldots, p_{k-1,1}, p_{k-1,2}}/\mathbb{Q})) \cong \mathbb{F}_2$$

with $Z(G)$ denoting the center of a group G. The fields $K_{p_{1,1}, p_{1,2}, \ldots, p_{k-1,1}, p_{k-1,2}}$ are extensively studied in [28]. To apply such a reflection principle one needs to find appropriate choices for a and b, which is not always possible in our setting. Indeed, a first problem is that the solubility of negative Pell is equivalent to $(\sqrt{d})$ being trivial in the narrow class group. This means that we have to compute the Artin pairing with d, which is not covered by equation (1.3). In this case one gets

$$\sum_{d \in C} \langle d, \chi_a + \chi_{\pi_1(d)} \rangle_{k, \mathbb{Q}(\sqrt{d})} = \mathrm{Frob}_{K_{p_{1,1}, p_{1,2}, \ldots, p_{k,1}, p_{k,2}}/\mathbb{Q}}(\infty).$$

This is problematic, since Smith shows equidistribution of the right-hand side and then uses ingenious combinatorics to deduce from this equidistribution of the left-hand side. To prove equidistribution of the right-hand side, we extend a reciprocity law first presented in [29]. This reciprocity law is a generalization of the classical quadratic reciprocity law and Rédei's reciprocity law [39] (see Stevenhagen's work for an extensive treatment [44] or Corsman's thesis [10]). Equidistribution of the right-hand side is then a consequence of the Chebotarev density theorem.

To make matters worse, the first Artin pairing $\mathrm{Art}_{1, \mathbb{Q}(\sqrt{d})}$ is symmetric for $d \in \mathcal{D}$. Therefore we would like to have a reflection principle of the shape

$$\sum_{d \in C} \langle a, \chi_a \rangle_{k+1, \mathbb{Q}(\sqrt{d})} = \cdots$$

We first show in Theorem 5.3 that the right-hand side resembles a spin symbol, see [20] for the precise definition of spin symbols. Then we will show in Theorem 5.5 that this particular spin symbol is trivial. In principle this is possible by adapting the argument in [20, Section 12] together with our description of the 2-torsion of class groups of multiquadratic fields [28]. We have however opted for a different argument based on Massey symbols and Hilbert reciprocity.

At first sight, it may seem rather problematic that the right-hand side is identically zero. However, we use Theorem 5.5 and a simple trick to compute

$$\sum_{d \in C} \langle a\pi_1(d) \cdot \ldots \cdot \pi_{k-1}(d), \chi_a + \chi_{\pi_1(d)} + \cdots + \chi_{\pi_{k-1}(d)} \rangle_{k, \mathbb{Q}(\sqrt{d})}.$$

This does give a reflection principle of the desired shape after an application of Theorem 3.2, which is a strengthening of the reciprocity law from [29].

A final obstacle comes from the fact that the cube C is one dimension smaller than the cubes appearing in [42]. This fact rules out the usual strategy of proving reflection principles, introduced in [42], by imposing physical equalities between certain 1-cochains. To overcome this issue, we introduce the formalism of profitable triples (see Section 4), a new method to prove reflection principles based on our novel reciprocity law Theorem 3.2.

Once these obstacles are overcome, the rest of the proof is a straightforward adaptation of Smith's work. Although we shall not prove it in this paper, it is not hard to extend our techniques to obtain the distribution of $2\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$ in the family $\mathcal{D}$.

There are several open problems where Smith's method faces similar issues because of symmetry properties of a certain pairing:

- show 100% non-vanishing of $L(\frac{1}{2}, \chi)$ over function fields[3];

- remove the assumption on rational 4-torsion points in [42, Theorem 1.1];

- show that Greenberg's conjecture holds for the cyclotomic $\mathbb{Z}_2$-extension for 100% of the real quadratic fields ordered by discriminant;

- study of the Galois module structure of the unit group for biquadratic (or more general abelian) extensions ordered by discriminant or conductor. A conjectural framework for odd degree abelian extensions is developed in [7];

- the strong form of Malle's conjecture for nilpotent extensions;

- the distribution of unramified G-extensions, where G is a 2-group. Heuristics and function field results are available for odd p-groups in [5, 6, 33, 48];

- deal with the distribution of 2-parts of class groups in the family $\mathbb{F}_q(t, \sqrt{D})$ with $q \equiv 1 \bmod 4$;

- obtain the distribution of $\mathrm{Cl}(K)[2^\infty]$ as K varies over cyclic degree 4 extensions;

- find the distribution of $\mathrm{Cl}(K)[2^\infty]$ as K varies over quadratic extensions over $\mathbb{Q}(i)$ or if K varies over biquadratic extensions containing $\mathbb{Q}(i)$.

It might be possible to extend our reflection principles to some of the above settings. This could then be combined with Smith's method. In some of the cases listed above there are additional roots of unity. In this case it is known that also some of the higher Artin pairings obey certain symmetry properties, see the work of Morgan–Smith [36] and Lipnowski–Sawin–Tsimerman [32]. It would be interesting to see the interplay between Smith's method, the techniques presented here and the additional symmetry properties.

Finally, we will mention some other results related to the Cohen–Lenstra heuristics. There is the classical work of Davenport–Heilbronn [13] on the first moment of $\mathrm{Cl}(K)[3]$ that predates the work of Cohen and Lenstra. The work of Davenport–Heilbronn was extended by Datskovsky–Wright [12] to general number fields and to a large class of 2-extensions by Lemke

---

[3]We thank Mark Shusterman for pointing this out to the authors. We hope to study this problem further in future joint work with Mark Shusterman.

Oliver–Wang–Wood [31], while [3] and [45] independently gave a secondary main term over the rational number field. There is also work of Bhargava [1, 2] on the number of S_4 and S_5-extensions. Over function fields the situation is much better understood thanks to the work of Ellenberg–Venkatesh–Westerland [15].

1.1 Notation and conventions

Throughout the paper we shall make use of the following notations.

- We use $\subseteq$ for inclusions and $\subset$ for strict inclusions.

- If $n \in \mathbb{Z}_{\geq 0}$, we define $[n] := \{1, \ldots, n\}$.

- If $X = X_1 \times \cdots \times X_r$ is a product space, we write $\pi_i : X \to X_i$ for the natural projection map.

- For a product space $X = X_1 \times \cdots \times X_r$ and $S \subseteq [r]$, we define

$$\mathrm{Cube}(X, S) = \prod_{i \in S} X_i^2 \times \prod_{i \in [r]-S} X_i.$$

  For $T \subseteq [r]$, we let π_T be the natural projection map from $\mathrm{Cube}(X, S)$ to

$$\prod_{i \in T \cap S} X_i^2 \times \prod_{i \in T \cap ([r]-S)} X_i.$$

  We write pr_1 and pr_2 for the two natural projection maps from X_i^2 to X_i.

- Let $X = X_1 \times \cdots \times X_r$, $S \subseteq [r]$ and $\bar{x} \in \mathrm{Cube}(X, S)$. If $T \subseteq S$, then $\bar{x}(T)$ is the subset of those $\bar{y} \in \mathrm{Cube}(X, T)$ such that

$$\pi_i(\bar{y}) \in \{\mathrm{pr}_1(\pi_i(\bar{x})), \mathrm{pr}_2(\pi_i(\bar{x}))\} \text{ for all } i \in S - T, \quad \pi_{[r]-(S-T)}(\bar{x}) = \pi_{[r]-(S-T)}(\bar{y}).$$

- If K is a field, we write G_K for its absolute Galois group.

- If K is a global field, we write Ω_K for its set of places.

- For $v \in \Omega_K$, we write K_v for the completion of K at v. If v is finite, then we write $\mathbb{F}_v$ for the residue field.

- We say that a finite place is odd if it does not lie above (2).

- If K is a local field, we write K^{unr} for the maximal unramified extension of K.

- We will sometimes use $\cdot$ and $\prod$ to denote the compositum of fields.

- If $a \in \mathbb{Q}^*$, then $\chi_a : G_{\mathbb{Q}} \to \mathbb{F}_2$ is the quadratic character of $G_{\mathbb{Q}}$ associated to $\mathbb{Q}(\sqrt{a})$. More generally, if K is a field of characteristic 0 and $\gamma \in K^*$, we will write χ_γ for the associated quadratic character.

- We will often implicitly view $\mathbb{F}_2$ as a $G_{\mathbb{Q}}$-module with the discrete topology and the trivial action.

- We write $\mathrm{Cl}(K)$ for the narrow class group of a number field K.

- If G is a profinite group, X is a discrete topological space and $\phi : G \to X$ is a continuous map, we define $N(\phi)$ to be the largest normal open subgroup through which ϕ factors; it is an exercise to show that there exists at least one normal open subgroup through which ϕ factors, so that the above definition makes sense. In case G is a Galois group, we denote by $L(\phi)$ the field extension corresponding to $N(\phi)$, and call it *the field of definition*.

- Let p be a prime. Let $K/\mathbb{Q}$ be a quadratic extension in which p ramifies. Then we write $\mathrm{Up}_{K/\mathbb{Q}}(p)$ for the unique place of K above p. More generally, if a is a positive, squarefree integer composed of primes p ramifying in $K/\mathbb{Q}$, we define $\mathrm{Up}_{K/\mathbb{Q}}(a)$ to be the unique integral ideal with norm a.

- If A is a set of quadratic characters from $G_{\mathbb{Q}}$ to $\mathbb{F}_2$, we define $\mathbb{Q}(A)$ to be the fixed field of $\bigcap_{\chi \in A} \ker(\chi)$.

- We call an integer $n \in \mathbb{Z}$ squarefree if $p \mid n$ implies $p^2 \nmid n$. In particular, squarefree integers can be of any sign.

Acknowledgements

2   Preliminaries

The goal of this section is to fix a number of choices used in the rest of this paper and to introduce raw cocycles, expansion maps and Artin pairings. Fix once and for all a separable closure $\mathbb{Q}^{\mathrm{sep}}$ of $\mathbb{Q}$. We also fix, for each place v of $\mathbb{Q}$, a separable closure $\mathbb{Q}_v^{\mathrm{sep}}$ of $\mathbb{Q}_v$. We further choose an embedding
$$i_v : \mathbb{Q}^{\mathrm{sep}} \to \mathbb{Q}_v^{\mathrm{sep}}.$$

Such an embedding induces a continuous, injective homomorphism
$$i_v^* : G_{\mathbb{Q}_v} \to G_{\mathbb{Q}}.$$

From now on all our number fields are implicitly taken inside our fixed separable closure $\mathbb{Q}^{\mathrm{sep}}$.

We denote by $\mathbb{Q}^{\text{pro-2}}$ the union of all finite Galois subextensions of $\mathbb{Q}^{\text{sep}}/\mathbb{Q}$ whose degree is a power of 2 and we write

$$\mathcal{G}_{\mathbb{Q}}^{\text{pro-2}} := \text{Gal}(\mathbb{Q}^{\text{pro-2}}/\mathbb{Q})$$

for the corresponding Galois group. Let $\pi_{\text{pro-2}} : G_{\mathbb{Q}} \to \mathcal{G}_{\mathbb{Q}}^{\text{pro-2}}$ be the natural projection map.

For each finite place v of $\mathbb{Q}$, we let

$$I_v := \ker(G_{\mathbb{Q}_v} \to G_{\mathbb{F}_v}) = \text{Gal}(\mathbb{Q}_v^{\text{sep}}/\mathbb{Q}_v^{\text{unr}}).$$

be the inertia group at v. We denote by $\mathcal{P}$ the collection of odd places of $\mathbb{Q}$. Let us recall the following basic fact.

Proposition 2.1. *We have*

$$I_v(2) := \pi_{\text{pro-2}} \circ i_v^*(I_v) \cong_{\text{top.gr.}} \mathbb{Z}_2$$

for each $v \in \mathcal{P}$.

Proof. Since v is odd, it follows from local class field theory[4] that the maximal pro-2-extension L of $\mathbb{Q}_v$ equals

$$\bigcup_{k=1}^{\infty} \mathbb{Q}_v \left(\zeta_{2^k}, \sqrt[2^k]{\pi} \right), \tag{2.1}$$

where π is a uniformizer at v. Let $I_v^{\text{pro-2}}$ be the maximal pro-2-quotient of I_v. Equation (2.1) implies that $I_v^{\text{pro-2}} \cong_{\text{top.gr.}} \mathbb{Z}_2$, since

$$\bigcup_{k=1}^{\infty} \mathbb{Q}_v \left(\zeta_{2^k} \right)$$

is an unramified extension of $\mathbb{Q}_v$ containing all roots of unity ζ_{2^k}. The continuous homomorphism $\pi_{\text{pro-2}} \circ i_v^* : I_v \to \mathcal{G}_{\mathbb{Q}}^{\text{pro-2}}$ induces a continuous homomorphism $f : I_v^{\text{pro-2}} \to \mathcal{G}_{\mathbb{Q}}^{\text{pro-2}}$ with the same image as $\pi_{\text{pro-2}} \circ i_v^*$. Using equation (2.1) one more time, we see that f is injective. Indeed, take any $a \in \mathbb{Q}$ with $v(a) = 1$. Since $\zeta_2 \in \mathbb{Q}$, the field

$$K := \bigcup_{k=1}^{\infty} \mathbb{Q} \left(\zeta_{2^k}, \sqrt[2^k]{a} \right)$$

is a pro-2 extension of $\mathbb{Q}$. Furthermore, $\mathbb{Q}_v \cdot i_v(K) = L$. This completes the proof. $\qquad\square$

Thanks to Proposition 2.1 there exists a topological generator of $I_v(2)$ for each odd place v. We make a choice σ_v of such a generator for the remainder of this paper. Write $I_2(2) := \pi_{\text{pro-2}} \circ i_2^*(I_2)$ and pick $\sigma_2(1), \sigma_2(2) \in I_2(2)$ such that

$$\chi_{-1}(\sigma_2(1)) = 1, \quad \chi_{-1}(\sigma_2(2)) = 0, \quad \chi_2(\sigma_2(1)) = 0, \quad \chi_2(\sigma_2(2)) = 1.$$

This is possible, since the extension $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ is totally ramified at (2).

---

[4] Alternatively, one can use an elementary argument based on [27, Proposition A.5].

Proposition 2.2. *The set*

$$\mathfrak{G} := \{\sigma_v : v \in \mathcal{P}\} \cup \{\sigma_2(1), \sigma_2(2)\}$$

is a minimal set of topological generators of $\mathcal{G}_{\mathbb{Q}}^{\text{pro-2}}$.

Proof. We will first argue that $\mathfrak{G}$ is a set of topological generators. Note that a subset S of a profinite group $\mathcal{G}$ topologically generates $\mathcal{G}$ if and only if $\pi(S)$ generates G in every continuous finite quotient $\pi : \mathcal{G} \to G$. So let $K/\mathbb{Q}$ be a finite 2-extension. We must show that (the images of) $\mathfrak{G}$ generates $G = \text{Gal}(K/\mathbb{Q})$.

But since G is a finite group, we know that a subset S generates if and only if it generates modulo the Frattini subgroup $\Phi(G)$. Furthermore, $\Phi(G) = G^2[G, G]$ for a finite 2-group G. Hence it suffices to show that $\mathfrak{G}$ generates $\text{Gal}(L/\mathbb{Q})$, where $L/\mathbb{Q}$ is an arbitrary multiquadratic extension. This is in turn equivalent to $\mathfrak{G}$ generating $\text{Gal}(M/\mathbb{Q})$ for every quadratic extension M of $\mathbb{Q}$, which is readily verified.

Finally, if we remove any element of $\mathfrak{G}$, it is not hard to find a quadratic extension $M/\mathbb{Q}$ in which $\mathfrak{G}$ does not generate. This shows the minimality claim. $\qquad\square$

From now on we denote by $\mathfrak{G}$ this fixed choice of topological generators of $\mathcal{G}_{\mathbb{Q}}^{\text{pro-2}}$. We shall often invoke the following basic fact.

Proposition 2.3. *Let $L/\mathbb{Q}$ be a finite Galois subextension of $\mathbb{Q}^{\text{pro-2}}/\mathbb{Q}$.*

(a) Let $v \in \mathcal{P}$. Then v is unramified in $L/\mathbb{Q}$ if and only if the image of σ_v in $\text{Gal}(L/\mathbb{Q})$ is the identity element. More precisely, the ramification index of v in $L/\mathbb{Q}$ equals

$$|\langle \text{proj}_{\mathcal{G}_{\mathbb{Q}}^{\text{pro-2}} \to \text{Gal}(L/\mathbb{Q})}(\sigma_v) \rangle|.$$

(b) If (2) is unramified in $L/\mathbb{Q}$, then both $\sigma_2(1)$ and $\sigma_2(2)$ have trivial image in $\text{Gal}(L/\mathbb{Q})$. More precisely, the ramification index of (2) in $L/\mathbb{Q}$ is divisible by

$$|\langle \text{proj}_{\mathcal{G}_{\mathbb{Q}}^{\text{pro-2}} \to \text{Gal}(L/\mathbb{Q})}(\sigma_2(1)), \text{proj}_{\mathcal{G}_{\mathbb{Q}}^{\text{pro-2}} \to \text{Gal}(L/\mathbb{Q})}(\sigma_2(2)) \rangle|.$$

Proof. We recall that, in general, the ramification index of v in $L/\mathbb{Q}$ equals

$$|(\text{proj}_{G_{\mathbb{Q}} \to \text{Gal}(L/\mathbb{Q})} \circ i_v^*)(I_v)|.$$

The projection map from $G_{\mathbb{Q}}$ to $\text{Gal}(L/\mathbb{Q})$ factors through $\mathcal{G}_{\mathbb{Q}}^{\text{pro-2}}$. Therefore part (a) is an immediate consequence of the definition of σ_v. To prove part (b) it suffices to observe that

$$\langle \text{proj}_{\mathcal{G}_{\mathbb{Q}}^{\text{pro-2}} \to \text{Gal}(L/\mathbb{Q})}(\sigma_2(1)), \text{proj}_{\mathcal{G}_{\mathbb{Q}}^{\text{pro-2}} \to \text{Gal}(L/\mathbb{Q})}(\sigma_2(2)) \rangle$$

is a subgroup of

$$(\text{proj}_{G_{\mathbb{Q}} \to \text{Gal}(L/\mathbb{Q})} \circ i_2^*)(I_2).$$

Hence the desired divisibility. $\qquad\square$

We write $\Gamma_{\mathbb{F}_2}(\mathbb{Q}) := \text{Hom}_{\text{top.gr.}}(G_{\mathbb{Q}}, \mathbb{F}_2)$ for the set of quadratic characters of $\mathbb{Q}$. We now recall some notation first introduced in [42]. Define

$$N := \frac{\mathbb{Q}_2}{\mathbb{Z}_2},$$

9

which we endow with the discrete topology and view as a $G_{\mathbb{Q}}$-module with trivial action. For each $\chi \in \Gamma_{\mathbb{F}_2}(\mathbb{Q})$, we denote by

$$N(\chi)$$

the $G_{\mathbb{Q}}$-module given by the topological abelian group N with the continuous action of $G_{\mathbb{Q}}$ defined by the formula

$$\sigma \cdot_{\chi} n := (-1)^{\chi(\sigma)} \cdot n$$

for each $\sigma \in G_{\mathbb{Q}}$ and $n \in N$. We now recall the basic material on raw cocycles and expansion maps that will be used throughout this paper.

2.1 Raw cocycles

For a given $\chi \in \Gamma_{\mathbb{F}_2}(\mathbb{Q})$, we denote by

$$\mathrm{Cocy}(G_{\mathbb{Q}}, N(\chi))$$

the group of continuous 1-cocycles from $G_{\mathbb{Q}}$ to the $G_{\mathbb{Q}}$-module $N(\chi)$ defined above. In case x is a squarefree integer, we will also use the notation $N(x) := N(\chi_x)$. We notice that the group $\mathrm{Cocy}(G_{\mathbb{Q}}, N(\chi))$ is a subgroup of the group of continuous 1-cochains $\mathrm{Map}_{\mathrm{cont}}(G_{\mathbb{Q}}, N)$. As such all these groups of 1-cocycles live in the common ambient group $\mathrm{Map}_{\mathrm{cont}}(G_{\mathbb{Q}}, N)$, which does not depend on χ. This simple observation plays a crucial role in the key Proposition 2.9. For a general continuous 1-cochain

$$\psi : G_{\mathbb{Q}} \to N$$

and a squarefree integer x, we define for each $\sigma, \tau \in G_{\mathbb{Q}}$ the coboundary

$$d_x(\psi)(\sigma, \tau) := -\psi(\sigma\tau) + (-1)^{\chi_x(\sigma)} \cdot \psi(\tau) + \psi(\sigma).$$

By definition ψ is in $\mathrm{Cocy}(G_{\mathbb{Q}}, N(\chi_x))$ if and only if $d_x(\psi)$ is identically zero.

Definition 2.4. *Whenever we consider the group $N \rtimes \mathbb{F}_2$, the implicit action of $\mathbb{F}_2$ on N is by $-\mathrm{id}$. The same applies for $N[2^s] \rtimes \mathbb{F}_2$ for $s \in \mathbb{Z}_{\geq 0}$.*

We will now demonstrate that elements ψ of $\mathrm{Cocy}(G_{\mathbb{Q}}, N(\chi))$ are essentially the same as certain homomorphisms from $G_{\mathbb{Q}}$ to $N \rtimes \mathbb{F}_2$.

Proposition 2.5. *Let $\psi \in \mathrm{Cocy}(G_{\mathbb{Q}}, N(\chi))$. Then the assignment*

$$G_{\mathbb{Q}} \to N(\chi) \rtimes \mathbb{F}_2,$$

given by

$$\sigma \mapsto (\psi(\sigma), \chi(\sigma)),$$

is a continuous group homomorphism. Conversely, given a continuous 1-cochain $\psi : G_{\mathbb{Q}} \to N$ such that

$$\sigma \mapsto (\psi(\sigma), \chi(\sigma))$$

is a group homomorphism from $G_{\mathbb{Q}}$ to $N(\chi) \rtimes \mathbb{F}_2$, we have that $\psi \in \mathrm{Cocy}(G_{\mathbb{Q}}, N(\chi))$. The restriction of ψ to $G_{\mathbb{Q}(\chi)}$ is a continuous group homomorphism.
In case $\psi(G_{\mathbb{Q}(\chi)}) \not\subseteq N[2]$, then the field of definition of ψ contains $\mathbb{Q}(\chi)$.

Proof. The first statement is straightforward. Since $N(\chi)$ is a trivial $G_{\mathbb{Q}(\chi)}$-module, the restriction of ψ to $G_{\mathbb{Q}(\chi)}$ is a 1-cocycle with the trivial action, and hence is a homomorphism. We now prove the last claim. By assumption there exists $\tau \in G_{\mathbb{Q}(\chi)}$ such that $2 \cdot \psi(\tau) \neq 0$. Let H be the largest normal open subgroup of $G_{\mathbb{Q}}$ through which ψ factors and let $\sigma \in H$. Then we have

$$\psi(\sigma) = \psi(\mathrm{id}) = 0,$$

since a 1-cocycle vanishes on the identity element. We now deduce that

$$\psi(\tau) = \psi(\sigma\tau) = (-1)^{\chi(\sigma)} \cdot \psi(\tau) + \psi(\sigma) = (-1)^{\chi(\sigma)} \cdot \psi(\tau).$$

Since $2 \cdot \psi(\tau) \neq 0$, we obtain the equality $\chi(\sigma) = 0$, which shows that $\ker(\chi) \supseteq H$ as desired. $\qquad\square$

Let $\psi \in \mathrm{Cocy}(G_{\mathbb{Q}}, N(\chi))$. Since ψ is continuous, $G_{\mathbb{Q}}$ is compact and N is discrete, the image of ψ is finite. Then it follows from Proposition 2.5 that the restriction of ψ gives an element of $(G_{\mathbb{Q}(\chi)}^{\mathrm{ab}})^{\vee}[2^{\infty}]$. We write

$$\mathrm{Cocy}_{\mathrm{unr}}(G_{\mathbb{Q}}, N(\chi))$$

for the inverse image of $\mathrm{Cl}(\mathbb{Q}(\chi))^{\vee}[2^{\infty}]$ under the above restriction map. The relevance of such 1-cocycles in this work comes from the fact that the Hilbert class field of a quadratic field is always a generalized dihedral extension over $\mathbb{Q}$. This is formalized in the following classical proposition.

Proposition 2.6. *Let $\chi \in \Gamma_{\mathbb{F}_2}(\mathbb{Q})$ and let $s \in \mathbb{Z}_{\geq 0}$. Then the natural restriction map*

$$\mathrm{Cocy}_{\mathrm{unr}}(G_{\mathbb{Q}}, N(\chi))[2^s] \to \mathrm{Cl}(\mathbb{Q}(\chi))^{\vee}[2^s]$$

is a split surjection of abelian groups. More precisely, the kernel is isomorphic to $\mathbb{Z}/2^s\mathbb{Z}$. Furthermore,

$$\psi \in 2 \cdot \mathrm{Cocy}_{\mathrm{unr}}(G_{\mathbb{Q}}, N(\chi))[2^{s+1}] \iff \psi|_{G_{\mathbb{Q}(\chi)}} \in 2 \cdot \mathrm{Cl}(\mathbb{Q}(\chi))^{\vee}[2^{s+1}]$$

for every $\psi \in \mathrm{Cocy}_{\mathrm{unr}}(G_{\mathbb{Q}}, N(\chi))[2^s]$.

Proof. Recall that $\mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$ acts on $\mathrm{Cl}(\mathbb{Q}(\chi))^{\vee}$ by $-\mathrm{id}$. This implies that all subgroups of $\mathrm{Cl}(\mathbb{Q}(\chi))^{\vee}$ are $G_{\mathbb{Q}}$-invariant, and hence define an extension that is Galois over $\mathbb{Q}$. Let us first show that the natural restriction map is surjective. Then, thanks to Proposition 2.5, it suffices to show that the natural surjection

$$\mathrm{Gal}(L/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$$

splits as a semidirect product for all cyclic 2-power extensions L of $\mathbb{Q}(\chi)$ unramified at all finite places.

Since $L/\mathbb{Q}(\chi)$ is unramified at all finite places, it follows that $L/\mathbb{Q}$ has ramification index at most 2 at all finite places. Therefore, thanks to Proposition 2.3, every element $\sigma \in \mathfrak{G}$ is sent to an involution under the natural quotient map $\pi : \mathcal{G}_{\mathbb{Q}}^{\mathrm{pro}\text{-}2} \to \mathrm{Gal}(L/\mathbb{Q})$. Since $\mathfrak{G}$ is a set of topological generators of $\mathcal{G}_{\mathbb{Q}}^{\mathrm{pro}\text{-}2}$ (see Proposition 2.2), there exists $\sigma \in \mathfrak{G}$ such that $\chi(\sigma) = 1$. Then $\pi(\sigma)$ is a non-trivial involution of $\mathrm{Gal}(L/\mathbb{Q})$ that projects to the generator of $\mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$. This yields the desired splitting.

Furthermore, the above argument also shows that the surjection

$$\mathrm{Gal}(H_{2^\infty}(\mathbb{Q}(\chi))/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$$

splits as a semidirect product, where $H_{2^\infty}(\mathbb{Q}(\chi))$ is the largest abelian 2-power extension of $\mathbb{Q}(\chi)$ unramified at all finite places. Fix an element $\sigma \in \mathrm{Gal}(H_{2^\infty}(\mathbb{Q}(\chi))/\mathbb{Q})$ projecting to a generator of $\mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$. Then, a simple calculation, using the semidirect product structure of $\mathrm{Gal}(H_{2^\infty}(\mathbb{Q}(\chi))/\mathbb{Q})$, shows that the elements of

$$\ker\left(\mathrm{Cocy}_{\mathrm{unr}}(G_\mathbb{Q}, N(\chi))[2^s] \to \mathrm{Cl}(\mathbb{Q}(\chi))^\vee[2^s]\right)$$

are entirely determined by their value on σ. Conversely, the elements in the kernel can take any desired value on σ. This identifies the kernel with $N(\chi)[2^s]$, which also proves that the surjection $\mathrm{Cocy}_{\mathrm{unr}}(G_\mathbb{Q}, N(\chi))[2^s] \to \mathrm{Cl}(\mathbb{Q}(\chi))^\vee[2^s]$ is split, since $\mathbb{Z}/2^s\mathbb{Z}$ is injective as a $\mathbb{Z}/2^s\mathbb{Z}$-module.

The final conclusion is now a trivial consequences of such a splitting applied both to s and to $s+1$. $\qquad\square$

Remark 2.7. *If* (2) *is unramified in the extension $L(\psi)/\mathbb{Q}$ or if* (2) *has residue field degree* 1 *in the extension $L(\psi)/\mathbb{Q}$, then the following stronger conclusion holds. For each cocycle $\psi \in \mathrm{Cocy}_{\mathrm{unr}}(G_\mathbb{Q}, N(\chi))[2^s]$, we have that*

$$\psi \in 2 \cdot \mathrm{Cocy}(G_\mathbb{Q}, N(\chi))[2^{s+1}] \iff \psi|_{G_{\mathbb{Q}(\chi)}} \in 2 \cdot \mathrm{Cl}(\mathbb{Q}(\chi))^\vee[2^{s+1}].$$

A proof of this stronger claim is given during the proof of Theorem 5.10 and used again in the proof of Theorem 5.11.

We now give the definition of raw cocycles, which is repeatedly used throughout this text.

Definition 2.8. *Let χ be a non-trivial element of $\Gamma_{\mathbb{F}_2}(\mathbb{Q})$ and let $s \in \mathbb{Z}_{\geq 0}$. We say that a sequence*

$$(\psi_i)_{0 \leq i \leq s}$$

with $\psi_i \in \mathrm{Cocy}_{\mathrm{unr}}(G_\mathbb{Q}, N(\chi))[2^i]$ is a raw cocycle in case $2 \cdot \psi_{i+1} = \psi_i$ for each $0 \leq i \leq s-1$. If we want to stress the dependence on $N(\chi)$, we say that ψ_i is a raw cocycle for $N(\chi)$.

To give a raw cocycle as in Definition 2.8 is clearly the same as giving a cocycle $\psi_s \in \mathrm{Cocy}_{\mathrm{unr}}(G_\mathbb{Q}, N(\chi))$ with $2^s \cdot \psi_s = 0$. We shall sometimes, by abuse of terminology, say that ψ_s is a raw cocycle, under this identification (and with the ψ_i automatically defined by the equation $\psi_i := 2^{s-i}\psi_s$). Furthermore, whenever the index j of ψ_j is negative, we use the convention $\psi_j = 0$, which conveniently preserves the equation $2 \cdot \psi_{i+1} = \psi_i$.

We now present an important combinatorial calculation. This result is taken from [42, page 17]. We give a detailed proof for the sake of completeness. Let $s \in \mathbb{Z}_{>0}$ and let $(p_i(1), p_i(2))_{i \in [s]}$ be $2s$ distinct primes, all of them coprime to the squarefree integer d_0. Let now

$$C := \{p_1(1), p_1(2)\} \times \ldots \times \{p_s(1), p_s(2)\} \times \{d_0\}.$$

We will often identify a point $x \in C$ with the squarefree integer $d_0 \cdot \prod_{i \in [s]} \pi_i(x)$. Given a finite collection of squarefree numbers H, we denote by χ_H the continuous 1-cochain from $G_\mathbb{Q}$ to $\mathbb{F}_2$ given by

$$\sigma \mapsto \prod_{x \in H} \chi_x(\sigma),$$

where the product is the usual multiplication in $\mathbb{F}_2$. By abuse of notation we also view χ_H as an indicator function valued in $\{0, 1\}$. For each subset T of $[s]$, we write C_T for the subset of $x \in C$ such that $\pi_i(x) = p_i(2)$ for all $i \in T$.

Proposition 2.9. *Let $j \in \mathbb{Z}_{>0}$ and let C be as above. Suppose that we are given a raw cocycle $\psi_j(x)$ for $N(x)$ for each $x \in C$. Let $x_0 \in C$. Then*

$$d_{x_0}\left(\sum_{x \in C} \psi_j(x)\right)(\sigma, \tau) = \sum_{\varnothing \neq T \subseteq [s]} \chi_{\{p_i(1)p_i(2):i \in T\}}(\sigma) \cdot (-1)^{|T|+1+\chi_{x_0}(\sigma)} \cdot \left(\sum_{x \in C_T} \psi_{j-|T|}(x)(\tau)\right).$$

Remark 2.10. *We emphasize that here and later in the paper the sum*

$$\sum_{x \in C} \psi_j(x)$$

takes place in the space $\mathrm{Map}_{\mathrm{cont}}(G_{\mathbb{Q}}, N)$.

Proof. Let $x \in C$. For each $\sigma, \tau \in G_{\mathbb{Q}}$ we compute

$$d_{x_0}(\psi_j(x))(\sigma, \tau) = -\psi_j(x)(\sigma\tau) + (-1)^{\chi_{x_0}(\sigma)} \cdot \psi_j(x)(\tau) + \psi_j(x)(\sigma)$$

$$= -\left((-1)^{\chi_x(\sigma)} \cdot \psi_j(x)(\tau) + \psi_j(x)(\sigma)\right) + (-1)^{\chi_{x_0}(\sigma)} \cdot \psi_j(x)(\tau) + \psi_j(x)(\sigma)$$

$$= (-1)^{\chi_{x_0}(\sigma)} \cdot (-(-1)^{\chi_{xx_0}(\sigma)} + 1) \cdot \psi_j(x)(\tau),$$

where the second equality follows from the definition of $\mathrm{Cocy}(G_{\mathbb{Q}}, N(x))$.

Observe that the function from $G_{\mathbb{Q}}$ to $\mathbb{Z}_2 = \mathrm{End}_{\mathbb{Z}_2\text{-mod}}(N)$ given by $\sigma \mapsto -(-1)^{\chi_{xx_0}(\sigma)} + 1$ factors through $\mathrm{Gal}(\mathbb{Q}(\{\sqrt{p_i(1)p_i(2)} : i \in [s]\})/\mathbb{Q})$. The $\mathbb{Z}_2$-module of functions from the finite Galois group $\mathrm{Gal}(\mathbb{Q}(\{\sqrt{p_i(1)p_i(2)} : i \in [s]\})/\mathbb{Q})$ to $\mathbb{Z}_2$ is free of rank 2^s, and a basis of functions is provided by $\{\chi_{\{p_i(1)p_i(2):i \in T\}}\}_{T \subseteq [s]}$. One could proceed now by explicitly writing down the indicator functions of elements of $\mathrm{Gal}(\mathbb{Q}(\{\sqrt{p_i(1)p_i(2)} : i \in [s]\})/\mathbb{Q})$ in terms of this basis and use this to expand the function $\sigma \mapsto -(-1)^{\chi_{xx_0}(\sigma)} + 1$ in terms of this basis. However, in [42, page 17] one finds a shortcut to quickly obtain this expansion, which we explain next.

We identify the projection of σ in $\mathrm{Gal}(\mathbb{Q}(\{\sqrt{p_i(1)p_i(2)} : i \in [s]\})/\mathbb{Q})$ with the largest $V \subseteq [s]$ such that $\chi_{\{p_i(1)p_i(2):i \in V\}}(\sigma) = 1$. We denote this subset by T_σ. Similarly, we identify each $x \in C$ with the subset of $[s]$, denoted by T_x, consisting of those $i \in [s]$ such that $\pi_i(x) = p_i(2)$. We now rewrite

$$-(-1)^{\chi_{xx_0}(\sigma)} + 1 = (-1) \cdot (-1)^{|T_x \cap T_\sigma|} + 1$$

$$= (-1) \cdot (1 - 2)^{|T_x \cap T_\sigma|} + 1$$

$$= \sum_{\varnothing \neq U \subseteq T_x \cap T_\sigma} (-1)^{|U|+1} 2^{|U|}.$$

Hence we obtain

$$d_{x_0}(\psi_j(x))(\sigma, \tau) = (-1)^{\chi_{x_0}(\sigma)} \cdot \left(\sum_{\varnothing \neq U \subseteq T_x \cap T_\sigma} (-1)^{|U|+1} 2^{|U|}\right) \cdot \psi_j(x)(\tau)$$

$$= (-1)^{\chi_{x_0}(\sigma)} \cdot \left(\sum_{\varnothing \neq U \subseteq T_x \cap T_\sigma} (-1)^{|U|+1} \psi_{j-|U|}(x)(\tau)\right).$$

We now let x vary in C and invoke the linearity of d_{x_0}. This gives

$$d_{x_0}\left(\sum_{x\in C}\psi_j(x)\right)(\sigma,\tau) = \sum_{x\in C}(-1)^{\chi_{x_0}(\sigma)}\cdot\left(\sum_{\varnothing\neq U\subseteq T_x\cap T_\sigma}(-1)^{|U|+1}\psi_{j-|U|}(x)(\tau)\right).$$

We exchange the order of summation and observe that for a given non-empty $U\subseteq[s]$ we get a contribution only from those pairs (x,σ) such that $U\subseteq T_x$ and $U\subseteq T_\sigma$. The first containment can be rewritten as $x\in C_U$. The second containment can be rewritten as $\chi_{\{p_i(1)p_i(2):i\in U\}}(\sigma) = 1$, since this equality means, by definition of T_σ, exactly that $U\subseteq T_\sigma$. Hence we get

$$d_{x_0}\left(\sum_{x\in C}\psi_j(x)\right)(\sigma,\tau) = \sum_{\varnothing\neq U\subseteq[s]}\chi_{\{p_i(1)p_i(2):i\in U\}}(\sigma)\cdot(-1)^{|U|+1+\chi_{x_0}(\sigma)}\cdot\left(\sum_{x\in C_U}\psi_{j-|U|}(x)(\tau)\right)$$

as desired. $\qquad\square$

We will often use the following version of Proposition 2.9.

Corollary 2.11. *Let $j\in\mathbb{Z}_{>0}$, let C be as above and let $x_0\in C$. Suppose that we are given a raw cocycle $\psi_j(x)$ for $N(x)$ for each $x\in C-\{x_0\}$. Then*

$$d_{x_0}\left(\sum_{\substack{x\in C\\x\neq x_0}}\psi_j(x)\right)(\sigma,\tau) = \sum_{\varnothing\neq T\subseteq[s]}\chi_{\{p_i(1)p_i(2):i\in T\}}(\sigma)\cdot(-1)^{|T|+1+\chi_{x_0}(\sigma)}\cdot\left(\sum_{x\in C_T}\psi_{j-|T|}(x)(\tau)\right).$$

Proof. Define $\psi_j(x_0) = 0$ and apply Proposition 2.9. $\qquad\square$

2.2 Expansion maps

We start by recalling a definition from [28, Definition 3.21]. We write $\mathbb{F}_2^A$ for the free $\mathbb{F}_2$-vector space on the set A.

Definition 2.12. *Let $X\subseteq\Gamma_{\mathbb{F}_2}(\mathbb{Q})$ be a linearly independent finite set and let $\chi_0\in X$. An expansion map with support X and pointer χ_0 is a continuous group homomorphism*

$$\psi:G_{\mathbb{Q}}\to\mathbb{F}_2[\mathbb{F}_2^{X-\{\chi_0\}}]\rtimes\mathbb{F}_2^{X-\{\chi_0\}}$$

such that

- *$\pi_\chi\circ\psi = \chi$ for every $\chi\in X-\{\chi_0\}$, where $\pi_\chi:\mathbb{F}_2[\mathbb{F}_2^{X-\{\chi_0\}}]\rtimes\mathbb{F}_2^{X-\{\chi_0\}}\to\mathbb{F}_2$ is the natural projection;*

- *$\pi\circ\psi = \chi_0$, where $\pi:\mathbb{F}_2[\mathbb{F}_2^{X-\{\chi_0\}}]\rtimes\mathbb{F}_2^{X-\{\chi_0\}}\to\mathbb{F}_2$ is the unique non-trivial character that sends the subgroup $\{0\}\rtimes\mathbb{F}_2^{X-\{\chi_0\}}$ to 0.*

An expansion map is automatically surjective, since it surjects by construction on the quotient of $\mathbb{F}_2[\mathbb{F}_2^{X-\{\chi_0\}}]\rtimes\mathbb{F}_2^{X-\{\chi_0\}}$ by its Frattini subgroup. Although we shall not make use of it, we mention that

$$\mathbb{F}_2[\mathbb{F}_2^{X-\{\chi_0\}}]\rtimes\mathbb{F}_2^{X-\{\chi_0\}}\cong\mathbb{F}_2\wr\mathbb{F}_2^{X-\{\chi_0\}},$$

where $\wr$ is the wreath product. We will now give an alternative characterization of expansion maps based on the material in [28, Section 3.3]. Consider the isomorphism

$$\mathbb{F}_2[\mathbb{F}_2^{X-\{\chi_0\}}] \cong \mathbb{F}_2[\{t_x : x \in X - \{\chi_0\}\}]/(\{t_x^2 : x \in X - \{\chi_0\}\})$$

obtained by sending t_x to $1 \cdot \mathrm{id} + 1 \cdot e_x$, where $e_x \in \mathbb{F}_2^{X-\{\chi_0\}}$ is the vector that is 1 exactly on the x-th coordinate. Observe that the collection of squarefree monomials $t_Y := \prod_{y \in Y} t_y$, as Y varies through the subsets of $X - \{\chi_0\}$, give a basis of the $\mathbb{F}_2$-vector space

$$\mathbb{F}_2[\{t_x : x \in X - \{\chi_0\}\}]/(\{t_x^2 : x \in X - \{\chi_0\}\}).$$

Hence projection on the monomials t_Y gives rise to continuous 1-cochains

$$\phi_Y(\psi) : G_\mathbb{Q} \to \mathbb{F}_2$$

for every $Y \subseteq X - \{\chi_0\}$. These 1-cochains allow us to reconstruct ψ using the formula

$$\psi(g) = \left(\sum_{Y \subseteq X-\{\chi_0\}} \phi_Y(\psi)(g) t_Y, (\chi(g))_{\chi \in X-\{\chi_0\}} \right). \tag{2.2}$$

Let $d : \mathrm{Map}(G_\mathbb{Q}^k, \mathbb{F}_2) \to \mathrm{Map}(G_\mathbb{Q}^{k+1}, \mathbb{F}_2)$ be the operator that sends a map $\phi \in \mathrm{Map}(G_\mathbb{Q}^k, \mathbb{F}_2)$ to

$$(d\phi)(g_1, \ldots, g_{k+1}) = \phi(g_2, \ldots, g_{k+1}) + \phi(g_1, \ldots, g_k) + \sum_{i=1}^{k} \phi(g_1, \ldots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \ldots, g_{k+1}).$$

From equation (2.2) and the composition law for the semidirect product we deduce that

$$(d\phi_Y(\psi))(g_1, g_2) = \sum_{\varnothing \subsetneq S \subseteq Y} \chi_S(g_1) \phi_{Y-S}(\psi)(g_2), \tag{2.3}$$

where $\chi_S := \prod_{\chi \in S} \chi$. Equation (2.3) is just [42, equation (2.2)]. Conversely, if we have a system of maps $(\phi_Y)_{Y \subseteq X-\{\chi_0\}}$ satisfying equation (2.3) and $\phi_\varnothing = \chi_0$, then we obtain an expansion map ψ with support X and pointer χ_0 using equation (2.2).

We now show that for each finite linearly independent set $X \subseteq \Gamma_{\mathbb{F}_2}(\mathbb{Q})$ and $\chi_0 \in X$, there exists at most one expansion map, denoted $\psi(\mathfrak{G})$, with support X and pointer χ_0 such that $\phi_Y(\psi(\mathfrak{G}))(\sigma) = 0$ for all non-empty subsets $Y \subseteq X - \{\chi_0\}$ and all $\sigma \in \mathfrak{G}$. Indeed, let ψ be such an expansion map. We claim that $\psi(\sigma)$ is determined for every $\sigma \in \mathfrak{G}$. But this follows from equation (2.2), our assumption $\phi_Y(\psi)(\sigma) = 0$ and the fact that $\chi(\sigma)$ is prescribed for every $\chi \in \Gamma_{\mathbb{F}_2}(\mathbb{Q})$ and $\sigma \in \mathfrak{G}$. Since $\mathfrak{G}$ is a set of topological generators of $\mathcal{G}_\mathbb{Q}^{\mathrm{pro}\text{-}2}$ by Proposition 2.2, the homomorphism ψ is completely determined by its values on $\mathfrak{G}$. This yields the desired uniqueness.

If there exists such an expansion map $\psi(\mathfrak{G})$, we write

$$\phi_{S;d}(\mathfrak{G})$$

for the 1-cochain $\phi_{X-\{\chi_0\}}(\psi(\mathfrak{G}))$, where S is the set of squarefree integers corresponding to the characters in $X - \{\chi_0\}$ and d is the squarefree integer corresponding to χ_0. In this way, whenever we have a non-negative integer s, a set of squarefree integers S of cardinality s and

15

a squarefree integer a_{s+1} such that S together with a_{s+1} spans a $s+1$-dimensional space in $\frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$, we have at most one 1-cochain

$$\phi_{S;a_{s+1}}(\mathfrak{G})$$

satisfying the above properties. In case we have one, we will say that $\phi_{S;a_{s+1}}(\mathfrak{G})$ exists. We shall refer to such 1-cochains as *normalized expansion maps*.

Lemma 2.13. *Let* $s \in \mathbb{Z}_{\geq 1}$. *Let* S *be a set of squarefree integers of cardinality* s *and let* x_1, x_2, x_3 *also be squarefree integers with* $x_1 x_2 = x_3$ *in* $\mathbb{Q}^*/\mathbb{Q}^{*2}$. *Suppose that* $\phi_{S;x_j}(\mathfrak{G})$ *exists for* $j \in [2]$. *Then* $\phi_{S;x_3}(\mathfrak{G})$ *exists and furthermore*

$$\phi_{S;x_3}(\mathfrak{G}) = \phi_{S;x_1}(\mathfrak{G}) + \phi_{S;x_2}(\mathfrak{G}).$$

Now suppose that $A = \{a_1, \ldots, a_s\}$, $B = \{b_1, \ldots, b_s\}$ *and* $C = \{c_1, \ldots, c_s\}$ *are sets of squarefree integers such that there exists* $j \in [s]$ *with*

$$a_i = b_i = c_i \text{ for all } i \in [s] - \{j\} \quad \text{and} \quad a_j b_j = c_j \text{ in } \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}.$$

Let x *be a squarefree integer. Suppose that* $\phi_{A;x}(\mathfrak{G})$ *and* $\phi_{B;x}(\mathfrak{G})$ *exist. Then* $\phi_{C;x}(\mathfrak{G})$ *exists and*

$$\phi_{C;x}(\mathfrak{G}) = \phi_{A;x}(\mathfrak{G}) + \phi_{B;x}(\mathfrak{G}).$$

Proof. Let us prove the first part, the second part being similar. We proceed by induction on s. First suppose that $s = 1$ and consider

$$\phi := \phi_{a_1;x_1}(\mathfrak{G}) + \phi_{a_1;x_2}(\mathfrak{G}).$$

It follows from equation (2.3) that

$$d\phi(\sigma, \tau) = \chi_{a_1}(\sigma) \cdot \chi_{x_1 x_2}(\tau) = \chi_{a_1}(\sigma) \cdot \chi_{x_3}(\tau)$$

Since ϕ vanishes at all $\sigma \in \mathfrak{G}$, we conclude that $\phi_{a_1;x_3}(\mathfrak{G})$ exists. Now suppose that $s > 1$. Again we consider

$$\phi := \phi_{S;x_1}(\mathfrak{G}) + \phi_{S;x_2}(\mathfrak{G}).$$

It follows from equation (2.3) and the induction hypothesis that

$$d\phi(\sigma, \tau) = \sum_{\varnothing \subsetneq T \subseteq S} \chi_T(\sigma) \cdot \phi_{S-T;x_3}(\mathfrak{G})(\tau).$$

Furthermore, ϕ vanishes at all $\sigma \in \mathfrak{G}$. Therefore $\phi_{S;x_3}(\mathfrak{G})$ exists. $\qquad\square$

The following proposition examines the field of definition of $\phi_{S;d}$ in terms of $\phi_{T;d}$ for $T \subset S$. The proof is straightforward group theory and we leave it to the reader.

Proposition 2.14. *Let* $X \subseteq \Gamma_{\mathbb{F}_2}(\mathbb{Q})$ *be a linearly independent finite set of cardinality at least 2 and let* $\chi_0 \in X$. *Let*

$$\psi : G_\mathbb{Q} \to \mathbb{F}_2[\mathbb{F}_2^{X-\{\chi_0\}}] \rtimes \mathbb{F}_2^{X-\{\chi_0\}}$$

be an expansion map with support X *and pointer* χ_0. *Then* $L(\phi_{X-\{\chi_0\}}(\psi))$ *coincides with the field* $(\mathbb{Q}^{\mathrm{sep}})^{\ker(\psi)}$. *This field is a multiquadratic extension of* $\mathbb{Q}(X - \{\chi_0\})$ *given by the quadratic characters*

$$\{\phi_Y(\psi)|_{G_{\mathbb{Q}(X-\{\chi_0\})}} : Y \subseteq X - \{\chi_0\}\}.$$

Writing

$$M(\psi) := \mathbb{Q}(X) \cdot \prod_{Y \subsetneq X - \{\chi_0\}} L(\phi_Y(\psi)),$$

we have that $L(\phi_{X-\{\chi_0\}}(\psi))/M(\psi)$ is a central $\mathbb{F}_2$-extension. Furthermore,

$$\mathrm{Gal}(L(\phi_{X-\{\chi_0\}}(\psi))/M(\psi))$$

equals the center of $\mathrm{Gal}(L(\phi_{X-\{\chi_0\}}(\psi))/\mathbb{Q})$.

Following the notation of Proposition 2.14, we will also use the notation

$$M(\phi_{X-\{\chi_0\}}(\psi)) := M(\psi)$$

in the rest of the paper. In the next proposition we give a sense of the ramification behavior in the field of definition of a normalized expansion map.

Proposition 2.15. *Let n be a positive integer. Suppose that $a_1, \ldots, a_{n+1}$ are squarefree, pairwise coprime and not equal to 1. Suppose that $a_i \equiv 1 \bmod 8$ for each $i \in [n]$ and that $\phi_{\{a_1,\ldots,a_n\};a_{n+1}}(\mathfrak{G})$ exists. Then the extension*

$$L(\phi_{\{a_1,\ldots,a_n\};a_{n+1}}(\mathfrak{G}))/\mathbb{Q}(\{\sqrt{a_i} : i \in [n]\})$$

is a multiquadratic extension containing $\mathbb{Q}(\sqrt{a_{n+1}})$. Furthermore, the multiquadratic extension

$$L(\phi_{\{a_1,\ldots,a_n\};a_{n+1}}(\mathfrak{G}))/\mathbb{Q}(\{\sqrt{a_i} : i \in [n+1]\})$$

is unramified at all finite places.

Proof. We will abbreviate $A = \{a_1, \ldots, a_n\}$. Proposition 2.14 implies that the extension $L(\phi_{A;a_{n+1}}(\mathfrak{G}))/\mathbb{Q}(\{\sqrt{a_i} : i \in [n]\})$ is a multiquadratic extension containing the field $\mathbb{Q}(\sqrt{a_{n+1}})$. We now focus on the ramification claims.

Let us first prove this for a place $v \in \mathcal{P}$ coprime to all the a_i. Then combining equation (2.2) with the definition of normalized expansion maps, we see that σ_v is sent to the identity element of $\mathrm{Gal}(L(\phi_{A;a_{n+1}}(\mathfrak{G}))/\mathbb{Q})$. Hence the extension $L(\phi_{A;a_{n+1}}(\mathfrak{G}))/\mathbb{Q}$ is unramified at v in view of Proposition 2.3.

Next, since $a_i \equiv 1 \bmod 8$ for all $i \in [n]$, it follows from equation (2.3), combined with the definition of normalized expansion maps, that the map

$$\phi_{\{a_i : i \in T\};a_{n+1}}(\mathfrak{G}) \circ i_2^*$$

is an unramified quadratic character of $G_{\mathbb{Q}_2}$ for each subset $\varnothing \subset T \subseteq [n]$, . Hence it follows from equation (2.2) that the homomorphism $\psi_{A;a_{n+1}}(\mathfrak{G}) \circ i_2^*$ factors through the kernel of $(\chi_5, \chi_{a_{n+1}})$. As such, the extension $L(\phi_{A;a_{n+1}}(\mathfrak{G}))/\mathbb{Q}(\{\sqrt{a_i} : i \in [n+1]\})$ is unramified at any place above (2).

Finally, suppose that $v \in \mathcal{P}$ divides one of the a_i. Observe that, by the coprimality conditions, there exists exactly one $i_0 \in [n]$ such that $v \mid a_{i_0}$. It follows from the definition of normalized expansion maps, combined with equation (2.2), that $\psi_{A;a_{n+1}}(\mathfrak{G})(\sigma_v)$ is an involution. Therefore Proposition 2.3 implies that the ramification index of v in $L(\phi_{A;a_{n+1}}(\mathfrak{G}))/\mathbb{Q}$ equals 2. Since the ramification index of v in $\mathbb{Q}(\{\sqrt{a_i} : i \in [n+1]\})/\mathbb{Q}$ is also 2, we conclude that any place of $\mathbb{Q}(\{\sqrt{a_i} : i \in [n+1]\})$ above v is unramified in

$$L(\phi_{A;a_{n+1}}(\mathfrak{G}))/\mathbb{Q}(\{\sqrt{a_i} : i \in [n+1]\}).$$

This ends the proof. $\qquad\qquad\square$

The following criterion gives an inductive procedure for creating expansion maps, see also [42, Proposition 2.1].

Proposition 2.16. *Let $a_1, \ldots, a_{s+1}$ be odd, squarefree integers that are pairwise coprime. Assume that $a_1, \ldots, a_s > 1$ and $a_{s+1} \neq 1$. Further suppose that*

$$\left(\frac{a_j}{p} \right) = 1 \tag{2.4}$$

for all distinct $i, j \in [s+1]$ and all primes p dividing a_i. Then $\phi_{\{a_i : i \in [s]\}; a_{s+1}}(\mathfrak{G})$ exists if $\phi_{\{a_i : i \in [s] - \{j\}\}; a_{s+1}}(\mathfrak{G})$ exists for all $j \in [s]$ and every prime divisor p of a_j splits completely in $L(\phi_{\{a_i : i \in [s] - \{j\}\}; a_{s+1}}(\mathfrak{G}))$.

Remark 2.17. *The converse of Proposition 2.16 is also true, but we shall not need or prove it here.*

Proof. We claim that there exists a continuous 1-cochain $\phi : G_{\mathbb{Q}} \to \mathbb{F}_2$ such that

$$d\phi(\sigma, \tau) = \sum_{\varnothing \subset S \subseteq [s]} \left(\prod_{j \in S} \chi_{a_j}(\sigma) \right) \cdot \phi_{\{a_i : i \in [s] - S\}; a_{s+1}}(\mathfrak{G})(\tau) =: \theta(\sigma, \tau).$$

Once such a ϕ exists, we certainly have that $\phi(\mathrm{id}) = 0$. Since ϕ is continuous, this implies that $\phi(\sigma) = 0$ except for possibly finitely many $\sigma \in \mathfrak{G}$. Then the proposition follows by twisting ϕ by the unique quadratic character $\chi : G_{\mathbb{Q}} \to \mathbb{F}_2$ such that $\phi(\sigma) = \chi(\sigma)$ for all $\sigma \in \mathfrak{G}$.

To prove the claim, we first show that θ is a 2-cocycle. If ψ satisfies $\psi(\sigma, \tau) = \phi_1(\sigma) \cdot \phi_2(\tau)$ with $\phi_1, \phi_2 : G_{\mathbb{Q}} \to \mathbb{F}_2$, then we have the formula

$$(d\psi)(\sigma, \tau, \mu) = \phi_1(\sigma) \cdot d\phi_2(\tau, \mu) + d\phi_1(\sigma, \tau) \cdot \phi_2(\mu).$$

We combine this with the equations

$$d \left(\prod_{j \in T} \chi_{a_j} \right)(\sigma, \tau) = \sum_{\varnothing \subset S \subset T} \left(\prod_{j \in S} \chi_{a_j}(\sigma) \right) \cdot \left(\prod_{j \in T - S} \chi_{a_j}(\tau) \right)$$

for all $T \subseteq [s]$ and

$$d\phi_{\{a_i : i \in T\}; a_{s+1}}(\mathfrak{G})(\sigma, \tau) = \sum_{\varnothing \subset S \subseteq T} \left(\prod_{j \in S} \chi_{a_j}(\sigma) \right) \cdot \phi_{\{a_i : i \in T - S\}; a_{s+1}}(\mathfrak{G})(\tau)$$

for all strict subsets T of $[s]$ to deduce that θ is indeed a 2-cocycle. Hence the claim is equivalent to the class of θ vanishing in $H^2(G_{\mathbb{Q}}, \mathbb{F}_2)$, which is in turn equivalent to the restriction of θ vanishing in $H^2(G_{\mathbb{Q}_v}, \mathbb{F}_2)$ for all places v of $\mathbb{Q}$ by class field theory.

If v is the infinite place, then θ becomes the zero map when restricted to $G_{\mathbb{R}}$ since the a_i are positive for $i \in [s]$. If v is an odd, finite place, then we distinguish two cases. If v does not divide any of the a_i, then the restriction of θ to $G_{\mathbb{Q}_v}$ factors through the maximal unramified extension of $\mathbb{Q}_v$. It follows that θ is in the image of the inflation map from

$$H^2(\mathrm{Gal}(\mathbb{Q}_v^{\mathrm{unr}}/\mathbb{Q}_v), \mathbb{F}_2) = H^2(\hat{\mathbb{Z}}, \mathbb{F}_2) = 0,$$

which implies that θ is trivial at such places v. Now suppose that v divides a_j for some j. If $j = s + 1$, then equation (2.4) implies that θ becomes the zero map when restricted to $G_{\mathbb{Q}_v}$. Therefore θ is certainly trivial in $H^2(G_{\mathbb{Q}_v}, \mathbb{F}_2)$. Instead suppose that $j \in [s]$. Now observe that our assumptions imply that $\phi_{\{a_i : i \in [s] - \{j\}\}; a_{s+1}}(\mathfrak{G})$ is the zero map when restricted to $G_{\mathbb{Q}_v}$. Then it follows from equation (2.4) that θ is also locally trivial at such v. We have now dealt with all odd places and the infinite place. Then θ also vanishes locally at the unique 2-adic place of $\mathbb{Q}$ by Hilbert reciprocity. $\qquad\square$

Finally, we need some additional maps that can be thought of as degenerate expansion maps with two indices. Let $a \in \mathcal{D}$. Then observe that

$$\chi_a \cup \chi_a$$

vanishes in $H^2(G_{\mathbb{Q}}, \mathbb{F}_2)$. There is a unique map

$$\phi_{a;a}(\mathfrak{G}) : G_{\mathbb{Q}} \to \mathbb{F}_2$$

such that

$$(d\phi_{a;a}(\mathfrak{G}))(\sigma, \tau) = \chi_a(\sigma) \cdot \chi_a(\tau)$$

and $\phi_{a;a}(\mathfrak{G})$ vanishes at all elements of $\mathfrak{G}$. If $a > 1$, then $L(\phi_{a;a}(\mathfrak{G}))$ is a cyclic degree 4 extension of $\mathbb{Q}$ with its unique quadratic subextension equal to $\mathbb{Q}(\sqrt{a})$. Indeed, one can write $\mathbb{Z}/4\mathbb{Z}$ set-theoretically as $\mathbb{F}_2 \times \mathbb{F}_2$ with the group law given by

$$(x, y) * (x', y') = (x + x' + yy', y + y').$$

Then the $\mathbb{Z}/4\mathbb{Z}$-character corresponding to $\phi_{a;a}(\mathfrak{G})$ is the map

$$\sigma \mapsto (\phi_{a;a}(\mathfrak{G})(\sigma), \chi_a(\sigma)).$$

Take $v \in \mathcal{P}$ and suppose that v is unramified in $\mathbb{Q}(\sqrt{a})$. Then the above map sends σ_v to $(0, 0)$, which is the identity. We deduce from Proposition 2.3 that all $v \in \mathcal{P}$ ramifying in $L(\phi_{a;a}(\mathfrak{G}))/\mathbb{Q}$ must divide a. In case v divides a, then the ramification index of v in $L(\phi_{a;a}(\mathfrak{G}))/\mathbb{Q}$ is 4 thanks to Proposition 2.3. The above statements also apply to $v = (2)$ in case $2 \mid a$.

Suppose now that 2 does not divide a. Observe that a is then either 1 or 5 modulo 8. In case a is 1 modulo 8, then $\phi_{a;a}(\mathfrak{G}) \circ i_2^*$ becomes a quadratic character, and since it vanishes on $\sigma_2(1), \sigma_2(2)$ it must be an unramified quadratic character. Therefore, in this case, (2) does not ramify in $L(\phi_{a;a}(\mathfrak{G}))/\mathbb{Q}$.

In case a is 5 modulo 8, then there exists $\phi' : \mathrm{Gal}(\mathbb{Q}_2^{\mathrm{unr}}/\mathbb{Q}_2) \to \mathbb{F}_2$ with $(d\phi')(\sigma, \tau) = \chi_a(\sigma) \cdot \chi_a(\tau)$. Indeed, this 1-cochain comes from the $\mathbb{Z}/4\mathbb{Z}$-character $G_{\mathbb{Q}_2} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}_{16}/\mathbb{Q}_2)$. Hence $\phi_{a;a}(\mathfrak{G}) - \phi'$ is a quadratic character in $\Gamma_{\mathbb{F}_2}(\mathbb{Q}_2)$. However, it vanishes on $\sigma_2(1), \sigma_2(2)$, since each of the two 1-cochains do. Hence it must be in the span of the unramified quadratic character of $\mathbb{Q}_2$. It follows that $(\phi_{a;a}(\mathfrak{G}), \chi_a)$ is unramified at (2). We summarize our results in the next lemma.

Lemma 2.18. *Let $a \in \mathcal{D}$ be greater than 1. Then the extension $L(\phi_{a;a}(\mathfrak{G}))/\mathbb{Q}$ is a $\mathbb{Z}/4\mathbb{Z}$-extension of $\mathbb{Q}$ ramifying exactly at those places where $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ ramifies. Furthermore, the ramification index of such places equals 4.*

2.3 The Artin pairing

Let A be a finite abelian 2-group and let $s \in \mathbb{Z}_{\geq 1}$. Denote by

$$A^\vee := \text{Hom}_{\text{ab.gr.}}\left(A, \ \frac{\mathbb{Q}_2}{\mathbb{Z}_2}\right)$$

the dual group. We define the pairing

$$\langle -, - \rangle_{\text{Art}_s(A)} : 2^{s-1} \cdot A[2^s] \times 2^{s-1} \cdot A^\vee[2^s] \to \mathbb{F}_2$$

by the formula

$$\langle a, \chi \rangle_{\text{Art}_s(A)} := \psi(a),$$

where ψ is any element of $A^\vee$ with $2^{s-1} \cdot \psi = \chi$. Observe that changing the choice of ψ amounts to taking an element of the shape $\psi + \psi'$ with $\psi' \in A^\vee[2^{s-1}]$. This does not affect the resulting pairing, since a is in $2^{s-1} \cdot A[2^s]$ and thus vanishes when paired, through the canonical duality pairing, with $A^\vee[2^{s-1}]$. Also observe that the pairing is valued in $\mathbb{F}_2$, as we claimed, since $a \in A[2]$ and ψ is a group homomorphism. Thus we have shown that the pairing does not depend on the choice of ψ and is valued in $\mathbb{F}_2$.

We claim that the left kernel and the right kernel of $\langle -, - \rangle_{\text{Art}_s(A)}$ actually coincide with, respectively, $2^s \cdot A[2^{s+1}]$ and $2^s \cdot A^\vee[2^{s+1}]$. Indeed, a moment reflection shows that

$$\langle -, - \rangle_{\text{Art}_s(A)} = \langle -, - \rangle_{\text{Art}_1(2^{s-1} \cdot A)}.$$

In this last equality we are implicitly identifying $(2^{s-1} \cdot A)^\vee$ and $2^{s-1} \cdot A^\vee$, through the standard inclusion of $(2^{s-1} \cdot A)^\vee$ in $A^\vee$ induced by the natural surjection $A \twoheadrightarrow 2^{s-1} \cdot A$ given by multiplication by 2^{s-1}. Hence the claim follows from the case $s = 1$, which is an immediate consequence of the duality theory of finite dimensional vector spaces over $\mathbb{F}_2$.

In case x is a squarefree integer different from 1 and $A = \text{Cl}(\mathbb{Q}(\sqrt{x}))[2^\infty]$, we will simply write

$$\langle -, - \rangle_{\text{Art}_s(x)} := \langle -, - \rangle_{\text{Art}_s(\text{Cl}(\mathbb{Q}(\sqrt{x}))[2^\infty])}.$$

In what follows we will canonically identify $\text{Cl}(\mathbb{Q}(\sqrt{x}))[2^\infty]$ with the largest quotient of $\text{Cl}(\mathbb{Q}(\sqrt{x}))$ which is a 2-group: the natural projection map from the former to the latter induces an isomorphism. In this way, via the Artin reciprocity map, $\text{Cl}(\mathbb{Q}(\sqrt{x}))[2^\infty]$ is identified with

$$\text{Gal}(H_{2^\infty}(\mathbb{Q}(\sqrt{x}))/\mathbb{Q}(\sqrt{x})),$$

where we recall that $H_{2^\infty}(\mathbb{Q}(\sqrt{x}))$ is the largest extension of $\mathbb{Q}(\sqrt{x})$ inside $\mathbb{Q}^{\text{sep}}$ that is abelian, unramified at all finite places of $\mathbb{Q}(\sqrt{x})$ and of degree a power of 2. This allows us to reinterpret the Artin pairing $\langle -, - \rangle_{\text{Art}_s(x)}$ as the Artin symbol of a 2-torsion ideal class in a cyclic degree 2^s-extension of $\mathbb{Q}(\sqrt{x})$ unramified at all finite places. We will repeatedly use throughout the text this way of computing $\langle -, - \rangle_{\text{Art}_s(x)}$.

3 Higher Rédei reciprocity

This section generalizes one of the central results in [29], which is a generalization of the classical Rédei reciprocity law (in turn a generalization of quadratic reciprocity).

3.1 Statement of the reciprocity law

Let $n \in \mathbb{Z}_{\geq 1}$ and let $A \subseteq \Gamma_{\mathbb{F}_2}(\mathbb{Q})$ with $|A| = n$. Let χ_1, χ_2 be two distinct elements of $\Gamma_{\mathbb{F}_2}(\mathbb{Q}) - A$ and put

$$A_1 := A \cup \{\chi_1\}, \quad A_2 := A \cup \{\chi_2\}.$$

Given a finite Galois extension $L/\mathbb{Q}$, we denote by $\mathrm{Ram}(L/\mathbb{Q})$ the set of places of $\mathbb{Q}$ that ramify in the extension $L/\mathbb{Q}$. Furthermore, for a collection of characters $T \subseteq \Gamma_{\mathbb{F}_2}(\mathbb{Q})$, we recall that $\mathbb{Q}(T)$ denotes the corresponding multiquadratic extension of $\mathbb{Q}$.

Write ∞ for the infinite place of $\mathbb{Q}$. We assume that, as χ varies in A, the n sets $\mathrm{Ram}(\mathbb{Q}(\chi)/\mathbb{Q})$ are non-empty, pairwise disjoint and none of them contains ∞ (in other words $\mathbb{Q}(A)/\mathbb{Q}$ is totally real). This forces A to be a linearly independent set of characters over $\mathbb{F}_2$. Additionally, we assume that $\mathrm{Ram}(\mathbb{Q}(\chi_1)/\mathbb{Q})$ and $\mathrm{Ram}(\mathbb{Q}(\chi_2)/\mathbb{Q})$ are non-empty and disjoint from $\cup_{\chi \in A}\mathrm{Ram}(\mathbb{Q}(\chi)/\mathbb{Q})$, which certainly implies that χ_1 is linearly independent from A, and similarly for χ_2.

Suppose that we are given two expansion maps

$$\psi_1, \psi_2 : G_{\mathbb{Q}} \twoheadrightarrow \mathbb{F}_2[\mathbb{F}_2^A] \rtimes \mathbb{F}_2^A$$

with supports A_1, A_2 and pointers χ_1, χ_2 respectively. Write $(\phi_{1,B})_{B \subseteq A}, (\phi_{2,B})_{B \subseteq A}$ for the corresponding system of continuous 1-cochains from $G_{\mathbb{Q}}$ to $\mathbb{F}_2$ satisfying $\phi_{1,\varnothing} = \chi_1, \phi_{2,\varnothing} = \chi_2$. Thanks to Proposition 2.14, $L(\psi_1)$ and $L(\psi_2)$ are central $\mathbb{F}_2$-extensions of respectively $M(\psi_1)$ and $M(\psi_2)$. We will impose some further conditions on χ_1 and χ_2, which we will refer to as the *coprimality constraints* on the pointers.

First of all, we demand that $\mathrm{Ram}(\mathbb{Q}(\chi_1)/\mathbb{Q}) \cap \mathrm{Ram}(\mathbb{Q}(\chi_2)/\mathbb{Q}) \subseteq \{(2)\}$. Next we demand that $\mathrm{inv}_2(\chi_1 \cup \chi_2) = 0$ and that at least one between χ_1 and χ_2 vanishes on $\sigma_2(2)$. Finally, we require (2) to split completely in $\mathbb{Q}(A)/\mathbb{Q}$. If all these conditions are met, we say that the pointers satisfy the coprimality constraints.

We give one more definition before stating our reciprocity law. We remark that whenever we have a 4-tuple as above, then for each subset $T' \subseteq A$ the 1-cochains $\phi_{T'}(\psi_1) \circ i_2^*, \phi_{T'}(\psi_2) \circ i_2^*$ are quadratic characters from $G_{\mathbb{Q}_2}$ to $\mathbb{F}_2$, as one can see by combining equation (2.3) with the fact that (2) splits completely in $\mathbb{Q}(A)/\mathbb{Q}$.

Definition 3.1. *Let $(A_1, A_2, \psi_1, \psi_2)$ be a 4-tuple as above. We call $(A_1, A_2, \psi_1, \psi_2)$ Rédei admissible if the following four conditions hold*

- *if ∞ splits completely in $\mathbb{Q}(A_1 \cup A_2)/\mathbb{Q}$, then ∞ splits completely in $M(\psi_1)M(\psi_2)/\mathbb{Q}$ as well.*

- *whenever $\{i, j\} = \{1, 2\}$ and ∞ ramifies in $L(\psi_i)/\mathbb{Q}$, then ∞ splits completely in $M(\psi_j)/\mathbb{Q}$.*

- *whenever $\{i, j\} = \{1, 2\}$, if a place w of $\mathbb{Q}(A)$, lying above a place $v \in \mathcal{P}$, ramifies in the extension $L(\psi_i)/\mathbb{Q}(A)$, then v splits completely in $M(\psi_j)/\mathbb{Q}$. Furthermore, we also demand that v is unramified in $L(\psi_j)/\mathbb{Q}$;*

- *whenever $L(\psi_1)L(\psi_2)/\mathbb{Q}$ is ramified at (2), then there exist i, j with $\{i, j\} = \{1, 2\}$ such that ψ_i is a normalized expansion map satisfying $\chi_i(\sigma_2(2)) = 0$ and $\phi_T(\psi_i) \circ i_2^* = 0$ for each $\varnothing \neq T \subsetneq A$. Furthermore, the characters $\chi_i \circ i_2^*$ and $\phi_{T'}(\psi_j) \circ i_2^*$ are orthogonal with respect to the local Hilbert pairing at (2) for each $T' \subseteq A$.*

We say that (χ_1, χ_2) is the pointer vector *of the 4-tuple and that A is the* base set *of the 4-tuple.*

Let $(A_1, A_2, \psi_1, \psi_2)$ be a Rédei admissible 4-tuple with pointer vector (χ_1, χ_2). Then each place $v \in \mathrm{Ram}(\mathbb{Q}(\chi_1)/\mathbb{Q}) \cap \mathcal{P}$ is unramified in $L(\psi_2)/\mathbb{Q}$. Indeed, this follows from the third condition in Definition 3.1 combined with the fact that $\mathrm{Ram}(\chi_1)$ is disjoint from $\mathrm{Ram}(\chi)$ for each $\chi \in A$. Consequently, it makes sense to speak of the Artin class $\mathrm{Art}(v, L(\psi_2)/\mathbb{Q})$ for each place $v \in \mathrm{Ram}(\mathbb{Q}(\chi_1)/\mathbb{Q}) \cap \mathcal{P}$. Furthermore, this Artin symbol lands in $\mathrm{Gal}(L(\psi_2)/M(\psi_2))$, which is the center of $\mathrm{Gal}(L(\psi_2)/\mathbb{Q})$ (see Proposition 2.14) of size equal to 2 and hence can uniquely be identified with $\mathbb{F}_2$. Therefore $\mathrm{Art}(v, L(\psi_2)/\mathbb{Q})$ is a well-defined element of $\mathbb{F}_2$. Symmetrically, the same holds if we swap the roles of 1 and 2.

Next, whenever $\{i, j\} = \{1, 2\}$ and ∞ ramifies in $\mathbb{Q}(\chi_i)/\mathbb{Q}$, then ∞ splits completely in $M(\psi_j)/\mathbb{Q}$ by the second condition of Definition 3.1. Consequently the Artin symbol $\mathrm{Art}(\infty, L(\psi_j)/\mathbb{Q})$ is also an element of the center $\mathrm{Gal}(L(\psi_j)/M(\psi_j))$ and hence is a well-defined element of $\mathbb{F}_2$.

Whenever (2) ramifies in $L(\psi_1)L(\psi_2)/\mathbb{Q}$, let $\{i, j\} = \{1, 2\}$ be as in the last condition of Definition 3.1. Then, in case $\chi_i \circ i_2^* = 0$, (2) splits completely in $M(\psi_i)/\mathbb{Q}$ and (2) is unramified in $L(\psi_i)/\mathbb{Q}$. Consequently, the Artin symbol $\mathrm{Art}((2), L(\psi_i)/\mathbb{Q})$ is also an element of the center $\mathrm{Gal}(L(\psi_i)/M(\psi_i))$ and thus a well-defined element of $\mathbb{F}_2$.

Instead suppose that $\chi_i \circ i_2^* \neq 0$. Then $L(\psi_i)/\mathbb{Q}(\chi_i)$ is unramified at $\mathrm{Up}_{\mathbb{Q}(\chi_i)/\mathbb{Q}}(2)$, thanks to Proposition 2.15, and this place splits completely in $M(\psi_i)/\mathbb{Q}(\chi_i)$. Consequently, the Artin symbol $\mathrm{Art}(\mathrm{Up}_{\mathbb{Q}(\chi_i)/\mathbb{Q}}(2), L(\psi_i)/\mathbb{Q}(\chi_i))$ is well-defined and an element of the center $\mathrm{Gal}(L(\psi_i)/M(\psi_i))$ and therefore a well-defined element of $\mathbb{F}_2$. By abuse of notation we will sometimes denote this symbol as $\mathrm{Art}((2), L(\psi_i)/\mathbb{Q})$. Also, observe that in case $\chi_i \circ i_2^* = \chi_5$, then it must be that $\chi_j(\sigma_2(2)) = 0$, thanks to the fact that χ_i is orthogonal to χ_j with respect to the local Hilbert pairing at (2).

Finally, for a quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, we put

$$\widetilde{\mathrm{Ram}}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \begin{cases} \mathrm{Ram}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \setminus (2) & \text{if } d \text{ has even 2-adic valuation} \\ \mathrm{Ram}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) & \text{otherwise.} \end{cases}$$

We can now state the reciprocity law.

Theorem 3.2. *Let $(A_1, A_2, \psi_1, \psi_2)$ be a Rédei admissible 4-tuple with pointer vector (χ_1, χ_2). Then*

$$\sum_{v \in \widetilde{\mathrm{Ram}}(\mathbb{Q}(\chi_1)/\mathbb{Q})} \mathrm{Art}(v, L(\psi_2)/\mathbb{Q}) = \sum_{v' \in \widetilde{\mathrm{Ram}}(\mathbb{Q}(\chi_2)/\mathbb{Q})} \mathrm{Art}(v', L(\psi_1)/\mathbb{Q}).$$

3.2 Proof of Theorem 3.2

Take a Rédei admissible 4-tuple $(A_1, A_2, \psi_1, \psi_2)$ with pointer vector (χ_1, χ_2) and base set A. We derive from equation (2.3) that the tuple of 1-cochains $(\phi_{i,B})_{B \subseteq A}$ becomes a tuple of quadratic characters when restricted to $G_{\mathbb{Q}(A)}$ for every $i \in \{1, 2\}$. Furthermore, it follows directly from the definition of an expansion map that the character $\phi_{i,A}$ generates a rank 1 free module over the ring $\mathbb{F}_2[\mathrm{Gal}(\mathbb{Q}(A)/\mathbb{Q})]$ for every $i \in \{1, 2\}$, and furthermore the corresponding Galois extension of $\mathbb{Q}$ equals $L(\psi_i)$.

For each $B \subseteq A$ we denote by $\alpha_{i,B} \in \frac{\mathbb{Q}(B)^*}{\mathbb{Q}(B)^{*2}}$ the unique element, provided by Kummer theory, corresponding to the restriction of $\phi_{i,B}$ to $G_{\mathbb{Q}(B)}$ (which is a quadratic character).

Our next proposition is a generalization of the well-known connection between D_4-extensions and solution sets of certain conics, see for instance [44, Section 5], which also explains how this phenomenon is related to Rédei symbols.

Proposition 3.3. *We have for all $i \in \{1, 2\}$ and all $B \subseteq A$ that*

$$N_{\mathbb{Q}(A)/\mathbb{Q}(B)}(\alpha_{i,A}) = \alpha_{i,B}$$

as elements of $\frac{\mathbb{Q}(B)^*}{\mathbb{Q}(B)^{*2}}$.

Proof. From the recursive formula (2.3) we see that it suffices to show that

$$N_{\mathbb{Q}(A)/\mathbb{Q}(A-\{a\})}(\alpha_{i,A}) = \alpha_{i,A-\{a\}} \quad \text{in} \quad \frac{\mathbb{Q}(A-\{a\})^*}{\mathbb{Q}(A-\{a\})^{*2}}$$

for all $a \in A$: the full proposition is then obtained by applying this repeatedly.

By Kummer theory, this is the same as showing that the co-restriction of the character $\phi_{i,A}$ from $G_{\mathbb{Q}(A)}$ to $G_{\mathbb{Q}(A-\{a\})}$ equals the character $\phi_{i,A-\{a\}}$. To this end, let us recall the following basic fact. Let $G_1 \subseteq G_2$ be a continuous inclusion of profinite groups with $[G_2 : G_1] = 2$. If $\chi : G_1 \to \mathbb{F}_2$ and $\chi' : G_2 \to \mathbb{F}_2$ are two continuous characters, then the co-restriction of χ to G_2 equals χ' if and only if

$$\chi(\sigma^2) = \chi'(\sigma) \tag{3.1}$$

and

$$\chi(\sigma\tau\sigma^{-1}) + \chi(\tau) = \chi'(\tau) \tag{3.2}$$

for each $\sigma \in G_2 - G_1$, $\tau \in G_1$. Equation (3.2) only implies that the co-restriction of χ equals χ' as characters of the index 2 subgroup G_1. This leaves two possibilities for the character χ from the larger group G_2: the two possibilities constitute a single coset under the subgroup generated by the character $\epsilon : G_2 \twoheadrightarrow \frac{G_2}{G_1} = \mathbb{F}_2$. Said differently, equation (3.2) forces the co-restriction of χ to be in the set $\{\chi', \chi' + \epsilon\}$. These two cases can be distinguished by means of equation (3.1).

Returning to our setup, we will now explain how equation (3.2) follows from the definition of expansion maps as coordinates of monomials in a semidirect product. Here $G_{\mathbb{Q}(A)}$ plays the role of G_1 and $G_{\mathbb{Q}(A-\{a\})}$ plays the role of G_2. We claim that

$$\phi_{i,A}(\sigma\tau\sigma^{-1}) + \phi_{i,A}(\tau) = \phi_{i,A-\{a\}}(\tau) \tag{3.3}$$

for each $\sigma \in G_{\mathbb{Q}(A-\{a\})} - G_{\mathbb{Q}(A)}$ and $\tau \in G_{\mathbb{Q}(A)}$. To prove the claim, observe that $\ker(\psi_i)$ is contained in the kernel of all the quadratic characters $\phi_{i,A}, (1+\sigma)\phi_{i,A}, \phi_{i,A-\{a\}}$, since it gives a normal extension of $\mathbb{Q}$ containing the kernel of the first and the third.

Hence it suffices to check equation (3.3) in the quotient given by $\ker(\psi_i)$ or equivalently in $\operatorname{im}(\psi_i)$. The group $\psi_i(G_{\mathbb{Q}(A)})$ equals $\mathbb{F}_2[\mathbb{F}_2^A] \rtimes \{0\}$. The character $\phi_{i,A}$ is the projection on the monomial t_A, the character $\phi_{i,A-\{a\}}$ is the projection on the monomial $t_{A-\{a\}}$ and σ acts as multiplication by $1 + t_a$, since $\sigma \in G_{\mathbb{Q}(A-\{a\})} - G_{\mathbb{Q}(A)}$. This yields the identity

$$\sum_{T \subseteq A} (\phi_{i,T}(\sigma\tau\sigma^{-1}) + \phi_{i,T}(\sigma)) \cdot t_T = (1 + \sigma) \cdot \left(\sum_{T \subseteq A} \phi_{i,T}(\tau) \cdot t_T \right)$$

$$= t_a \cdot \left(\sum_{T \subseteq A} \phi_{i,T}(\tau) \cdot t_T \right) = \sum_{T \subseteq A-\{a\}} \phi_{i,T}(\tau) \cdot t_{T \cup \{a\}}$$

for all $\tau \in \mathbb{F}_2[\mathbb{F}_2^A] \rtimes \{0\}$. Comparing the t_A-coefficients gives precisely the desired conclusion.

It remains to check equation (3.1), which forces the norm relation to hold as characters of the larger group $G_{\mathbb{Q}(A-\{a\})}$. To this end, pick $\sigma \in G_{\mathbb{Q}(A-\{a\})} - G_{\mathbb{Q}(A)}$, and plug in (σ, σ) in equation (2.3). The left hand side equals $\phi_{i,A}(\sigma^2)$, which is the quantity we are after, while the right hand side equals $\phi_{i,A-\{a\}}(\sigma)$. This establishes the proposition. $\qquad\square$

Our next result is a direct consequence of Proposition 3.3.

Corollary 3.4. *Let $i \in \{1, 2\}$.*

(a) Let v be a finite place of $\mathbb{Q}$ that splits completely in $\mathbb{Q}(A)/\mathbb{Q}$. Then $v \in \widetilde{\mathrm{Ram}}(\mathbb{Q}(\chi_i)/\mathbb{Q})$ if and only if

$$|\{w \in \Omega_{\mathbb{Q}(A)} : w \mid v, w(\alpha_{i,A}) \equiv 1 \bmod 2\}| \equiv 1 \bmod 2.$$

(b) We have $\infty \in \widetilde{\mathrm{Ram}}(\mathbb{Q}(\chi_i)/\mathbb{Q})$ if and only if

$$|\{\sigma : \mathbb{Q}(A) \to \mathbb{R} : \sigma(\alpha_{i,A}) < 0\}| \equiv 1 \bmod 2.$$

Proof. We shall explain the argument for part (a) and leave part (b), which can be proven similarly, to the reader. Recall that $\phi_{i,\varnothing} = \chi_i$ for $i \in \{1, 2\}$ and that $\mathbb{Q}(\chi_i) = \mathbb{Q}(\sqrt{\alpha_{i,\varnothing}})$. Let us start by observing that

$$v \in \widetilde{\mathrm{Ram}}(\mathbb{Q}(\chi_i)/\mathbb{Q}) \iff v(\alpha_{i,\varnothing}) \equiv 1 \bmod 2 \tag{3.4}$$

for all finite places v of $\mathbb{Q}$. Furthermore, Proposition 3.3, applied to $B := \varnothing$, yields

$$N_{\mathbb{Q}(A)/\mathbb{Q}}(\alpha_{i,A}) = \alpha_{i,\varnothing}.$$

Since v splits completely in $\mathbb{Q}(A)$ by assumption, this shows that

$$\sum_{\substack{w \in \Omega_{\mathbb{Q}(A)} \\ w|v}} w(\alpha_{i,A}) \equiv v(\alpha_{i,\varnothing}) \bmod 2. \tag{3.5}$$

The corollary is now a consequence of equations (3.4) and (3.5). $\qquad\square$

We will now prove a general lemma about local fields. If K is a local field, we denote by $(-,-)_K$ the Hilbert pairing on $\frac{K^*}{K^{*2}}$. For a place v of a number field L we will write, by abuse of notation, $(-,-)_v$ for the pairing $(-,-)_{L_v}$.

Lemma 3.5. *Let p be a finite place of $\mathbb{Q}$ and let K be a finite extension of $\mathbb{Q}_p$. Let α be the unique class of $\frac{K^*}{K^{*2}}$ corresponding to the unramified quadratic extension $K(\sqrt{\alpha})$. Then the linear functional*

$$(\alpha, -)_K : \frac{K^*}{K^{*2}} \to \mathbb{F}_2$$

equals the reduction of $v_K(-)$ modulo 2.

Proof. Let π be a uniformizer of K. The local Artin map θ_K sends π to the generator of $\mathrm{Gal}(K(\sqrt{\alpha})/K)$, which implies that the Hilbert symbol $(\alpha, \pi)_K$ is non-trivial. Since this holds for all uniformizers, the lemma follows. $\qquad\square$

We will make use of one final ingredient. If w is a real place of a number field L (i.e. a place corresponding to an embedding $\sigma : L \to \mathbb{R}$), we put

$$w(\alpha) = \begin{cases} 0 & \text{if } \sigma(\alpha) > 0 \\ 1 & \text{otherwise.} \end{cases}$$

Let v be a place of $\mathbb{Q}$. Suppose that that there exists a place $w \in \Omega_{\mathbb{Q}(A)}$ dividing v such that w ramifies in $L(\psi_1)/\mathbb{Q}(A)$. In that case we remark that $\text{Art}(v, L(\psi_2)/\mathbb{Q})$ is a well-defined element of $\mathbb{F}_2$ (see also the remarks preceding Theorem 3.2), and similarly if we swap the roles of 1 and 2.

Proposition 3.6. *The following statements hold.*

(a.1) Let v be a finite rational place and let $w \in \Omega_{\mathbb{Q}(A)}$ be a place lying above v. Suppose that w is unramified in $L(\psi_1) \cdot L(\psi_2)/\mathbb{Q}(A)$. Then

$$(\alpha_{1,A}, \alpha_{2,A})_w = 0.$$

(a.2) Suppose that $\infty \notin \text{Ram}(\mathbb{Q}(\chi_1)/\mathbb{Q}) \cup \text{Ram}(\mathbb{Q}(\chi_2)/\mathbb{Q})$. Then the value of $(\alpha_{1,A}, \alpha_{2,A})_w$ is the same for all places $w \in \Omega_{\mathbb{Q}(A)}$ lying above ∞.

(b) Suppose that (2) ramifies in $L(\psi_1)L(\psi_2)/\mathbb{Q}$. Let $\{i, j\} = \{1, 2\}$ be as in the fourth point of Definition 3.1. Then

$$(\alpha_{1,A}, \alpha_{2,A})_w = w(\alpha_{j,A}) \cdot \text{Art}((2), L(\psi_i)/\mathbb{Q})$$

for every $w \in \Omega_{\mathbb{Q}(A)}$ lying above (2), where the product is taken in $\mathbb{F}_2$.

(c) Let $\{1, 2\} = \{i, j\}$. Let v be a rational place not equal to (2) and let $w \in \Omega_{\mathbb{Q}(A)}$ be a place lying above v. Suppose that w ramifies in $L(\psi_i)/\mathbb{Q}(A)$. Then

$$(\alpha_{1,A}, \alpha_{2,A})_w = w(\alpha_{i,A}) \cdot \text{Art}(v, L(\psi_j)/\mathbb{Q}),$$

where the product is taken in $\mathbb{F}_2$.

Proof of Proposition 3.6 part (a.1). Let v and w be as in the statement. Our assumptions imply that the extensions $L(\psi_1)/\mathbb{Q}(A)$ and $L(\psi_2)/\mathbb{Q}(A)$ are unramified at all places of $\Omega_{\mathbb{Q}(A)}$ above v. Now, since the fields $L(\psi_1), L(\psi_2)$ are respectively equal to the Galois closure (over $\mathbb{Q}$) of the quadratic extensions $\mathbb{Q}(A)(\sqrt{\alpha_{1,A}})/\mathbb{Q}(A), \mathbb{Q}(A)(\sqrt{\alpha_{2,A}})/\mathbb{Q}(A)$, it follows that the classes of $\alpha_{1,A}, \alpha_{2,A}$ are unramified classes in $\frac{\mathbb{Q}(A)_w^*}{\mathbb{Q}(A)_w^{*2}}$. But, thanks to Lemma 3.5, the Hilbert symbol between two unramified classes is trivial. $\square$

Proof of Proposition 3.6 part (a.2). By definition ∞ splits completely in $\mathbb{Q}(A)$. Since $\infty \notin \text{Ram}(\mathbb{Q}(\chi_1)/\mathbb{Q}) \cup \text{Ram}(\mathbb{Q}(\chi_2)/\mathbb{Q})$, we deduce from Definition 3.1 that ∞ splits completely in $M(\psi_1)M(\psi_2)$.

Observe that $\alpha_{1,A}$ and $\alpha_{2,A}$ are $G_{\mathbb{Q}}$-invariants of respectively $\frac{M(\psi_1)^*}{M(\psi_1)^{*2}}$ and $\frac{M(\psi_2)^*}{M(\psi_2)^{*2}}$. Hence the conjugates of $\alpha_{i,A}$ are equal to $\alpha_{i,A}$ times a square in $M(\psi_i)$. In particular, $\sigma(\alpha_{i,A})$ equals $\sigma'(\alpha_{i,A})$ times the square of a real number for all real embeddings $\sigma, \sigma' : \mathbb{Q}(A) \to \mathbb{R}$. Therefore $\sigma(\alpha_{i,A})$ has constantly the same sign as we vary $\sigma : \mathbb{Q}(A) \to \mathbb{R}$ over all real embeddings. Since the Hilbert symbol in the local field $\mathbb{R}$ is entirely determined by the sign of its two entries, the result follows. $\square$

Proof of Proposition 3.6 part (b). The inclusion $i_2 : \mathbb{Q}^{\mathrm{sep}} \to \mathbb{Q}_2^{\mathrm{sep}}$ provides us with a unique place $\mathfrak{t} \in \Omega_{\mathbb{Q}(A)}$ above (2), namely the place $\mathfrak{t}$ corresponding to the absolute value obtained by composing i_2 with the canonical absolute value of $\mathbb{Q}_2^{\mathrm{sep}}$. Recalling that $\mathrm{Gal}(\mathbb{Q}(A)/\mathbb{Q})$ acts transitively (and in this case freely) on the 2^n places of $\Omega_{\mathbb{Q}(A)}$ above (2), it suffices to take any element σ of $\mathrm{Gal}(\mathbb{Q}(A)/\mathbb{Q})$, and show the desired conclusion for

$$(\alpha_{i,A}, \alpha_{j,A})_{\sigma(\mathfrak{t})} = (\sigma^{-1}(\alpha_{i,A}), \sigma^{-1}(\alpha_{j,A}))_{\mathfrak{t}}.$$

We now apply Proposition 3.3 and rewrite the right hand side as

$$(\alpha_{i,A}\gamma_i, \alpha_{j,A}\gamma_j)_{\mathfrak{t}} = (\alpha_{i,A}, \alpha_{j,A}\gamma_j)_{\mathfrak{t}}(\gamma_i, \alpha_{j,A}\gamma_j)_{\mathfrak{t}}, \tag{3.6}$$

where γ_h belongs to $\langle \{\alpha_{h,T}\}_{T \subsetneq A}\rangle$ for $h \in \{i,j\}$. We know that $\phi_T(\psi_i) \circ i_2^*$ is the trivial character, whenever $\varnothing \neq T \subsetneq A$, by the fourth condition of Definition 3.1. It follows that γ_i is in the span of $\alpha_{i,\varnothing}$ locally at $\mathfrak{t}$. Since $\alpha_{i,\varnothing}$ pairs trivially with all the $\alpha_{j,T}$ by assumption, equation (3.6) becomes

$$(\alpha_{i,A}, \alpha_{j,A}\gamma_j)_{\mathfrak{t}} = (\alpha_{i,A}, \sigma^{-1}(\alpha_{j,A}))_{\mathfrak{t}}.$$

Note that the character $\alpha_{i,A}$ is *unramified* locally at $\mathfrak{t}$, since ψ_i is a *normalized* expansion map. Therefore we conclude, by means of Lemma 3.5, that this Hilbert symbol equals $\mathfrak{t}(\sigma^{-1}(\alpha_{j,A})) = \sigma(\mathfrak{t})(\alpha_{j,A})$ in case $\alpha_{i,A}$ is the unique non-trivial unramified quadratic class at $\mathfrak{t}$, and equals 0 in case $\alpha_{i,A}$ is trivial. But now observe that the triviality of the unramified character $\alpha_{i,A}$ locally at $\mathfrak{t}$ precisely coincides with the triviality of the symbol $\mathrm{Art}((2), L(\psi_i)/\mathbb{Q})$. Hence the result is

$$\sigma(\mathfrak{t})(\alpha_{j,A}) \cdot \mathrm{Art}((2), L(\psi_i)/\mathbb{Q})$$

as desired. $\qquad\square$

Proof of Proposition 3.6 part (c). Let us firstly suppose that v is a finite place (hence in $\mathcal{P}$) and let $w \in \Omega_{\mathbb{Q}(A)}$ be above v. Observe that $L(\psi_j)/\mathbb{Q}(A)$ is unramified at w by definition.

Furthermore, $\alpha_{j,A}$ is a $G_{\mathbb{Q}}$-invariant class in $\frac{M(\psi_j)^*}{M(\psi_j)^{*2}}$. It follows that $\sigma(\alpha_{j,A})$ always lands in the same unramified class c of $\frac{\mathbb{Q}_v^*}{\mathbb{Q}_v^{*2}}$ as we vary over the 2^n embeddings of $\mathbb{Q}(A)$ into $\mathbb{Q}_v$. Recalling that

$$L(\psi_j) = M(\psi_j)\left(\sqrt{\alpha_{j,A}}\right)$$

and that v splits completely in $M(\psi_j)/\mathbb{Q}$ by assumption, we see that c is trivial if and only if $\mathrm{Art}(v, L(\psi_j)/\mathbb{Q})$ is trivial. Lemma 3.5 shows that

$$(\alpha_{i,A}, \alpha_{j,A})_w = \begin{cases} w(\alpha_{i,A}) & \text{if } \mathrm{Art}(v, L(\psi_j)/\mathbb{Q}) \text{ is non-trivial} \\ 0 & \text{if } \mathrm{Art}(v, L(\psi_j)/\mathbb{Q}) \text{ is trivial.} \end{cases}$$

This proves part (c) in case v is finite.

It remains to treat the case where v equals the infinite place ∞ of $\mathbb{Q}$. Let $w \in \Omega_{\mathbb{Q}(A)}$ be above v. If $w(\alpha_{i,A}) = 0$, then the proposition is correct, because the Hilbert symbol $(-,-)_{\mathbb{R}}$ vanishes in case one of the two entries is positive. Finally, suppose that $w(\alpha_{i,A}) = 1$. Recalling one more time that $\alpha_{j,A}$ is a $G_{\mathbb{Q}}$-invariant class in $\frac{M(\psi_j)^*}{M(\psi_j)^{*2}}$, we see that the sign of $\sigma(\alpha_{j,A})$ does not depend on the embedding $\sigma : \mathbb{Q}(A) \to \mathbb{R}$. Furthermore, since ∞ splits completely in $M(\psi_j)/\mathbb{Q}$, it follows from $L(\psi_j) = M(\psi_j)(\sqrt{\alpha_{j,A}})$ that this sign is positive if and only if $\mathrm{Art}(\infty, L(\psi_j)/\mathbb{Q})$ is trivial. $\qquad\square$

We will now prove the main result of this section.

Proof of Theorem 3.2. Hilbert's reciprocity law yields

$$\sum_{w \in \Omega_{\mathbb{Q}(A)}} (\alpha_{1,A}, \alpha_{2,A})_w = 0. \tag{3.7}$$

Suppose that $w \in \Omega_{\mathbb{Q}(A)}$ does not ramify in the extension $L(\psi_1)L(\psi_2)/\mathbb{Q}(A)$. If w is a finite place, then we obtain that $(\alpha_{1,A}, \alpha_{2,A})_w = 0$ thanks to Proposition 3.6 part $(a.1)$. If w is an infinite place, then we certainly have

$$\infty \notin \widetilde{\mathrm{Ram}}(\mathbb{Q}(\chi_1)/\mathbb{Q}) \cup \widetilde{\mathrm{Ram}}(\mathbb{Q}(\chi_2)/\mathbb{Q}).$$

We deduce from Proposition 3.6 part $(a.2)$ that the total contribution coming from all the places of $\Omega_{\mathbb{Q}(A)}$ above ∞ equals 2^n times the same number, which is 0 since $n \geq 1$.

Now suppose that w ramifies in $L(\psi_1)L(\psi_2)/\mathbb{Q}(A)$. Let us first treat the case where w ramifies in $L(\psi_1)/\mathbb{Q}(A)$ and write v for the place of $\mathbb{Q}$ below w. Then thanks to Proposition 3.6, part (b) and part (c), we obtain that

$$(\alpha_{1,A}, \alpha_{2,A})_w = w(\alpha_{1,A}) \cdot \mathrm{Art}(v, L(\psi_2)/\mathbb{Q}).$$

By assumption v splits completely in the extension $M(\psi_2)/\mathbb{Q}$, so it certainly splits completely in the extension $\mathbb{Q}(A)/\mathbb{Q}$. Corollary 3.4 shows that

$$\sum_{\substack{w \in \Omega_{\mathbb{Q}(A)} \\ w|v}} (\alpha_{1,A}, \alpha_{2,A})_w = \begin{cases} \mathrm{Art}(v, L(\psi_2)/\mathbb{Q}) & \text{if } v \in \widetilde{\mathrm{Ram}}(\mathbb{Q}(\chi_1)/\mathbb{Q}) \\ 0 & \text{otherwise.} \end{cases}$$

The same conclusion holds by swapping the roles of 1 and 2. After grouping all $w \in \Omega_{\mathbb{Q}(A)}$ lying above the same rational place v together, equation (3.7) becomes

$$\sum_{v \in \widetilde{\mathrm{Ram}}(\mathbb{Q}(\chi_1)/\mathbb{Q})} \mathrm{Art}(v, L(\psi_2)/\mathbb{Q}) + \sum_{v' \in \widetilde{\mathrm{Ram}}(\mathbb{Q}(\chi_2)/\mathbb{Q})} \mathrm{Art}(v', L(\psi_1)/\mathbb{Q}) = 0,$$

which can be rewritten as

$$\sum_{v \in \widetilde{\mathrm{Ram}}(\mathbb{Q}(\chi_1)/\mathbb{Q})} \mathrm{Art}(v, L(\psi_2)/\mathbb{Q}) = \sum_{v' \in \widetilde{\mathrm{Ram}}(\mathbb{Q}(\chi_2)/\mathbb{Q})} \mathrm{Art}(v', L(\psi_1)/\mathbb{Q}).$$

This completes the proof of the theorem. □

4 Profitable triples

The next two sections provide a novel way to gain class group data on one point of a cube of quadratic fields from class group data available on the other points. We will informally refer to this as a reflection principle. Since the material is of a rather technical nature, we will now provide an overview of what is going to unfold below, and its main differences with [42, Theorem 2.8]. We hope in this way to provide some guiding intuition for the reader.

The key concept is that of a *profitable triple*. Roughly speaking, with respect to [42, Theorem 2.8], we have less control over the raw cocycles that we encounter in our reflection

principles. However, the rather general form of Theorem 3.2 allows us to still obtain a reflection principle, where the relative governing fields are reasonably similar to the expansion maps $\phi_{\{p_i(1)p_i(2):i\in[s]\};p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G})$ appearing in [42, Theorem 2.8].

Another novel feature is that we repeatedly invoke Theorem 3.2 during the proof of our reflection principles, where the level of generality of Definition 3.1 allows us to have remarkably little knowledge of the raw cocycles and expansion maps involved, but still gives sufficient control over the relevant splitting conditions. In contrast, [42, Theorem 2.8] does not require as input any form of reciprocity law. Although we shall not prove it here, our techniques are able to prove a result eerily similar to [42, Theorem 2.8], except that the roles of $T(w_a)$ and $T(w_b)$ are interchanged. We remark that in the setup of [42, Theorem 2.8] it is not at all obvious how to achieve such a result.

Our approach might seem surprising at first, since in the reflection principles of Smith [42] it is customary to find exact relations among raw cocycles and expansion maps and only in a later step physically plug an Artin symbol in such relations. In contrast, in our setup of profitable triples, we have remarkably loose control on the relations between the raw cocycles and expansion maps. It is a crucial appeal to the reciprocity law of Theorem 3.2 that gives the reflection principle. Most of the constraints we put on our raw cocycles are merely to meet the conditions of Theorem 3.2 to allow such a reciprocity law to come into play.

Let $s \in \mathbb{Z}_{\geq 1}$ and let

$$C := \{p_1(1), p_1(2)\} \times \cdots \times \{p_s(1), p_s(2)\} \times \{d_0\},$$

where $(p_i(1), p_i(2))_{i\in[s]}$ are $2s$ distinct, positive, odd prime numbers satisfying $p_i(1)p_i(2) \equiv 1 \bmod 8$ for each $i \in [s]$, and $\prod_{i\in[s]} p_i(1)p_i(2)$ is coprime to the positive squarefree integer d_0. Thanks to this assumption, we can identify each element $((p_i(f(i)))_{i\in[s]}, d_0)$ of C with the squarefree integer $d_0 \cdot \prod_{i=1}^s p_i(f(i))$, where f is any function from $[s]$ to $[2]$. We denote by

$$x_0 := d_0 \cdot \prod_{i=1}^s p_i(1).$$

For each $i \in [s]$ and each $h \in [2]$ we denote by $C_{p_i(h)}$ the subset of $x \in C$ consisting of those elements satisfying $\pi_i(x) = p_i(h)$. More generally, for each $T \subseteq [s]$ and for each function f from T to $\{1, 2\}$, we denote by $C_{(p_i(f(i)))_{i\in T}}$ the subset of C consisting of those x such that $\pi_i(x) = p_i(f(i))$ for each $i \in T$. This notation will be often invoked for the function f constantly equal to 2, for which we give the following special notation in order to lighten up our formulas. We denote by C_T the subset of $x \in C$ such that $i \in T$ implies $\pi_i(x) = p_i(2)$.

Let a be a divisor of d_0. Suppose that we are given a tuple

$$(\psi_{s+1}(x))_{x\in C-\{x_0\}},$$

where $\psi_{s+1}(x)$ is a raw cocycle for $N(x)$ for each $x \in C - \{x_0\}$ satisfying

$$\psi_1(x) = 2^s \cdot \psi_{s+1}(x) = \chi_a. \tag{4.1}$$

Remark 4.1. *Observe that equation (4.1) implies that a is positive. Indeed, since $s+1 \geq 2$, equation (4.1) implies that $\chi_a \cup \chi_{-x}$ vanishes in $H^2(G_\mathbb{Q}, \mathbb{F}_2)$ for each x in $C - \{x_0\}$. Since x is positive, taking the Hilbert symbol at the unique infinite place of $\mathbb{Q}$ forces $a > 0$.*

We next make a crucial definition.

Definition 4.2. *Let* $(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})$ *be a triple as above. We call the triple* $(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})$ profitable *if for each* $i \in [s]$

- *we have*

$$\left(\sum_{x \in C_T} \psi_{s+1-|T|}(x) \right) (\sigma_{p_i(2)}) = 0$$

  for each $T \subseteq [s]$ *containing* i;

- *we have*

$$\sum_{x \in C_{p_i(2)}} \psi_{s-1}(x) = 0; \tag{4.2}$$

- *the map* $\phi_{\{p_j(1)p_j(2):j \in [s] - \{i\}\}; p_i(1)p_i(2)}(\mathfrak{G})$ *exists;*

- *every prime* l *dividing* d_0 *splits completely in*

$$L(\phi_{\{p_j(1)p_j(2):j \in [s] - \{i\}\}; p_i(1)p_i(2)}(\mathfrak{G}))/\mathbb{Q};$$

- (2) *and* ∞ *split completely in* $M(\phi_{\{p_j(1)p_j(2):j \in [s] - \{i\}\}; p_i(1)p_i(2)}(\mathfrak{G}))/\mathbb{Q};$

Remark 4.3. *We claim that the second condition in Definition 4.2 implies that*

$$\sum_{x \in C_T} \psi_{s-|T|}(x) = 0$$

for each $\varnothing \neq T \subseteq [s]$. *To see this, fix some* $j \in [s]$ *and apply the operator* d_{x_0} *to equation (4.2). Then we get*

$$\sum_{\varnothing \neq T \subseteq [s] - \{i\}} \chi_{\{p_k(1)p_k(2):k \in T\}}(\sigma) \cdot (-1)^{|T|+1+\chi_{x_0}(\sigma)} \cdot \left(\sum_{x \in C_T} \psi_{s-|T|}(x)(\tau) \right)$$

by Proposition 2.9. Now evaluate the resulting expression at (σ, τ) *satisfying* $\chi_{p_j(1)p_j(2)}(\sigma) = 1$ *and* $\chi_{p_k(1)p_k(2)}(\sigma) = 0$ *for all* $k \in [s] - \{i, j\}$. *This gives*

$$\sum_{x \in C_{\{i,j\}}} \psi_{s-2}(x) = 0.$$

Iterating this argument we obtain the desired conclusion.

We will often make use of the following important observation, which, informally put, says that the various quadratic fields, corresponding to the points of C, coincide locally at (2) and at the common ramified primes in the cube.

Proposition 4.4. *Let* $(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})$ *be a profitable triple. Let* p *be a prime divisor of* d_0 *or let* $p = 2$. *Then we have*

$$\mathbb{Q}_p(\sqrt{x}) = \mathbb{Q}_p(\sqrt{x_0})$$

for each $x \in C$. *Moreover, we have for each* $i \in [s]$, *each* $h \in [2]$ *and all* $x, x' \in C_{p_i(h)}$

$$\mathbb{Q}_{p_i(h)}(\sqrt{x}) = \mathbb{Q}_{p_i(h)}(\sqrt{x'}).$$

Proof. The case $p = 2$ readily follows from the requirement that $p_i(1)p_i(2) \equiv 1 \bmod 8$ for each $i \in [s]$. Every odd prime divisor p of d_0 splits completely in

$$L(\phi_{\{p_j(1)p_j(2):j\in[s]-\{i\}\};p_i(1)p_i(2)}(\mathfrak{G}))/\mathbb{Q}$$

by assumption. This certainly implies that p splits completely in $\mathbb{Q}(\sqrt{p_i(1)p_i(2)})$ for each $i \in [s]$, which immediately gives us the desired conclusion.

Finally, take distinct indices $i, j \in [s]$. Since $s + 1 \geq 2$, the map $\phi_{p_j(1)p_j(2);p_i(1)p_i(2)}(\mathfrak{G})$ exists. This map satisfies

$$(d\phi_{p_j(1)p_j(2);p_i(1)p_i(2)}(\mathfrak{G}))(\sigma, \tau) = \chi_{p_j(1)p_j(2)}(\sigma)\chi_{p_i(1)p_i(2)}(\tau).$$

Hence the right hand side is trivial in $H^2(G_{\mathbb{Q}}, \mathbb{F}_2)$. Therefore it is trivial in $H^2(G_{\mathbb{Q}_{p_i(h)}}, \mathbb{F}_2)$ for all $h \in [2]$. This means that $p_j(1)p_j(2)$ is a square modulo $p_i(h)$, which proves the last assertion. $\qquad\square$

Before we present the main theorem on profitable triples, we will state a useful lemma. When we apply Lemma 4.5 later, Proposition 4.4 will guarantee that the decomposition groups of the field $\mathbb{Q}(\{\sqrt{x} : x \in S\})$ are indeed cyclic.

Lemma 4.5. *Let S be a set of squarefree integers all greater than 1. Assume that the decomposition group of (2) in the field $K = \mathbb{Q}(\{\sqrt{x} : x \in S\})$ is cyclic. Let $k \geq 1$ be an integer and suppose that we are given raw cocycles $\psi_{k+1}(x)$ for $N(x)$ for each $x \in S$. Then*

(i) if p does not ramify in K, p is unramified in

$$\prod_{x\in S} L(\psi_{k+1}(x));$$

(ii) suppose that p ramifies in K. Then the ramification index of p in

$$\prod_{x\in S} L(\psi_{k+1}(x))$$

equals 2. Now assume that all decomposition groups of $K/\mathbb{Q}$ are cyclic. Then, if p ramifies in $\mathbb{Q}(\sqrt{x})$ for every $x \in S$, the residue field degree of p in

$$\prod_{x\in S} L(\psi_k(x))$$

equals 1.

Proof. Straightforward. $\qquad\square$

Let a profitable triple $(C, \chi_a, (\psi_{s+1}(x))_{x\in C-\{x_0\}})$ and a subset $\varnothing \subseteq T \subsetneq [s]$ be given. To this data we associate the map

$$\psi_T(C, \chi_a, (\psi_{s+1}(x))_{x\in C-\{x_0\}}) := \sum_{x\in C_{[s]-T}} \psi_{|T|+1}(x).$$

Note that the above definition also makes sense for $T = [s]$ in case we are further given a raw cocycle $\psi_{s+1}(x_0)$.

Theorem 4.6. Let $(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})$ be a profitable triple. Then there exists a raw cocycle $\psi_{s+1}(x_0)$ for $N(x_0)$ such that the following two properties hold

- for each $i \in [s]$ we have that

$$\sum_{x \in C} \psi_i(x) = 0; \tag{4.3}$$

- the tuple

$$(\psi_T(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}}))_{T \subseteq [s]}$$

is an expansion map $\psi(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})$ with support $\{\chi_{p_i(1)p_i(2)} : i \in [s]\} \cup \{\chi_a\}$ and pointer χ_a. Furthermore, if $v \in \mathcal{P}$ ramifies in

$$L(\psi(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}}))/\mathbb{Q}(\{\sqrt{p_i(1)p_i(2)} : i \in [s]\}),$$

then v divides d_0. The ramification index of $v \in \Omega_{\mathbb{Q}}$ is at most 2 in the extension $L(\psi(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}}))/\mathbb{Q}$. Finally, the 1-cochain

$$\phi_T(\psi(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})) \circ i_2^* = \psi_T(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}}) \circ i_2^*$$

is a quadratic character contained in the span of $\{\chi_5, \chi_{x_0}\}$ for each subset $T \subseteq [s]$. If (2) ramifies in $\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}$, then $\phi_T(\psi(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})) \circ i_2^*$ is a quadratic character contained in the span of $\{\chi_{x_0}\}$ for each $T \subsetneq [s]$.

Proof. We claim that

$$\psi_s(x_0) := -\sum_{\substack{x \in C \\ x \neq x_0}} \psi_s(x) \tag{4.4}$$

is a raw cocycle for $N(x_0)$ lifting χ_a. Since $2^s - 1$ is odd, we certainly have

$$2^{s-1}\psi_s(x_0) = -\sum_{\substack{x \in C \\ x \neq x_0}} 2^{s-1}\psi_s(x) = -\sum_{\substack{x \in C \\ x \neq x_0}} \chi_a = \chi_a.$$

Furthermore, it follows from Proposition 2.9 that

$$d_{x_0}(\psi_s(x_0))(\sigma, \tau) = \sum_{\varnothing \neq T \subseteq [s]} \chi_{\{p_i(1)p_i(2):i \in T\}}(\sigma) \cdot \left(\sum_{x \in C_T} \psi_{s-|T|}(x)(\tau) \right),$$

which is zero term by term thanks to equation (4.2) of Definition 4.2 and Remark 4.3. This, together with Proposition 2.5, gives a field extension corresponding to the homomorphism

$$G_{\mathbb{Q}} \to N(x_0)[2^s] \rtimes \mathbb{F}_2, \quad \sigma \mapsto (\psi_s(x_0)(\sigma), \chi_{x_0}(\sigma)),$$

where the generator of $\mathbb{F}_2$ acts by $-\mathrm{id}$ on $N(x_0)$. Our next goal is to show that the extension $L(\psi_s(x_0))\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}(\sqrt{x_0})$ is unramified at all finite places. By equation (4.4), we have an inclusion

$$L(\psi_s(x_0)) \subseteq \prod_{\substack{x \in C \\ x \neq x_0}} L(\psi_s(x)). \tag{4.5}$$

31

Then Lemma 4.5 implies that $L(\psi_s(x_0))\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}(\sqrt{x_0})$ is unramified at all finite places not lying above some $p_i(2)$.

It remains to show that $L(\psi_s(x_0))\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}(\sqrt{x_0})$ is unramified for any place of $\mathbb{Q}(\sqrt{x_0})$ above $p_i(2)$. Recall from Proposition 2.5 that the Galois extension $L(\psi_s(x))\mathbb{Q}(\sqrt{x})/\mathbb{Q}$ is given by the homomorphism from $G_\mathbb{Q}$ to $N(x)[2^s] \rtimes \mathbb{F}_2$ defined by the formula

$$\sigma \mapsto (\psi_s(x)(\sigma), \chi_x(\sigma)).$$

Notice that $p_i(2)$ is unramified in the extension $L(\psi_s(x))/\mathbb{Q}$ for each $x \in C_{p_i(1)} - \{x_0\}$. Then it follows from Proposition 2.3 that $\psi_s(x)(\sigma_{p_i(2)}) = 0$ for all $x \in C_{p_i(1)} - \{x_0\}$. Hence, the first condition of Definition 4.2 together with the definition of $\psi_s(x_0)$ implies that

$$(\psi_s(x_0)(\sigma_{p_i(2)}), \chi_{x_0}(\sigma_{p_i(2)})) = \mathrm{id}.$$

Invoking one more time Proposition 2.5 and Proposition 2.3, we conclude that $p_i(2)$ is unramified in $L(\psi_s(x_0))/\mathbb{Q}$ as desired. Since we have shown that $L(\psi_s(x_0))/\mathbb{Q}(\sqrt{x_0})$ is unramified at all finite places of $\mathbb{Q}(\sqrt{x_0})$, we conclude that $\psi_s(x_0)$ is a raw cocycle for $N(x_0)$ lifting χ_a, which satisfies equation (4.3) by construction.

In order to prove the existence of $\psi_{s+1}(x_0)$ with $2\psi_{s+1}(x_0) = \psi_s(x_0)$ we will instead show the equivalent statement that $\mathrm{Up}_{\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}}(p)$ splits completely in $L(\psi_s(x_0))\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}(\sqrt{x_0})$ for each prime p ramifying in $\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}$ (here we use the material in Subsection 2.3 and Proposition 2.6). This is in turn equivalent to

$$i_p(L(\psi_s(x_0))) \subseteq \mathbb{Q}_p(\sqrt{x_0}) \tag{4.6}$$

for each prime p ramifying in $\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}$.

Let us begin with the case that p divides d_0 (or $p = 2$ in case x_0 is 3 modulo 4). For all such choices of p, equation (4.6) is a consequence of Lemma 4.5 and equation (4.5). We are now left with proving the sought inclusion for $p_i(1)$ for each $i \in [s]$. First of all we claim that $i_{p_i(1)}(L(\psi_s(x))) \subseteq \mathbb{Q}_{p_i(1)}(\sqrt{x_0})$ for each $x \in C_{p_i(1)} - \{x_0\}$. Indeed, the Artin symbol of $\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(p_i(1))$ in $\mathrm{Gal}(L(\psi_s(x))\mathbb{Q}(\sqrt{x})/\mathbb{Q}(\sqrt{x}))$ vanishes thanks to the equation $2 \cdot \psi_{s+1}(x) = \psi_s(x)$ and the claim is a consequence of Proposition 4.4. Therefore noticing that

$$L(\psi_s(x_0)) \subseteq \left(\prod_{x \in C_{p_i(1)} - \{x_0\}} L(\psi_s(x))\right) L\left(\sum_{x \in C_{p_i(2)}} \psi_s(x)\right),$$

we see that it is enough to show that $i_{p_i(1)}(L(\sum_{x \in C_{p_i(2)}} \psi_s(x))) \subseteq \mathbb{Q}_{p_i(1)}$. Hence it suffices to show that $p_i(1)$ splits completely in the extension

$$L\left(\sum_{x \in C_{p_i(2)}} \psi_s(x)\right)/\mathbb{Q}.$$

Define $\widetilde{C} := C_{p_i(2)}$. We start by observing that equation (4.2) combined with Remark 4.3 and Proposition 2.9 implies that

$$\left(\sum_{x \in \widetilde{C}_{[s]-\{i\}-T}} \psi_{|T|+1}(x)\right)_{T \subseteq [s]-\{i\}}$$

is an expansion map, say E, with support set equal to $\{\chi_{p_j(1)p_j(2)} : j \in [s] - \{i\}\} \cup \{\chi_a\}$ and pointer χ_a.

We claim that $p_i(2)$ splits completely in $L(E)$. Let us first show that $p_i(2)$ is unramified in $L(E)$. We obtain, as an immediate consequence of equation (2.2) and the first point of Definition 4.2, that $\sigma_{p_i(2)}$ is mapped to the identity element via E. Then $p_i(2)$ is indeed unramified by Proposition 2.3. Since $L(E)$ is contained in $\prod_{x \in C_{p_i(2)}} L(\psi_s(x))$, it follows from Lemma 4.5 that $p_i(2)$ has residue field degree 1 in $L(E)$ implying the claim.

We next claim that

$$i_{p_i(1)}\left(M\left(\sum_{x \in \widetilde{C}} \psi_s(x)\right)\right) \subseteq \mathbb{Q}_{p_i(1)} \quad \text{and} \quad i_{p_i(1)}\left(L\left(\sum_{x \in \widetilde{C}} \psi_s(x)\right)\right) \subseteq \mathbb{Q}_{p_i(1)}^{\mathrm{unr}}. \quad (4.7)$$

The second containment in equation (4.7) is clear, since $p_i(1)$ is unramified in $L(\psi_s(x))$ for every $x \in \widetilde{C}$. Thanks to Proposition 2.9 the first condition is equivalent to $p_i(1)$ splitting completely in

$$L\left(\sum_{x \in C_T} \psi_{s-1}(x)\right)$$

for every $T \subseteq [s]$ of size 2 containing i. Let us first observe that the above field is contained in the compositum of $L(\psi_s(x))$ for x satisfying $\pi_i(x) = p_i(2)$. Hence

$$i_{p_i(1)}\left(L\left(\sum_{x \in C_T} \psi_{s-1}(x)\right)\right) \subseteq \mathbb{Q}_{p_i(1)}^{\mathrm{unr}}. \quad (4.8)$$

Next observe that

$$\sum_{x \in C_T} \psi_{s-1}(x) = -\sum_{x \in C_{(p_i(1),p_j(2))}} \psi_{s-1}(x)$$

thanks to equation (4.2), where $T = \{i, j\}$. It follows from Lemma 4.5 that $p_i(1)$ has residue field degree 1 in $L(\sum_{x \in C_{(p_i(1),p_j(2))}} \psi_{s-1}(x))$. Therefore we have

$$i_{p_i(1)}\left(L\left(\sum_{x \in C_T} \psi_{s-1}(x)\right)\right) \subseteq \mathbb{Q}_{p_i(1)}(\sqrt{x_0}). \quad (4.9)$$

We derive from equations (4.8) and (4.9) that

$$i_{p_i(1)}\left(L\left(\sum_{x \in C_T} \psi_{s-1}(x)\right)\right) \subseteq \mathbb{Q}_{p_i(1)}(\sqrt{x_0}) \cap \mathbb{Q}_{p_i(1)}^{\mathrm{unr}} = \mathbb{Q}_{p_i(1)}.$$

This establishes equation (4.7).

We are now in position to show that the 4-tuple

$$(\{\chi_{p_j(1)p_j(2)} : j \in [s] - \{i\}\} \cup \{\chi_a\}, \{\chi_{p_j(1)p_j(2)} : j \in [s] - \{i\}\} \cup \{\chi_{p_i(1)p_i(2)}\},$$

$$\left(\sum_{x \in \widetilde{C}_{[s]-\{i\}-T}} \psi_{|T|+1}(x)\right)_{T \subseteq [s]-\{i\}}, (\phi_{\{p_j(1)p_j(2):j \in T\};p_i(1)p_i(2)}(\mathfrak{G}))_{T \subseteq [s]-\{i\}})$$

is Rédei admissible. From this we will derive, by an application of Theorem 3.2, the desired splitting of $p_i(1)$. Let us start by checking the coprimality conditions among the pointers. Observe that a and $p_i(1)p_i(2)$ do not share any common prime divisor by construction. Furthermore, a is positive, see Remark 4.1, and $p_i(1)p_i(2)$ is obviously positive. Finally, we have $p_i(1)p_i(2) \equiv 1 \bmod 8$ by assumption, hence the desired orthogonality at 2 between χ_a and $\chi_{p_i(1)p_i(2)}$, with respect to the Hilbert pairing, is evidently satisfied.

We now check Rédei admissability. To lighten the notational burden, we denote, as in Section 3, by ψ_1 the first expansion map and by ψ_2 the second expansion map appearing in the 4-tuple above.

Let us start by examining the infinite place. It follows from Remark 4.1 that ∞ splits completely in the field $\mathbb{Q}(\{\sqrt{p_k(1)p_k(2)} : k \in [s]\}, \sqrt{a})$. Hence we need to check that ∞ splits completely in $M(\psi_1)M(\psi_2)$. The field $L(\psi_s(x))$ is totally real for each $x \in \widetilde{C}$ thanks to the equation $2 \cdot \psi_{s+1}(x) = \psi_s(x)$. Therefore their compositum is totally real and thus we conclude that $M(\psi_1)$ is totally real. Regarding $M(\psi_2)$ this is explicitly prescribed in the fifth point of Definition 4.2.

Let us now consider the place (2). It follows from the fifth condition of Definition 4.2 that (2) splits completely in the extension $L(\psi_2)/\mathbb{Q}$. Therefore, in view of Definition 3.1, there is no further condition to check for ψ_1.

It remains to examine the odd places dividing d_0 or places of the form $p_j(h)$ for some $j \in [s]$ and $h \in [2]$. Indeed, $L(\psi_1)/\mathbb{Q}$ does not ramify at any other odd place by Lemma 4.5, while Proposition 2.15 implies that $L(\psi_2)/\mathbb{Q}$ ramifies only at primes of the form $p_j(h)$ for $j \in [s]$ and $h \in [2]$. So let us take an odd prime p dividing d_0. Thanks to the fourth condition of Definition 4.2 p splits completely in $L(\psi_2)/\mathbb{Q}$.

We now examine the place $p_j(h)$ with j different from i. Then we claim that each place above $p_j(h)$ is unramified in

$$L(\psi_1)L(\psi_2)/\mathbb{Q}(\{\sqrt{p_k(1)p_k(2)} : k \in [s] - \{i\}\}).$$

In fact we make the stronger claim that $\sigma_{p_j(h)}$ has order at most 2 when projected to the Galois groups $\mathrm{Gal}(L(\psi_1)/\mathbb{Q})$ and $\mathrm{Gal}(L(\psi_2)/\mathbb{Q})$. This implies the original claim, since the ramification index of $p_j(h)$ in $\mathbb{Q}(\{\sqrt{p_k(1)p_k(2)} : k \in [s] - \{i\}\})/\mathbb{Q}$ already equals 2, since j is different from i. For ψ_1, observe that this holds for each individual Galois group $\mathrm{Gal}(L(\psi_s(x))/\mathbb{Q})$, since the extension $L(\psi_s(x))/\mathbb{Q}(\sqrt{x})$ is unramified for each $x \in \tilde{C}$. For ψ_2, observe that normalized expansion maps send every $\sigma \in \mathfrak{G}$ to an involution by construction.

We are now left with the places $p_i(1)$ and $p_i(2)$. But we have already shown above that $L(\psi_1)/\mathbb{Q}$ is unramified at both of them, and even that $p_i(2)$ splits completely therein. Furthermore, we have established, see equation (4.7), that $p_i(1)$ splits completely in $M(\psi_1)/\mathbb{Q}$. Therefore the 4-tuple is Rédei admissible. We now apply Theorem 3.2. The relevant Artin symbols in $L(\psi_2)$ are zero thanks to the fourth point of Definition 4.2. We have already shown that $\mathrm{Art}(p_i(2), L(\psi_1)/\mathbb{Q})$ vanishes. Hence Theorem 3.2 yields that $p_i(1)$ splits completely in the field of definition of ψ_1.

Since $i \in [s]$ was arbitrary, we have completed the proof that $\psi_s(x_0)$ pairs trivially with $\mathrm{Cl}(\mathbb{Q}(\sqrt{x_0}))[2]$. Therefore there exists $\psi_{s+1}(x_0)$ with

$$2 \cdot \left(\sum_{x \in C} \psi_{s+1}(x) \right) = 0.$$

34

Invoking one more time Proposition 2.9 combined with equation (4.2) and Remark 4.3, we obtain that

$$\psi(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})$$

is an expansion map with support $\{\chi_{p_i(1)p_i(2)} : i \in [s]\} \cup \{\chi_a\}$ and pointer χ_a.

Let us now prove the final claims concerning the ramification locus of the extension $L(\psi(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}}))/\mathbb{Q}$. First of all, recall that (2) splits completely in the field $\mathbb{Q}(\{\sqrt{p_i(1)p_i(2)} : i \in [s]\})/\mathbb{Q}$, because of our assumption $p_i(1)p_i(2) \equiv 1 \mod 8$ for each $i \in [s]$. In view of Proposition 2.9 this also shows that the map $\phi_T(\psi(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})) \circ i_2^*$ is a character from $G_{\mathbb{Q}_2}$ to $\mathbb{F}_2$. The other claims are now a consequence of Lemma 4.5. $\square$

From now on we will refer to the maps $\psi_{s+1}(x_0)$ and $\psi(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})$ obtained in Theorem 4.6 as, respectively, the raw cocycle and the expansion map *attached* to the profitable triple $(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})$.

5 Reflection principles for profitable triples

We divide our reflection principles for profitable triples in three families. The final family of reflection principles is taken from Smith [42], and does not involve the notion of profitable triples.

5.1 Reflection principles for ∞

We say that a squarefree integer $d > 1$ is *special* in case it has no prime divisors congruent to 3 modulo 4. From now on we shall use the notation for s and C as given at the beginning of Section 4. We say that C is special in case all its elements are special. Let us start by defining -1-profitable triples. If $\phi_{\{a_i : i \in [s]\}; a_{s+1}}(\mathfrak{G})$ exists, then recall that

$$M(\phi_{\{a_i : i \in [s]\}; a_{s+1}}(\mathfrak{G})) = \mathbb{Q}(\{\chi_{a_i} : i \in [s]\}) \prod_{T \subsetneq [s]} L(\phi_{\{a_i : i \in T\}; a_{s+1}}(\mathfrak{G})).$$

Definition 5.1. Let $(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})$ be a special, profitable triple. We say that $(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})$ is a -1-profitable triple in case

- the map $\phi_{\{p_i(1)p_i(2) : i \in [s]\}; -1}(\mathfrak{G})$ exists;

- every odd prime divisor of d_0 splits completely in $M(\phi_{\{p_i(1)p_i(2) : i \in [s]\}; -1}(\mathfrak{G}))/\mathbb{Q}$;

- $(\sqrt{x}) \in 2^s \mathrm{Cl}(\mathbb{Q}(\sqrt{x}))[2^{s+1}]$ for each $x \in C$;

- the place $(1 + i)$ of $\mathbb{Q}(i)$ splits completely in $M(\phi_{\{p_i(1)p_i(2) : i \in [s]\}; -1}(\mathfrak{G}))/\mathbb{Q}(i)$.

Before stating out next theorem, we remind the reader that the splitting of $(\sqrt{x})$ in an unramified extension (at all finite places) of $\mathbb{Q}(\sqrt{x})$ is the same as the splitting behavior of an infinite place. Furthermore, we remind the reader of the conventions about $\mathrm{Art}(2, L(\psi_i)/\mathbb{Q})$ discussed after Definition 3.1.

Theorem 5.2. Let $(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})$ be a -1-profitable triple. Then

$$\chi_a \in 2^s \mathrm{Cl}(\mathbb{Q}(\sqrt{x_0}))^\vee [2^{s+1}].$$

Furthermore, each odd prime number $p \mid a$ splits completely in $M(\phi_{\{p_i(1)p_i(2):i\in[s]\};-1}(\mathfrak{G}))/\mathbb{Q}$, the place $(1+i)$ splits completely in $M(\phi_{\{p_i(1)p_i(2):i\in[s]\};-1}(\mathfrak{G}))/\mathbb{Q}(i)$ and

$$\sum_{x\in C}\langle(\sqrt{x}),\chi_a\rangle_{\mathrm{Art}_{s+1}(x)} = \sum_{p\mid a}\phi_{\{p_i(1)p_i(2):i\in[s]\};-1}(\mathfrak{G})(\mathrm{Frob}(p)).$$

Proof. Since $(C,\chi_a,(\psi_{s+1}(x))_{x\in C-\{x_0\}})$ is in particular a profitable triple, an application of Theorem 4.6 yields

$$\chi_a \in 2^s\mathrm{Cl}(\mathbb{Q}(\sqrt{x_0}))^\vee[2^{s+1}].$$

It is also clear that $(1+i)$ splits completely in $M(\phi_{\{p_i(1)p_i(2):i\in[s]\};-1}(\mathfrak{G}))/\mathbb{Q}(i)$ and that every odd prime p dividing a splits completely in $M(\phi_{\{p_i(1)p_i(2):i\in[s]\};-1}(\mathfrak{G}))/\mathbb{Q}$. Indeed, this is literally the second and fourth condition in Definition 5.1.

It remains to prove the last part of the theorem. Pick a raw cocycle $\psi_{s+1}(x_0)$ as in Theorem 4.6. Let $\psi(C,\chi_a,(\psi_{s+1}(x))_{x\in C-\{x_0\}})$ be the expansion map attached to the profitable triple. Denote by $\mathrm{Frob}(\infty)$ the generator of $\mathrm{Gal}(\mathbb{Q}_\infty^{\mathrm{sep}}/\mathbb{Q}_\infty)$. We claim that

$$\sum_{x\in C}\langle(\sqrt{x}),\chi_a\rangle_{\mathrm{Art}_{s+1}(x)} = \psi_{[s]}(C,\chi_a,(\psi_{s+1}(x))_{x\in C-\{x_0\}})(i_\infty^*(\mathrm{Frob}(\infty))). \tag{5.1}$$

Indeed, for each $x\in C$, we can write

$$\langle(\sqrt{x}),\chi_a\rangle_{\mathrm{Art}_{s+1}(x)} = \psi_{s+1}(x)(i_\infty^*(\mathrm{Frob}(\infty))),$$

and hence equation (5.1) follows from the equality

$$\sum_{x\in C}\psi_{s+1}(x) = \psi_{[s]}(C,\chi_a,(\psi_{s+1}(x))_{x\in C-\{x_0\}}).$$

We now show that the 4-tuple

$$(\{\chi_{p_i(1)p_i(2)} : i\in[s]\}\cup\{\chi_a\}, \{\chi_{p_i(1)p_i(2)} : i\in[s]\}\cup\{\chi_{-1}\},$$
$$\psi(C,\chi_a,(\psi_{s+1}(x))_{x\in C-\{x_0\}}), (\phi_{\{p_i(1)p_i(2):i\in T\};-1}(\mathfrak{G}))_{T\subseteq[s]})$$

is Rédei admissible. Once we have completed this task, then the desired conclusion follows at once from Theorem 3.2 combined with equation (5.1).

Let us start by examining the coprimality conditions. The coprimality condition at the odd places is satisfied since one of the two pointers is χ_{-1}. At ∞ we need to guarantee that a is positive, which follows from Remark 4.1. At (2) we need to guarantee that χ_{-1} and χ_a are orthogonal with respect to the local Hilbert pairing. Since a is special, χ_a is contained in the span of $\{\chi_2,\chi_5\}$ locally at 2. This last space is precisely the orthogonal complement of $\langle\chi_{-1}\rangle$ with respect to the local Hilbert pairing at 2.

It remains to check the conditions in Definition 3.1. In what follows we will denote, as in Section 3, by ψ_1 the first expansion map and by ψ_2 the second expansion map of the 4-tuple. The first condition of Definition 3.1 is trivially satisfied. Let us now check the second condition.

Observe that ∞ certainly ramifies in $\mathbb{Q}(i)/\mathbb{Q}$. Therefore we need to check that ∞ splits completely in $M(\psi_1)$. But the extension $L(\psi_s(x))/\mathbb{Q}$ is totally real for each $x\in C$ due to the equation $2\cdot\psi_{s+1}(x) = \psi_s(x)$. Hence the desired conclusion follows immediately, since $M(\psi_1)$ is contained in the compositum of totally real fields. We now check the third condition of

Definition 3.1. Thanks to Theorem 4.6 and Proposition 2.15, we only need to check the odd primes dividing d_0 and those of the form $p_i(h)$ for some $i \in [s]$ and some $h \in [2]$.

Let p be an odd prime dividing d_0. Then p splits completely in $M(\psi_2)/\mathbb{Q}$ by the second condition of Definition 5.1. Furthermore, p is unramified in $L(\psi_2)/\mathbb{Q}$ by Proposition 2.15. Let now $i \in [s]$ and $h \in [2]$. In this case we claim that every place of $\mathbb{Q}(\{\sqrt{p_j(1)p_j(2)} : j \in [s]\})$ above $p_i(h)$ stays unramified in $L(\psi_1)L(\psi_2)/\mathbb{Q}(\{\sqrt{p_j(1)p_j(2)} : j \in [s]\})$. To see this last claim, we use the last statement in Theorem 4.6 for ψ_1 and Proposition 2.15 for ψ_2.

It remains to check the fourth condition of Definition 3.1. We have $\chi_{-1}(\sigma_2(2)) = 0$ by construction of $\sigma_2(2)$. We will now verify that $\phi_T(\psi_2) \circ i_2^* = 0$ for each $\varnothing \subsetneq T \subsetneq [s]$. First observe that $\phi_T(\psi_2) \circ i_2^*$ is a quadratic character. Since ψ_2 is normalized, it follows that $\phi_T(\psi_2) \circ i_2^*$ is in the span of the unramified quadratic character. But $(1 + i)$ splits completely in $M(\psi_2)/\mathbb{Q}(i)$ by the fourth condition of Definition 5.1. This shows that $\phi_T(\psi_2) \circ i_2^* = 0$.

Finally, we need to check for each $T \subseteq [s]$ that the map $\phi_T(\psi_1)$ restricts to a quadratic character that is in the span of $\{\chi_5, \chi_2\}$, which is the orthogonal complement of $\langle \chi_{-1} \rangle$ with respect to the local Hilbert pairing at (2). This follows from the last part of Theorem 4.6 keeping in mind that x_0 is a special integer, which forces the span of $\{\chi_{x_0}, \chi_5\}$ to be contained in the span of $\{\chi_5, \chi_2\}$ locally at (2). This ends the proof that the 4-tuple is Rédei admissable, which, as explained above, concludes the proof of the theorem. □

5.2 Reflection principles for the self-pairing

We begin with two auxiliary results, which are the two fundamental steps towards the main results of this subsection, Theorem 5.6 and Theorem 5.7. Theorem 5.3 is a result similar to Theorem 5.2, if not a simpler one, in the sense that it does not invoke any further usage of reciprocity than already invoked in Theorem 4.6. Instead Theorem 5.5 is a genuinely novel result having no analogue in the previous reflection principles. It relies on Hilbert's reciprocity law in a critical manner.

Theorem 5.3. *Let $(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})$ be a profitable triple. Suppose that*

$$\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(a) \in 2^s \cdot \mathrm{Cl}(\mathbb{Q}(\sqrt{x}))[2^{s+1}]$$

for each $x \in C$. Then $\mathrm{Up}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(p)$ splits completely in $M(\psi(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}}))$ for each $p \mid a$. Furthermore, we have that

$$\chi_a \in 2^s \cdot \mathrm{Cl}(\mathbb{Q}(\sqrt{x_0}))^\vee[2^{s+1}]$$

and

$$\sum_{x \in C} \langle \mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(a), \chi_a \rangle_{\mathrm{Art}_{s+1}(x)} = \sum_{p \mid a} \psi_{[s]}(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})(\mathrm{Frob}(\mathrm{Up}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(p))).$$

Proof. For each prime $p \mid a$ the map i_p gives us a unique prime $\mathfrak{p}$ above p in

$$K := \mathbb{Q}(\{\sqrt{p_i(1)p_i(2)} : i \in [s]\}, \sqrt{x_0}).$$

For each $x \in C$ the extension $\mathbb{Q}(\sqrt{x})$ is inside K. Therefore we conclude that

$$KL(\psi_{s+1}(x))/K$$

is unramified at $\mathfrak{p}$ and

$$\langle \mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(a), \chi_a \rangle_{\mathrm{Art}_{s+1}(x)} = \sum_{p|a} \psi_{s+1}(x)(\mathrm{Frob}(\mathfrak{p})),$$

since p has residue field degree 1 in K by Proposition 4.4. Summing up all the contributions, we get

$$\sum_{p|a} \psi_{[s]}(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})(\mathrm{Frob}(\mathfrak{p})).$$

Lemma 4.5 implies that $\mathrm{Up}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(p)$ splits completely in $M(\psi(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})) \cdot K$ for each $p \mid a$. Therefore we can rewrite

$$\psi_{[s]}(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})(\mathrm{Frob}(\mathfrak{p}))$$

as

$$\psi_{[s]}(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})(\mathrm{Frob}(\mathrm{Up}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(p))).$$

We conclude that

$$\sum_{x \in C} \langle \mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(a), \chi_a \rangle_{\mathrm{Art}_{s+1}(x)} = \sum_{p|a} \psi_{[s]}(C, \chi_a, (\psi_{s+1}(x))_{x \in C - \{x_0\}})(\mathrm{Frob}(\mathrm{Up}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(p)))$$

as desired. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\square$

We are now going to abstract the crucial features of the cochains appearing on the right hand side of Theorem 5.3. As an auxiliary piece of notation, we remind the standard notation that one attaches to a finite Galois extension $F/\mathbb{Q}$ and to a prime number p

$$e_p(F/\mathbb{Q}) := \#(\mathrm{proj}(G_{\mathbb{Q}} \to \mathrm{Gal}(F/\mathbb{Q})) \circ i_p^*)(I_p),$$

and

$$f_p(F/\mathbb{Q}) := \frac{\#(\mathrm{proj}(G_{\mathbb{Q}} \to \mathrm{Gal}(F/\mathbb{Q})) \circ i_p^*)(G_{\mathbb{Q}_p})}{e_p(F/\mathbb{Q})}.$$

Definition 5.4. *Let $s \in \mathbb{Z}_{\geq 1}$. Let $\{a_1, \ldots, a_{s+1}\}$ be pairwise coprime, special squarefree integers greater than 1. An expansion map $(\phi_{\{a_i : i \in T\}; a_{s+1}})_{T \subseteq [s]}$ with support set $\{a_1, \ldots, a_{s+1}\}$ and pointer a_{s+1} is said to be* Pellian *in case*

- *for each finite prime p ramifying in $L(\phi_{\{a_i : i \in [s]\}; a_{s+1}})/\mathbb{Q}$, we have that*

$$e_p(L(\phi_{\{a_i : i \in [s]\}; a_{s+1}})/\mathbb{Q}) = e_p(M(\phi_{\{a_i : i \in [s]\}; a_{s+1}})/\mathbb{Q}) = 2$$

  and p is not 3 modulo 4;

- *we have*

$$f_p(M(\phi_{\{a_i : i \in [s]\}; a_{s+1}})/\mathbb{Q}) = 1$$

  for each finite prime p ramifying in $M(\phi_{\{a_i : i \in [s]\}; a_{s+1}})/\mathbb{Q}$;

- *the character χ_{a_i} is locally trivial at 2 for all $i \in [s]$;*

- *∞ splits completely in $M(\phi_{\{a_i : i \in [s]\}; a_{s+1}})/\mathbb{Q}$;*

- $\phi_{\{a_i:i\in T\};a_{s+1}}(\sigma_2(1)) = 0$ *for each* $T \subsetneq [s]$;

- *all prime divisors of a_i are unramified in*

$$L(\phi_{\{a_j:j\in[s]-\{i\}\};a_{s+1}})/\mathbb{Q}$$

for each $i \in [s]$.

Let p be a prime divisor of a_{s+1}. By definition of a Pellian expansion, we have that $\mathrm{Up}_{\mathbb{Q}(\sqrt{a_{s+1}})/\mathbb{Q}}(p)$ is unramified in $L(\phi_{\{a_i:i\in[s]\};a_{s+1}})$ and splits completely in $M(\phi_{\{a_i:i\in[s]\};a_{s+1}})$. Therefore we have that $\mathrm{Frob}(\mathrm{Up}_{\mathbb{Q}(\sqrt{a_{s+1}})/\mathbb{Q}}(p))$ is well-defined and lands in

$$\mathrm{Gal}(L(\phi_{\{a_i:i\in[s]\};a_{s+1}})/M(\phi_{\{a_i:i\in[s]\};a_{s+1}})) \cong \mathbb{F}_2.$$

We now give the second auxiliary result, which has some similarities with the computations in [20, Section 12].

Theorem 5.5. *Let $s \in \mathbb{Z}_{\geq 2}$. Let $\{a_1, \ldots, a_{s+1}\}$ be pairwise coprime, special squarefree integers. Let $(\phi_{\{a_i:i\in T\};a_{s+1}})_{T\subseteq[s]}$ be a Pellian expansion map with support $\{a_1, \ldots, a_{s+1}\}$ and pointer a_{s+1}. Then*

$$\sum_{p|a_{s+1}} \phi_{\{a_i:i\in[s]\};a_{s+1}}(\mathrm{Frob}(\mathrm{Up}_{\mathbb{Q}(\sqrt{a_{s+1}})/\mathbb{Q}}(p))) = 0.$$

Proof. Until specified, all intermediate assertions that we are going to make also apply to the case $s = 1$.

Construction of an auxiliary 1-cochain

Let us write $K := \mathbb{Q}(\{a_i : i \in [s] - \{1\}\})$. Observe that the restriction of $\phi_{\{a_i:i\in[s]-\{1\}\};a_{s+1}}$ to G_K is a quadratic character, while $\phi_{\{a_i:i\in[s]\};a_{s+1}}$ restricted to G_K is a 1-cochain whose differential equals the following cup product

$$(d\phi_{\{a_i:i\in[s]\};a_{s+1}})(\sigma,\tau) = \chi_{a_1}(\sigma) \cdot \phi_{\{a_i:i\in[s]-\{1\}\};a_{s+1}}(\tau)$$

of quadratic characters.

Thanks to the first point of Definition 5.4, the quadratic character $\phi_{\{a_i\}_{i\in[s]-\{1\}};a_{s+1}}$ does not ramify at odd finite places of K not possessing a primitive 4-th root of unity. As such the 2-cocycle

$$\theta(\sigma,\tau) := \phi_{\{a_i:i\in[s]-\{1\}\};a_{s+1}}(\sigma) \cdot \phi_{\{a_i:i\in[s]-\{1\}\};a_{s+1}}(\tau)$$

is locally trivial at all finite odd places of K. Furthermore, θ is trivial at all the 2^{s-1} infinite places of K, in virtue of the fourth point of Definition 5.4. We now examine the places above (2). Observe that by the third point (2) splits completely in K. Call $\mathfrak{t}$ the unique place of K given by i_2. Then $K_{\mathfrak{t}} = \mathbb{Q}_2$.

Recall that the set of characters $\chi \in \mathrm{Hom}_{\mathrm{top.gr.}}(G_{\mathbb{Q}_2}, \mathbb{F}_2)$ with $\chi \cup \chi = 0$ in $H^2(G_{\mathbb{Q}_2}, \mathbb{F}_2)$ forms a subspace thanks to the antisymmetry of the Hilbert symbol. Furthermore, it coincides precisely with the space of characters vanishing at $\sigma_2(1)$. To see this, remark that $\chi_2 \cup \chi_2$ and $\chi_5 \cup \chi_5$ are trivial (since $2^2 = 2 + 2$ and $5^2 = 5 + 5 \cdot 2^2$). Then, since both spaces are 2-dimensional, they must coincide.

Now, thanks to the fifth condition in Definition 5.4, we see that

$$\mathrm{inv}_{\mathfrak{t}}(\phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\sigma) \cdot \phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\tau)) = 0.$$

We now show it for all the other places above (2). Take any $\rho \in \mathrm{Gal}(K/\mathbb{Q})$. Observe that

$$\mathrm{inv}_{\rho(\mathfrak{t})}(\phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\sigma) \cdot \phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\tau)) =$$
$$\mathrm{inv}_{\mathfrak{t}}(\phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\rho \sigma \rho^{-1}) \cdot \phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\rho \tau \rho^{-1})).$$

Invoking Proposition 3.3, we see that $\phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\rho \sigma \rho^{-1})$ is in the span of

$$\{\phi_{\{a_i : i \in T\}; a_{s+1}} : T \subseteq [s] - \{1\}\}.$$

However, invoking again the fifth condition of Definition 5.4, we see that each $\phi_{\{a_i : i \in T\}; a_{s+1}}$ is in the subspace of $\chi \in \mathrm{Hom}_{\mathrm{top.gr.}}(G_{K_{\mathfrak{t}}}, \mathbb{F}_2)$ with

$$\mathrm{inv}_{\mathfrak{t}}(\chi \cup \chi) = 0.$$

Therefore we conclude that

$$\mathrm{inv}_{\mathfrak{t}}(\phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\rho \sigma \rho^{-1}) \cdot \phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\rho \tau \rho^{-1})) = 0$$

and hence

$$\mathrm{inv}_{\rho(\mathfrak{t})}(\phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\sigma) \cdot \phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\tau)) = 0.$$

We have proved that θ vanishes locally at all places above (2) as well. Hence we have completed the proof that the class of θ is locally trivial at all places of K. Therefore there exists a 1-cochain $\widetilde{\phi} : G_K \to \mathbb{F}_2$ with

$$(d\widetilde{\phi})(\sigma, \tau) = \theta(\sigma, \tau) = \phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\sigma) \cdot \phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\tau).$$

The possible choices of the cochain $\widetilde{\phi}$ form a coset under $\mathrm{Hom}_{\mathrm{top.gr.}}(G_K, \mathbb{F}_2)$. We are going to make a choice of $\widetilde{\phi}$ that will simplify the coming discussion. Since χ_{a_1} is a character that ramifies at some place, we can always choose a set $S_1(K)$ of odd prime ideals of O_K spanning $\frac{\mathrm{Cl}(K)}{2\mathrm{Cl}(K)}$ such that χ_{a_1} is locally trivial at each of them.

Let us call $S(K)$ the set of places of K that are in $S_1(K)$ or lie above (2) or ∞. We now claim that we can always make a choice of $\widetilde{\phi}$ such that $L(\widetilde{\phi})/K$ is unramified outside of $S(K)$ and the places where $L(\phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}})/K$ ramifies. Indeed, start with one cochain $\widetilde{\phi}_1 : G_K \to \mathbb{F}_2$ such that

$$(d\widetilde{\phi}_1)(\sigma, \tau) = \theta(\sigma, \tau) = \phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\sigma) \cdot \phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\tau).$$

Suppose first that the field extension $L(\widetilde{\phi}_1)/K$ ramifies at some place $\mathfrak{p}$ outside of $S(K)$ and the set of places where $L(\phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}})/K$ ramifies. By definition of $S(K)$ we can find an ideal J entirely supported in $S(K)$ such that $\mathfrak{p}J = (\gamma_{\mathfrak{p}}) \cdot I^2$ for some integral ideal I of $\mathcal{O}_K$ and some non-zero element $\gamma_{\mathfrak{p}}$ of K.

Observe that the quadratic character $\chi_{\gamma_{\mathfrak{p}}}$ ramifies at $\mathfrak{p}$ and its ramification locus is contained in $\{\mathfrak{p}\} \cup S(K)$. Furthermore, writing $\widetilde{\phi}_2 = \widetilde{\phi}_1 + \chi_{\gamma_{\mathfrak{p}}}$, we see that $L(\widetilde{\phi}_2)/K$ is unramified at $\mathfrak{p}$. Since $L(\widetilde{\phi}_1)/K$ ramifies at finitely many places, we get a 1-cochain $\widetilde{\phi}$ with the claimed properties by iterating this procedure. In what follows we consider this choice of $\widetilde{\phi}$.

Construction of a 2-cocycle

A quick calculation shows that

$$\widetilde{\theta}(\sigma,\tau) := \phi_{\{a_i : i \in [s]\}; a_{s+1}}(\sigma) \cdot \phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\tau) + \chi_{a_1}(\sigma) \cdot \widetilde{\phi}(\tau)$$

is a 2-cocycle, giving a class in $H^2(G_K, \mathbb{F}_2)$. Hence Hilbert reciprocity yields

$$\sum_{v \in \Omega_K} \operatorname{inv}_v(\widetilde{\theta}) = 0.$$

We next calculate for each $v \in \Omega_K$ the value of $\operatorname{inv}_v(\widetilde{\theta})$.

The infinite places

Observe that χ_{a_1} is locally trivial at any infinite place, since $a_1 > 0$. Furthermore, thanks to the fourth condition in Definition 5.4, we see that $\phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}$ is also locally trivial at each infinite place. We therefore conclude that the 2-cocycle $\widetilde{\theta}$ becomes literally the zero map when restricted to each decomposition group of an archimedean place of K. Hence $\operatorname{inv}_v(\widetilde{\theta}) = 0$ for each infinite place v of K.

Places above a_{s+1}

We distinguish two cases. Let first p be an odd prime factor of a_{s+1}. Clearly, p ramifies in $L(\phi_{\{a_i : i \in [s]\}; a_{s+1}})/\mathbb{Q}$. It follows that p splits completely in $K(\sqrt{a_1})$ thanks to the first and the second condition of Definition 5.4. Let $\mathfrak{p}$ be one of the 2^{s-1} places of Ω_K lying above p. Then χ_{a_1} is locally trivial at $\mathfrak{p}$, thanks to the just mentioned splitting of p in $K(\sqrt{a_1})$. We conclude that $\phi_{\{a_i : i \in [s]\}; a_{s+1}}$ and $\phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}$ are both quadratic characters locally at $\mathfrak{p}$. Therefore, locally at $\mathfrak{p}$, the 2-cocycle $\widetilde{\theta}$ becomes the cup product

$$\phi_{\{a_i : i \in [s]\}; a_{s+1}}(\sigma) \cdot \phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\tau).$$

This shows that

$$\operatorname{inv}_{\mathfrak{p}}(\widetilde{\theta}) = \operatorname{inv}_{\mathfrak{p}}(\phi_{\{a_i : i \in [s]\}; a_{s+1}}(\sigma) \cdot \phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\tau)).$$

It follows from the first and the second condition in Definition 5.4 that the set

$$\{\phi_{\{a_i : i \in T\}; a_{s+1}} : T \subsetneq [s]\}$$

spans the 1-dimensional space generated by $\chi_{a_{s+1}}$ locally at $\mathfrak{p}$. From this we deduce that

$$\phi_{\{a_i : i \in [s]\}; a_{s+1}}(\operatorname{Frob}(\operatorname{Up}_{\mathbb{Q}(\sqrt{a_{s+1}})/\mathbb{Q}}(p))) = 0$$

if and only if $\phi_{\{a_i : i \in [s]\}; a_{s+1}}$ lands in the space generated by $\chi_{a_{s+1}}$. In case $\phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}$ is locally trivial at $\mathfrak{p}$, we evidently get

$$\operatorname{inv}_{\mathfrak{p}}(\phi_{\{a_i : i \in [s]\}; a_{s+1}}(\sigma) \cup \phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\tau)) = 0.$$

Otherwise, $\phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}$ is non-trivial locally at $\mathfrak{p}$ and hence equals $\chi_{a_{s+1}}$ locally at $\mathfrak{p}$. Then we get

$$\operatorname{inv}_{\mathfrak{p}}(\phi_{\{a_i : i \in [s]\}; a_{s+1}}(\sigma) \cdot \phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\tau)) = \phi_{\{a_i : i \in [s]\}; a_{s+1}}(\operatorname{Frob}(\operatorname{Up}_{\mathbb{Q}(\sqrt{a_{s+1}})/\mathbb{Q}}(p))).$$

Indeed, the above Hilbert symbol vanishes if and only if $\phi_{\{a_i : i \in [s]\}; a_{s+1}}$ is in the space generated by the non-trivial character $\chi_{a_{s+1}}$, which, as we argued, is also decided by the Artin symbol. Finally, Corollary 3.4 implies that the total contribution of the places above p is precisely

$$\phi_{\{a_i : i \in [s]\}; a_{s+1}}(\mathrm{Frob}(\mathrm{Up}_{\mathbb{Q}(\sqrt{a_{s+1}})/\mathbb{Q}}(p))).$$

Suppose now that 2 divides a_{s+1}. We explain why the above argument works in this case as well. Thanks to the first and the second condition in Definition 5.4, we know that

$$\{\phi_{\{a_i : i \in T\}; a_{s+1}}|_{i_2^*(G_{\mathbb{Q}_2})} : T \subseteq [s]\}$$

spans a space that is at most 2-dimensional, containing $\chi_{a_{s+1}}$ and reaching dimension 2 if and only if χ_5 is therein. Again the symbol $\phi_{\{a_i : i \in [s]\}; a_{s+1}}(\mathrm{Frob}(\mathrm{Up}_{\mathbb{Q}(\sqrt{a_{s+1}})/\mathbb{Q}}(2)))$ detects whether the dimension is 2 and likewise for the Hilbert symbol

$$\mathrm{inv}_{\mathfrak{p}}(\phi_{\{a_i : i \in [s]\}; a_{s+1}}(\sigma) \cdot \phi_{\{a_i : i \in [s]-\{1\}\}; a_{s+1}}(\tau)) = \phi_{\{a_i : i \in [s]\}; a_{s+1}}(\mathrm{Frob}(\mathrm{Up}_{\mathbb{Q}(\sqrt{a_{s+1}})/\mathbb{Q}}(2)))$$

in case $\phi_{\{a_i : i \in [s]-\{1\}\}; a_{s+1}}$ is non-trivial locally at $\mathfrak{p}$. With these small differences, the rest of the proof is identical and one reaches again the conclusion that the final contribution above (2) is

$$\phi_{\{a_i : i \in [s]\}; a_{s+1}}(\mathrm{Frob}(\mathrm{Up}_{\mathbb{Q}(\sqrt{a_{s+1}})/\mathbb{Q}}(2))).$$

Hence we conclude that the total contribution from the places above the prime divisors of a_{s+1} is

$$\sum_{p | a_{s+1}} \phi_{\{a_i : i \in [s]\}; a_{s+1}}(\mathrm{Frob}(\mathrm{Up}_{\mathbb{Q}(\sqrt{a_{s+1}})/\mathbb{Q}}(p))).$$

The remaining places not dividing a_1

Suppose that v is a finite place of K above a prime q such that the residue field $\mathbb{F}_v$ is a non-trivial extension of $\mathbb{F}_q$. We claim that

$$\mathrm{inv}_v(\widetilde{\theta}) = 0. \tag{5.2}$$

Observe that q is unramified in $L(\phi_{\{a_i : i \in [s]\}; a_{s+1}})/\mathbb{Q}$ by the first and second condition of Definition 5.4. By our assumption on v, we have $\mathbb{F}_q^* \subseteq \mathbb{F}_v^{*2}$. Then the character χ_{a_i} is locally trivial at v for all $i \in [s]$, and therefore $\phi_{\{a_i : i \in [s]\}; a_{s+1}}(\sigma)$ and $\phi_{\{a_i : i \in [s]-\{1\}\}; a_{s+1}}(\tau)$ are both quadratic characters locally at v. Hence $\widetilde{\theta}$ becomes the cup product

$$\phi_{\{a_i : i \in [s]\}; a_{s+1}}(\sigma) \cdot \phi_{\{a_i : i \in [s]-\{1\}\}; a_{s+1}}(\tau)$$

of two unramified characters, which proves the claimed equation (5.2).

We are left with the finite places v with residue field degree one in K and not dividing a_{s+1}. Write q for the place of $\mathbb{Q}$ below v. Let us first consider v such that q is unramified in $L(\phi_{\{a_i : i \in [s]\}; a_{s+1}})/\mathbb{Q}$. Then q splits completely in K.

First suppose that v ramifies in $L(\widetilde{\phi})/K$. Then, by our choice of $S(K)$ if q is odd, and by the third condition of Definition 5.4 in case $q = 2$, we have that χ_{a_1} is trivial locally at q. Since q splits completely in K, we conclude that χ_{a_1} is also locally trivial at v. Therefore at all such places we are left with the cup product of two unramified characters and thus we get that the Hilbert symbol is trivial.

Next suppose that v is unramified in $L(\widetilde{\phi})/K$. For each such v we have that the restriction of $\widetilde{\theta}$ to G_{K_v} is in the image of the inflation

$$\inf : H^2(\mathrm{Gal}(K_v^{\mathrm{unr}}/K_v), \mathbb{F}_2) \to H^2(G_{K_v}, \mathbb{F}_2).$$

But we know that $\mathrm{Gal}(K_v^{\mathrm{unr}}/K_v) \cong \hat{\mathbb{Z}}$ and $H^2(\hat{\mathbb{Z}}, \mathbb{F}_2) = 0$, since any central extension of $\hat{\mathbb{Z}}$ is clearly trivial. We conclude that

$$\mathrm{inv}_v(\widetilde{\theta}) = 0$$

in this case.

Hence we have proved that the contribution from all the places above finite rational primes q unramified in $L(\phi_{\{a_i : i \in [s]\}; a_{s+1}})/\mathbb{Q}$ is pointwise 0. We now turn to the ramified places.

Among the remaining places, let us first examine those v for which q does not divide a_1. It follows from the second condition of Definition 5.4 that χ_{a_1} is locally trivial at such places. Hence we are left with

$$\phi_{\{a_i : i \in [s]\}; a_{s+1}}(\sigma) \cdot \phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\tau)$$

locally at v. Let us further suppose that q does not ramify in $K/\mathbb{Q}$. Then it must split completely in $K/\mathbb{Q}$. Now for each of the 2^{s-1} places above q where the quadratic character $\phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}$ of G_K ramifies, the invariant map is zero if $f_q(L(\phi_{\{a_i : i \in [s]\}; a_{s+1}})/\mathbb{Q}) = 1$ and non-zero if $f_q(L(\phi_{\{a_i : i \in [s]\}; a_{s+1}})/\mathbb{Q}) = 2$. Since q does not divide a_{s+1}, there is an even number of places above q ramifying in $\phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}$ in virtue of Corollary 3.4. Therefore the total contribution from such places is trivial.

In case $s \geq 2$, we still need to deal with the places q not dividing a_1 but dividing a_i for some $i \in [s] - \{1\}$. Take a place v above q and observe that both characters

$$\phi_{\{a_i : i \in [s]\}; a_{s+1}}, \quad \phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}$$

have even valuation at v, thanks to the first condition in Definition 5.4. Therefore the Hilbert symbol is trivial also in this case.

Places dividing a_1

We are now left with the v such that q divides a_1. Indeed, we have shown that the total contribution from all the other places not dividing a_{s+1} is trivial. Take now such a prime q dividing a_1. Observe that all the characters

$$\phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}$$

are locally trivial at v, thanks to the second and fifth condition of Definition 5.4. In particular $\widetilde{\phi}$ becomes a quadratic character locally at v and $\widetilde{\theta}$ becomes the cup product

$$\chi_{a_1}(\sigma) \cdot \widetilde{\phi}(\tau).$$

Furthermore, v is unramified in the cyclic degree 4 extension $L(\tilde{\phi})/K$ and splits in the unique quadratic subextension given by $\phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}$. Let us call

$$\widetilde{\psi} : G_K \twoheadrightarrow \mathbb{Z}/4\mathbb{Z}$$

the continuous epimorphism given by

$$\sigma \mapsto (\widetilde{\phi}(\sigma), \phi_{\{a_i : i \in [s] - \{1\}\}; a_{s+1}}(\sigma)),$$

where $\mathbb{Z}/4\mathbb{Z}$ is represented as $\mathbb{F}_2 \times \mathbb{F}_2$ with the product law

$$(a_1, b_1) * (a_2, b_2) = (a_1 + a_2 + b_1 b_2, b_1 + b_2).$$

We have that the total contribution from places above q dividing a_1 is

$$\sum_{\substack{v \in \Omega_K \\ v \mid q}} \widetilde{\psi}(\mathrm{Frob}(v)).$$

This is precisely the same as

$$(N_{K/\mathbb{Q}}(\widetilde{\psi}))(\mathrm{Frob}(q)).$$

Now $N_{K/\mathbb{Q}}(\widetilde{\psi})$ is a cyclic degree 4 character of $G_\mathbb{Q}$ lifting the quadratic character $\chi_{a_{s+1}}$, thanks to Proposition 3.3. As such it can be given by

$$\sigma \mapsto (\phi_{a_{s+1};a_{s+1}}(\mathfrak{G})(\sigma) + \chi(\sigma), \chi_{a_{s+1}}(\sigma)),$$

thanks to Lemma 2.18.

Study of the character χ

We claim that χ is a quadratic character that only ramifies at primes that split completely in $\mathbb{Q}(\sqrt{a_1})$. Indeed, observe that all the primes ramifying in K split completely in $\mathbb{Q}(\sqrt{a_1})$. Furthermore, $L(\widetilde{\psi})/K$ ramifies only at places of K that split completely in $\mathbb{Q}(\sqrt{a_1})$ by construction of $S(K)$, and the same is true for all the conjugates of $\widetilde{\psi}$. Therefore the field of definition $L(\phi_{a_{s+1};a_{s+1}}(\mathfrak{G}) + \chi)/\mathbb{Q}$ can ramify only at places where χ_{a_1} is locally trivial.

We will now show how this implies that χ has the desired property. By assumption the places (2) and ∞ split completely in $\mathbb{Q}(\sqrt{a_1})/\mathbb{Q}$, so we can focus entirely on the odd primes. We show that if an odd prime p ramifies in $\mathbb{Q}(\chi)/\mathbb{Q}$, then it must also ramify in $L(\phi_{a_{s+1};a_{s+1}}(\mathfrak{G}) + \chi)/\mathbb{Q}$, and thus, as we argued above, p must split completely in $\mathbb{Q}(\sqrt{a_1})/\mathbb{Q}$. Observe that, by definition, we have that

$$\phi_{a_{s+1};a_{s+1}}(\mathfrak{G})(\sigma_p) = 0,$$

and, by Proposition 2.3, we have that $\chi(\sigma_p) = 1$. It follows that

$$\sigma_p \mapsto (1, \chi_{a_{s+1}}(\sigma_p)) \neq (0, 0).$$

Therefore by Proposition 2.3 we conclude that p ramifies in $L(\phi_{a_{s+1};a_{s+1}}(\mathfrak{G}) + \chi)/\mathbb{Q}$, which establishes the claim.

End of proof

What we have proven so far applies also to the Pellian expansion map $\phi_{a_1;a_{s+1}}$, since we have not made use that $s \geq 2$ yet. But now we have

$$\sum_{p \mid a_{s+1}} \phi_{\{a_i : i \in [s]\};a_{s+1}}(\mathrm{Frob}(\mathrm{Up}_{\mathbb{Q}(\sqrt{a_{s+1}})/\mathbb{Q}}(p))) = \sum_{q \mid a_1}(\phi_{a_{s+1};a_{s+1}}(\mathfrak{G}) + \chi)(\mathrm{Frob}(q))$$

$$= \sum_{p \mid a_{s+1}} \phi_{a_1;a_{s+1}}(\mathrm{Frob}(\mathrm{Up}_{\mathbb{Q}(\sqrt{a_{s+1}})/\mathbb{Q}}(p))) = 0,$$

where the first equality follows from the above analysis for $\phi_{\{a_i:i\in[s]\};a_{s+1}}$, the second equality follows from the above analysis for $\phi_{a_1;a_{s+1}}$ (i.e. the case $s=1$) and the last equality follows from $s\geq 2$ and the first two conditions of Definition 5.4. $\qquad\square$

The following results are the main theorems of this subsection.

Theorem 5.6. *Let $s\in\mathbb{Z}_{\geq 2}$. Let $(C,\chi_a,(\psi_{s+1}(x))_{x\in C-\{x_0\}})$ be a -1-profitable triple. Suppose that $\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(a)\in 2^s\cdot\mathrm{Cl}(\mathbb{Q}(\sqrt{x}))[2^{s+1}]$ for each $x\in C$. Then we also have that*

$$\chi_a\in 2^s\cdot\mathrm{Cl}(\mathbb{Q}(\sqrt{x}))^{\vee}[2^{s+1}]$$

and

$$\sum_{x\in C}\langle\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(a),\chi_a\rangle_{\mathrm{Art}_{s+1}(x)}=0.$$

Proof. This is now a straightforward combination of Theorem 5.3 and Theorem 5.5. $\qquad\square$

Theorem 5.7. *Let $s\in\mathbb{Z}_{\geq 2}$. Let $(C,\chi_a,(\psi_{s+1}(x))_{x\in C-\{x_0\}})$ be a -1-profitable triple. Suppose that $\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(a)\in 2^s\cdot\mathrm{Cl}(\mathbb{Q}(\sqrt{x}))[2^{s+1}]$ for each $x\in C$. Then we also have that*

$$\chi_a\in 2^s\cdot\mathrm{Cl}(\mathbb{Q}(\sqrt{x}))^{\vee}[2^{s+1}]$$

and

$$\sum_{x\in C}\left\langle\frac{(\sqrt{x})}{\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(a)},\chi_{\frac{x}{a}}\right\rangle_{\mathrm{Art}_{s+1}(x)}=\sum_{p\mid a}\phi_{\{p_i(1)p_i(2):i\in[s]\};-1}(\mathfrak{G})(\mathrm{Frob}(p)).$$

Proof. Observe that

$$\left\langle\frac{(\sqrt{x})}{\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(a)},\chi_{\frac{x}{a}}\right\rangle_{\mathrm{Art}_{s+1}(x)}=\left\langle(\sqrt{x})\cdot\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(a),\chi_a\right\rangle_{\mathrm{Art}_{s+1}(x)}$$

$$=\left\langle\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(a),\chi_a\right\rangle_{\mathrm{Art}_{s+1}(x)}+\left\langle(\sqrt{x}),\chi_a\right\rangle_{\mathrm{Art}_{s+1}(x)}.$$

Hence the conclusion follows upon combining Theorem 5.2 and Theorem 5.6. $\qquad\square$

5.3 Standard reflection principles

We now establish the more classical reflection principles. Some of our arguments are different, but the material of this subsection is based on [42]. We include it here with proofs in order to keep our work self-contained.

Let s be a positive integer and let

$$C:=\{p_1(1),p_1(2)\}\times\cdots\times\{p_s(1),p_s(2)\}\times\{p_{s+1}(1),p_{s+1}(2)\}\times\{d_0\},$$

where $\{p_1(1),p_1(2),\ldots,p_{s+1}(1),p_{s+1}(2)\}$ is a set of $2s+2$ distinct prime numbers, each of them coprime with the positive squarefree integer d_0. Furthermore, we demand that $p_i(1)p_i(2)\equiv 1\bmod 8$ and that $p_i(1)p_i(2)$ is a square modulo every odd prime factor of d_0 for every $i\in[s]$. Let a be a divisor of d_0. As at the beginning of Section 4, we identify points in C with squarefree integers. We write

$$x_0:=d_0\cdot\prod_{i=1}^{s+1}p_i(1).$$

Suppose that we have for each $x \in C - \{x_0\}$ a raw cocycle $\psi_{s+1}(x)$ for $N(x)$ such that either

$$2^s \cdot \psi_{s+1}(x) = \chi_a$$

for each $x \in C - \{x_0\}$, or

$$2^s \cdot \psi_{s+1}(x) = \chi_{\pi_{s+1}(x)a}$$

for each $x \in C - \{x_0\}$, where we recall that π_{s+1} is the projection on the $s+1$-th coordinate of C. For convenience, the first case will be referred to as being *of type 1*, while the second case is said to be *of type 2*. We now make the two key definitions of this subsection. We begin with the notion of minimal triples.

Definition 5.8. *Suppose that* $(C, (\psi_{s+1}(x))_{x \in C - \{x_0\}}, \chi_a)$ *is a triple of type 1. We say that the triple is a* minimal triple *in case for each non-empty subset* $T \subseteq [s+1]$ *we have that*

$$\sum_{x \in C_T} \psi_{s-|T|+1}(x) = 0. \tag{5.3}$$

We next turn to the notion of governing triples.

Definition 5.9. *Suppose that* $(C, (\psi_{s+1}(x))_{x \in C - \{x_0\}}, \chi_a)$ *is a triple of type 2. We say that the triple is a* governing triple *in case*

- *for each* $T \subseteq [s]$ *the map* $\phi_{\{p_i(1)p_i(2):i \in T\}; p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G})$ *exists;*

- *for each non-empty* $T \subseteq [s]$, *we have*

$$\sum_{x \in C_T} \psi_{s-|T|+1}(x) = \phi_{\{p_i(1)p_i(2):i \in [s]-T\}; p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G});$$

- *for each* $T \subseteq [s+1]$ *with* $s+1 \in T$, *we have*

$$\sum_{x \in C_T} \psi_{s-|T|+1}(x) = 0.$$

We can now give the two main results of this subsection. We start with the one on minimal triples.

Theorem 5.10. *Let* $(C, (\psi_{s+1}(x))_{x \in C - \{x_0\}}, \chi_a)$ *be a minimal triple. Then*

$$\chi_a \in 2^s \cdot \mathrm{Cl}(\mathbb{Q}(\sqrt{x_0}))^\vee[2^{s+1}].$$

Moreover, we have the following results.

(i) Let $b \mid d_0$ *(resp.* $b \mid 2d_0$ *in case* $\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}$ *ramifies at 2) be such that*

$$\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(b) \in 2^s \cdot \mathrm{Cl}(\mathbb{Q}(\sqrt{x}))[2^{s+1}]$$

for each $x \in C$. *Then*

$$\sum_{x \in C} \langle \mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(b), \chi_a \rangle_{\mathrm{Art}_{s+1}(x)} = 0.$$

(ii) Instead suppose that

$$\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(x) \in 2^s \cdot \mathrm{Cl}(\mathbb{Q}(\sqrt{x}))[2^{s+1}]$$

for each $x \in C$. Then

$$\sum_{x \in C} \langle \mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(x), \chi_a \rangle_{\mathrm{Art}_{s+1}(x)} = 0.$$

Proof. Let us start by proving that $\chi_a \in 2^s \cdot \mathrm{Cl}(\mathbb{Q}(\sqrt{x_0}))^\vee[2^{s+1}]$. To this end, consider the 1-cochain $\psi_{s+1}(x_0) : G_{\mathbb{Q}} \to N[2^{s+1}]$ defined by

$$\psi_{s+1}(x_0) := - \sum_{x \in C : x \neq x_0} \psi_{s+1}(x).$$

We will show that $\psi_{s+1}(x_0)$ is a 1-cocycle for $N(x_0)$ with $2^s \cdot \psi_{s+1}(x_0) = \chi_a$. This last assertion follows immediately from

$$2^s \cdot \psi_{s+1}(x_0) = -(2^s - 1) \cdot \chi_a = \chi_a.$$

Let us next prove that $\psi_{s+1}(x_0) : G_{\mathbb{Q}} \to N(x_0)[2^{s+1}]$ is in fact a 1-cocycle. Thanks to Proposition 2.9 we have that

$$\begin{aligned}
(d_{x_0}\psi_{s+1}(x_0))(\sigma, \tau) &= \sum_{\varnothing \neq T \subseteq [s+1]} \chi_{\{p_i(1)p_i(2) : i \in T\}}(\sigma) \cdot (-1)^{|T|+1+\chi_{x_0}(\sigma)} \left(\sum_{x \in C_T} \psi_{s-|T|+1}(x)(\tau) \right) \\
&= 0,
\end{aligned}$$

where the last equation follows from our assumption

$$\sum_{x \in C_T} \psi_{s-|T|+1}(x) = 0,$$

see equation (5.3).

In particular it follows that $\psi_s(x_0) := 2 \cdot \psi_{s+1}(x_0)$ is a 1-cocycle with values in $N(x_0)[2^s]$. We claim that $\psi_s(x_0)$ once restricted to $G_{\mathbb{Q}(\sqrt{x_0})}$ naturally lands in $\mathrm{Cl}(\mathbb{Q}(\sqrt{x_0}))^\vee[2^s]$, i.e. that it yields a cyclic degree 2^s extension of $\mathbb{Q}(\sqrt{x_0})$ unramified at all finite places. Let us first consider a prime p that does not ramify in $\mathbb{Q}(\sqrt{x})$ for any $x \in C$. Then we simply observe that

$$L(\psi_s(x_0)) \subseteq \prod_{x \in C-\{x_0\}} L(\psi_s(x)). \tag{5.4}$$

Lemma 4.5 and equation (5.4) give the desired conclusion in this case.

We now consider the case of a prime p ramifying in $\mathbb{Q}(\sqrt{x})$ for every $x \in C$ or of the form $p_i(1)$ for some $i \in [s+1]$. Since p has ramification index 2 in $\prod_{x \in C-\{x_0\}} L(\psi_s(x))/\mathbb{Q}$ by Lemma 4.5 and since p ramifies in $\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}$, this case is also okay. We finally consider the case of an odd prime of the form $p_i(2)$ for some $i \in [s+1]$. Then we deduce from equation (5.3) that

$$\sum_{x \in C_{p_i(2)}} \psi_s(x) = 0,$$

which shows that

$$\psi_s(x_0) = - \sum_{\substack{x \in C-\{x_0\} \\ \pi_i(x)=p_i(1)}} \psi_s(x).$$

It follows that $L(\psi_s(x_0)) \cdot \mathbb{Q}(\sqrt{x_0})$ is contained in the compositum

$$\mathbb{Q}(\sqrt{x_0}) \cdot \left(\prod_{\substack{x \in C-\{x_0\} \\ \pi(x)=p_i(1)}} L(\psi_s(x)) \right).$$

The prime $p_i(2)$ visibly does not ramify in the above field, since $\mathbb{Q}(\sqrt{x})$ is unramified at $p_i(2)$ for each x with $\pi_i(x) = p_i(1)$ and $L(\psi_s(x)) \cdot \mathbb{Q}(\sqrt{x})/\mathbb{Q}(\sqrt{x})$ is unramified at all finite places of $\mathbb{Q}(\sqrt{x})$. This establishes the claim, since every place of $\mathbb{Q}$ either equals $p_i(1)$ or $p_i(2)$ for some $i \in [s+1]$, or ramifies in $\mathbb{Q}(\sqrt{x})$ for every $x \in C$, or is unramified in $\mathbb{Q}(\sqrt{x})$ for all $x \in C$.

We now prove that there exists a raw cocycle $\psi'_{s+1}(x_0)$ with $2 \cdot \psi'_{s+1}(x) = \psi_s(x_0)$. This is equivalent to showing that $\mathrm{Up}_{\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}}(p)$ has trivial Artin symbol in $\mathrm{Gal}(L(\psi_s(x_0)) \cdot \mathbb{Q}(\sqrt{x_0})/\mathbb{Q}(\sqrt{x_0}))$ for each prime p ramifying in $\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}$.

Let us first prove this for an odd prime p. Then, necessarily, p divides x_0. We are going to show that the mere existence of the lift $\psi_{s+1}(x_0)$, which itself is not guaranteed to be unramified, guarantees the existence of an unramified lift of $\psi_s(x_0)$. Thanks to the shape of the tame local Galois group, we see that $(\psi_{s+1}(x_0), \chi_{x_0}) \circ i_p^*$ induces a homomorphism

$$\mathbb{Z}_2 \rtimes p^{\mathbb{Z}_2} \to N(x_0)[2^{s+1}] \rtimes \mathbb{F}_2.$$

This homomorphism factors through the subgroup $2 \cdot \mathbb{Z}_2 \rtimes p^{\mathbb{Z}_2}$, since the order of the image of σ_p equals exactly 2. Indeed, elements with non-trivial second coordinate in the dihedral group $N(x_0)[2^{s+1}] \rtimes \mathbb{F}_2$ are all involutions and clearly $\chi_{x_0}(\sigma_p) = 1$. Hence $(\psi_{s+1}(x_0), \chi_{x_0}) \circ i_p^*$ induces a homomorphism $\mathbb{F}_2 \times p^{\mathbb{Z}_2} \to N(x_0)[2^{s+1}] \rtimes \mathbb{F}_2$, which surjects on the $\mathbb{F}_2$ component. This forces the restriction of the homomorphism to $G_{\mathbb{Q}_p(\sqrt{x_0})}$ to land in $N(x_0)[2]$, since no other element of $N(x_0)$ commutes with an element of the shape $(n, 1)$. But hence, when we project to $N(x_0)[2^s] \rtimes \mathbb{F}_2$, we obtain that

$$\psi_s(x_0)(\mathrm{Frob}(\mathrm{Up}_{\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}}(p))) = 0$$

as desired.

It remains to prove that $\mathrm{Up}_{\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}}(2)$ splits completely in $L(\psi_s(x_0)) \cdot \mathbb{Q}(\sqrt{x_0})/\mathbb{Q}(\sqrt{x_0})$ in case (2) ramifies in $\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}$. Recalling that $p_i(1)p_i(2) \equiv 1 \bmod 8$ for each $i \in [s+1]$ we find that (2) ramifies in $\mathbb{Q}(\sqrt{x})/\mathbb{Q}$ for every $x \in C$. Hence, the equation $2 \cdot \psi_{s+1}(x) = \psi_s(x)$ in $\mathrm{Cl}(\mathbb{Q}(\sqrt{x}))^\vee$ implies that $\psi_s(x)$ pairs trivially with the 2-torsion class $\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(2)$ for each $x \in C - \{x_0\}$. Therefore, keeping in mind that $\mathbb{Q}_2(\sqrt{x}) = \mathbb{Q}_2(\sqrt{x_0})$, we have that

$$i_2(L(\psi_s(x)) \cdot \mathbb{Q}(\sqrt{x})) \subseteq \mathbb{Q}_2(\sqrt{x_0}),$$

for each x in $C - \{x_0\}$, which implies

$$i_2(L(\psi_s(x_0)) \cdot \mathbb{Q}(\sqrt{x_0})) \subseteq \mathbb{Q}_2(\sqrt{x_0})$$

due to the inclusion (5.4). This means exactly that $\mathrm{Up}_{\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}}(2)$ splits completely in $L(\psi_s(x_0)) \cdot \mathbb{Q}(\sqrt{x_0})/\mathbb{Q}(\sqrt{x_0})$. This concludes our examination at (2).

We deduce the existence of a raw cocycle $\psi'_{s+1}(x)$ satisfying $2 \cdot \psi'_{s+1}(x) = \psi_s(x)$. In particular, we have shown that $\chi_a \in 2^s \cdot \mathrm{Cl}(\mathbb{Q}(\sqrt{x_0}))^{\vee}[2^{s+1}]$, which is the first part of the theorem. We now proceed with the proof of (i). The proof of (ii) is similar and is omitted. First of all notice that

$$\chi := \psi'_{s+1}(x_0) - \psi_{s+1}(x_0)$$

is a quadratic character. Indeed, χ is a 1-cocycle valued in $N(x_0)[2] = \mathbb{F}_2$, equipped with the only possible $G_{\mathbb{Q}}$-action, namely the trivial one. As we shall see, this observation will allow us to replace $\psi'_{s+1}(x_0)$ with $\psi_{s+1}(x_0)$ for the purpose of evaluating the Artin pairing. To take advantage of this, let us rewrite each of the Artin pairings as an Artin symbol taken from the same field extension.

To this end, fix $x \in C$ and a prime divisor p of b. The map i_p gives a unique place above p in

$$K := \mathbb{Q}(\{\sqrt{p_i(1)p_i(2)} : i \in [s+1]\}, \sqrt{x_0}).$$

Let us denote this place of K as $\mathfrak{p}$. Observe that the extension

$$L(\psi_{s+1}(x)) \cdot K / K$$

is abelian and unramified at $\mathfrak{p}$. Hence the Artin symbol of $\mathfrak{p}$ in this extension is a well-defined element of its Galois group. We claim that

$$\langle \mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(b), \chi_a \rangle = \sum_{p|b} \psi_{s+1}(x)|_{G_K}(\mathrm{Frob}(\mathfrak{p})).$$

Indeed, $p_i(1)p_i(2)$ is a square modulo each odd prime divisor p of b for all $i \in [s+1]$. Hence the residue field of p in $L(\psi_{s+1}(x)) \cdot K$ coincides with the residue field of p in $L(\psi_{s+1}(x))$. This implies that

$$\psi_{s+1}(x)|_{G_K}(\mathrm{Frob}(\mathfrak{p})) = \psi_{s+1}(x)|_{G_{\mathbb{Q}(\sqrt{x})}}(\mathrm{Frob}(\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(p))).$$

Hence our claim follows from the definition of the Artin pairing. Therefore we conclude that

$$\sum_{x \in C} \langle \mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(b), \chi_a \rangle_{\mathrm{Art}_{s+1}(x)} = \sum_{p|b} \left(\psi'_{s+1}(x_0)(\mathrm{Frob}(\mathfrak{p})) + \sum_{\substack{x \in C \\ x \neq x_0}} \psi_{s+1}(x)(\mathrm{Frob}(\mathfrak{p})) \right).$$

Recalling that $\chi = \psi'_{s+1}(x_0) - \psi_{s+1}(x_0)$ and recalling the definition of $\psi_{s+1}(x_0)$ we conclude that

$$\sum_{x \in C} \langle \mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(b), \chi_a \rangle_{\mathrm{Art}_{s+1}(x)} = \sum_{p|b} \chi|_{G_K}(\mathrm{Frob}(\mathfrak{p})).$$

Hence it suffices to show that

$$\sum_{p|b} \chi|_{G_K}(\mathrm{Frob}(\mathfrak{p})) = 0.$$

To this end we will conduct a more careful study of the character χ. First of all observe that

$$i_2(L(\psi_{s+1}(x_0)) \cdot L(\psi'_{s+1}(x_0))) \subseteq \mathbb{Q}_2(\sqrt{5}, \sqrt{x_0}).$$

Therefore, since $\mathbb{Q}(\chi) \subseteq L(\psi_{s+1}(x_0)) \cdot L(\psi'_{s+1}(x_0))$, we conclude that at least one of χ and $\chi + \chi_{x_0}$ is unramified at (2). Let us pick one such character unramified at (2) and call this choice χ'. We now claim that

$$\chi' := \sum_{\substack{i\in[s+1] \\ h\in[2]}} \lambda_{i,h}\chi_{p_i(h)^*} + \sum_{\substack{l|d_0 \\ l\neq 2}} \lambda_l \chi_{l^*},$$

where the various $\lambda_{i,h}$ and λ_l are in $\mathbb{F}_2$ and n^* is the unique integer satisfying $|n^*| = n$ and $n^* \equiv 1 \mod 4$. Indeed, the character χ' is unramified at (2) and χ' certainly does not ramify at any odd prime not dividing $p_1(1)p_1(2)\ldots p_{s+1}(1)p_{s+1}(2) \cdot d_0$, since

$$\mathbb{Q}(\chi') \subseteq L(\psi_{s+1}(x_0)) \cdot L(\psi'_{s+1}(x_0)) \cdot \mathbb{Q}(\sqrt{x_0}).$$

This establishes the claim. Hence it suffices to prove that

$$\sum_{p|b} \chi_{x_0}|_{G_K}(\mathrm{Frob}(\mathfrak{p})) = 0$$

and

$$\sum_{p|b} \chi_{t^*}|_{G_K}(\mathrm{Frob}(\mathfrak{p})) = 0$$

for each odd prime t dividing $p_1(1)p_1(2)\ldots p_{s+1}(1)p_{s+1}(2) \cdot d_0$. The first equation is trivial, since χ_{x_0} is identically 0 when restricted to G_K. Let us show the second equation. Each p dividing b splits completely in $\mathbb{Q}(\sqrt{p_i(1)p_i(2)})$ for each $i \in [s+1]$. It follows that

$$\chi_{t^*}|_{G_K}(\mathrm{Frob}(\mathfrak{p})) = \chi_{t^*}|_{G_{\mathbb{Q}(\sqrt{x})}}(\mathrm{Frob}(\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(p))),$$

where x is any element of C with $t \mid x$. This yields

$$\sum_{p|b} \chi_{t^*}|_{G_K}(\mathrm{Frob}(\mathfrak{p})) = \langle \mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(b), \chi_{t^*}\rangle_1 = 0,$$

where the last equality follows from our assumption $\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(b) \in 2 \cdot \mathrm{Cl}(\mathbb{Q}(\sqrt{x}))$. $\qquad\square$

We now turn to the main result on governing triples. The proof is similar to the one given for Theorem 5.10, however there are a few technical differences. Below we report only the steps in the proof where the argument differs.

Theorem 5.11. *Let* $(C, (\psi_{s+1}(x))_{x\in C-\{x_0\}}, \chi_a)$ *be a governing triple. Then*

$$\chi_{p_{s+1}(1)\cdot a} \in 2^s \cdot \mathrm{Cl}(\mathbb{Q}(\sqrt{x_0}))^{\vee}[2^{s+1}].$$

Suppose that $b \mid d_0$ *is such that*

$$\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(b) \in 2^s \cdot \mathrm{Cl}(\mathbb{Q}(\sqrt{x}))[2^{s+1}]$$

for each $x \in C$. *Then every* $p \mid b$ *splits completely in* $M(\phi_{\{p_i(1)p_i(2):i\in[s]\};p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G}))/\mathbb{Q}$, *is unramified in* $L(\phi_{\{p_i(1)p_i(2):i\in[s]\};p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G}))/\mathbb{Q}$ *and*

$$\sum_{x\in C} \langle \mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(b), \chi_a\rangle_{\mathrm{Art}_{s+1}(x)} = \sum_{p|b} \phi_{\{p_i(1)p_i(2):i\in[s]\};p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G})(\mathrm{Frob}(p)).$$

Proof. We start by showing that $\chi_{p_{s+1}(1)\cdot a} \in 2^s \cdot \mathrm{Cl}(\mathbb{Q}(\sqrt{x_0}))^\vee[2^{s+1}]$. Consider the 1-cochain

$$\psi_{s+1}(x_0) := \phi_{\{p_i(1)p_i(2):i\in[s]\};p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G}) - \sum_{\substack{x\in C \\ x\neq x_0}} \psi_{s+1}(x).$$

We have

$$2^s \cdot \psi_{s+1}(x_0) = 2^s \cdot \phi_{\{p_i(1)p_i(2):i\in[s]\};p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G}) - \sum_{\substack{x\in C \\ x\neq x_0}} \chi_{\pi_{s+1}(x)\cdot a}$$

$$= 0 - \chi_{p_{s+1}(1)\cdot a} = \chi_{p_{s+1}(1)\cdot a},$$

since the 1-cochain $\phi_{\{p_i(1)p_i(2):i\in[s]\};p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G})$ is valued in $\mathbb{F}_2$ and $s \geq 1$. Let us next prove that $\psi_{s+1}(x_0): G_\mathbb{Q} \to N(x_0)[2^{s+1}]$ is in fact a 1-cocycle for $N(x_0)$. Thanks to Proposition 2.9 we have that

$$(d_{x_0}\psi_{s+1}(x_0))(\sigma,\tau) = \sum_{\substack{\varnothing\neq T\subseteq[s+1] \\ s+1\notin T}} \chi_{\{p_i(1)p_i(2):i\in T\}}(\sigma) \cdot$$

$$\left((-1)^{|T|+1+\chi_{x_0}(\sigma)} \left(\sum_{x\in C_T} \psi_{s-|T|+1}(x)(\tau) \right) - \phi_{\{p_i(1)p_i(2):i\in[s]\};p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G})(\tau) \right),$$

where we have used the third condition of Definition 5.9 to remove the terms with $s+1 \in T$. It follows from the second condition of Definition 5.9 that the above expression is identically zero.

Certainly, $\psi_s(x_0) := 2 \cdot \psi_{s+1}(x_0)$ is a 1-cocycle with values in $N(x_0)[2^s]$. We claim that $\psi_s(x_0)$ once restricted to $G_{\mathbb{Q}(\sqrt{x_0})}$ naturally lands in $\mathrm{Cl}(\mathbb{Q}(\sqrt{x_0}))^\vee[2^s]$ so that it yields a cyclic degree 2^s extension of $\mathbb{Q}(\sqrt{x_0})$ unramified at all finite places. Following the proof of Theorem 5.10, we obtain the claim for all places lying above (2), all odd primes dividing d_0 and all odd primes not dividing any $x \in C$.

It remains to treat the places lying above a prime of the form $p_j(h)$ with $j \in [s+1]$ and $h \in [2]$. Let us begin with the case $j \in [s]$ and $h = 2$. Then we can rewrite $\psi_s(x_0)$ as

$$-\sum_{x\in C_{p_j(2)}} \psi_s(x) - \sum_{x\in C_{p_j(1)}-\{x_0\}} \psi_s(x).$$

We now invoke the second condition of Definition 5.9, with $T := \{j\}$, and we get

$$\psi_s(x_0) = \phi_{\{p_i(1)p_i(2):i\in[s]-\{j\}\};p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G}) - \sum_{x\in C_{p_j(1)}-\{x_0\}} \psi_s(x).$$

By construction of the 1-cochain $\phi_{\{p_i(1)p_i(2):i\in[s]-\{j\}\};p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G})$ and by our assumption $j \in [s]$ we deduce that

$$\phi_{\{p_i(1)p_i(2):i\in[s]-\{j\}\};p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G})(\sigma_{p_j(2)}) = 0.$$

Now notice that

$$\sum_{x\in C_{p_j(1)}-\{x_0\}} \psi_s(x)(\sigma_{p_j(2)}) = 0,$$

since every individual field $L(\psi_s(x))/\mathbb{Q}$ is unramified above $p_j(2)$ for each $x \in C_{p_j(1)}$. This demonstrates that the homomorphism $(\psi_s(x_0), \chi_{x_0})$ maps $\sigma_{p_j(2)}$ to the identity and therefore $p_j(2)$ is unramified in the extension $L(\psi_s(x_0))/\mathbb{Q}$ by Proposition 2.3.

We now consider $j = s + 1$ and $h = 2$. We still rewrite $\psi_s(x_0)$ as

$$- \sum_{x \in C_{p_j(2)}} \psi_s(x) - \sum_{x \in C_{p_j(1)} - \{x_0\}} \psi_s(x),$$

but this time we invoke the third condition of Definition 5.9 with $T = \{s + 1\}$ to obtain that

$$\psi_s(x_0) = - \sum_{x \in C_{p_j(1)} - \{x_0\}} \psi_s(x).$$

The field of definition of $\psi_s(x_0)$ is contained in

$$\prod_{x \in C_{p_{s+1}(1)} - \{x_0\}} L(\psi_s(x)).$$

The prime $p_{s+1}(2)$ is unramified in the above field, since $p_{s+1}(2)$ is unramified in $\mathbb{Q}(\sqrt{x})/\mathbb{Q}$ for each $x \in C_{p_{s+1}(1)}$ and furthermore $L(\psi_s(x))\mathbb{Q}(\sqrt{x})/\mathbb{Q}(\sqrt{x})$ is unramified at all finite places.

We finally consider the primes of the form $p_j(1)$ for some $j \in [s + 1]$. We observe that

$$L(\psi_s(x_0)) \subseteq \prod_{x \in C - \{x_0\}} L(\psi_s(x))$$

and that $\sigma_{p_j(1)}$ has order at most 2 in $\mathrm{Gal}(L(\psi_s(x))/\mathbb{Q})$ for each x in $C - \{x_0\}$. Hence it has order at most 2 in $\mathrm{Gal}(L(\psi_s(x_0))/\mathbb{Q})$, which, by means of Proposition 2.3, implies that the ramification index of $p_j(1)$ in $L(\psi_s(x_0))\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}$ is exactly 2. But the prime $p_j(1)$ ramifies in the extension $\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}$ and therefore the place $\mathrm{Up}_{\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}}(p_j(1))$ is unramified in $L(\psi_s(x_0))\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}(\sqrt{x_0})$. We have now verified that $\psi_s(x_0)$ restricts to an unramified character of $G_{\mathbb{Q}(\sqrt{x_0})}$.

At this point we follow the argument in the proof of Theorem 5.10 to deduce that $\psi_s(x_0)$ is in $2 \cdot \mathrm{Cl}(\mathbb{Q}(\sqrt{x_0}))^\vee$. Indeed, all that we used in that proof was the existence of a lift (by multiplication of 2) of $\psi_s(x_0)$ in the space of cocycles from $G_\mathbb{Q}$ to $N(x_0)$, which, of course, is also available in this proof (namely $\psi_{s+1}(x_0)$). Let $\psi'_{s+1}(x_0)$ be a raw cocycle with $2 \cdot \psi'_{s+1}(x_0) = \psi_s(x_0)$. The examination of the quadratic character

$$\chi := \psi'_{s+1}(x_0) - \psi_{s+1}(x_0)$$

can be reproduced almost verbatim also in this argument with the only difference being that we invoke Proposition 2.15 to control the ramification coming from the 1-cochain

$$\phi_{\{p_i(1)p_i(2) : i \in [s]\}; p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G}).$$

We now justify the claim that each prime p dividing b splits completely in the extension

$$M(\phi_{\{p_i(1)p_i(2) : i \in [s]\}; p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G}))/\mathbb{Q}$$

and is unramified in the extension

$$L(\phi_{\{p_i(1)p_i(2) : i \in [s]\}; p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G}))/\mathbb{Q}.$$

This last conclusion is just Proposition 2.15. In order to show that p splits completely in $M(\phi_{\{p_i(1)p_i(2):i\in[s]\};p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G}))$, we invoke the second condition of Definition 5.9. Then we see that it suffices to show that

$$i_p(L(\psi_s(x))) \subseteq \mathbb{Q}_p(\sqrt{x_0}) \tag{5.5}$$

for each x in $C - \{x_0\}$. Indeed, this forces

$$i_p(M(\phi_{\{p_i(1)p_i(2):i\in[s]\};p_{s+1}(1)p_{s+1}(2)}(\mathfrak{G}))) \subseteq \mathbb{Q}_p^{\mathrm{unr}} \cap \mathbb{Q}_p(\sqrt{x_0}) = \mathbb{Q}_p$$

as we want. But equation (5.5) follows from Lemma 4.5. From here onwards, the rest of the proof is identical to the proof of Theorem 5.10. $\qquad\square$

6 Combinatorial results

In this section we recall for the reader's convenience the main combinatorial results from Smith's work [42, Section 3-4].

6.1 Additive systems

One of the key tools in Smith's work is the notion of an additive system. It provides a convenient abstract framework for our algebraic results.

Definition 6.1. *Let $X_1, \ldots, X_r$ be non-empty finite sets, let $X = X_1 \times \cdots \times X_r$ and let $S \subseteq [r]$. An additive system on (X, S) is a tuple $(C_T, C_T^{\mathrm{acc}}, F_T, A_T)_{T \subseteq S}$, indexed by the subsets $T \subseteq S$, satisfying the following properties*

- *we have $C_T \subseteq C_T^{\mathrm{acc}} \subseteq \mathrm{Cube}(X, T)$, $F_T : C_T \to A_T$ is a function and A_T is a finite $\mathbb{F}_2$-vector space;*

- *we have*
$$C_T^{\mathrm{acc}} = \{\bar{x} \in C_T : F_T(\bar{x}) = 0\}$$
and furthermore
$$C_T = \{\bar{x} \in \mathrm{Cube}(X, T) : \bar{x}(T - \{i\}) \subseteq C_{T-\{i\}}^{\mathrm{acc}} \text{ for all } i \in T\}$$
for all $\varnothing \neq T \subseteq S$;

- *suppose that $\bar{x}_1, \bar{x}_2, \bar{x}_3 \in C_T$ and suppose that there exists $i \in T$ and $p_1, p_2, p_3 \in X_i$ such that*
$$\pi_{[r]-\{i\}}(\bar{x}_1) = \pi_{[r]-\{i\}}(\bar{x}_2) = \pi_{[r]-\{i\}}(\bar{x}_3)$$
and
$$\pi_i(\bar{x}_1) = (p_1, p_2), \pi_i(\bar{x}_2) = (p_2, p_3), \pi_i(\bar{x}_3) = (p_1, p_3).$$
Then we have
$$F_T(\bar{x}_1) + F_T(\bar{x}_2) = F_T(\bar{x}_3). \tag{6.1}$$

The most important feature of additive systems is that we have good control over the density of C_S^{acc}.

Proposition 6.2. *Take non-empty finite sets $X_1, \ldots, X_r$, take $X = X_1 \times \cdots \times X_r$ and take a subset $S \subseteq [r]$. Let $(C_T, C_T^{\mathrm{acc}}, F_T, A_T)_{T \subseteq S}$ be an additive system on (X, S) such that $|A_T| \leq a$ for all $T \subseteq S$, and write δ for the density of $C_\varnothing^{\mathrm{acc}}$ in X. Then we have*

$$\frac{|C_S^{\mathrm{acc}}|}{|\mathrm{Cube}(X, S)|} \geq \delta^{2^{|S|}} \cdot a^{-3^{|S|}}.$$

Proof. This is first proven in [42, Proposition 3.2] and reproven in [30, Proposition 2.2]. $\square$

6.2 Ramsey theory

The following result allows us to find structured subsets of any $Y \subseteq X$ provided that Y has sufficiently large density in X.

Lemma 6.3. *Take non-empty finite sets $X_1, \ldots, X_r$ and take $X = X_1 \times \cdots \times X_r$. Suppose that Y is a subset of X of cardinality at least $\delta \cdot |X|$. We further assume that $2^{-r-1} > \delta > 0$ and we let $b \geq 1$ be an integer satisfying*

$$b \leq \left(\frac{\log \min_{i \in [r]} |X_i|}{5 \log \delta^{-1}} \right)^{1/(r-1)}.$$

Then there exist subsets $Z_i \subseteq X_i$ with $|Z_i| = b$ for all $i \in [r]$ such that

$$Z_1 \times \cdots \times Z_r \subseteq Y.$$

Proof. This is [42, Lemma 4.1], where their d is our r and their r is our b. $\square$

Remark 6.4. *As Smith [42, p. 6] already remarks, this lemma is sharp up to a change of constant. Indeed, take a random subset Y of $[2^N]^r$. Then the probability that Y contains a given product set $Z_1 \times \cdots \times Z_r$, where $|Z_i| = b$ for each $i \in [r]$, equals $(1/2)^{b^r}$. There are at most 2^{Nrb} such sets $Z_1 \times \cdots \times Z_r$. Hence we see that, as soon as $b > (rN)^{1/(r-1)}$, a random subset Y of $[2^N]^r$ fails the conclusion of the lemma with positive probability.*

We now state Smith's main combinatorial result. It provides the crucial connection between our equidistribution results based on the Chebotarev density theorem and the reflection principles. Let $X = X_1 \times \cdots \times X_r$ and let $S \subseteq [r]$. Define

$$V = \mathrm{Map}(X, \mathbb{F}_2), \quad W = \mathrm{Map}(\mathrm{Cube}(X, S), \mathbb{F}_2).$$

We say that $\bar{x} \in \mathrm{Cube}(X, S)$ is degenerate if there exists $i \in S$ with

$$\mathrm{pr}_1(\pi_i(\bar{x})) = \mathrm{pr}_2(\pi_i(\bar{x})).$$

We define $\Sigma : V \to W$ to be the linear map given by

$$\Sigma F(\bar{x}) = \begin{cases} \sum_{x \in \bar{x}(\varnothing)} F(x) & \text{if } \bar{x} \text{ is not degenerate} \\ 0 & \text{if } \bar{x} \text{ is degenerate.} \end{cases}$$

We denote the image of Σ by $\mathrm{Add}(X, S)$. More generally, we define for a subset $Y \subseteq X$ a map from $\mathrm{Map}(Y, \mathbb{F}_2)$ to $\mathrm{Map}(\mathrm{Cube}(X, S), \mathbb{F}_2)$ by

$$\Sigma F(\bar{x}) = \begin{cases} \sum_{x \in \bar{x}(\varnothing)} F(x) & \text{if } \bar{x} \text{ is not degenerate and } \bar{x}(\varnothing) \subseteq Y \\ 0 & \text{if } \bar{x} \text{ is degenerate.} \end{cases}$$

By abuse of notation, we will also denote this map by Σ.

Lemma 6.5. *Let $X_1, \ldots, X_r$ be finite, non-empty sets, let $X = X_1 \times \cdots \times X_r$ and let $S \subseteq [r]$. Then*

$$\dim_{\mathbb{F}_2} \mathrm{Add}(X, S) = \prod_{i \in S}(|X_i| - 1) \cdot \prod_{i \in [r] - S} |X_i|.$$

Proof. This follows from [27, Proposition 9.3] by taking $l = 2$. $\square$

Given an additive system $\mathfrak{A} = (C_T, C_T^{\mathrm{acc}}, F_T, A_T)_{T \subseteq S}$ on (X, S), we set

$$C(\mathfrak{A}) := \bigcap_{i \in S} \left\{ \bar{x} \in \mathrm{Cube}(X, S) : \bar{x}(S - \{i\}) \cap C_{S-\{i\}}^{\mathrm{acc}} \neq \varnothing \right\}.$$

We say that $\mathfrak{A}$ is (a, S)-acceptable if $|A_T| \leq a$ for all $T \subseteq S$ and $\bar{x} \in C(\mathfrak{A})$ implies $\bar{x}(\varnothing) \subseteq C_\varnothing^{\mathrm{acc}}$.

Proposition 6.6. *There exists an absolute constant $A > 0$ such that the following holds. Take non-empty finite sets $X_1, \ldots, X_r$, take $X = X_1 \times \cdots \times X_r$ and take $S \subseteq [r]$. Let $a \geq 2$ and $\epsilon > 0$ be such that $\epsilon < a^{-1}$ and*

$$\log \min_{i \in S} |X_i| \geq A \cdot 6^r \cdot \log \epsilon^{-1}.$$

Then there exists $g \in \mathrm{Add}(X, S)$ such that for all (a, S)-acceptable additive systems

$$\mathfrak{A} = (C_T, C_T^{\mathrm{acc}}, F_T, A_T)_{T \subseteq S}$$

on (X, S) and for all $F : C_\varnothing^{\mathrm{acc}} \to \mathbb{F}_2$ satisfying $\Sigma F(\bar{x}) = g(\bar{x})$ for all $\bar{x} \in C(\mathfrak{A})$, we have

$$\frac{|C_\varnothing^{\mathrm{acc}}|}{2} - \epsilon \cdot |X| \leq |F^{-1}(0)| \leq \frac{|C_\varnothing^{\mathrm{acc}}|}{2} + \epsilon \cdot |X|.$$

Proof. This is [42, Proposition 4.4]. $\square$

6.3 Galois groups

In this subsection we describe the structure of some important Galois groups that we shall encounter later. To do so, we will introduce some notation. If $X_1, \ldots, X_r$ are non-empty, finite sets of odd prime numbers, we write $K(X_1 \times \cdots \times X_r)$ for the compositum of $\mathbb{Q}(\sqrt{p})$ with p lying in some X_j. If $\bar{x} \in \mathrm{Cube}(X, S)$ and $d \neq 1$ is an integer coprime to all elements of X, then we say that the expansion map

$$\phi_{\bar{x};d}$$

exists if $\bar{x}$ is degenerate or if the expansion map

$$\phi_{\{\mathrm{pr}_1(\pi_i(\bar{x})) \cdot \mathrm{pr}_2(\pi_i(\bar{x})): i \in S\};d}(\mathfrak{G})$$

exists. In case $\bar{x}$ is degenerate, we define the field of definition of $\phi_{\bar{x};d}$ to be $\mathbb{Q}$. The coming results are very similar to [42, Proposition 2.4].

Lemma 6.7. *Let $r \in \mathbb{Z}_{\geq 1}$. Take non-empty, disjoint, finite sets of odd prime numbers $X_1, \ldots, X_r$ with product X. Let $i \in [r]$ and suppose that the map $\phi_{\pi_{[r]-\{i\}}(\bar{x});\mathrm{pr}_1(\pi_i(\bar{x}))\mathrm{pr}_2(\pi_i(\bar{x}))}$ exists for all $\bar{x} \in \mathrm{Cube}(X, [r])$. For $S \subseteq [r] - \{i\}$ write*

$$M_S := K(X) \prod_{\bar{x} \in \mathrm{Cube}(X, S \cup \{i\})} L(\phi_{\pi_S(\bar{x});\mathrm{pr}_1(\pi_i(\bar{x}))\mathrm{pr}_2(\pi_i(\bar{x}))}).$$

Then we have

$$\log_2 \left[\prod_{\substack{S \subseteq [r]-\{i\} \\ |S|=j+1}} M_S : \prod_{\substack{S' \subseteq [r]-\{i\} \\ |S'|=j}} M_{S'} \right] = \sum_{\substack{S \subseteq [r]-\{i\} \\ |S|=j+1}} \prod_{k \in S \cup \{i\}} (|X_k| - 1).$$

for all integers $0 \leq j \leq r - 2$.

Proof. Write

$$M_j := \prod_{\substack{S' \subseteq [r]-\{i\} \\ |S'|=j}} M_{S'}.$$

Let $S \subseteq [r] - \{i\}$ with $|S| = j + 1$. Note that

$$\phi_{\pi_S(\bar{x});\mathrm{pr}_1(\pi_i(\bar{x}))\mathrm{pr}_2(\pi_i(\bar{x}))}$$

is a quadratic character when restricted to M_j and gives a central $\mathbb{F}_2$-extension of $\mathrm{Gal}(M_j/\mathbb{Q})$ by Proposition 2.14. Enumerate X_k as $\{p_{k,1}, \ldots, p_{k,|X_k|}\}$ and define

$$T_{k,l} = \{p_{k,l}, p_{k,l+1}\}$$

for $l \in [|X_k| - 1]$. For $T \subseteq [r] - \{i\}$, let $\mathrm{Basis}(X, T)$ be the set of $\bar{x} \in \mathrm{Cube}(X, T \cup \{i\})$ such that for every $k \in T \cup \{i\}$ there is some l satisfying

$$\{\mathrm{pr}_1(\pi_k(\bar{x})), \mathrm{pr}_2(\pi_k(\bar{x}))\} = T_{k,l}.$$

It follows from Proposition 2.14 that

$$\bigcup_{\substack{S \subseteq [r]-\{i\} \\ |S|=j+1}} \bigcup_{\bar{x} \in \mathrm{Basis}(X,S)} \{\phi_{\pi_S(\bar{x});\mathrm{pr}_1(\pi_i(\bar{x}))\mathrm{pr}_2(\pi_i(\bar{x}))}\}$$

generates the dual of $\mathrm{Gal}(M_{j+1}/M_j)$. We claim that the above characters are also linearly independent, which clearly implies the lemma. Here we caution the reader that two distinct elements $\bar{x}_1, \bar{x}_2 \in \mathrm{Basis}(X, S)$ can give rise to the same character. This happens precisely when

$$\{\mathrm{pr}_1(\pi_k(\bar{x}_1)), \mathrm{pr}_2(\pi_k(\bar{x}_1))\} = \{\mathrm{pr}_1(\pi_k(\bar{x}_2)), \mathrm{pr}_2(\pi_k(\bar{x}_2))\}$$

for all $k \in S \cup \{i\}$. This defines an equivalence relation on $\mathrm{Basis}(X, S)$, which we denote by $\sim$. To prove the claim, let $c_{\bar{x}} \in \mathbb{F}_2$ be such that

$$\sum_{\substack{S \subseteq [r]-\{i\} \\ |S|=j+1}} \sum_{\bar{x} \in \mathrm{Basis}(X,S)/\sim} c_{\bar{x}} \cdot \phi_{\pi_S(\bar{x});\mathrm{pr}_1(\pi_i(\bar{x}))\mathrm{pr}_2(\pi_i(\bar{x}))}(\sigma) = 0 \tag{6.2}$$

for all $\sigma \in G_{M_j}$. We define the operator β_j by

$$\beta_j \phi = \phi([\sigma_1, [\sigma_2, [\ldots [\sigma_{j+1}, \sigma_{j+2}]]]])$$

for $\phi \in \mathrm{Map}(G_{M_j}, \mathbb{F}_2)$ and $\sigma_1, \ldots, \sigma_{j+2} \in G_{\mathbb{Q}}$. This is well-defined, since the nilpotency degree of $\mathrm{Gal}(M_j/\mathbb{Q})$ is $j+1$. Writing ϕ for $\phi_{\pi_S(\bar{x}); \mathrm{pr}_1(\pi_i(\bar{x})) \mathrm{pr}_2(\pi_i(\bar{x}))}$, we compute

$$
\begin{aligned}
\phi([\sigma, \tau]) &= \phi(\sigma\tau) + \phi(\tau\sigma) + d\phi([\sigma, \tau], \tau\sigma) \\
&= \phi(\sigma\tau) + \phi(\tau\sigma) \\
&= d\phi(\sigma, \tau) + d\phi(\tau, \sigma),
\end{aligned}
$$

where the second equality uses equation (2.3) and the fact that quadratic characters vanish on commutators. Utilizing equation (2.3) again and inducting on j yields

$$\beta_j \phi_{\pi_S(\bar{x}); \mathrm{pr}_1(\pi_i(\bar{x})) \mathrm{pr}_2(\pi_i(\bar{x}))} = \sum_{\substack{f:[j+2] \to S \cup \{i\} \\ f \text{ is a bijection} \\ f(j+1)=i \text{ or } f(j+2)=i}} \prod_{1 \le k \le j+2} \chi_{\mathrm{pr}_1(\pi_{f(k)}(\bar{x})) \mathrm{pr}_2(\pi_{f(k)}(\bar{x}))}(\sigma_k),$$

where we again use that $d\phi(\tau, \sigma) = 0$ if τ is a commutator. Hence β_j induces a homomorphism from $\mathrm{Gal}(M_{j+1}/M_j)^\vee$ to the set of bilinear maps from $\mathrm{Gal}(K(X)/\mathbb{Q})^{j+2}$ to $\mathbb{F}_2$. Observe that the bilinear maps

$$\left\{ (\sigma_1, \ldots, \sigma_{j+2}) \mapsto \prod_{1 \le m \le j+2} \chi_{p_{k_m, l_m} \cdot p_{k_m, l_m+1}}(\sigma_m) \right\}_{k_1 \in [r], \ldots, k_{j+2} \in [r], l_1 \in [|X_{k_1}|-1], \ldots, l_{j+2} \in [|X_{k_{j+2}}|-1]}$$

are linearly independent. Therefore, applying β_j to equation (6.2), we see that $c_{\bar{x}} = 0$, which completes the proof. □

Lemma 6.8. *Let $r \in \mathbb{Z}_{\ge 1}$ be given. Let $X_1, \ldots, X_r$ be non-empty, disjoint, finite sets of odd prime numbers, let X be their product and let $i \in [r]$. Assume that the map*

$$\phi_{\pi_{[r]-\{i\}}(\bar{x}); \mathrm{pr}_1(\pi_i(\bar{x})) \mathrm{pr}_2(\pi_i(\bar{x}))}$$

exists for all $\bar{x} \in \mathrm{Cube}(X, [r])$. Write

$$M_\circ(X) := K(X) \prod_{S \subset [r]-\{i\}} \prod_{\bar{x} \in \mathrm{Cube}(X, S \cup \{i\})} L(\phi_{\pi_S(\bar{x}); \mathrm{pr}_1(\pi_i(\bar{x})) \mathrm{pr}_2(\pi_i(\bar{x}))})$$

Then we have

$$[M_\circ(X) : K(X)] = \prod_{\varnothing \subset S \subset [r]-\{i\}} 2^{\prod_{j \in S \cup \{i\}}(|X_j|-1)}. \tag{6.3}$$

Also let $Y_1, \ldots, Y_r$ be non-empty, disjoint, finite sets of odd prime numbers and let Y be their product. Assume that the map $\phi_{\pi_{[r]-\{i\}}(\bar{x}); \mathrm{pr}_1(\pi_i(\bar{x})) \mathrm{pr}_2(\pi_i(\bar{x}))}$ exists for all $\bar{x} \in \mathrm{Cube}(Y, [r])$. Suppose that $|X_j \cap Y_j| = 1$ for all $j \in [r]$ and $X_j \cap Y_k = \varnothing$ for distinct j and k. Then we have

$$M_\circ(X) \cap M_\circ(Y) = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r}),$$

where p_j is the unique element of $X_j \cap Y_j$.

Proof. Equation (6.3) follows immediately from Lemma 6.7. For the second part, $\supseteq$ is obvious, so it remains to prove $\subseteq$. But the arguments from Lemma 6.7 imply that $M_\circ(X)/K(X)K(Y)$ and $M_\circ(Y)/K(X)K(Y)$ are disjoint extensions. Then $M_\circ(X) \cap M_\circ(Y)$ is a subfield of $K(X)K(Y)$ only ramified at 2 and $p_1, \ldots, p_r$. This readily implies $\subseteq$. $\qquad\square$

Lemma 6.9. *Take an integer $r \in \mathbb{Z}_{\geq 2}$. Let $X_1, \ldots, X_r$ be non-empty, disjoint, finite sets of odd prime numbers, let X be their product and let $i \in [r]$. Suppose that the map*

$$\phi_{\pi_{[r]-\{i\}}(\bar{x}); \mathrm{pr}_1(\pi_i(\bar{x}))\mathrm{pr}_2(\pi_i(\bar{x}))}$$

exists for all $\bar{x} \in \mathrm{Cube}(X, [r])$. Write

$$M_\circ := K(X) \prod_{S \subset [r]-\{i\}} \prod_{\bar{x} \in \mathrm{Cube}(X, S \cup \{i\})} L(\phi_{\pi_S(\bar{x}); \mathrm{pr}_1(\pi_i(\bar{x}))\mathrm{pr}_2(\pi_i(\bar{x}))})$$

and

$$M := K(X) \prod_{\bar{x} \in \mathrm{Cube}(X, [r])} L(\phi_{\pi_{[r]-\{i\}}(\bar{x}); \mathrm{pr}_1(\pi_i(\bar{x}))\mathrm{pr}_2(\pi_i(\bar{x}))}).$$

Then the map f, that sends $\sigma \in \mathrm{Gal}(M/M_\circ)$ to the function g_σ in $\mathrm{Add}(X, [r])$ given by

$$\bar{x} \mapsto \phi_{\pi_{[r]-\{i\}}(\bar{x}); \mathrm{pr}_1(\pi_i(\bar{x}))\mathrm{pr}_2(\pi_i(\bar{x}))}(\sigma),$$

is a group isomorphism.

Proof. First of all, we have to check that f is well-defined, that is $g_\sigma \in \mathrm{Add}(X, [r])$. This follows from Proposition 2.14. Next recall that

$$\phi_{\pi_{[r]-\{i\}}(\bar{x}); \mathrm{pr}_1(\pi_i(\bar{x}))\mathrm{pr}_2(\pi_i(\bar{x}))}$$

is a quadratic character when restricted to $G_{M_\circ}$. Since σ fixes $M_\circ$, it follows that f is a group homomorphism.

Furthermore, $\phi_{\pi_{[r]-\{i\}}(\bar{x}); \mathrm{pr}_1(\pi_i(\bar{x}))\mathrm{pr}_2(\pi_i(\bar{x}))}$ gives a central $\mathbb{F}_2$-extension of $\mathrm{Gal}(M_\circ/\mathbb{Q})$ by Proposition 2.14, and hence the restrictions of the $\phi_{\pi_{[r]-\{i\}}(\bar{x}); \mathrm{pr}_1(\pi_i(\bar{x}))\mathrm{pr}_2(\pi_i(\bar{x}))}$ to $G_{M_\circ}$ together generate the dual of $\mathrm{Gal}(M/M_\circ)$. This shows that f is injective. Since $r \geq 2$, we deduce from Lemma 6.7 that

$$|\mathrm{Gal}(M/M_\circ)| = 2^{\prod_{j \in [r]}(|X_j|-1)}.$$

Therefore our lemma follows from Lemma 6.5. $\qquad\square$

Finally, we will need a version of the above lemmata in case the pointer is an arbitrary fixed squarefree integer $d \neq 1$.

Lemma 6.10. *Let $r \in \mathbb{Z}_{\geq 1}$ be given. Let $X_1, \ldots, X_r$ be non-empty, disjoint, finite sets of odd prime numbers and write $X = X_1 \times \cdots \times X_r$. Also suppose that $d \neq 1$ is a squarefree integer coprime with all the primes in X. Suppose that the map*

$$\phi_{\bar{x}; d}$$

exists for all $\bar{x} \in \mathrm{Cube}(X, [r])$. Write

$$M_\circ(X) := \prod_{i \in [r]} \prod_{\bar{x} \in \mathrm{Cube}(X, [r])} L(\phi_{\pi_{[r]-\{i\}}(\bar{x}); \mathrm{pr}_1(\pi_i(\bar{x}))\mathrm{pr}_2(\pi_i(\bar{x}))}) \times \prod_{T \subset [r]} \prod_{\bar{x} \in \mathrm{Cube}(X, T)} L(\phi_{\bar{x}; d})$$

and

$$M(X) := M_\circ(X) \prod_{\bar{x} \in \mathrm{Cube}(X,[r])} L(\phi_{\bar{x};d}).$$

Then we have

$$[M(X) : M_\circ(X)] = 2^{\prod_{j \in [r]}(|X_j|-1)}$$

and

$$[M_\circ(X) : K(X)] = \prod_{\varnothing \subset S \subset [r]} 2^{\prod_{j \in S}(|X_j|-1)} \cdot \prod_{\substack{(i,S) \\ \{i\} \subset S \subseteq [r] \\ i \neq \max(S)}} 2^{\prod_{j \in S}(|X_j|-1)}.$$

Furthermore, the map f, that sends $\sigma \in \mathrm{Gal}(M(X)/M_\circ(X))$ to $g_\sigma \in \mathrm{Add}(X,[r])$ given by

$$\bar{x} \mapsto \phi_{\bar{x};d}(\sigma),$$

is a group isomorphism between $\mathrm{Gal}(M(X)/M_\circ(X))$ and $\mathrm{Add}(X,[r])$. Finally, let $Y_1, \ldots, Y_r$ satisfy the same conditions as $X_1, \ldots, X_r$ and write Y for their product. We also assume that $|X_j \cap Y_j| = 1$ for all $j \in [r]$ and $X_j \cap Y_k = \varnothing$ for distinct j and k. Then

$$M_\circ(X) \cap M_\circ(Y) = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r}, \sqrt{d}),$$

where p_j is the unique element of $X_j \cap Y_j$.

Proof. The proof proceeds among the same lines as for the other lemmata presented in this subsection. The condition $i \neq \max(S)$ is imposed because we have the relation

$$\sum_{i \in S} \phi_{\pi_{S-\{i\}}(\bar{x}); \mathrm{pr}_1(\pi_i(\bar{x}))\mathrm{pr}_2(\pi_i(\bar{x}))} = \chi_{\{\mathrm{pr}_1(\pi_j(\bar{x}))\mathrm{pr}_2(\pi_j(\bar{x})) : j \in S\}}$$

for all $|S| \geq 1$. Using the operator $\beta_{|S|-2}$ one sees that there are no further relations, since for every $\varnothing \subsetneq T \subsetneq S$, there exists a bijection $f : [|S|] \to S$ such that

$$|\{i \in T : f(|S|-1) = i \text{ or } f(|S|) = i\}|$$

is odd. $\qquad\square$

7 Equidistribution of the first Artin pairing

In this section we will recall and reprove some important results from [8, Section 4-5], which are directly based on [42, Section 5-6] of Smith's work. Although most of the material in this section is rather similar to [8, Section 4-5] and [42, Section 5-6], we have simplified some of the proofs.

The main theorem of this section is Theorem 7.13, which improves on earlier work of Fouvry and Klüners [18]. In [18, Corollary 2] one finds the limiting distribution[5] of the 4-rank of special discriminants. Here we give an error term and prove that the implied constant is effectively computable. It is worth mentioning that the work in [8, Theorem 5.15] also

---

[5]We remark that Fouvry and Klüners proceed by computing the moments of the 4-rank, while we do not. In particular there is no direct analogue of their [18, Theorem 3] in our work.

provides an error term, but there it was not shown that the implied constant is effectively computable.

From now on $X_1, \ldots, X_r$ denote disjoint, non-empty sets of prime numbers (always equal to 1 or 2 modulo 4) and we let $X = X_1 \times \cdots \times X_r$ be the corresponding product space. There is an injection from X to $\mathcal{D}$ by sending $x = (x_1, \ldots, x_r) \in X$ to $x_1 \cdot \ldots \cdot x_r$. We shall often implicitly think of elements of X as squarefree integers in this way.

7.1 Prime divisors

Let us first consider some desirable properties of elements in $\mathcal{D}$.

Definition 7.1. *Let $N \geq 10^{1000}$ and let $d \in \mathcal{D}$. Write $p_1, \ldots, p_r$ for the prime divisors of d ordered such that*

$$p_1 < \cdots < p_r.$$

Put

$$D_1 := e^{(\log \log N)^{1/10}}, \quad C_0 := \sqrt{\log \log \log N}.$$

We say that $d \in \mathcal{D}$ is N-nice if the following three properties are all satisfied

- *$p_i > D_1$ implies $2p_i < p_{i+1}$;*

- *we have*

$$\left| \frac{1}{2} \log \log p_i - i \right| < C_0^{1/5} \max(i, C_0)^{4/5} \text{ for all } 1 \leq i < \frac{r}{3}; \tag{7.1}$$

- *there exists some i satisfying $\frac{r^{1/2}}{2} < i < \frac{r}{2}$ and*

$$\log p_i \geq (\log \log p_i)^2 \cdot \log \log \log N \cdot \sum_{j=1}^{i-1} \log p_j.$$

Define $\mathcal{D}_r(N)$ to be the subset of $d \in \mathcal{D}(N)$ with $\omega(d) = r$, where $\omega(d)$ equals the number of distinct prime divisors of d.

Theorem 7.2. *We have*

$$\bigcup_{|r - \frac{1}{2} \log \log N| \geq (\log \log N)^{2/3}} |\mathcal{D}_r(N)| \ll \frac{|\mathcal{D}(N)|}{(\log \log N)^{1/100}}. \tag{7.2}$$

Furthermore, for all $A > 0$, there exist $C_1, C_2, N_0 > 0$ such that for all $r \leq A \log \log N$ and all $N \geq N_0$

$$\frac{C_1 N}{\log N} \cdot \frac{(\frac{1}{2} \log \log N)^{r-1}}{(r-1)!} \leq |\mathcal{D}_r(N)| \leq \frac{C_2 N}{\log N} \cdot \frac{(\frac{1}{2} \log \log N)^{r-1}}{(r-1)!}. \tag{7.3}$$

Now suppose that r satisfies

$$\left| r - \frac{1}{2} \log \log N \right| < (\log \log N)^{2/3}. \tag{7.4}$$

Then we also have

$$\frac{|\{d \in \mathcal{D}_r(N) : d \text{ is not } N\text{-nice}\}|}{|\mathcal{D}_r(N)|} \ll \frac{1}{e^{(\log \log \log N)^{1/4}}}.$$

Proof. Equation (7.2) follows from the Erdős–Kac theorem, while equation (7.3) can be found on [8, p. 13]. The second part is [8, Theorem 4.1], which is based on [42, Theorem 5.4]. $\square$

7.2 Preboxes and Legendre symbols

We will now introduce the notion of preboxes. Their usefulness lies in the simplicity of their definition, which makes preboxes suitable for inductive arguments. Later on we shall define the similar, but more stringent, notion of boxes, which will be the objects we naturally encounter in our final section.

Definition 7.3. *A prebox is a pair (X, P), where $P, X_1, \ldots, X_r$ are disjoint sets of primes all 1 or 2 modulo 4 and $X = X_1 \times \cdots \times X_r$. We assume that there exist real numbers*

$$2 < s_1 < t_1 < \cdots < s_r < t_r$$

such that $X_i \subseteq (s_i, t_i]$ for all $i \in [r]$ and $P \subseteq (1, s_1]$.

Recall that the first Artin pairing of $d \in \mathcal{D}$ is determined by the quadratic behavior between the prime divisors of d. This prompts the following definition. Write ι for the unique group isomorphism from $\mathbb{F}_2$ to $\{\pm 1\}$.

Definition 7.4. *Let (X, P) be a prebox. Define*

$$M_r = \{(i, j) : i, j \in [r], i < j\}, \quad M_{r,P} := [r] \times P.$$

Let $\mathcal{M}_r \subseteq M_r$ and $\mathcal{M}_{r,P} \subseteq M_{r,P}$ and let $a : \mathcal{M}_r \sqcup \mathcal{M}_{r,P} \to \mathbb{F}_2$, where $\sqcup$ denotes disjoint union. Then we define $X(a)$ to be the subset of $(x_1, \ldots, x_r) \in X$ satisfying

$$\left(\frac{x_i}{x_j} \right) = \iota(a(i, j)) \text{ for all } (i, j) \in \mathcal{M}_r \text{ and } \left(\frac{x_i}{p} \right) = \iota(a(i, p)) \text{ for all } (i, p) \in \mathcal{M}_{r,P}.$$

Our aim is to prove an equidistribution statement for $X(a)$ for certain desirable preboxes. One undesirable property is the presence of a Siegel zero, which we define now.

Definition 7.5. *For a real number $0.5 > c > 0$, we define $\mathcal{S}(c)$ to be the (conjecturally empty) set of squarefree integers d such that $L(s, \chi_d)$ has a real zero in the region*

$$1 - \frac{c}{\log(|d| + 4)} \leq s \leq 1.$$

List the elements of $\mathcal{S}(c)$ as $d_1, d_2, \ldots$ in such a way that $|d_1| \leq |d_2| \leq \ldots$. By Landau's theorem, there exists a sufficiently small $c_{\text{Landau}} > 0$ such that $|d_i|^2 \leq |d_{i+1}|$. We fix such a c_{Landau} for the remainder of the paper.

Let (X, P) be a prebox. We say that (X, P) is Siegel-free above a real number $t > 0$ if there does not exist some $|d_i| > t$ and some $x \in X$ such that d_i divides $x \prod_{p \in P} p$.

Our next proposition is the first of a series of two on equidistribution of Legendre symbols. In our first result we shall avoid some delicate issues with small primes by making extra assumptions on the map $a : \mathcal{M}_r \sqcup \mathcal{M}_{r,P} \to \mathbb{F}_2$ and the X_i, see equation (7.5). Later we shall see how to deal with the small primes. The next proposition is directly based on [42, Proposition 6.3]. Watkins [46] observed that A can be effectively computed by using an effective lower bound for Siegel zeroes.

Proposition 7.6. *Let $c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8 > 0$ be real numbers such that*

$$c_3 > 1, \quad c_5 > 3, \quad c_6 > 1, \quad \frac{1}{8} > c_8 + \frac{c_7 \log 2}{2} + \frac{1}{c_1} + \frac{c_2 c_4}{2}.$$

There exists an effectively computable constant $A > 0$, depending only on the real numbers $c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8$, such that the following holds.

Let (X, P) be a prebox with $s_1 > A$. Assume that (X, P) is Siegel-free above some real number t satisfying $s_1 > t > A$. Take subsets $\mathcal{M}_r \subseteq M_r$ and $\mathcal{M}_{r,P} \subseteq M_{r,P}$ and take $a : \mathcal{M}_r \sqcup \mathcal{M}_{r,P} \to \mathbb{F}_2$. Suppose that $1 \le k \le r$ is an integer such that $(i, p) \in \mathcal{M}_{r,P}$ implies $i > k$. Furthermore, we assume that

$$X_i = \left\{ p \in (s_i, t_i] : p \equiv 1 \bmod 4 \text{ and } \left(\frac{p}{p'} \right) = \iota(a(i, p')) \text{ for all } (i, p') \in \mathcal{M}_{r,P} \right\} \tag{7.5}$$

for all $i > k$. Moreover, we assume that

(i) $|P| \le \log t_i - i$ for all $i \in [r]$;

(ii) $t_1 > r^{c_1}$ and $t_k < e^{t_1^{c_2}}$;

(iii) we have

$$|X_i| \ge \frac{2^{c_3 i} \cdot t_i}{(\log t_i)^{c_4}}$$

for all $i \in [r]$;

(iv) if $k \ne r$, we assume that

$$t_{k+1} > \max \left(e^{(\log t_1)^{c_5}}, e^{t^{c_6}} \right);$$

(v) we assume that $k \le \lceil c_7 \log t_1 \rceil$. Furthermore, we assume that for all $i \le r$ and all $i + c_7 \log t_i \le j \le r$ that

$$t_j > e^{(\log t_i)^{c_5}}.$$

Then we have

$$\left| |X(a)| - \frac{|X|}{2^{|\mathcal{M}_r|}} \right| \le \frac{r|X|}{t_1^{c_8 + 1/c_1} \cdot 2^{|\mathcal{M}_r|}} \le \frac{|X|}{t_1^{c_8} \cdot 2^{|\mathcal{M}_r|}}.$$

Proof. The last inequality follows immediately from our assumption (ii). We will prove the first inequality by induction on r. For $r = 1$ we have $k = 1$ and $\mathcal{M}_r = M_r = \mathcal{M}_{r,P} = M_{r,P} = \varnothing$. We conclude that $X(a) = X$, so the inequality holds. Now suppose that $r > 1$.

Let $x_1 \in X_1$ and let $2 \le i \le r$ be an integer. We define

$$X_i(a, x_1) := \left\{ p \in X_i : \left(\frac{x_1}{p} \right) = \iota(a(1, i)) \right\}$$

if $(1, i) \in \mathcal{M}_r$. It will be convenient to set $X_i(a, x_1) := X_i$ in case $(1, i) \notin \mathcal{M}_r$. We claim that

$$\left| |X_i(a, x_1)| - \frac{1}{2} |X_i| \right| \le \frac{|X_i|}{t_1} \tag{7.6}$$

for all $i > k$ with $(1, i) \in \mathcal{M}_r$, provided that we pick A sufficiently large. Define

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

Let $\chi : \mathrm{Gal}(K/\mathbb{Q}) \to \{\pm 1\}$ be a non-trivial character. Then there exists a squarefree integer $D \neq 1$ such that χ factors through $\mathbb{Q}(\sqrt{D})$. Therefore the Chebotarev density theorem gives the estimate

$$\sum_{s_i < p < t_i} \chi(\mathrm{Frob}_p) \ll t_i^{\beta} + t_i \cdot e^{\frac{-c \log t_i}{\sqrt{\log t_i + \log |D|}}} \cdot (\log t_i |D|)^4 \tag{7.7}$$

for some absolute constant $c > 0$, see for example [24, Theorem 5.13]. We have the effective lower bound

$$1 - \beta \gg_\epsilon \frac{1}{|D|^{1/2+\epsilon}}$$

for every $\epsilon > 0$. Furthermore, by the Siegel-free assumption we have $|D| \leq t$ in this case. Then assumption (iv) together with $c_6 > 1$ implies

$$1 - \beta \gg_\epsilon \frac{1}{|D|^{1/2+\epsilon}} \geq \frac{1}{t^{1/2+\epsilon}} \gg \frac{1}{(\log t_i)^{1/2}}, \tag{7.8}$$

if we pick ϵ sufficiently small in terms of c_6. Now observe that

$$\log |D| \ll (|P| + 2) \log t_1 \ll (\log t_1)^2 \ll (\log t_i)^{2/c_5} \tag{7.9}$$

by assumption (i) and (iv). Plugging equations (7.8) and (7.9) in equation (7.7) we obtain

$$\sum_{s_i < p < t_i} \chi(\mathrm{Frob}_p) \ll \frac{t_i}{e^{(\log t_i)^{1/3}}},$$

where we used that $c_5 > 3$. We conclude that

$$\left| |X_i(a, x_1)| - \frac{1}{2}|X_i| \right| \ll \frac{[K : \mathbb{Q}] \cdot t_i}{e^{(\log t_i)^{1/3}}}.$$

Since $[K : \mathbb{Q}] \ll t_1 < e^{(\log t_i)^{1/c_5}}$ and since $c_5 > 3$, we deduce from assumption (iii) that

$$\left| |X_i(a, x_1)| - \frac{1}{2}|X_i| \right| \leq \frac{|X_i|}{t_1}$$

upon taking A sufficiently large. This establishes equation (7.6).

Next consider the case $1 < i \leq k$ and suppose that $(1, i) \in \mathcal{M}_r$. Choose real numbers c_9 and c_{10} such that

$$c_9 + c_{10} < \frac{1}{4} - c_2 c_4, \quad c_9 > c_7 \log 2 + c_8 + \frac{1}{c_1}, \quad c_{10} > c_8 + \frac{1}{c_1}.$$

Note that there exist such real numbers, since

$$\frac{1}{8} > c_8 + \frac{c_7 \log 2}{2} + \frac{1}{c_1} + \frac{c_2 c_4}{2}$$

by assumption. Call $x_1 \in X_1$ bad if there exists $(1, i) \in \mathcal{M}_r$ with

$$\left| |X_i(a, x_1)| - \frac{1}{2}|X_i| \right| \geq \frac{|X_i|}{t_1^{c_{10}}},$$

which implies $i \leq k$ by equation (7.6). Write X_1^{bad} for the subset of $x_1 \in X_1$ that are bad. We claim that

$$|X_1^{\text{bad}}| \leq \frac{k \cdot |X_1|}{t_1^{c_9}}. \tag{7.10}$$

The large sieve implies that for all $\epsilon > 0$

$$\sum_{x_1 \in X_1} \left| \sum_{x_i \in X_i} \left(\frac{x_1}{x_i} \right) \right| \ll_\epsilon t_i \cdot t_1^{3/4 + \epsilon},$$

see for example [42, Proposition 6.6]. Then we get

$$\sum_{x_1 \in X_1} \left| \sum_{x_i \in X_i} \left(\frac{x_1}{x_i} \right) \right| \ll_\epsilon \frac{|X_1| \cdot |X_i|}{t_1^{1/4 - c_2 c_4 - \epsilon}} \tag{7.11}$$

thanks to assumptions (ii) and (iii). Now fix $0 < \epsilon < 1/4 - c_2 c_4 - c_9 - c_{10}$. Applying equation (7.11) with $\epsilon/2$ and taking A sufficiently large in terms of $\epsilon/2$, we get

$$\sum_{x_1 \in X_1} \left| \sum_{x_i \in X_i} \left(\frac{x_1}{x_i} \right) \right| \leq \frac{|X_1| \cdot |X_i|}{t_1^{-1/4 + c_2 c_4 + \epsilon}}.$$

This quickly implies equation (7.10), therefore establishing the claim. We now split $X(a)$ depending on x_1

$$\left| |X(a)| - \frac{|X|}{2^{|\mathcal{M}_r|}} \right| \leq \sum_{\substack{x_1 \in X_1^{\text{bad}}}} \sum_{\substack{x \in X(a) \\ \pi_1(x) = x_1}} 1 + \left| \left(\sum_{\substack{x_1 \notin X_1^{\text{bad}}}} \sum_{\substack{x \in X(a) \\ \pi_1(x) = x_1}} 1 \right) - \frac{|X|}{2^{|\mathcal{M}_r|}} \right|. \tag{7.12}$$

To deal with the first term, fix some $x_1 \in X_1^{\text{bad}}$. We move x_1 to P and apply the induction hypothesis to the prebox

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

Write k_{old} for the current value of k and k_{new} for the value of k to which we apply the induction hypothesis. Then we take $k_{\text{new}} \geq k_{\text{old}} - 1$ to be the smallest integer such that

$$t_{k_{\text{new}}+2} > \max(e^{(\log t_2)^{c_5}}, e^{t^{c_6}}).$$

We take $k_{\text{new}} = r - 1$ if no such integer exists. Assumptions (i) and (ii) are satisfied, since

$$e^{t_2^{c_2}} > e^{(\log t_2)^{c_5}}$$

for A sufficiently large. Furthermore, assumption (iii) follows from $c_3 > 1$ and our bounds on X_i if we take A sufficiently large. Meanwhile assumption (iv) holds by construction of k_{new}. To check assumption (v), we distinguish two cases. If $k_{\text{new}} = k_{\text{old}} - 1$, then assumption (v) holds. Otherwise note that

$$k_{\text{new}} + 2 \leq 2 + \lceil c_7 \log t_2 \rceil$$

and hence $k_{\text{new}} \leq \lceil c_7 \log t_2 \rceil$ as desired. Having checked all the conditions, we apply the induction hypothesis, which leads to the bound

$$\sum_{\substack{x \in X(a) \\ \pi_1(x)=x_1}} 1 \leq 2^{-|\mathcal{M}_r|+k+1} \cdot \frac{|X|}{|X_1|}$$

for A sufficiently large, since $(1 + \frac{2}{t_1})^r - 1$ is small by assumption (ii) and the inequality $c_1 > 8$. Therefore we deduce that

$$\sum_{\substack{x \in X(a) \\ \pi_1(x) \in X_1^{\text{bad}}}} 1 \leq k \cdot 2^{-|\mathcal{M}_r|+k+1} \cdot \frac{|X|}{t_1^{c_9}} \leq \frac{|X|}{t_1^{c_8+1/c_1} \cdot 2^{|\mathcal{M}_r|+2}}, \tag{7.13}$$

thanks to assumption (v) and the choice of c_9. Next we turn our attention to bounding

$$\left| \left(\sum_{x_1 \notin X_1^{\text{bad}}} \sum_{\substack{x \in X(a) \\ \pi_1(x)=x_1}} 1 \right) - \frac{|X|}{2^{|\mathcal{M}_r|}} \right|.$$

We move x_1 to P and apply the induction hypothesis to the prebox

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

Since $x_1 \notin X_1^{\text{bad}}$, we see that all the assumptions are satisfied. Let M be the number of pairs of the shape $(1,j)$ in $\mathcal{M}_r$. Writing $X(x_1)$ for the above product space, the induction hypothesis shows that

$$\left| |X(x_1)(a)| - \frac{|X(x_1)|}{2^{|\mathcal{M}_r|-M}} \right| \leq \frac{(r-1)|X(x_1)|}{t_1^{c_8+1/c_1} \cdot 2^{|\mathcal{M}_r|-M}}, \tag{7.14}$$

where we have implicitly restricted a in the obvious way. Using that $x_1 \notin X_1^{\text{bad}}$ once more, we see that

$$\left| 2^M |X(x_1)| - \frac{|X|}{|X_1|} \right| \leq \frac{|X|}{|X_1|} \cdot \left(\left(1 + \frac{2}{t_1^{c_{10}}}\right)^k \cdot \left(1 + \frac{2}{t_1}\right)^r - 1 \right)$$

$$\leq \frac{|X|}{100 \cdot t_1^{c_8+1/c_1} \cdot |X_1|} \tag{7.15}$$

for A sufficiently large, where we used that $r < t_1^{1/c_1}$, $k \leq \lceil c_7 \log t_1 \rceil$ and $c_{10} > c_8 + 1/c_1$. We obtain from equations (7.14) and (7.15)

$$\left| |X(x_1)(a)| - \frac{|X|}{2^{|\mathcal{M}_r|} \cdot |X_1|} \right| \leq \frac{(r-1/2)|X|}{t_1^{c_8+1/c_1} \cdot 2^{|\mathcal{M}_r|} \cdot |X_1|}.$$

We conclude that

$$\left| \left(\sum_{\substack{x_1 \notin X_1^{\mathrm{bad}}}} \sum_{\substack{x \in X(a) \\ \pi_1(x) = x_1}} 1 \right) - \frac{|X|}{2^{|\mathcal{M}_r|}} \right| \leq \frac{(r - 1/4)|X|}{t_1^{c_8 + 1/c_1} \cdot 2^{|\mathcal{M}_r|}}. \tag{7.16}$$

Inserting equations (7.13) and (7.16) in equation (7.12) finishes the proof of the induction step. $\qquad\square$

Our next goal is to deal with the small primes. We shall only be able to achieve savings by introducing some extra averaging. Write $\mathcal{P}_r$ for the set of permutations of $[r]$ and write $\mathcal{P}_r(k)$ for the $\sigma \in \mathcal{P}_r$ such that $\sigma(i) = i$ for all $i > k$. Given $a : M_r \sqcup M_{r,P} \to \mathbb{F}_2$, we will use the convention that $a(j, i)$ equals $a(i, j)$ for $j > i$. We then define $\sigma(a)$ to be

$$\sigma(a)(i, j) := a(\sigma^{-1}(i), \sigma^{-1}(j)), \quad \sigma(a)(i, p) := a(\sigma^{-1}(i), p).$$

Given integers $k_1 \geq k_0 \geq 0$, we define $X_{k_0, k_1}^{\mathrm{trun}}(\sigma, a)$ to be the set of $x = (x_1, \ldots, x_r) \in X$ such that

$$\left(\frac{x_i}{x_j} \right) = \iota(a(\sigma^{-1}(i), \sigma^{-1}(j))) \text{ for all } i, j \in [k_1] \text{ with } \sigma^{-1}(i) < \sigma^{-1}(j) \text{ and } \min(i, j) \leq k_0$$

and furthermore

$$\left(\frac{x_i}{p} \right) = \iota(a(\sigma^{-1}(i), p)) \text{ for all } (i, p) \in [k_1] \times P.$$

We remark that the number of distinct elements $i, j \in [k_1]$ with $\sigma^{-1}(i) < \sigma^{-1}(j)$ and $\min(i, j) \leq k_0$ equals

$$C(k_0, k_1) := \frac{1}{2}(k_0^2 - k_0) + k_0(k_1 - k_0).$$

In particular, this number does not depend on σ. Roughly speaking, $X_{k_0, k_1}^{\mathrm{trun}}(\sigma, a)$ imposes the conditions of $\sigma(a)$ on the small primes. This makes it possible to apply Proposition 7.6 to $X_{k_0, k_1}^{\mathrm{trun}}(\sigma, a)$. The next entirely combinatorial lemma offers a convenient tool to reduce to $X_{k_0, k_1}^{\mathrm{trun}}(\sigma, a)$, see also [42, Proposition 6.7] for a similar result.

Lemma 7.7. *Let (X, P) be a prebox. Let $0 \leq k_0 \leq k_1 \leq k_2 \leq r$ be integers such that*

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

Then we have for all $x \in X$

$$\sum_{a : M_r \sqcup M_{r,P} \to \mathbb{F}_2} \left(\frac{k_2!}{2^{C(k_0, k_1) + k_1 |P|}} - |\{\sigma \in \mathcal{P}_r(k_2) : x \in X_{k_0, k_1}^{\mathrm{trun}}(\sigma, a)\}| \right)^2 \leq$$

$$\frac{2^{k_0 + |P| + 1} \cdot k_1^2}{k_2} \cdot 2^{-2C(k_0, k_1) - 2k_1 |P| + |M_r \sqcup M_{r,P}|} \cdot (k_2!)^2.$$

Proof. Write

$$B(x, a) := \{\sigma \in \mathcal{P}_r(k_2) : x \in X_{k_0, k_1}^{\mathrm{trun}}(\sigma, a)\}.$$

We start by computing

$$\sum_{a:M_r \sqcup M_{r,P} \to \mathbb{F}_2} |B(x,a)| = \sum_{\sigma \in \mathcal{P}_r(k_2)} |\{a : M_r \sqcup M_{r,P} \to \mathbb{F}_2 : x \in X_{k_0,k_1}^{\text{trun}}(\sigma, a)\}|$$

$$= \sum_{\sigma \in \mathcal{P}_r(k_2)} \frac{2^{|M_r \sqcup M_{r,P}|}}{2^{C(k_0,k_1)+k_1|P|}} = k_2! \cdot \frac{2^{|M_r \sqcup M_{r,P}|}}{2^{C(k_0,k_1)+k_1|P|}}. \qquad (7.17)$$

Next, we compute

$$\sum_{a:M_r \sqcup M_{r,P} \to \mathbb{F}_2} |B(x,a)|^2 = \sum_{\sigma_1,\sigma_2 \in \mathcal{P}_r(k_2)} |\{a : M_r \sqcup M_{r,P} \to \mathbb{F}_2 : x \in X_{k_0,k_1}^{\text{trun}}(\sigma_1, a) \cap X_{k_0,k_1}^{\text{trun}}(\sigma_2, a)\}|.$$

For now we fix $\sigma_1, \sigma_2 \in \mathcal{P}_r(k_2)$ and we aim to bound

$$N(\sigma_1, \sigma_2) := |\{a : M_r \sqcup M_{r,P} \to \mathbb{F}_2 : x \in X_{k_0,k_1}^{\text{trun}}(\sigma_1, a) \cap X_{k_0,k_1}^{\text{trun}}(\sigma_2, a)\}|.$$

We introduce the quantities

$$I_{k_1,k_2}(\sigma_1, \sigma_2) := |\{i \in [k_2] : \sigma_1(i) \le k_1, \sigma_2(i) \le k_1\}|$$

and

$$S(\sigma_1, \sigma_2) := \{(i,j) \in M_r : (\sigma_1(i), \sigma_1(j)), (\sigma_2(i), \sigma_2(j)) \in [k_0] \times [k_1] \cup [k_1] \times [k_0]\}$$

and

$$T(\sigma_1, \sigma_2) := \{(i,p) \in M_{r,P} : \sigma_1(i) \in [k_1], \sigma_2(i) \in [k_1]\}.$$

Then $x \in X_{k_0,k_1}^{\text{trun}}(\sigma_1, a) \cap X_{k_0,k_1}^{\text{trun}}(\sigma_2, a)$ gives at least

$$2C(k_0, k_1) + 2k_1|P| - |S(\sigma_1, \sigma_2)| - |T(\sigma_1, \sigma_2)|$$

conditions on a. But we have the upper bounds

$$|S(\sigma_1, \sigma_2)| \le I_{k_1,k_2}(\sigma_1, \sigma_2) \cdot k_0, \quad |T(\sigma_1, \sigma_2)| \le I_{k_1,k_2}(\sigma_1, \sigma_2) \cdot |P|.$$

The first upper bound comes from the injective map

$$S(\sigma_1, \sigma_2) \to \{i \in [k_2] : \sigma_1(i) \le k_1, \sigma_2(i) \le k_1\} \times [k_0]$$

given by

$$(i,j) \mapsto (\sigma_1^{-1}(\max(\sigma_1(i), \sigma_1(j))), \min(\sigma_1(i), \sigma_1(j))),$$

while the second upper bound is straightforward. This yields the bound

$$N(\sigma_1, \sigma_2) \le \frac{2^{|M_r \sqcup M_{r,P}|}}{2^{2C(k_0,k_1)+2k_1|P|-I_{k_1,k_2}(\sigma_1,\sigma_2)\cdot(k_0+|P|)}}.$$

Having bounded $N(\sigma_1, \sigma_2)$, we next fix some $I \le k_1$. We will bound the number of pairs $(\sigma_1, \sigma_2) \in \mathcal{P}_r(k_2) \times \mathcal{P}_r(k_2)$ with

$$I_{k_1,k_2}(\sigma_1, \sigma_2) = I.$$

There are $\binom{k_2}{I}$ ways to pick the indices that map to $[k_1]$ under σ_1 and σ_2. Once we have picked these indices, we can extend them to a pair $(\sigma_1, \sigma_2) \in \mathcal{P}_r(k_2) \times \mathcal{P}_r(k_2)$ in at most

$$\left(\frac{k_1!}{(k_1 - I)!} \cdot (k_2 - I)! \right)^2$$

ways. Indeed, suppose that $B \subseteq [k_2]$ is the set of indices mapping to $[k_1]$ under σ_1 and σ_2, so that $|B| = I$. Then there are

$$k_1! \cdot (k_1! - 1) \cdot \ldots \cdot (k_1! - I + 1)$$

possibilities for σ_1 to send B to $[k_1]$, and similarly for σ_2. Furthermore, there are at most $(k_2 - I)!$ choices where σ_1 can send the indices in $[k_2] \setminus B$, and similarly for σ_2. We conclude that the total number of pairs (σ_1, σ_2) with given $I_{k_1, k_2}(\sigma_1, \sigma_2) = I$ is bounded by

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

We deduce that

$$\sum_{a: M_r \sqcup M_{r,P} \to \mathbb{F}_2} |B(x, a)|^2 = \sum_{\sigma_1, \sigma_2 \in \mathcal{P}_r(k_2)} |\{a : M_r \sqcup M_{r,P} \to \mathbb{F}_2 : x \in X_{k_0, k_1}^{\mathrm{trun}}(\sigma_1, a) \cap X_{k_0, k_1}^{\mathrm{trun}}(\sigma_2, a)\}|$$

$$= \sum_{\sigma_1, \sigma_2 \in \mathcal{P}_r(k_2)} N(\sigma_1, \sigma_2)$$

$$\leq k_2!^2 \cdot \sum_{I \geq 0} \left(\frac{k_1^2}{k_2} \right)^I \cdot \frac{2^{|M_r \sqcup M_{r,P}|}}{2^{2C(k_0, k_1) + 2k_1 |P| - I \cdot (k_0 + |P|)}}$$

$$= (k_2!)^2 \cdot \frac{2^{|M_r \sqcup M_{r,P}|}}{2^{2C(k_0, k_1) + 2k_1 |P|}} \cdot \frac{k_2}{k_2 - 2^{k_0 + |P|} k_1^2}, \tag{7.18}$$

where the last equality uses that

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

so the geometric series converges. The lemma follows upon combining equations (7.17) and (7.18) with the inequality $2^{k_0 + |P| + 1} k_1^2 < k_2$. $\qquad \square$

We will now deal with the small primes. The coming proposition is directly based on [42, Theorem 6.4].

Proposition 7.8. *Take real numbers* $c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9, c_{10}, c_{11}, c_{12}$ *satisfying*

$$c_3 > 1, \quad c_5 > 3, \quad c_6 > 1, \quad \frac{1}{8} > c_8 + \frac{c_7 \log 2}{2} + \frac{1}{c_1} + \frac{c_2 c_4}{2},$$

$$c_{10} \log 2 + 2c_{11} + 2c_{12} < 1, \quad c_{11} + c_{12} < c_9.$$

There exists an effectively computable constant $A > 0$, *depending only on the real numbers* $c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9, c_{10}, c_{11}, c_{12}$, *such that the following holds.*

Let (X, P) *be a prebox such that* X_i *equals the set of primes in the interval* $(s_i, t_i]$ *that are* 1 *or* 2 *modulo* 4. *Let* $0 \leq k_0 < k_1 < k_2 \leq r$ *be integers such that* $k_2 > A$. *We assume that* (X, P) *is Siegel-free above some real number* t *satisfying* $s_{k_0 + 1} > t > A$. *Moreover, suppose that*

(i) $|P| \leq \log t_i - i$ for all $k_0 < i \leq r$;

(ii) $t_{k_0+1} > r^{c_1}$ and $t_{k_1} < e^{t_{k_0+1}^{c_2}}$;

(iii) we have
$$|X_i| \geq \frac{2^{|P|+c_3 i} \cdot k_2^{c_9} \cdot t_i}{(\log t_i)^{c_4}}$$
for all $k_0 < i \leq r$;

(iv) we assume that
$$t_{k_1+1} > \max\left(e^{(\log t_{k_0+1})^{c_5}}, e^{t^{c_6}}\right);$$

(v) we assume that $k_1 - k_0 \leq \lceil c_7 \log t_{k_0+1} \rceil$. Furthermore, we assume that for all $k_0 < i \leq r$ and all $i + c_7 \log t_i \leq j \leq r$ that
$$t_j > e^{(\log t_i)^{c_5}};$$

(vi) $k_0 + |P| < c_{10} \log k_2$ and $\log k_1 < c_{11} \log k_2$.

Then we have
$$\sum_{a: M_r \sqcup M_{r,P} \to \mathbb{F}_2} \left| \frac{k_2! \cdot |X|}{2^{|M_r \sqcup M_{r,P}|}} - \sum_{\sigma \in \mathcal{P}_r(k_2)} |X(\sigma(a))| \right| \leq k_2! \cdot |X| \cdot (k_2^{-c_{12}} + t_{k_0+1}^{-c_8}).$$

Proof. We readily reduce to the case where $|X_i| = 1$ for $i \in [k_0]$. Henceforth we shall assume that $X_i = \{x_i\}$ for $i \in [k_0]$. It follows from the triangle inequality that
$$\sum_{a: M_r \sqcup M_{r,P} \to \mathbb{F}_2} \left| \frac{k_2! \cdot |X|}{2^{|M_r \sqcup M_{r,P}|}} - \sum_{\sigma \in \mathcal{P}_r(k_2)} |X(\sigma(a))| \right|$$

is bounded by
$$\sum_{a: M_r \sqcup M_{r,P} \to \mathbb{F}_2} \left| \frac{k_2! \cdot |X|}{2^{|M_r \sqcup M_{r,P}|}} - \sum_{\sigma \in \mathcal{P}_r(k_2)} \frac{|X_{k_0,k_1}^{\mathrm{trun}}(\sigma, a)|}{2^{|M_r \sqcup M_{r,P}| - C(k_0,k_1) - k_1|P|}} \right| +$$
$$\sum_{\sigma \in \mathcal{P}_r(k_2)} \sum_{a: M_r \sqcup M_{r,P} \to \mathbb{F}_2} \left| \frac{|X_{k_0,k_1}^{\mathrm{trun}}(\sigma, a)|}{2^{|M_r \sqcup M_{r,P}| - C(k_0,k_1) - k_1|P|}} - |X(\sigma(a))| \right|.$$

By the triangle inequality the first sum is at most
$$\frac{2^{C(k_0,k_1)+k_1|P|}}{2^{|M_r \sqcup M_{r,P}|}} \sum_{a: M_r \sqcup M_{r,P} \to \mathbb{F}_2} \sum_{x \in X} \left| \frac{k_2!}{2^{C(k_0,k_1)+k_1|P|}} - |\{\sigma \in \mathcal{P}_r(k_2) : x \in X_{k_0,k_1}^{\mathrm{trun}}(\sigma, a)\}| \right|.$$

An application of Lemma 7.7 and the Cauchy–Schwarz inequality shows that the above is bounded by
$$\left(\frac{2^{k_0+|P|+1} \cdot k_1^2}{k_2} \right)^{1/2} \cdot k_2! \cdot |X| \leq \frac{k_2! \cdot |X|}{2 \cdot k_2^{c_{12}}}, \tag{7.19}$$

where the last inequality follows for sufficient A from assumption (vi) and $c_{10} \log 2 + 2c_{11} + 2c_{12} < 1$. Let us now consider the second sum. Fix $\sigma \in \mathcal{P}_r(k_2)$ and $a : M_r \sqcup M_{r,P} \to \mathbb{F}_2$. We aim to bound each

$$\left| \frac{|X_{k_0,k_1}^{\text{trun}}(\sigma, a)|}{2^{|M_r \sqcup M_{r,P}| - C(k_0,k_1) - k_1|P|}} - |X(\sigma(a))| \right|$$

individually. Without loss of generality we may assume that

$$\left(\frac{x_i}{x_j} \right) = \iota(a(\sigma^{-1}(i), \sigma^{-1}(j))) \text{ for all distinct } i, j \in [k_0],$$

since otherwise $X(\sigma(a))$ and $X_{k_0,k_1}^{\text{trun}}(\sigma, a)$ are empty. If $i > k_0$, define $X_i^{\text{trim}}(\sigma, a)$ to be the subset of $x_i \in X_i$ such that

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

We turn $X_{k_0,k_1}^{\text{trun}}(\sigma, a)$ in a prebox (X', P') by taking P' to be the union of the primes $x_1, \ldots, x_{k_0}$ with P and by taking $X' = X_1' \times \cdots \times X_{r-k_0}'$, where

$$X_i' = \begin{cases} X_{i+k_0}^{\text{trim}}(\sigma, a) & \text{if } i \in [k_1 - k_0] \\ X_{i+k_0} & \text{if } i > k_1 - k_0. \end{cases}$$

It follows from the Chebotarev density theorem that

$$\left| |X_i^{\text{trim}}(\sigma, a)| - \frac{|X_i|}{2^{k_0 + |P|}} \right| \leq \frac{|X_i|}{t_{k_0 + 1}} \tag{7.20}$$

for all $i > k_1$. Therefore, in case

$$|X_i'| \geq \frac{|X_{i+k_0}|}{2^{k_0 + |P|} \cdot k_2^{c_9}} \text{ for all } i \in [r - k_0],$$

we apply Proposition 7.6 to $(X'', P'') := (X_{k_0+1}^{\text{trim}}(\sigma, a) \times \cdots \times X_r^{\text{trim}}(\sigma, a), P')$ to obtain the bound

$$\left| \frac{|X''|}{2^{\frac{(r-k_0)(r-k_0-1)}{2}}} - |X(\sigma(a))| \right| \leq \frac{|X''|}{2 \cdot t_{k_0+1}^{c_8} \cdot 2^{|M_r \sqcup M_{r,P}| - C(k_0,k_1) - k_1|P|}},$$

where we save an extra factor 2 by taking the c_8 of Proposition 7.6 slightly smaller than our c_8. This implies

$$\left| \frac{|X_{k_0,k_1}^{\text{trun}}(\sigma, a)|}{2^{|M_r \sqcup M_{r,P}| - C(k_0,k_1) - k_1|P|}} - |X(\sigma(a))| \right| \leq \frac{|X_{k_0,k_1}^{\text{trun}}(\sigma, a)|}{t_{k_0+1}^{c_8} \cdot 2^{|M_r \sqcup M_{r,P}| - C(k_0,k_1) - k_1|P|}} \tag{7.21}$$

thanks to equation (7.20). Instead suppose that

$$|X_i'| < \frac{|X_{i+k_0}|}{2^{k_0 + |P|} \cdot k_2^{c_9}}$$

for some $i \in [r - k_0]$. Then certainly i must be in $[k_1 - k_0]$, and we call the pair (σ, a) bad at i. For every given $\sigma \in \mathcal{P}_r(k_2)$ and $j \in [k_1 - k_0]$, we define an equivalence relation on the set of maps $a : M_r \sqcup M_{r,P} \to \mathbb{F}_2$ by declaring $a \sim_{\sigma,j} a'$ if

$$a(\sigma^{-1}(j'), \sigma^{-1}(j + k_0)) = a'(\sigma^{-1}(j'), \sigma^{-1}(j + k_0)) \text{ for all } j' \in [k_0]$$

and

$$a(\sigma^{-1}(j+k_0),p) = a'(\sigma^{-1}(j+k_0),p) \text{ for all } p \in P.$$

If the pair (σ,a) is bad at j and if $a' \sim_{\sigma,j} a$, then (σ,a') is also bad at j. The trivial bound yields that in a given equivalence class represented by a'

$$\sum_{\substack{a:M_r \sqcup M_{r,P} \to \mathbb{F}_2 \\ (\sigma,a) \text{ bad} \\ a \sim_{\sigma,j} a'}} \left| \frac{|X_{k_0,k_1}^{\mathrm{trun}}(\sigma,a)|}{2^{|M_r \sqcup M_{r,P}| - C(k_0,k_1) - k_1|P|}} - |X(\sigma(a))| \right| \le \frac{|X|}{2^{k_0+|P|} \cdot k_2^{c_9}}.$$

Since there are at most $2^{k_0+|P|}$ equivalence classes and at most $k_1 \cdot k_2!$ equivalence relations $\sim_{\sigma,j}$, we get after summing over all σ and all j

$$\sum_{\sigma \in \mathcal{P}_r(k_2)} \sum_{\substack{a:M_r \sqcup M_{r,P} \to \mathbb{F}_2 \\ (\sigma,a) \text{ bad}}} \left| \frac{|X_{k_0,k_1}^{\mathrm{trun}}(\sigma,a)|}{2^{|M_r \sqcup M_{r,P}| - C(k_0,k_1) - k_1|P|}} - |X(\sigma(a))| \right| \le k_1 \cdot k_2! \cdot \frac{|X|}{k_2^{c_9}} \le \frac{k_2! \cdot |X|}{2 \cdot k_2^{c_{12}}}$$

$$(7.22)$$

thanks to assumption (vi) and the inequality $c_{11} + c_{12} < c_9$. Furthermore, equation (7.21) implies that

$$\sum_{\sigma \in \mathcal{P}_r(k_2)} \sum_{\substack{a:M_r \sqcup M_{r,P} \to \mathbb{F}_2 \\ (\sigma,a) \text{ not bad}}} \left| \frac{|X_{k_0,k_1}^{\mathrm{trun}}(\sigma,a)|}{2^{|M_r \sqcup M_{r,P}| - C(k_0,k_1) - k_1|P|}} - |X(\sigma(a))| \right| \le \frac{k_2! \cdot |X|}{t_{k_0+1}^{c_8}}, \qquad (7.23)$$

since for a given σ the sets $X_{k_0,k_1}^{\mathrm{trun}}(\sigma,a)$ partition X and there are

$$2^{|M_r \sqcup M_{r,P}| - C(k_0,k_1) - k_1|P|}$$

maps $a : M_r \sqcup M_{r,P} \to \mathbb{F}_2$ with the same $X_{k_0,k_1}^{\mathrm{trun}}(\sigma,a)$. Adding the bounds from equations (7.19), (7.22) and (7.23), we get the proposition. $\qquad \square$

7.3 Boxes

We are now ready to define boxes. We recall that

$$D_1 = e^{(\log \log N)^{1/10}}.$$

Also define

$$D_{\mathrm{Siegel}} := e^{(\log \log N)^{1/100}}.$$

Definition 7.9. *Let $N \ge 10^{1000}$, let r be a positive integer and let $0 \le k \le r$. Let $\mathbf{t} = (p_1,\ldots,p_k,s_{k+1},\ldots,s_r)$, where the p_i are prime numbers congruent to 1 or 2 modulo 4 and the s_j are real numbers satisfying*

$$p_1 < \cdots < p_k < D_1, \quad D_1 \le s_{k+1} < \cdots < s_r, \quad s_i < \frac{2}{3}s_{i+1} \text{ for all } k < i < r.$$

To $\mathbf{t}$ we associate a product space $X(\mathbf{t}) = X_1 \times \cdots \times X_r$ as follows

71

- *for $1 \le i \le k$ we have $X_i = \{p_i\}$;*

- *for all $k < i \le r$ we have that X_i consists of the prime numbers (1 or 2 modulo 4) in the interval*
$$\left(s_i, s_i \cdot \left(1 + \frac{1}{C_{\text{compr}}} \right) \right],$$

where $100 \le C_{\text{compr}} \le (\log N)^{100}$ is a real number. If N is sufficiently large, then the sets X_i are disjoint and non-empty, so that we may naturally view $X(\mathbf{t})$ as a subset of $\mathcal{D}$. We call a product space $X = X_1 \times \cdots \times X_r$ a (N,k,r)-box if there is some $\mathbf{t}$ such that $X = X(\mathbf{t})$ and $X \subseteq \mathcal{D}(N)$. We say that X is an excellent (N,k,r)-box if additionally there is $d \in X$ that is N-nice and

$$\left\{ \alpha \prod_{i \in S} \pi_i(x) : x \in X, S \subseteq [r], \alpha \in \{1,-1\}, \left| \alpha \prod_{i \in S} \pi_i(x) \right| > D_{\text{Siegel}} \right\} \cap \mathcal{S}(c_{\text{Landau}}) = \varnothing.$$

The next proposition is [42, Proposition 6.9], although our proof is more similar to the one appearing in Watkins [46].

Theorem 7.10. *Let $N \ge 10^{1000}$ be a real number and let r be a positive integer satisfying equation (7.4). Let $V, W \subseteq \mathcal{D}_r(N)$ and let $\epsilon > 0$ be such that*

$$|W| > (1 - \epsilon) \cdot |\mathcal{D}_r(N)|.$$

Suppose that

$$||V \cap X| - \delta \cdot |X|| \le \epsilon \cdot |X|$$

for all integers k and all (N,k,r)-boxes X such that $X \cap W \ne \varnothing$. Then

$$|V| = \delta \cdot |\mathcal{D}_r(N)| + O\left(\left(\epsilon + \frac{1}{e^{(\log \log \log N)^{1/4}}} \right) \cdot |\mathcal{D}_r(N)| + \left| \mathcal{D}_r(N) - \mathcal{D}_r\left(\frac{N}{\left(1 + \frac{1}{C_{\text{compr}}}\right)^r} \right) \right| \right).$$

Proof. Define
$$e_i = D_1 \cdot \left(1 + \frac{1}{C_{\text{compr}}} \right)^i.$$

Let $\mathcal{C}$ be the collection of product spaces $X = X_1 \times \cdots \times X_r$ that are (N,k,r)-boxes for some integer k such that
$$s_i \in \{e_0, e_1, e_2, \dots\}$$

for all $k+1 \le i \le r$ and such that $X \cap W \ne \varnothing$. If we take distinct $X, Y \in \mathcal{C}$, then we see that $X \cap Y = \varnothing$. Furthermore, in case $d \in \mathcal{D}_r(N)$ is not in some product space $X \in \mathcal{C}$, then we see that d fails the first condition of Definition 7.1 (and hence d is not N-nice) or $d \notin W$ or

$$d \ge N \left(1 + \frac{1}{C_{\text{compr}}} \right)^{-r}.$$

Write $\mathcal{D}_r^{\text{bad}}(N)$ for this set of d. Then we have

$$||V| - \delta \cdot |\mathcal{D}_r(N)|| \le 2 \cdot |\mathcal{D}_r^{\text{bad}}(N)| + \sum_{X \in \mathcal{C}} ||V \cap X| - \delta \cdot |X||.$$

The latter term is bounded by $\epsilon \cdot |\mathcal{D}_r(N)|$ thanks to our assumption

$$||V \cap X| - \delta \cdot |X|| \leq \epsilon \cdot |X|.$$

Furthermore, it follows from Theorem 7.2 and

$$|W| > (1 - \epsilon) \cdot |\mathcal{D}_r(N)|$$

that

$$|\mathcal{D}_r^{\mathrm{bad}}(N)| \ll \left(\epsilon + \frac{1}{e^{(\log\log\log N)^{1/4}}} \right) \cdot |\mathcal{D}_r(N)| + \left| \mathcal{D}_r(N) - \mathcal{D}_r \left(N \left(1 + \frac{1}{C_{\mathrm{compr}}} \right)^{-r} \right) \right|.$$

This gives the theorem. $\qquad\square$

Remark 7.11. *If $(\log N)^{1-\epsilon} \geq C_{\mathrm{compr}} \geq r^{1+\epsilon}$, then one can show that*

$$\left| \mathcal{D}_r(N) - \mathcal{D}_r \left(N \left(1 + \frac{1}{C_{\mathrm{compr}}} \right)^{-r} \right) \right| \ll_\epsilon \frac{|\mathcal{D}_r(N)|}{r^\epsilon},$$

and hence we get a genuine error term in Theorem 7.10. However, since we have the luxury to also average over r later on, we have opted to use the trivial bound

$$\sum_r \left| \mathcal{D}_r(N) - \mathcal{D}_r \left(N \left(1 + \frac{1}{C_{\mathrm{compr}}} \right)^{-r} \right) \right| \leq |\mathcal{D}(N)| - \left| \mathcal{D} \left(N \left(1 + \frac{1}{C_{\mathrm{compr}}} \right)^{-r} \right) \right|$$

and the classical asymptotic formula

$$|\mathcal{D}(N)| = \frac{CN}{\sqrt{\log N}} \cdot \left(1 + O\left(\frac{1}{\log N} \right) \right)$$

for some $C > 0$.

From now on we shall take

$$C_{\mathrm{compr}} := (\log\log N)^{50}.$$

We remark that Theorem 7.10 works equally well for the set of odd or even radicands, or in fact any congruence conditions on our radicands. Keeping this in mind, we see that all our proofs also work if we order by the discriminant instead. We will now deal with Siegel zeroes, see also [42, Proposition 6.10].

Proposition 7.12. *Let $N \geq t \geq 10^{1000}$ be real numbers and let r be a positive integer satisfying equation (7.4). Let $f_1, f_2, f_3, \dots$ be a sequence of squarefree integers greater than t such that $f_{i+1} > f_i^2$. Define*

$$W(f_i) := \{x \in \mathcal{D}_r(N) : \text{ there is a } (N, k, r)\text{-box } X \text{ and } x' \in X \text{ such that } f_i \mid x' \text{ and } x \in X\}.$$

Suppose that $\log N \geq (\log t)^3$. Then

$$\left| \bigcup_{i \geq 1} W(f_i) \right| \ll \frac{|\mathcal{D}_r(N)|}{\log t}.$$

Proof. We factor $f_i = p_1 \cdot \ldots \cdot p_m$. Suppose that $x \in W(f_i)$. Then there exist prime factors $q_1, \ldots, q_m$ of x such that

$$p_i = q_i \text{ for } p_i < D_1, \quad \frac{p_i}{2} < q_i < 2p_i \text{ for } p_i \geq D_1.$$

First suppose that $f_i < N^{2/3}$. Since r satisfies equation (7.4), it follows from equation (7.3) that

$$|W(f_i)| \leq \left| \mathcal{D}_{r-m} \left(\frac{2^m N}{f_i} \right) \right| \cdot \prod_{p_i \geq D_1} |\{q_i \text{ prime} : p_i/2 < q_i < 2p_i\}|$$

$$\leq \frac{C^m \cdot |\mathcal{D}_r(N)|}{f_i} \cdot \prod_{p_i \geq D_1} \frac{p_i}{\log p_i} \ll \frac{|\mathcal{D}_r(N)|}{\log f_i}$$

for some absolute constant $C > 0$. Since $f_i > t^{2^i}$, we deduce that

$$\left| \bigcup_{\substack{i \geq 1 \\ f_i < N^{2/3}}} W(f_i) \right| \ll \frac{|\mathcal{D}_r(N)|}{\log t}.$$

Next suppose that $f_i \geq N^{2/3}$. Since $f_{i+1} \geq N^{4/3}$, it follows that $W(f_j)$ is empty for $j \geq i+1$. Therefore it remains to bound $|W(f_i)|$. We have

$$|W(f_i)| \leq \frac{N}{f_i} \cdot \prod_{p_i \geq D_1} |\{q_i \text{ prime} : p_i/2 < q_i < 2p_i\}|$$

$$\leq \frac{N}{f_i} \cdot \prod_{p_i \geq D_1} \frac{2p_i}{\log p_i} \ll \frac{N}{\log f_i} \ll \frac{N}{\log N}$$

for N sufficiently large. A final appeal to equation (7.3) shows that this is within the error term thanks to our assumption $\log N \geq (\log t)^3$. $\qquad \square$

We can now prove the main result of this section. Let $D_{2,n}$ be the set of $d \in \mathcal{D}$ such that $\mathrm{rk}_4 \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) = n$. Write $P_{\mathrm{Sym}}(r, n)$ for the probability that a symmetric $r \times r$ matrix with coefficients in $\mathbb{F}_2$ has kernel of dimension n with respect to the uniform probability measure.

Theorem 7.13. *Let $N \geq 10^{1000}$ be a real number and let $n \geq 0$ be an integer. Then we have*

$$\frac{|D_{2,n} \cap \mathcal{D}(N)|}{|\mathcal{D}(N)|} = \lim_{s \to \infty} P_{\mathrm{Sym}}(s, n) + O \left(\frac{1}{e^{(\log \log \log N)^{1/4}}} \right).$$

The implied constant is effectively computable.

Better error terms are available in the literature, see [8, 42, 46], with the best result due to Watkins [46]. One can also find the above result in earlier work of Fouvry and Klüners [18], albeit without an error term. We have not yet used (and will not use in this section) the third point in the definition of N-nice. Similarly, one can pick C_0 substantially larger than we did for the purposes of this section. The improvements available in the literature come from a better upper bound in Theorem 7.2 in this more relaxed setting.

Proof. By Remark 7.11 and by equation (7.2) it suffices to show that

$$\frac{|D_{2,n} \cap \mathcal{D}_r(N)|}{|\mathcal{D}_r(N)|} = \lim_{s \to \infty} P_{\text{Sym}}(s, n) + O\left(\frac{1}{e^{(\log \log \log N)^{1/4}}}\right) +$$
$$O\left(\left|\mathcal{D}_r(N) - \mathcal{D}_r\left(N\left(1 + \frac{1}{C_{\text{compr}}}\right)^{-r}\right)\right|\right)$$

with r satisfying equation (7.4). By the explicit formulas in [34], we readily bound the difference

$$P_{\text{Sym}}(r - 1, n) - \lim_{s \to \infty} P_{\text{Sym}}(s, n).$$

We apply Theorem 7.10 with W equal to the largest subset of the N-nice elements in $\mathcal{D}_r(N)$ disjoint form the $W(d_i)$ with $|d_i| > D_{\text{Siegel}}$, see Definition 7.5 for the definition of d_i. It follows from Theorem 7.2 and Proposition 7.12 with $t = D_{\text{Siegel}}$ that

$$|\mathcal{D}_r(N)| - |W| \ll \frac{|\mathcal{D}_r(N)|}{e^{(\log \log \log N)^{1/4}}}.$$

Hence it suffices to show that

$$\frac{|D_{2,n} \cap X|}{|X|} = P_{\text{Sym}}(r - 1, n) + O\left(\frac{1}{e^{(\log \log \log N)^{1/4}}}\right) \tag{7.24}$$

for every (N, k, r)-excellent box X. We apply Proposition 7.8 to $(X, \varnothing)$ with

$$(c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9, c_{10}, c_{11}, c_{12}) = \left(100, \frac{1}{10^9}, 5, 10^6, 5, 5, \frac{1}{100}, \frac{1}{100}, 5, \frac{1}{5}, \frac{1}{5}, \frac{1}{5}\right),$$

$k_0 = k$, k_1 the smallest integer such that

$$t_{k_1+1} > \max(e^{(\log t_{k+1})^5}, e^{t^5})$$

and $k_2 = r$. It follows from equations (7.1) and (7.4) that all the conditions of Proposition 7.8 are satisfied for N sufficiently large. We conclude that

$$\sum_{a:M_r \to \mathbb{F}_2} \left|\frac{r! \cdot |X|}{2^{r(r-1)/2}} - \sum_{\sigma \in \mathcal{P}_r} |X(\sigma(a))|\right| \leq r! \cdot |X| \cdot (r^{-1/5} + t_{k+1}^{-1/100}) \tag{7.25}$$

for N sufficiently large. To $a : M_r \to \mathbb{F}_2$ we associate a matrix $A(a)$ as follows: the (i, j)-th entry of $A(a)$ equals $a(i, j)$ if $i \neq j$ and

$$a(i, i) = \sum_{k \neq i} a(i, k). \tag{7.26}$$

Then $A(a)$ is a symmetric $r \times r$ matrix with row sum zero. In this way we have created a bijection between maps $M_r \to \mathbb{F}_2$ and symmetric $r \times r$ matrices with row sum zero. Write $A'(a)$ for the matrix obtained form $A(a)$ by dropping the last column and last row of $A(a)$. Then we get a bijection between maps $M_r \to \mathbb{F}_2$ and symmetric $(r - 1) \times (r - 1)$ matrices. If $x \in X(a)$, then we have

$$\text{rk}_4 \text{Cl}(\mathbb{Q}(\sqrt{x})) = -1 + \dim_{\mathbb{F}_2} \ker(A(a)) = \dim_{\mathbb{F}_2} \ker(A'(a)) \tag{7.27}$$

thanks to classical work of Rédei. Since we have

$$\dim_{\mathbb{F}_2} \ker(A(a)) = \dim_{\mathbb{F}_2} \ker(A(\sigma(a))),$$

equation (7.24) follows from equations (7.25) and (7.27). □

8 Proof of Theorem 1.1

Let $D_{k,n}$ be the set of $d \in \mathcal{D}$ such that $\mathrm{rk}_{2^k}\mathrm{Cl}(\mathbb{Q}(\sqrt{d})) = n$ and furthermore $(\sqrt{d}) \in 2^{k-1}\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))$. Define $D_{k,n}(N)$ for the subset of $d \in D_{k,n}$ with $d < N$. We write $P(m, n, j)$ for the probability that a $m \times n$ matrix, chosen uniformly at random with coefficients in $\mathbb{F}_2$, has right kernel of rank j. Let $A_{\mathrm{Comb}} > 0$ be a choice of real number such that Proposition 6.6 holds. Define

$$c = \frac{1}{A_{\mathrm{Comb}} \cdot 10^{10}}.$$

In this section we shall establish the following theorem.

Theorem 8.1. *There are real numbers $A, N_0 > 0$ such that for all reals $N > N_0$, all integers $m \geq 2$ and all sequences of integers $n_2, \ldots, n_{m+1} \geq 0$*

$$\left\| \left| \bigcap_{i=2}^{m+1} D_{i,n_i}(N) \right| - \frac{P(n_m, n_m, n_{m+1})}{2^{n_m}} \cdot \left| \bigcap_{i=2}^{m} D_{i,n_i}(N) \right| \right\| \leq \frac{A \cdot |\mathcal{D}(N)|}{(\log\log\log\log N)^{\frac{c}{m^2 6^m}}}.$$

We remark that the $m = 2$ case of the above theorem was already established in [8, Theorem 6.1]. Therefore it remains to prove Theorem 8.1 for $m \geq 3$. It is perhaps worth emphasizing once more that from the 16-rank onwards, the class group behaves rather differently than for the 8-rank. This leads to substantial differences between the reflection principles presented here and those in [8].

The assumption $m \geq 3$ means then that we do not have to reprove some of the results from [8]. We will use this assumption in particular when applying Theorem 5.6 (we remark that $m = 3$ corresponds to $s = 2$). Note that Theorem 5.6 is not correct when $s = 1$, which shows the qualititive difference between the 16-rank and the 8-rank. This is certainly related to the fact that there are no governing fields for the 16-rank, while there are governing fields for the 8-rank. For a precise statement, see [26, Theorem 3], which builds on earlier work in [20].

The error term from [8] was later substantially improved by Watkins [47]. Let us now show that Theorem 8.1 implies Theorem 1.1. The argument is very similar to the material in [29, Appendix A].

Proof that Theorem 8.1 implies Theorem 1.1. We will show that [43, Conjecture 3.4(i)] and [43, Conjecture 3.4(ii)] hold. Then, as already argued immediately after [43, Conjecture 3.4], we get Theorem 1.1. We also remark that [43, Conjecture 3.4(ii)] follows from the results of Fouvry–Klüners [18, Corollary 2] (or, alternatively, our Theorem 7.13), so it remains to verify [43, Conjecture 3.4(i)]. Define for every integer $m \in \mathbb{Z}_{\geq 0}$ the quantities

$$P_2^-(m) = \liminf_{X \to \infty} \frac{|\mathcal{D}^-(X) \cap D_{2,m}(X)|}{|D_{2,m}(X)|}, \quad P_2^+(m) = \limsup_{X \to \infty} \frac{|\mathcal{D}^-(X) \cap D_{2,m}(X)|}{|D_{2,m}(X)|}.$$

The content of [43, Conjecture 3.4(i)] is that

$$P_2^-(m) = P_2^+(m) = \frac{1}{2^{m+1} - 1}. \tag{8.1}$$

It follows from Theorem 8.1 that $P_2^-(m) = P_2^+(m)$ for all m, and hence

$$P_2(m) = \lim_{X \to \infty} \frac{|\mathcal{D}^-(X) \cap D_{2,m}(X)|}{|D_{2,m}(X)|}$$

exists. From the Markov chain behavior in Theorem 8.1, we similarly deduce that

$$P_3(m,n) = \lim_{X \to \infty} \frac{|\mathcal{D}^-(X) \cap D_{2,m}(X) \cap D_{3,n}(X)|}{|D_{2,m}(X) \cap D_{3,n}(X)|}$$

exists and equals $P_2(n)$ for all pairs of integers $m \geq n \geq 0$. Now consider the identity

$$\frac{|\mathcal{D}^-(X) \cap D_{2,m}(X)|}{|D_{2,m}(X)|} = \sum_{n=0}^{m} \frac{|\mathcal{D}^-(X) \cap D_{2,m}(X) \cap D_{3,n}(X)|}{|D_{2,m}(X) \cap D_{3,n}(X)|} \cdot \frac{|D_{2,m}(X) \cap D_{3,n}(X)|}{|D_{2,m}(X)|}.$$

Taking $X \to \infty$, we obtain

$$P_2(m) = \sum_{n=0}^{m} P_3(m,n) \cdot \frac{P(m,m,n)}{2^m} = \sum_{n=0}^{m} P_2(n) \cdot \frac{P(m,m,n)}{2^m}. \tag{8.2}$$

We recall the identity [29, eq. (A.2)]

$$\frac{1}{2^{m+1} - 1} = \sum_{n=0}^{m} \frac{1}{2^{n+1} - 1} \cdot \frac{P(m,m,n)}{2^m}.$$

Together with equation (8.2) and $P_2(0) = 1$, this implies equation (8.1). $\qquad \square$

8.1 Boxes

To prove Theorem 8.1, we are going to cover $\mathcal{D}(N)$ by boxes X with some desirable properties.

Theorem 8.2. *There are real numbers $A, N_0 > 0$ such that for all reals $N > N_0$, all integers $m \geq 3$, all sequences of integers $n_2, \ldots, n_{m+1} \geq 0$, all integers r satisfying equation (7.4), all integers $0 \leq k \leq r$ and all excellent (N,k,r)-boxes X*

$$\left\| \left| X \cap \bigcap_{i=2}^{m+1} D_{i,n_i}(N) \right| - \frac{P(n_m, n_m, n_{m+1})}{2^{n_m}} \cdot \left| X \cap \bigcap_{i=2}^{m} D_{i,n_i}(N) \right| \right\| \leq \frac{A \cdot |X|}{(\log\log\log\log N)^{\frac{c}{m^2 6^m}}}.$$

Proof that Theorem 8.2 implies Theorem 8.1. By equation (7.2) of Theorem 7.2 we have

$$\bigcup_{|r - \frac{1}{2}\log\log N| \geq (\log\log N)^{2/3}} |\mathcal{D}_r(N)| \ll \frac{N}{(\log\log N)^{1/100}}.$$

Hence, by Remark 7.11, it suffices to prove that there exist real numbers $A', N_0 > 0$ such that

$$\left\| \left| \mathcal{D}_r(N) \cap \bigcap_{i=2}^{m+1} D_{i,n_i}(N) \right| - \frac{P(n_m, n_m, n_{m+1})}{2^{n_m}} \cdot \left| \mathcal{D}_r(N) \cap \bigcap_{i=2}^{m} D_{i,n_i}(N) \right| \right\|$$

$$\leq \frac{A' \cdot |\mathcal{D}_r(N)|}{(\log\log\log\log N)^{\frac{c}{m^2 6^m}}} + A' \cdot \left| \mathcal{D}_r(N) - \mathcal{D}_r\left(N\left(1 + \frac{1}{C_{\text{compr}}} \right)^{-r} \right) \right|$$

for all real numbers $N > N_0$ and all positive integers r satisfying equation (7.4). Now apply Theorem 7.10 twice with

$$V = \mathcal{D}_r(N) \cap \bigcap_{i=2}^{m+1} D_{i,n_i}(N) \quad \text{and} \quad V' = \mathcal{D}_r(N) \cap \bigcap_{i=2}^{m} D_{i,n_i}(N)$$

and with W the maximal subset of $\mathcal{D}_r(N)$ that intersects trivially with all the $W(d_i)$ for $d_i > D_{\text{Siegel}}$ and also intersects trivially with the set

$$\{d \in \mathcal{D}_r(N) : d \text{ is not } N\text{-nice}\}.$$

To apply Theorem 7.10, we need a lower bound for $|W|$ and a good estimate for $|V \cap X|$ and $|V' \cap X|$ for boxes X that intersect W non-trivially (note that such boxes are (N, k, r)-excellent). From Theorem 7.2 and Proposition 7.12 we get the required lower bound for W. Let X be a box that intersects W non-trivially. Repeated application of Theorem 8.2 yields

$$\left| |V \cap X| - \left(\prod_{i=2}^{m} \frac{P(n_i, n_i, n_{i+1})}{2^{n_i}} \right) \cdot |X \cap D_{2,n_2}(N)| \right| \leq \sum_{i=2}^{m} \frac{A \cdot |X|}{(\log \log \log \log N)^{\frac{c}{i^2 6^i}}}$$

$$\leq \frac{2A \cdot |X|}{(\log \log \log \log N)^{\frac{c}{m^2 6^m}}}$$

for N sufficiently large, and similarly for $|V' \cap X|$. Here we used that

$$(\log \log \log \log N)^{\frac{c}{m^2 6^m}} \geq 2,$$

which we may always assume, since otherwise Theorem 8.1 is trivially true. Inserting the estimate for $|X \cap D_{2,n_2}(N)|$ from equation (7.24) shows that

$$\left| |V \cap X| - \left(\prod_{i=2}^{m} \frac{P(n_i, n_i, n_{i+1})}{2^{n_i}} \right) \cdot P_{\text{Sym}}(r-1, n_2) \cdot |X| \right| \leq \frac{3A \cdot |X|}{(\log \log \log \log N)^{\frac{c}{m^2 6^m}}}$$

for N sufficiently large, and likewise for $|V' \cap X|$. This finishes the proof of the reduction step. $\qquad \square$

8.2 Genericity

We will split X as the union over $X(a)$ and then prove equidistribution for most a. If X is an excellent (N, k, r)-box, then there exists $x \in X$ and an integer k_{gap} satisfying $\frac{r^{1/2}}{2} < k_{\text{gap}} + 1 < \frac{r}{2}$ and

$$\log x_{k_{\text{gap}}+1} \geq (\log \log x_{k_{\text{gap}}+1})^2 \cdot \log \log \log N \cdot \sum_{j=1}^{k_{\text{gap}}} \log x_j, \tag{8.3}$$

where $x = (x_1, \ldots, x_r)$. From now on fix such a choice of k_{gap}.

Definition 8.3. *Let $X = X_1 \times \cdots \times X_r$ be a product space, let $S \subseteq [r]$ and let $Q \in \prod_{i \in S} X_i$. We say that Q is a-consistent with $a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2$ if*

$$\left(\frac{\pi_i(Q)}{\pi_j(Q)} \right) = \iota(a(i, j)) \text{ for all distinct } i, j \in S.$$

We define $X(a, Q)$ to be the subset of $x \in X(a)$ for which $\pi_S(x) = Q$. Finally, given $j \in [r] - S$, let $X_j(a, Q)$ be the subset of $p \in X_j$ with

$$\left(\frac{\pi_i(Q)}{p} \right) = \iota(a(i, j))$$

for all $i \in S$.

Definition 8.4. *Let r be a positive integer and let $a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2$. Recall that we have associated to $a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2$ a $r \times r$ matrix that we call $A(a)$, see equation (7.26). The left and right kernel of $A(a)$ are naturally subspaces of $\mathbb{F}_2^r$, and viewed as such they coincide and contain the element $R := (1, \ldots, 1)$. Let us call this subspace $V_{a,2}$. We say that $a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2$ is (N, m)-generic for a box X if*

- *putting*

$$n_{\max} := \left\lfloor \sqrt{\frac{10c}{m^2 6^m} \log \log \log \log \log N} \right\rfloor,$$

  we have

$$\dim V_{a,2} \leq n_{\max}; \tag{8.4}$$

- *we have for all $j > k$*

$$|X_j(a, Q)| \geq \frac{|X_j|}{(\log s_{k+1})^{100}}, \tag{8.5}$$

  where Q is the unique element of $X_1 \times \cdots \times X_k$. Furthermore, Q is a-consistent;

- *setting α_{pre} to be the number of integers i satisfying $k_{\mathrm{gap}}/2 \leq i \leq k_{\mathrm{gap}}$, we have for all elements $w \in V_{a,2} \setminus \langle R \rangle$ and all $j \in \mathbb{F}_2$*

$$\left| \left| \left\{ i \in [r] : \frac{k_{\mathrm{gap}}}{2} \leq i \leq k_{\mathrm{gap}} \text{ and } \pi_i(w) = j \right\} \right| - \frac{\alpha_{\mathrm{pre}}}{2} \right| \leq \frac{k_{\mathrm{gap}}}{\log \log \log N} \tag{8.6}$$

  and

$$\left| |\{ i \in [r] : k_{\mathrm{gap}} < i \leq 2k_{\mathrm{gap}} \text{ and } \pi_i(w) = j \}| - \frac{k_{\mathrm{gap}}}{2} \right| \leq \frac{k_{\mathrm{gap}}}{\log \log \log N}. \tag{8.7}$$

Equation (8.6) and equation (8.7) give us very fine control over $V_{a,2}$ as the following lemma shows, see also [8, Lemma 6.9].

Lemma 8.5. *Suppose that $a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2$ is (N, m)-generic for a box X. Suppose that $w_1, \ldots, w_d, R \in V_{a,2}$ are linearly independent. Then we have for all $\mathbf{v} \in \mathbb{F}_2^d$*

$$\left| \left| \left\{ i \in [r] : \frac{k_{\mathrm{gap}}}{2} \leq i \leq k_{\mathrm{gap}} \text{ and } \pi_i(w_j) = \pi_j(\mathbf{v}) \text{ for all } 1 \leq j \leq d \right\} \right| - \frac{\alpha_{\mathrm{pre}}}{2^d} \right| \leq \frac{3^d \cdot k_{\mathrm{gap}}}{\log \log \log N}$$

and similarly

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

Proof. Let us prove the first part by induction on d, the second part follows using the same argument. For $d = 0$ the statement follows immediately from the definition of α_{pre}, while for $d = 1$ the statement falls as a consequence of equation (8.6). Now suppose that $d > 1$ and define for $\mathbf{w} \in \mathbb{F}_2^d$

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

Let $\mathbf{v} \in \mathbb{F}_2^d$ be given and define $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ as the unique unordered triple of distinct vectors that have the same projection as $\mathbf{v}$ on the first $d-2$ coordinates but are not equal to $\mathbf{v}$. We have the inequalities

$$2\left| f(\mathbf{v}) - \frac{\alpha_{\mathrm{pre}}}{2^d} \right| \leq \left| \left(\sum_{i=1}^{3} f(\mathbf{v}) + f(\mathbf{v}_i) \right) - \frac{3\alpha_{\mathrm{pre}}}{2^{d-1}} \right| + \left| \frac{\alpha_{\mathrm{pre}}}{2^{d-2}} - f(\mathbf{v}) - \sum_{i=1}^{3} f(\mathbf{v}_i) \right|$$

$$\leq \left(\sum_{i=1}^{3} \left| f(\mathbf{v}) + f(\mathbf{v_i}) - \frac{\alpha_{\mathrm{pre}}}{2^{d-1}} \right| \right) + \left| \frac{\alpha_{\mathrm{pre}}}{2^{d-2}} - f(\mathbf{v}) - \sum_{i=1}^{3} f(\mathbf{v}_i) \right|$$

$$\leq \frac{(3 \cdot 3^{d-1} + 3^{d-2}) \cdot k_{\mathrm{gap}}}{\log \log \log N},$$

where the last inequality follows from the induction hypothesis applied to $w_1, \ldots, w_{d-2}$ and $w_1, \ldots, w_{d-2}, w$ with $w \in \{w_{d-1}, w_d, w_{d-1} + w_d\}$. $\qquad \square$

Instead of controlling the 2^k-ranks of the narrow class group, we will control the full Artin pairing of the narrow class group, which is a finer invariant than just the sequence of 2^k-ranks. We will make this precise in our next definition.

Definition 8.6. *Let X be a box and let $a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2$. A sequence of bilinear pairings $\{\mathrm{Art}_i : A_i \times B_i \to \mathbb{F}_2\}_{2 \leq i < m}$, is called valid if*

- *$A_2 = B_2 = V_{a,2}$;*

- *the left kernel of Art_i is A_{i+1} and the right kernel of Art_i is B_{i+1} for $2 \leq i < m-1$;*

- *R is in the right kernel of Art_i for $2 \leq i < m$.*

The sequence is called Pellian if furthermore R is in the left kernel of Art_i for all $2 \leq i < m$. For such a sequence of bilinear pairings, we define A_m to be the left kernel of Art_{m-1} and B_m to be the right kernel of Art_{m-1}.

Meanwhile for $x \in X$, we get for every integer $k \geq 1$ a pairing

$$\mathrm{Art}_{k,x} : 2^{k-1}\mathrm{Cl}(\mathbb{Q}(\sqrt{x}))[2^k] \times 2^{k-1}\mathrm{Cl}^{\vee}(\mathbb{Q}(\sqrt{x}))[2^k] \to \mathbb{F}_2,$$

see Subsection 2.3. Genus theory gives natural surjections $\mathbb{F}_2^r \to \mathrm{Cl}(\mathbb{Q}(\sqrt{x}))[2]$ and $\mathbb{F}_2^r \to \mathrm{Cl}^{\vee}(\mathbb{Q}(\sqrt{x}))[2]$. More explicitly, the map $\mathbb{F}_2^r \to \mathrm{Cl}(\mathbb{Q}(\sqrt{x}))[2]$ is given by

$$(e_1, \ldots, e_r) \mapsto \mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}} \left(\prod_{i=1}^{r} p_i^{e_i} \right)$$

and the map $\mathbb{F}_2^r \to \mathrm{Cl}^{\vee}(\mathbb{Q}(\sqrt{x}))[2]$ is given by

$$(e_1, \ldots, e_r) \mapsto \sum_{i=1}^{r} e_i \chi_{p_i},$$

where $x = p_1 \cdot \ldots \cdot p_r$ with $p_1 < \cdots < p_r$. Pulling back, this induces a pairing

$$\mathbb{F}_2^r \times \mathbb{F}_2^r \to \mathbb{F}_2,$$

and for $x \in X(a)$ the left and right kernel both equal $V_{a,2}$. Then we get natural surjections $V_{a,2} \to 2\mathrm{Cl}(\mathbb{Q}(\sqrt{x}))[4]$ and $V_{a,2} \to 2\mathrm{Cl}^{\vee}(\mathbb{Q}(\sqrt{x}))[4]$ and hence a pairing

$$V_{a,2} \times V_{a,2} \to \mathbb{F}_2.$$

Continuing this process gives for each $x \in X(a)$ a valid sequence of Artin pairings, which we will also call $\mathrm{Art}_{k,x}$. Furthermore, the negative Pell equation is soluble for x if and only if its sequence of Artin pairings is Pellian.

We then define for a sequence of valid Artin pairings $\{\mathrm{Art}_i\}_{2 \leq i < m}$

$$X(a, \{\mathrm{Art}_i\}_{2 \leq i < m}) := \{x \in X(a) : \text{ the Artin pairing of } x \text{ equals } \{\mathrm{Art}_i\}_{2 \leq i < m}\}.$$

We will now reduce to the case where $a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2$ is (N, m)-generic for X and the first $m - 1$ Artin pairings are given. The next theorem essentially says that the Artin pairing is a random pairing on $A_m \times B_m$ except that R must always be in the right kernel.

Theorem 8.7. *There are real numbers $A, N_0 > 0$ such that for all reals $N > N_0$, all integers $m \geq 3$, all integers r satisfying equation (7.4), all integers $0 \leq k \leq r$, all excellent (N, k, r)-boxes X, all (N, m)-generic $a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2$ for X, all Pellian sequences of Artin pairings $\{\mathrm{Art}_k\}_{2 \leq k < m}$ and all Artin pairings $\mathrm{Art}_m : A_m \times B_m \to \mathbb{F}_2$ with R in the right kernel*

$$\left| |X(a, \{\mathrm{Art}_k\}_{2 \leq k \leq m})| - \frac{|X(a, \{\mathrm{Art}_k\}_{2 \leq k < m})|}{2^{\dim_{\mathbb{F}_2} A_m \cdot (-1 + \dim_{\mathbb{F}_2} A_m)}} \right| \leq \frac{A \cdot |X(a)|}{(\log \log \log \log N)^{\frac{100c}{m6^m}}}.$$

Proof that Theorem 8.7 implies Theorem 8.2. We claim that there exists an absolute constant $A' > 0$ such that

$$\sum_{\substack{a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2 \\ a \text{ not } (N,m)\text{-generic}}} |X(a)| \leq A' \cdot |X| \cdot 2^{\frac{-2c \log \log \log \log \log N}{m^2 6^m}}. \tag{8.8}$$

As a first step, we estimate

$$\sum_{\substack{a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2 \\ (8.5) \text{ fails for some } j > k}} |X(a)|. \tag{8.9}$$

For every $j > k$ we define an equivalence relation $\sim_j$ by setting $a \sim_j a'$ if and only if $a(i, j) = a'(i, j)$ for all $1 \leq i \leq k$. Note that if $a \sim_j a'$, then equation (8.5) fails for a if and only if it fails for a'. By our choice of C_0, D_1 and equation (7.1), we see that

$$k \leq \frac{1}{5} \log \log \log N$$

for N sufficiently large. Hence $\sim_j$ has at most

$$2^k \leq 2^{\frac{1}{5} \log \log \log N}$$

equivalence classes. Furthermore, in a given equivalence class we have the trivial bound

$$\left| \bigcup_{\substack{a \sim_j a' \\ |X_j(a',Q)| \leq \frac{|X|}{(\log s_{k+1})^{100}}}} X(a) \right| \leq \frac{|X|}{(\log s_{k+1})^{100}}.$$

81

Summing over all $j > k$ and summing over all equivalence classes gives the desired estimate for equation (8.9).

We return to bounding equation (8.8), and thanks to our upper bound for equation (8.9), it suffices to bound the union of $|X(a)|$ for a failing equation (8.4), equation (8.6) or equation (8.7). If σ is a permutation of $[r]$, then we recall that

$$\sigma(a)(i,j) = a(\sigma^{-1}(i), \sigma^{-1}(j)).$$

Note that a satisfies equation (8.4) if and only if $\sigma(a)$ does.

Take k_2 to be the largest integer smaller than $k_{\mathrm{gap}}/2$ and suppose that σ is a permutation of $[r]$ fixing all indices greater than k_2: recall that $\mathcal{P}_r(k_2)$ denotes the set of such permutations. For any such permutation σ, we have that a satisfies equation (8.6) if and only if $\sigma(a)$ does, and similarly for equation (8.7). We apply Proposition 7.8 to obtain

$$\sum_{a:M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2} \left| \frac{k_2! \cdot |X|}{2^{|M_r|+|M_{r,\varnothing}|}} - \sum_{\sigma \in \mathcal{P}_r(k_2)} |X(\sigma(a))| \right| \leq \frac{k_2! \cdot |X|}{k_2^{b_1}} \leq \frac{k_2! \cdot |X|}{(\log\log N)^{b_1 b_2}} \tag{8.10}$$

for some absolute constants $b_1, b_2 > 0$. Here we used equation (7.4) to obtain the lower bound $k_2 \geq (\log\log N)^{b_2}$ for N sufficiently large. We will now give an upper bound for

$$\frac{|\{a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2 : a \text{ fails equation (8.4) or (8.6) or (8.7)}\}|}{|\{a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2\}|}. \tag{8.11}$$

Note that this is an entirely combinatorial problem about certain symmetric $r \times r$ matrices. Once this is done, equation (8.10) will give the desired upper bound for equation (8.8).

After dropping a row and a column from $A(a)$, we see that $A(a)$ is a random symmetric matrix. By the explicit formulas for the number of symmetric matrices with a given rank in [34], we see that the proportion of $a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2$ with $\dim_{\mathbb{F}_2} V_{a,2} > n_{\max}$ is bounded by

$$O\left(2^{\frac{-2c \log\log\log\log\log N}{m^2 6^m}}\right),$$

which disposes with the a failing equation (8.4).

Next we bound the proportion of $a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2$ failing equation (8.6), a similar argument works for equation (8.7). The proportion of $w \in \mathbb{F}_2^r$ with

$$\left| \left| \left\{ i \in [r] : \frac{k_{\mathrm{gap}}}{2} \leq i \leq k_{\mathrm{gap}} \text{ and } \pi_i(w) = j \right\} \right| - \frac{\alpha_{\mathrm{pre}}}{2} \right| > \frac{k_{\mathrm{gap}}}{\log\log\log N} \tag{8.12}$$

is bounded by

$$O\left(e^{-(\log\log\log N)^{-2} \cdot k_{\mathrm{gap}}}\right)$$

thanks to Hoeffding's inequality. For any given $w \in \mathbb{F}_2^r \setminus \langle R \rangle$ we have that the proportion of $a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2$ with $w \in V_{a,2}$ is bounded by $O(2^{-r})$. Using this for all $w \in \mathbb{F}_2^r \setminus \langle R \rangle$ satisfying equation (8.12) then shows that the proportion of $a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2$ failing equation (8.6) is also bounded by

$$O\left(e^{-(\log\log\log N)^{-2} \cdot k_{\mathrm{gap}}}\right).$$

Since $k_{\text{gap}} > r^{1/2}/2$, it follows from equation (7.4) that this fits in the error term. We conclude that equation (8.11) is bounded by

$$A_1 \cdot 2^{\frac{-2c \log \log \log \log \log N}{m^2 6^m}}$$

for some absolute constant $A_1 > 0$. Then equation (8.10) implies that there exists an absolute constant $A_2 > 0$ such that

$$\sum_{\substack{a: M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2 \\ a \text{ not } (N,m)\text{-generic}}} |X(a)| \leq A_2 \cdot |X| \cdot 2^{\frac{-2c \log \log \log \log \log N}{m^2 6^m}}.$$

Therefore we have established the claimed equation (8.8). To complete the proof of the reduction step, we split X as the union over $X(a)$, removing all a that are not (N,m)-generic. For the a that are (N,m)-generic, we split each $X(a)$ over all sequences of Artin pairings and use Theorem 8.7. Observe that there are at most

$$2^{m(\dim_{\mathbb{F}_2} V_{a,2})^2} \leq 2^{mn_{\max}^2}$$

sequences of Artin pairings. By the choice of $n_{\max}$, we complete the proof of the reduction step. $\qquad\square$

The next reduction step is a straightforward application of orthogonality of characters.

Theorem 8.8. *There are real numbers $A, N_0 > 0$ such that for all reals $N > N_0$, all integers $m \geq 3$, all integers r satisfying equation (7.4), all integers $0 \leq k \leq r$, all excellent (N,k,r)-boxes X, all (N,m)-generic $a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2$ for X, all Pellian sequences of Artin pairings $\{\text{Art}_k\}_{2 \leq k < m}$ and all non-trivial linear maps $F : \{A_m \times B_m \to \mathbb{F}_2$ bilinear with R in the right kernel$\} \to \mathbb{F}_2$*

$$\left| \sum_{x \in X(a, \{\text{Art}_k\}_{2 \leq k < m})} \iota(F(\text{Art}_{m,x})) \right| \leq \frac{A \cdot |X(a)|}{(\log \log \log \log N)^{\frac{100c}{m6^m}}}.$$

The plan is to fix all but m or $m+1$ indices of the box X, and then apply the algebraic and combinatorial results from Sections 5 and 6. The indices of the box that we do not fix are called *variable indices*. We now lay out exactly what properties we demand from these variable indices as a function of F.

Definition 8.9. *Define for $2 \leq i \leq m$*

$$C_i := A_i \cap B_i, \quad d_i := -1 + \dim_{\mathbb{F}_2} C_i, \quad n_i := -1 + \dim_{\mathbb{F}_2} A_i.$$

Pick a basis $v_1, \ldots, v_{n_m}, R$ of A_m and a basis $w_1, \ldots, w_{n_m}, R$ of B_m such that

$$v_i = w_i \text{ for all } 1 \leq i \leq d_m.$$

Hence $v_1, \ldots, v_{d_m}, R$ is a basis of C_m. We extend the basis $w_1, \ldots, w_{n_m}, R$ of B_m to a basis

$$w_1, \ldots, w_{n_2}, R$$

of $V_{a,2}$ such that $w_1, \ldots, w_{n_i}, R$ is a basis of B_i for all $2 \leq i \leq m$. Write $\mathrm{Mat}(a, b, K)$ for the set of $a \times b$ matrices over a field K. Using our basis, $\mathrm{Art}_{m,x}$ is naturally an element of $\mathrm{Mat}(n_m + 1, n_m + 1, \mathbb{F}_2)$. More precisely, the entry (i, j) of the associated matrix is

$$\mathrm{Art}_{m,x}(v_i, w_j)$$

for $i, j \in [n_m]$, and we use the last row and column for the pairing with R. Since R is in the right kernel of $\mathrm{Art}_{m,x}$, we shall from now on implicitly view $\mathrm{Art}_{m,x}$ also as an element of $\mathrm{Mat}(n_m + 1, n_m, \mathbb{F}_2)$.

Let E_{j_3, j_4} be the matrix with a 1 on the entry (j_3, j_4) and 0 everywhere else. Define $F_{j_1, j_2} : \mathrm{Mat}(n_m + 1, n_m, \mathbb{F}_2) \to \mathbb{F}_2$ be the unique linear map that sends the matrix E_{j_3, j_4} to 1 if and only if $j_1 = j_3$ and $j_2 = j_4$. Then we can write write any linear map $F : \mathrm{Mat}(n_m + 1, n_m, \mathbb{F}_2) \to \mathbb{F}_2$ as

$$F = \sum_{\substack{1 \leq j_1 \leq n_m + 1 \\ 1 \leq j_2 \leq n_m}} c_{j_1, j_2} F_{j_1, j_2}, \quad c_{j_1, j_2} \in \mathbb{F}_2.$$

For every non-trivial map F, we pick a pair (j_1, j_2) satisfying $c_{j_1, j_2} = 1$ according to the following rules. In case there exists (j_1, j_2) such that $c_{j_1, j_2} = 1$, such that $j_1 \leq n_m$ and such that one of the following three conditions is satisfied

- $n_m \geq j_1 > d_m$ or

- $n_m \geq j_2 > d_m$ or

- $1 \leq j_1, j_2 \leq d_m$ and $c_{j_2, j_1} = 0$,

then we fix such a choice of (j_1, j_2). We say that we are in case I. If there is no such pair (j_1, j_2), but we have $c_{n_m + 1, j} = 1$ for some j, then we fix a choice of $(j_1, j_2) = (n_m + 1, j)$ and we say that we are in case II. Again if there is no such pair (j_1, j_2), but we have $c_{j,j} = 1$ for some j, then we fix $(j_1, j_2) = (j, j)$ and we say that we are in case III. Finally, in the remaining cases we fix a pair (j_1, j_2) with $j_1 \neq j_2$ and $c_{j_1, j_2} = c_{j_2, j_1} = 1$ and we say that we are in case IV. Observe that we can always find such a pair (j_1, j_2) since F is assumed to be non-trivial.

We say that a subset S of the integers is a set of variable indices for a non-trivial linear map $F : \mathrm{Mat}(n_m + 1, n_m, \mathbb{F}_2) \to \mathbb{F}_2$ if the following properties are satisfied

- if we are in case I, then we demand that S contains $m + 1$ elements of which $m - 1$ elements are contained in

$$\{k_{\mathrm{gap}}/2 \leq i \leq k_{\mathrm{gap}}\} \cap \bigcap_{l=1}^{n_2} \{i \in [r] : \pi_i(w_l) = 0\},$$

one element is contained in the intersection of $\{k_{\mathrm{gap}}/2 \leq i \leq k_{\mathrm{gap}}\}$ with

$$\bigcap_{\substack{1 \leq l \leq n_m \\ j_2 \leq d_m \Rightarrow l \neq j_2}} \{i \in [r] : \pi_i(v_l) = 0\} \cap \bigcap_{\substack{1 \leq l \leq n_m \\ l \neq j_2}} \{i \in [r] : \pi_i(w_l) = 0\} \cap \{i \in [r] : \pi_i(w_{j_2}) = 1\},$$

and one element is contained in the intersection of $\{k_{\mathrm{gap}} < i \leq 2k_{\mathrm{gap}}\}$ with

$$\bigcap_{\substack{1 \leq l \leq n_m \\ l \neq j_1}} \{i \in [r] : \pi_i(v_l) = 0\} \cap \bigcap_{\substack{1 \leq l \leq n_m \\ j_1 \leq d_m \Rightarrow l \neq j_1}} \{i \in [r] : \pi_i(w_l) = 0\} \cap \{i \in [r] : \pi_i(v_{j_1}) = 1\};$$

- *if we are in case II, then we pick S such that $|S| = m$, of which $m-1$ are contained in*

$$\{k_{\mathrm{gap}}/2 \leq i \leq k_{\mathrm{gap}}\} \cap \bigcap_{l=1}^{n_2}\{i \in [r] : \pi_i(w_l) = 0\}$$

and one element is contained in the intersection of $\{k_{\mathrm{gap}} < i \leq 2k_{\mathrm{gap}}\}$ with

$$\bigcap_{\substack{1 \leq l \leq n_m \\ j_2 \leq d_m \Rightarrow l \neq j_2}} \{i \in [r] : \pi_i(v_l) = 0\} \cap \bigcap_{\substack{1 \leq l \leq n_m \\ l \neq j_2}} \{i \in [r] : \pi_i(w_l) = 0\} \cap \{i \in [r] : \pi_i(w_{j_2}) = 1\};$$

- *if we are in case III, recall that $j = j_1 = j_2$. We choose S such that $|S| = m$, of which $m-1$ are contained in*

$$\{k_{\mathrm{gap}}/2 \leq i \leq k_{\mathrm{gap}}\} \cap \bigcap_{\substack{l=1 \\ l \neq j}}^{n_2}\{i \in [r] : \pi_i(w_l) = 0\} \cap \{i \in [r] : \pi_i(w_j) = 1\},$$

and one element is contained in

$$\{k_{\mathrm{gap}} < i \leq 2k_{\mathrm{gap}}\} \cap \bigcap_{l=1}^{n_m}\{i \in [r] : \pi_i(v_l) = \pi_i(w_l) = 0\};$$

- *if we are in case IV, then we pick S such that $|S| = m$, of which $m-1$ are contained in*

$$\{k_{\mathrm{gap}}/2 \leq i \leq k_{\mathrm{gap}}\} \cap \bigcap_{\substack{l=1 \\ l \neq j_2}}^{n_2} \{i \in [r] : \pi_i(w_l) = 0\} \cap \{i \in [r] : \pi_i(w_{j_2}) = 1\},$$

and one element is contained in the intersection of $\{k_{\mathrm{gap}} < i \leq 2k_{\mathrm{gap}}\}$ with

$$\bigcap_{\substack{l=1 \\ l \neq j_1}}^{n_m}\{i \in [r] : \pi_i(v_l) = \pi_i(w_l) = 0\} \cap \{i \in [r] : \pi_i(v_{j_1}) = 1\}.$$

Define i_{Cheb} to be the unique element of $S \cap \{k_{\mathrm{gap}} < i \leq 2k_{\mathrm{gap}}\}$.

Note that we may always assume that

$$m < \log\log\log\log\log\log N, \tag{8.13}$$

since otherwise Theorem 8.1 is trivially true. Then Lemma 8.5 shows that for every non-trivial bilinear map F we can find a set of variable indices S for F, provided that we take N sufficiently large. For the final reduction step of this subsection, we fix all primes before k_{gap} except those in S. For a point $Q \in \prod_{i \in [k_{\mathrm{gap}}] - S} X_i$, define $X(a, Q, \{\mathrm{Art}_k\}_{2 \leq k < m})$ to be the subset of $x \in X(a, \{\mathrm{Art}_k\}_{2 \leq k < m})$ for which $\pi_{[k_{\mathrm{gap}}] - S}(x) = Q$.

Theorem 8.10. *There are real numbers $A, N_0 > 0$ such that for all reals $N > N_0$, all integers $m \geq 3$, all integers r satisfying equation (7.4), all integers $0 \leq k \leq r$, all excellent (N, k, r)-boxes X, all (N, m)-generic $a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2$ for X, all Pellian sequences of Artin pairings*

$\{\mathrm{Art}_k\}_{2 \leq k < m}$, *all non-trivial linear maps* $F : \mathrm{Mat}(n_m + 1, n_m, \mathbb{F}_2) \to \mathbb{F}_2$, *all variable indices* S *for* F *and all a-consistent* $Q \in \prod_{i \in [k_{\mathrm{gap}}] - S} X_i$ *such that*

$$|X_j(a, Q)| \geq 4^{-m \cdot k_{\mathrm{gap}}} \cdot |X_j| \tag{8.14}$$

for all $j \in S \cap [k_{\mathrm{gap}}]$, *we have*

$$\left| \sum_{x \in X(a, Q, \{\mathrm{Art}_k\}_{2 \leq k < m})} \iota(F(\mathrm{Art}_{m,x})) \right| \leq \frac{A \cdot |X(a, Q)|}{(\log \log \log \log N)^{\frac{100c}{m6^m}}}.$$

Proof that Theorem 8.10 implies Theorem 8.8. First, we use the triangle inequality

$$\left| \sum_{x \in X(a, \{\mathrm{Art}_k\}_{2 \leq k < m})} \iota(F(\mathrm{Art}_{m,x})) \right| \leq \sum_{Q \in \prod_{i \in [k_{\mathrm{gap}}] - S} X_i} \left| \sum_{x \in X(a, Q, \{\mathrm{Art}_k\}_{2 \leq k < m})} \iota(F(\mathrm{Art}_{m,x})) \right|.$$

In case Q satisfies equation (8.14), the desired upper bound follows immediately from Theorem 8.10. It remains to bound

$$\sum_{\substack{Q \in \prod_{i \in [k_{\mathrm{gap}}] - S} X_i \\ Q \text{ fails equation (8.14)}}} \left| \sum_{x \in X(a, Q, \{\mathrm{Art}_k\}_{2 \leq k < m})} \iota(F(\mathrm{Art}_{m,x})) \right| \leq \sum_{\substack{Q \in \prod_{i \in [k_{\mathrm{gap}}] - S} X_i \\ Q \text{ fails equation (8.14)}}} |X(a, Q)|.$$

Let Q' be the unique element of $X_1 \times \cdots \times X_k$ and let X' be the product space

$$\prod_{i \in [k_{\mathrm{gap}}] - S - [k]} X_i(a, Q').$$

We apply Proposition 7.6 to (X', Q') to deduce that the number of a-consistent elements $Q \in \prod_{i \in [k_{\mathrm{gap}}] - S} X_i(a, Q')$ is bounded by

$$\frac{2 \cdot |X'|}{2^{\frac{(k_{\mathrm{gap}} - |S| - k)(k_{\mathrm{gap}} - |S| - k - 1)}{2}}}.$$

Note that condition (*iii*) of Proposition 7.6 is satisfied thanks to equation (8.5). Let us now bound $|X(a, Q)|$ for each individual Q. Since Q fails equation (8.14), we have

$$\prod_{i \in S \cap [k_{\mathrm{gap}}]} |X_i(a, Q)| \leq \frac{\prod_{i \in S \cap [k_{\mathrm{gap}}]} |X_i|}{4^{m \cdot k_{\mathrm{gap}}}} \leq \frac{\prod_{i \in S \cap [k_{\mathrm{gap}}]} |X_i(a, Q')|}{4^{m \cdot k_{\mathrm{gap}}}} \cdot (\log s_{k+1})^{100m}.$$

Therefore

$$|X(a, Q)| \leq \frac{\prod_{i \in S} |X_i(a, Q')|}{4^{m \cdot k_{\mathrm{gap}}}} \cdot (\log s_{k+1})^{100m} \cdot \max_{P \in \prod_{i \in S} X_i} X(a, P \times Q).$$

But for $i > k_{\mathrm{gap}}$, we apply the Chebotarev density theorem to obtain

$$|X_i(a, P \times Q)| = \frac{|X_i(a, Q')|}{2^{k_{\mathrm{gap}} - k}} \cdot \left(1 + O\left(e^{-k_{\mathrm{gap}}}\right)\right).$$

86

We apply Proposition 7.6 to

$$(X, P) \leftarrow \left(\prod_{i \in [r] - [k_{\text{gap}}]} X_i(a, P \times Q), \varnothing \right), \quad k \leftarrow r - k_{\text{gap}}$$

to deduce that

$$\left| |X(a, P \times Q)| - \frac{\prod_{i > k_{\text{gap}}} |X_i(a, P \times Q)|}{2^{\frac{(r - k_{\text{gap}})(r - k_{\text{gap}} - 1)}{2}}} \right| \leq \frac{\prod_{i > k_{\text{gap}}} |X_i(a, P \times Q)|}{\log N \cdot 2^{\frac{(r - k_{\text{gap}})(r - k_{\text{gap}} - 1)}{2}}}.$$

We conclude that

$$\sum_{\substack{Q \in \prod_{i \in [k_{\text{gap}}] - S} X_i \\ Q \text{ fails equation (8.14)}}} |X(a, Q)| \leq$$

$$\frac{4 \cdot (\log s_{k+1})^{100m} \cdot \prod_{i \in [r] - [k]} |X_i(a, Q')|}{2^{\frac{(k_{\text{gap}} - k - |S|)(k_{\text{gap}} - k - |S| - 1)}{2}} \cdot 4^{m \cdot k_{\text{gap}}} \cdot 2^{(k_{\text{gap}} - k) \cdot (r - k_{\text{gap}}) + \frac{(r - k_{\text{gap}})(r - k_{\text{gap}} - 1)}{2}}}. \quad (8.15)$$

A final application of Proposition 7.6 to the prebox

$$\left(\prod_{i \in [r] - [k]} X_i(a, Q'), Q' \right)$$

shows that

$$2|X(a)| \geq \frac{\prod_{i \in [r] - [k]} |X_i(a, Q')|}{2^{(r - k)(r - k - 1)}}. \quad (8.16)$$

The proposition follows from equations (8.15) and (8.16). $\qquad \square$

8.3 A second moment computation

We have now arrived at a critical point of the proof. We have a rather unstructured set $X(a, Q, \{\text{Art}_k\}_{2 \leq k < m})$. To make matters even worse, we do not know yet that the expansion maps exist to apply our algebraic theorems. We will cover $X(a, Q, \{\text{Art}_k\}_{2 \leq k < m})$ by small product spaces and then use a second moment trick to reduce to such product spaces. We will then be able to apply the algebraic and combinatorial results from the previous sections.

Definition 8.11. *Let N, m, k, r, X, a, Q, $\{\text{Art}_k\}_{2 \leq k < m}$, F and S be as above. Put*

$$M_{\text{box}} := \left\lfloor (\log \log \log \log N)^{\frac{1}{5(m+1)}} \right\rfloor.$$

It follows from equation (8.13) that $M_{\text{box}} \geq 2$ for sufficiently large N. Define

$$S' := S \cap [k_{\text{gap}}],$$

so that $S = S' \cup \{i_{\text{Cheb}}\}$. Let $Z_i \subseteq X_i$ for $i \in S'$ and put

$$Z := \prod_{i \in S'} Z_i.$$

We say that Z is a great product space if

- $|Z_i| = M_{\mathrm{box}}$ for all $i \in S'$;

- $Z_i \subseteq X_i(a, Q)$ for all $i \in S'$;

- we have for all $z \in Z$ and all distinct $i, j \in S'$

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

- if we are in case I, let i_{char} be the unique index in S' with $\pi_{i_{\mathrm{char}}}(w_{j_2}) = 1$. Then we want that for all subsets $T \subseteq S' - \{i_{\mathrm{char}}\}$, all $\bar{z} \in \mathrm{Cube}(Z, T \cup \{i_{\mathrm{char}}\})$, there exists an expansion map $\phi_{\pi_T(\bar{z}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{z}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{z}))}$, in which all primes in Q, (2) and ∞ split completely in case $T \subset S' - \{i_{\mathrm{char}}\}$. We put

$$M_\circ(Z) := \prod_{T \subset S' - \{i_{\mathrm{char}}\}} \prod_{\bar{z} \in \mathrm{Cube}(Z, T \cup i_{\mathrm{char}})} L(\phi_{\pi_T(\bar{z}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{z}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{z}))})$$

and

$$M(Z) := \prod_{\bar{z} \in \mathrm{Cube}(Z, S')} L(\phi_{\pi_{S' - \{i_{\mathrm{char}}\}}(\bar{z}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{z}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{z}))});$$

- if we are in case II, III or IV, we demand that for all subsets $T \subseteq S'$, all $\bar{z} \in \mathrm{Cube}(Z, T)$ and all $i \in T$, there exists an expansion map $\phi_{\pi_{T - \{i\}}(\bar{z}); \mathrm{pr}_1(\pi_i(\bar{z}))\mathrm{pr}_2(\pi_i(\bar{z}))}$ in which all primes in Q, (2) and ∞ split completely. Furthermore, for all subsets $T \subseteq S'$, all $\bar{z} \in \mathrm{Cube}(Z, T)$, there exists an expansion map $\phi_{\pi_T(\bar{z}); -1}$, in which all odd primes in Q and $\mathrm{Up}_{\mathbb{Q}(i)/\mathbb{Q}}(2)$ split completely in case $T \subset S'$. Set

$$M_\circ(Z) := \prod_{i \in S'} \prod_{\bar{z} \in \mathrm{Cube}(Z, S')} L(\phi_{\pi_{S' - \{i\}}(\bar{z}); \mathrm{pr}_1(\pi_i(\bar{z}))\mathrm{pr}_2(\pi_i(\bar{z}))}) \times \prod_{T \subset S'} \prod_{\bar{z} \in \mathrm{Cube}(Z, T)} L(\phi_{\pi_T(\bar{z}); -1})$$

and

$$M(Z) := \prod_{\bar{z} \in \mathrm{Cube}(Z, S')} L(\phi_{\pi_{S'}(\bar{z}); -1}).$$

For $i > k_{\mathrm{gap}}$, define $X_i(a, Q, M_\circ(Z))$ to be those primes $p \in X_i(a, Q)$ that split completely in $M_\circ(Z)$ and

$$\left(\frac{z}{p}\right) = \iota(a(j,i)) \text{ for all } j \in S' \text{ and all } z \in Z_j.$$

This is equivalent to Frob_p landing in a given central element of the Galois group of the compositum of $M_\circ(Z)$ and $\mathbb{Q}(\sqrt{z})$ with z equal to -1, a prime in Q or a prime in Z_j for some $j \in S'$. If Z is a great product space, we define

$$\widetilde{Z} := Q \times Z \times \prod_{i > k_{\mathrm{gap}}} X_i(a, Q, M_\circ(Z)).$$

The following lemma constructs an additive system that will aid us in producing expansion maps. Define

$$X_{\mathrm{pre}} := \prod_{i \in S'} X_i(a, Q).$$

Lemma 8.12. *Let $W \subseteq X_{\mathrm{pre}}$. Then there exists an additive system $(C_T, C_T^{\mathrm{acc}}, F_T, A_T)_{T \subseteq S'}$ on (X_{pre}, S') with the following properties*

- $C_\varnothing^{\mathrm{acc}} = W$;

- $|A_T| \le 2^{(|S'|+100) \cdot (k_{\mathrm{gap}} + |S'| + 100)}$ *for all $T \subseteq S'$;*

- *suppose that we are in case I. If $\bar{x} \in C_{S'}^{\mathrm{acc}}$, then there exists an expansion map*

$$\phi_{\pi_{S'-\{i_{\mathrm{char}}\}}(\bar{x}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{x}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{x}))}.$$

  Furthermore, for $i_{\mathrm{char}} \in T \subset S'$ and $\bar{x} \in C_T^{\mathrm{acc}}$, there exists an expansion map

$$\phi_{\pi_{T-\{i_{\mathrm{char}}\}}(\bar{x}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{x}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{x}))}$$

  in which all primes in Q, all primes in $\pi_{S'-T}(\bar{x})$, (2) and ∞ split completely;

- *suppose that we are in case II, III or IV. If $\bar{x} \in C_{S'}^{\mathrm{acc}}$, then $\phi_{\pi_{S'}(\bar{x}); -1}$ exists. Furthermore, all odd primes in Q, all primes in $\pi_{S'-T}(\bar{x})$ and $\mathrm{Up}_{\mathbb{Q}(i)/\mathbb{Q}}(2)$ split completely in $\phi_{\pi_T(\bar{x}); -1}$ for all $T \subset S'$ and $\bar{x} \in C_T^{\mathrm{acc}}$. Finally, we demand that for all $T \subseteq S'$, all $\bar{x} \in C_T^{\mathrm{acc}}$ and all $i \in T$, there exists an expansion map $\phi_{\pi_{T-\{i\}}(\bar{x}); \mathrm{pr}_1(\pi_i(\bar{x}))\mathrm{pr}_2(\pi_i(\bar{x}))}$ in which all primes in Q, all primes in $\pi_{S'-T}(\bar{x})$, (2) and ∞ split completely.*

Proof. Let us deal with case I, the other cases being analogous. Take $C_\varnothing = W$ and take $F_\varnothing$ to be the zero map. We will now inductively construct the maps F_T for T a non-empty subset of S', which determine the additive system. If $T = \{i\}$, we let $F_{\{i\}}$ be the map that sends $\bar{x} \in C_{\{i\}}$ to

$$\iota^{-1}\left(\frac{\mathrm{pr}_1(\pi_i(\bar{x}))\mathrm{pr}_2(\pi_i(\bar{x}))}{q}\right),$$

where q runs over all prime divisors of Q, all primes in $\pi_j(\bar{x})$ for $j \ne i$ and the prime (2). Now suppose that $|T| > 1$. If $i_{\mathrm{char}} \notin T$, we let F_T be the zero map. So suppose that $i_{\mathrm{char}} \in T$ and take $\bar{x} \in C_T$. From the induction hypothesis it follows that for all $T' \subset T$ there exists an expansion map

$$\phi_{\pi_{T'-\{i_{\mathrm{char}}\}}(\bar{x}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{x}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{x}))}$$

in which all primes in Q, all primes in $\pi_{S'-T'}(\bar{x})$, (2) and ∞ split completely. In particular, it follows from Proposition 2.16 that

$$\phi_{\pi_{T-\{i_{\mathrm{char}}\}}(\bar{x}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{x}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{x}))}$$

exists. Furthermore, we know that the Frobenius symbol of a prime in Q, a prime in $\pi_{S'-T}(\bar{x})$, (2) or ∞ lands in

$$Z(\mathrm{Gal}(L(\phi_{\pi_{T-\{i_{\mathrm{char}}\}}(\bar{x}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{x}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{x}))})/\mathbb{Q})) \cong \mathbb{F}_2.$$

Indeed, recall that $L(\phi_{\pi_{T-\{i_{\mathrm{char}}\}}(\bar{x}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{x}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{x}))})$ is a central $\mathbb{F}_2$-extension of

$$\mathbb{Q}\left(\left\{\sqrt{\mathrm{pr}_1(\pi_i(\bar{x}))\mathrm{pr}_2(\pi_i(\bar{x}))} : i \in T\right\}\right) \cdot \prod_{T' \subset T} L(\phi_{\pi_{T'-\{i_{\mathrm{char}}\}}(\bar{x}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{x}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{x}))})$$

by Proposition 2.14. Now let F_T be the map that sends $\bar{x} \in C_T$ to

$$\phi_{\pi_{T-\{i_{\mathrm{char}}\}}(\bar{x});\mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{x}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{x}))}(\mathrm{Frob}(q)),$$

where q is a prime divisor of Q, a prime in $\pi_{S'-T}(\bar{x})$, (2) or ∞. Since $\mathrm{Frob}(q)$ lands in the center, it follows from Lemma 2.13 that F_T satisfies equation (6.1). $\qquad\square$

Our next theorem is our final reduction step. We will reduce to spaces of the shape $X(a, Q, \{\mathrm{Art}_k\}_{2 \le k < m}) \cap \widetilde{Z}$ with Z a great product space.

Theorem 8.13. *There are real numbers $A, N_0 > 0$ such that for all reals $N > N_0$, all integers $m \ge 3$, all integers r satisfying equation (7.4), all integers $0 \le k \le r$, all excellent (N, k, r)-boxes X, all (N, m)-generic $a : M_r \sqcup M_{r,\varnothing} \to \mathbb{F}_2$ for X, all Pellian sequences of Artin pairings $\{\mathrm{Art}_k\}_{2 \le k < m}$, all non-trivial linear maps $F : \mathrm{Mat}(n_m + 1, n_m, \mathbb{F}_2) \to \mathbb{F}_2$, all variable indices S for F, all a-consistent $Q \in \prod_{i \in [k_{\mathrm{gap}}]-S} X_i$ and all great product spaces Z*

$$\left| \sum_{x \in X(a, Q, \{\mathrm{Art}_k\}_{2 \le k < m}) \cap \widetilde{Z}} \iota(F(\mathrm{Art}_{m,x})) \right| \le \frac{A \cdot |X(a, Q) \cap \widetilde{Z}|}{(\log \log \log \log N)^{\frac{100c}{m6^m}}}.$$

Proof that Theorem 8.13 implies Theorem 8.10. We set

$$R := \left\lfloor e^{e^{\frac{k_{\mathrm{gap}}}{5}}} \right\rfloor$$

and we let Z_{pre} be those $z \in X_{\mathrm{pre}}$ satisfying

$$\left(\frac{\pi_i(z)}{\pi_j(z)} \right) = \iota(a(i, j)) \text{ for all distinct } i, j \in S'.$$

Choose a sequence $Z_1, \ldots, Z_t$ of maximal length satisfying the following properties

- each $Z_i \subseteq Z_{\mathrm{pre}}$ is a great product space;
- we have that $|Z_i \cap Z_j| \le 1$ for all distinct $i, j \in [t]$;
- every $z \in Z_{\mathrm{pre}}$ is in at most R of the Z_i.

Define $Z_{\mathrm{pre,bad}}$ to be the subset of $z \in Z_{\mathrm{pre}}$ that are in less than R of the Z_i and write δ for the density of $Z_{\mathrm{pre,bad}}$ in X_{pre}.

As a first step we aim to upper bound δ. By a straightforward greedy algorithm we can find a subset W of $Z_{\mathrm{pre,bad}}$ of density at least $\delta/RM_{\mathrm{box}}^m$ such that $|W \cap Z_i| \le 1$ for all $i \in [t]$. We apply Proposition 6.2 with the additive system from Lemma 8.12 with W equal to $C_\varnothing^{\mathrm{acc}}$. This shows that the density of $C_{S'}^{\mathrm{acc}}$ in $\mathrm{Cube}(X_{\mathrm{pre}}, S')$ is at least

$$\delta' := \left(\frac{\delta}{2^{(|S'|+100)\cdot(k_{\mathrm{gap}}+|S'|+100)}RM_{\mathrm{box}}^m} \right)^{3^m}.$$

Now given $x_0 \in W$, we define

$$W(x_0) = \{x \in W : c(x_0, x) \in C_{S'}^{\mathrm{acc}}\},$$

where $c(x_0, x)$ is the unique $\bar{x} \in \text{Cube}(X_{\text{pre}}, S')$ such that

$$\text{pr}_1(\pi_i(\bar{x})) = \pi_i(x_0), \quad \text{pr}_2(\pi_i(\bar{x})) = \pi_i(x).$$

There is a natural injective map from $C_{S'}^{\text{acc}}$ to the disjoint union of the $W(x_0)$ as x_0 runs through W. This map sends $\bar{x}$ to the unique pair $(w, x_0) \in W \times W$ satisfying

$$\pi_i(w) = \text{pr}_1(\pi_i(\bar{x})) \text{ for all } i \in S', \quad \pi_i(x_0) = \text{pr}_2(\pi_i(\bar{x})) \text{ for all } i \in S'.$$

Hence we deduce that

$$|C_{S'}^{\text{acc}}| \leq |X_{\text{pre}}| \cdot \max_{x_0 \in W} |W(x_0)|,$$

so that there exists x_0 such that the density of $W(x_0)$ in X_{pre} is at least δ'. Fix such a x_0. Now if we were to find subsets $W_i \subseteq X_i(a, Q)$ such that $|W_i| = M_{\text{box}}$ and

$$\prod_{i \in S'} W_i \subseteq W(x_0),$$

we could extend the sequence $Z_1, \ldots, Z_t$ to a longer sequence. Since this is impossible by our choice of $Z_1, \ldots, Z_t$, we apply the contrapositive of Lemma 6.3 to deduce that

$$5M_{\text{box}}^m > \frac{\log \min_{i \in S'} |X_i(a, Q)|}{\log \delta'^{-1}}.$$

It follows from equation (8.14) and equation (7.1) that

$$|X_i(a, Q)| \geq e^{e^{\frac{3}{10} k_{\text{gap}}}}$$

for N sufficiently large. We conclude that

$$\delta \leq e^{-\frac{1}{4} e^{k_{\text{gap}}}} \tag{8.17}$$

for N sufficiently large. Now we split

$$\left| \sum_{x \in X(a, Q, \{\text{Art}_k\}_{2 \leq k < m})} \iota(F(\text{Art}_{m,x})) \right| \leq \left| \sum_{\substack{x \in X(a, Q, \{\text{Art}_k\}_{2 \leq k < m}) \\ \pi_{S'}(x) \notin Z_{\text{pre,bad}}}} \iota(F(\text{Art}_{m,x})) \right| + \left| \sum_{\substack{x \in X(a, Q) \\ \pi_{S'}(x) \in Z_{\text{pre,bad}}}} 1 \right| \tag{8.18}$$

with the latter sum fitting in the error term by equation (8.17) and two applications of Proposition 7.6 (namely to $X(a, Q)$ and to the subset of $X(a, Q)$ projecting to a given element in $Z_{\text{pre, bad}}$). So it remains to deal with the former sum.

Now for $x \in X(a, Q)$ with $\pi_{S'}(x) \notin Z_{\text{pre,bad}}$, we write $\Lambda(x)$ for the number of $i \in [t]$ for which $x \in \widetilde{Z}_i$. We will compute the first and second moment of $\Lambda(x)$, and then use this to bring Theorem 8.13 into play. We have

$$\sum_{\substack{x \in X(a, Q) \\ \pi_{S'}(x) \notin Z_{\text{pre,bad}}}} \Lambda(x) = \sum_{\substack{z \in Z_{\text{pre}} \\ z \notin Z_{\text{pre,bad}}}} \sum_{\substack{x \in X(a, Q) \\ \pi_{S'}(x) = z}} \sum_{i \in [t]} \mathbf{1}_{x \in \widetilde{Z}_i}$$

$$= \sum_{\substack{z \in Z_{\text{pre}} \\ z \notin Z_{\text{pre,bad}}}} \sum_{i \in [t]} |X(a, Q) \cap \widetilde{Z}_i \cap \pi_{S'}^{-1}(z)|. \tag{8.19}$$

Fix some $z \in Z_{\mathrm{pre}} \setminus Z_{\mathrm{pre,bad}}$. Define

$$L(Q) := \mathbb{Q}(\{\sqrt{-1}\} \cup \{\sqrt{\pi_j(z)} : j \in S'\} \cup \{\sqrt{\pi_j(Q)} : j \in [k_{\mathrm{gap}}] - S'\}).$$

Write $d(M_{\mathrm{box}}, m)$ for the degree of $L(Q)M_\circ(\widetilde{Z}_i)$ over $L(Q)$. Crucially, $d(M_{\mathrm{box}}, m)$ does not depend on i by Lemma 6.8 and Lemma 6.10. Since our box X is Siegel-less, the Chebotarev density theorem [42, Proposition 6.5] yields for $i > k_{\mathrm{gap}}$

$$|X_i(a, Q, M_\circ(Z))| = \frac{|X_i(a, Q \times \{z\})|}{d(M_{\mathrm{box}}, m)} \left(1 + O\left(e^{-2k_{\mathrm{gap}}}\right)\right).$$

Here we use equation (8.3) and a well-known result of Heilbronn [23] to deal with potential Siegel zeroes. It follows from two applications of Proposition 7.6 to the preboxes

$$\left(\prod_{i \in [r] - [k_{\mathrm{gap}}]} X_i(a, Q \times \{z\}), \varnothing\right), \quad \left(\prod_{i \in [r] - [k_{\mathrm{gap}}]} X_i(a, Q, M_\circ(Z)), \varnothing\right)$$

that

$$|X(a, Q) \cap \widetilde{Z}_i \cap \pi_{S'}^{-1}(z)| = \mathbf{1}_{z \in Z_i} \cdot \frac{|X(a, Q) \cap \pi_{S'}^{-1}(z)|}{d(M_{\mathrm{box}}, m)^{r - k_{\mathrm{gap}}}} \left(1 + O\left(e^{-k_{\mathrm{gap}}}\right)\right).$$

Continuing the computation in equation (8.19) gives

$$\sum_{\substack{x \in X(a, Q) \\ \pi_{S'}(x) \notin Z_{\mathrm{pre,bad}}}} \Lambda(x) = \frac{R|X(a, Q)|}{d(M_{\mathrm{box}}, m)^{r - k_{\mathrm{gap}}}} \left(1 + O\left(e^{-k_{\mathrm{gap}}}\right)\right), \tag{8.20}$$

since every $z \in Z_{\mathrm{pre}} \setminus Z_{\mathrm{pre,bad}}$ is in precisely R of the Z_i. Having computed the first moment, we now consider the second moment

$$\sum_{\substack{x \in X(a, Q) \\ \pi_{S'}(x) \notin Z_{\mathrm{pre,bad}}}} \Lambda(x)^2.$$

For distinct i and j, we see that the assumption $|Z_i \cap Z_j| \leq 1$ gives that $L(Q)M_\circ(\widetilde{Z}_i)M_\circ(\widetilde{Z}_j)$ has degree $d(M_{\mathrm{box}}, m)^2$ over $L(Q)$ by Lemma 6.8 and Lemma 6.10. Then, following the first moment computation, we obtain

$$\sum_{\substack{x \in X(a, Q) \\ \pi_{S'}(x) \notin Z_{\mathrm{pre,bad}}}} \Lambda(x)^2 = \frac{R^2|X(a, Q)|}{d(M_{\mathrm{box}}, m)^{2(r - k_{\mathrm{gap}})}} \left(1 + O\left(e^{-k_{\mathrm{gap}}}\right)\right). \tag{8.21}$$

It follows from equation (8.20), equation (8.21) and Chebyshev's inequality that outside a set of density $O(e^{-k_{\mathrm{gap}}/2})$ in the set of $x \in X(a, Q)$ satisfying $\pi_{S'}(x) \notin Z_{\mathrm{pre,bad}}$, we have that

$$\left| \Lambda(x) - \frac{R}{d(M_{\mathrm{box}}, m)^{r - k_{\mathrm{gap}}}} \right| \leq \frac{Re^{\frac{-k_{\mathrm{gap}}}{4}}}{d(M_{\mathrm{box}}, m)^{r - k_{\mathrm{gap}}}}. \tag{8.22}$$

Recalling equation (8.18), it suffices to bound

$$\left| \sum_{\substack{x \in X(a,Q,\{\mathrm{Art}_k\}_{2 \le k < m}) \\ \pi_{S'}(x) \notin Z_{\mathrm{pre,bad}}}} \iota(F(\mathrm{Art}_{m,x})) \right|.$$

By the triangle inequality this is bounded by

$$\frac{d(M_{\mathrm{box}},m)^{r-k_{\mathrm{gap}}}}{R} \cdot \left| \sum_{i \in [t]} \sum_{x \in X(a,Q,\{\mathrm{Art}_k\}_{2 \le k < m}) \cap \widetilde{Z}_i} \iota(F(\mathrm{Art}_{m,x})) \right| +$$

$$\left| \sum_{\substack{x \in X(a,Q,\{\mathrm{Art}_k\}_{2 \le k < m}) \\ \pi_{S'}(x) \notin Z_{\mathrm{pre,bad}}}} \iota(F(\mathrm{Art}_{m,x})) - \frac{d(M_{\mathrm{box}},m)^{r-k_{\mathrm{gap}}}}{R} \sum_{i \in [t]} \sum_{x \in X(a,Q,\{\mathrm{Art}_k\}_{2 \le k < m}) \cap \widetilde{Z}_i} \iota(F(\mathrm{Art}_{m,x})) \right|.$$

$$(8.23)$$

It follows from Theorem 8.13 that the former sum is bounded by

$$A \cdot \frac{d(M_{\mathrm{box}},m)^{r-k_{\mathrm{gap}}}}{R \cdot (\log \log \log \log N)^{\frac{100c}{m6^m}}} \cdot \sum_{i \in [t]} |X(a,Q) \cap \widetilde{Z}_i|.$$

Now observe that

$$\sum_{i \in [t]} |X(a,Q) \cap \widetilde{Z}_i| \le \sum_{\substack{x \in X(a,Q) \\ \pi_{S'}(x) \notin Z_{\mathrm{pre,bad}}}} \Lambda(x) + \sum_{\substack{x \in X(a,Q) \\ \pi_{S'}(x) \in Z_{\mathrm{pre,bad}}}} R.$$

To bound the first term above, we use equation (8.20). For the second term, we use equation (8.17) and the argument immediately following equation (8.18).

Finally, to deal with the latter sum in equation (8.23), we first take care of the points projecting to an element in $Z_{\mathrm{pre,bad}}$. Then it remains to bound

$$\left| \sum_{\substack{x \in X(a,Q,\{\mathrm{Art}_k\}_{2 \le k < m}) \\ \pi_{S'}(x) \notin Z_{\mathrm{pre,bad}}}} \iota(F(\mathrm{Art}_{m,x})) - \frac{d(M_{\mathrm{box}},m)^{r-k_{\mathrm{gap}}}}{R} \sum_{i \in [t]} \sum_{\substack{x \in X(a,Q,\{\mathrm{Art}_k\}_{2 \le k < m}) \cap \widetilde{Z}_i \\ \pi_{S'}(x) \notin Z_{\mathrm{pre,bad}}}} \iota(F(\mathrm{Art}_{m,x})) \right|,$$

which is at most

$$\sum_{\substack{x \in X(a,Q,\{\mathrm{Art}_k\}_{2 \le k < m}) \\ \pi_{S'}(x) \notin Z_{\mathrm{pre,bad}}}} \left| 1 - \frac{d(M_{\mathrm{box}},m)^{r-k_{\mathrm{gap}}}}{R} \cdot \Lambda(x) \right|.$$

We split the above sum depending on whether x satisfies equation (8.22). To deal with the x failing equation (8.22), we use the trivial bound $\Lambda(x) \le R$. This completes the proof. $\qquad \square$

8.4 Finishing the proof

It remains to prove Theorem 8.13. The main technical input that we need is an additive system as in Proposition 6.6, which we will construct in the first part of the proof.

Proof of Theorem 8.13. For every non-zero $v \in V_{a,2}$ and for every $x \in X(a, Q)$, we choose a raw cocycle $(\psi_i(x, v))_{0 \le i \le t(x,v)}$ such that

$$\psi_1(x, v) = \sum_{\substack{1 \le j \le r \\ \pi_j(v)=1}} \chi_{\pi_j(x)}$$

with $t(x, v)$ maximal among the set of such raw cocycles. Recall that we fixed a basis

$$w_1, \ldots, w_{n_2}, R$$

of $V_{a,2}$ such that

$$w_1, \ldots, w_{n_i}, R$$

is a basis of B_i for all $2 \le i \le m$, where we recall that $n_i := -1 + \dim_{\mathbb{F}_2} B_i$ (we also set $n_1 := n_2$). We also remind the reader that we fixed a pair of integers (j_1, j_2) associated to the linear map $F : \mathrm{Mat}(n_m + 1, n_m, \mathbb{F}_2) \to \mathbb{F}_2$.

Desired properties of an additive system

We start the proof by constructing an additive system $\mathfrak{A} = (C_T, C_T^{\mathrm{acc}}, F_T, A_T)_{T \subseteq S}$ on $(\widetilde{Z}, S)$ such that

(a) $C_\varnothing^{\mathrm{acc}} = X(a, Q, \{\mathrm{Art}_k\}_{2 \le k < m}) \cap \widetilde{Z}$;

(b) $\mathfrak{A}$ is $(2^{(n_{\max}+10)(n_{\max}+2m+10)}, S)$-acceptable;

(c) suppose that we are in case *I*. Then we have for all $\bar{x} \in C(\mathfrak{A})$

$$(\Sigma F')(\bar{x}) = \phi_{\pi_{S'-\{i_{\mathrm{char}}\}}(\bar{x});\mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{x}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{x}))}(\mathrm{Frob}(\mathrm{pr}_1(\pi_{i_{\mathrm{Cheb}}}(\bar{x}))))+$$
$$\phi_{\pi_{S'-\{i_{\mathrm{char}}\}}(\bar{x});\mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{x}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{x}))}(\mathrm{Frob}(\mathrm{pr}_2(\pi_{i_{\mathrm{Cheb}}}(\bar{x})))),$$

where $F' : X(a, Q, \{\mathrm{Art}_k\}_{2 \le k < m}) \cap \widetilde{Z} \to \mathbb{F}_2$ is the function that sends x to $F(\mathrm{Art}_{m,x})$. If we are in case *II*, *III* or *IV*, then we have

$$(\Sigma F')(\bar{x}) = \phi_{\pi_{S'}(\bar{x});-1}(\mathrm{Frob}(\mathrm{pr}_1(\pi_{i_{\mathrm{Cheb}}}(\bar{x})))) + \phi_{\pi_{S'}(\bar{x});-1}(\mathrm{Frob}(\mathrm{pr}_2(\pi_{i_{\mathrm{Cheb}}}(\bar{x}))));$$

(d) suppose that we are in case *I*. Let $|T| < m$ and let $1 \le j \le n_{|T|+1}$. Denote by $\mathcal{W}$ the set $\{j_1, j_2\}$ if $j_1 \le d_m$ and $\{j_2\}$ otherwise. Then we further demand that $\bar{x} \in C_T^{\mathrm{acc}}$ implies that

- if $T \subseteq S' - \{i_{\mathrm{char}}\}$ or $j \le n_m$, we have

$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|}(x, w_j) = 0 \tag{8.24}$$

for $j \notin \mathcal{W}$;

- if $i_{\text{char}} \in T$, we have

$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|}(x, w_{j_2}) = \phi_{\pi_{T - \{i_{\text{char}}\}}(\bar{x}); \mathrm{pr}_1(\pi_{i_{\text{char}}}(\bar{x})) \mathrm{pr}_2(\pi_{i_{\text{char}}}(\bar{x}))}; \qquad (8.25)$$

- if $i_{\text{char}} \notin T$, we have

$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|}(x, w_{j_2}) = 0; \qquad (8.26)$$

- if $i_{\text{Cheb}} \notin T$ and $j_1 \in \mathcal{W}$, we have

$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|}(x, w_{j_1}) = 0; \qquad (8.27)$$

- if $T \neq \varnothing$, we have

$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|+1}(x, w_j)(\sigma_{\pi_i(\bar{x})}) = 0 \qquad (8.28)$$

for all $i \in S - T$.

If we are in case II, III or IV, take $\varnothing \subseteq T \subset S$ and $1 \leq j \leq n_{|T|+1}$. Now suppose that we are in case II. Then $\bar{x} \in C_T^{\text{acc}}$ implies that

- if $T \subseteq S'$ or $j \leq n_m$, we have

$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|}(x, w_j) = 0$$

for $j \neq j_2$;
- if $T \neq \varnothing$, we have

$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|+1}(x, w_j)(\sigma_{\pi_i(\bar{x})}) = 0$$

for $j \neq j_2$ and all $i \in S - T$;
- if $i_{\text{Cheb}} \notin T$, we have

$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|}(x, w_{j_2}) = 0;$$

- if $i_{\text{Cheb}} \notin T$ and $T \neq \varnothing$, we have

$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|+1}(x, w_{j_2})(\sigma_{\pi_i(\bar{x})}) = 0$$

for all $i \in S - T$.

Next we deal with case III. In this case we demand that $\bar{x} \in C_T^{\text{acc}}$ implies that

- if $T \subseteq S'$ or $j \leq n_m$, we have

$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|}(x, w_j) = 0$$

for $j \neq j_2$;

- if $T \neq \varnothing$, we have
$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|+1}(x, w_j)(\sigma_{\pi_i(\bar{x})}) = 0$$
for $j \neq j_2$ and all $i \in S - T$;
- if $i_{\text{Cheb}} \notin T$, we have
$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|}(x, w_{j_2} + R) = 0;$$
- if $i_{\text{Cheb}} \notin T$ and $T \neq \varnothing$, we have
$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|+1}(x, w_{j_2} + R)(\sigma_{\pi_i(\bar{x})}) = 0$$
for all $i \in S - T$.

Finally, suppose that we are in case IV. Then we will ensure that $\bar{x} \in C_T^{\text{acc}}$ implies that

- if $T \subseteq S'$ or $j \leq n_m$, we have
$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|}(x, w_j) = 0$$
for $j \notin \{j_1, j_2\}$. Furthermore, we have
$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|}(x, w_{j_1} + w_{j_2} + R) = 0;$$
- if $T \neq \varnothing$, we have
$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|+1}(x, w_j)(\sigma_{\pi_i(\bar{x})}) = 0$$
for $j \notin \{j_1, j_2\}$ and all $i \in S - T$, and furthermore
$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|+1}(x, w_{j_1} + w_{j_2} + R)(\sigma_{\pi_i(\bar{x})}) = 0$$
for all $i \in S - T$;
- if $i_{\text{Cheb}} \notin T$, we have
$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|}(x, w_{j_1}) = 0$$
and
$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|}(x, w_{j_2} + R) = 0;$$
- if $i_{\text{Cheb}} \notin T$ and $T \neq \varnothing$, we have
$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|+1}(x, w_{j_1})(\sigma_{\pi_i(\bar{x})}) = 0$$
for all $i \in S - T$ and
$$\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|+1}(x, w_{j_2} + R)(\sigma_{\pi_i(\bar{x})}) = 0$$
for all $i \in S - T$.

To achieve this, we will first put

$$C_\varnothing^{\mathrm{acc}} := X(a, Q, \{\mathrm{Art}_k\}_{2 \le k < m}) \cap \widetilde{Z},$$

so that $\mathfrak{A}$ indeed satisfies property (a). Observe that an additive system $\mathfrak{A}$ is completely determined by $C_\varnothing^{\mathrm{acc}}$ and the maps F_T. Our goal is now to construct the maps $F_T : C_T \to A_T$ (with $|A_T| \le 2^{(n_{\max}+10)(n_{\max}+2m+10)}$) such that property (d) holds. We will then show that $\mathfrak{A}$ also satisfies properties (b) and (c).

Construction of the additive system

In order to construct F_T, we will suppose that we are in case I with the other cases being similar and we proceed by induction on $|T|$. If $T = \varnothing$ or if $|T| \ge m$, we let F_T be the zero map. Let $0 < |T| < m$ and let $1 \le j \le n_{|T|+1}$. We assume that $T \subseteq S' - \{i_{\mathrm{char}}\}$ if $j > n_m$. Now take $\bar{x} \in C_T$ and define

$$\psi(\bar{x}, j) := \begin{cases} \displaystyle\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|}(x, w_j) & \text{if } j \ne j_2 \text{ or } i_{\mathrm{char}} \notin T \\ \phi_{\pi_{T-\{i_{\mathrm{char}}\}}(\bar{x}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{x})) \mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{x}))} + \displaystyle\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|}(x, w_j) & \text{if } j = j_2 \text{ and } i_{\mathrm{char}} \in T \end{cases}$$

for $j \ne j_1$. Further define

$$\psi(\bar{x}, j_1) := \begin{cases} \displaystyle\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|}(x, w_{j_1}) & \text{if } i_{\mathrm{Cheb}} \notin T \text{ or } j_1 \notin \mathcal{W} \\ 0 & \text{if } i_{\mathrm{Cheb}} \in T \text{ and } j_1 \in \mathcal{W}. \end{cases}$$

A priori $\psi(\bar{x}, j)$ is a 1-cochain from $G_\mathbb{Q}$ with values in N. But since $\bar{x} \in C_T$, it follows from Proposition 2.9 that

$$d\psi(\bar{x}, j) = 0,$$

so $\psi(\bar{x}, j)$ is a quadratic character. Furthermore, using once more that $\bar{x} \in C_T$, we find that

$$\psi(\bar{x}, j)(\sigma_p) = 0 \tag{8.29}$$

for all $p \in \{\mathrm{pr}_1(\pi_i(\bar{x})), \mathrm{pr}_2(\pi_i(\bar{x}))\}$ and all $i \in T$ provided that $|T| \ge 2$. In case $|T| = 1$, we may directly verify equation (8.29). It follows that $\psi(\bar{x}, j)$ is an unramified quadratic character of $\mathbb{Q}(\sqrt{x})$ for all $x \in \bar{x}(\varnothing)$. Take a prime $p = \pi_j(\bar{x})$ with $j \in [r] - T$. We claim that the place $\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(p)$ splits completely in the extension $L(\psi(\bar{x}, j))\mathbb{Q}(\sqrt{x})/\mathbb{Q}(\sqrt{x})$. Since $j \le n_{|T|+1}$, $\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(p)$ certainly splits completely in $L(\psi_{|T|}(x, w_j))\mathbb{Q}(\sqrt{x})/\mathbb{Q}(\sqrt{x})$ for every $x \in \bar{x}(\varnothing)$, and p splits completely in

$$L(\phi_{\pi_{T-\{i_{\mathrm{char}}\}}(\bar{x}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{x})) \mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{x}))})/\mathbb{Q}$$

by assumption. This clearly implies the claim.

If N is sufficiently large, it follows from equation (8.7) that there exists an injective map $f : [n_2] \to [r] - S - \{1\}$ such that

$$\pi_{f(i)}(w_j) = 1 \iff i = j$$

for all $i, j \in [n_2]$. Similarly, there exists $i_0 \in [r] - S - \{1\}$ such that

$$\pi_{i_0}(w_j) = 0 \text{ for all } j \in [n_2].$$

Choose a point $x_0 \in \bar{x}(\varnothing)$. Define $F_{T,1}$ to be the map that sends $\bar{x}$ to the tuple

$$\Big(\psi(\bar{x}, j)(\mathrm{Frob}(\mathrm{Up}_{\mathbb{Q}(\sqrt{x_0})/\mathbb{Q}}(\pi_i(x_0)))) \Big)_{1 \le j \le n_{|T|+1}, i \in T},$$

define $F_{T,2}$ to be the map that sends $\bar{x}$ to the tuple

$$\left(\Big(\psi(\bar{x}, j)(\sigma_{\pi_{i_0}(x_0)}) \Big)_{1 \le j \le n_{|T|+1}}, \Big(\psi(\bar{x}, j)(\sigma_{\pi_{f(i)}(x_0)}) \Big)_{1 \le j \le n_{|T|+1}, i \in [n_2]} \right)$$

and finally define $F_{T,3}$ to be the map that sends $\bar{x}$ to the tuple

$$\left(\sum_{x \in \bar{x}(\varnothing)} \psi_{|T|+1}(x, w_j)(\sigma_{\pi_i(x_0)}) \right)_{1 \le j \le n_{|T|+1}, i \in S - T}.$$

Since $\pi_{f(i)}(x_0)$, $\pi_{i_0}(x_0)$ and $\pi_i(x_0)$ (for $i \in S - T$) do not depend on the choice of $x_0 \in \bar{x}(\varnothing)$, one readily verifies that $F_{T,2}$ and $F_{T,3}$ satisfy equation (6.1). We will now argue that $F_{T,1}$ also satisfies equation (6.1). To this end, observe that $\bar{x}(\varnothing) \subseteq X(a)$ by our choice of $C_{\varnothing}^{\mathrm{acc}}$. From this we deduce that $F_{T,1}$ also does not depend on the choice of x_0. Then $F_{T,1}$ also satisfies equation (6.1). Finally, we define F_T to be the map

$$(F_{T,1}, F_{T,2}, F_{T,3})$$

in case $T \subseteq S' - \{i_{\mathrm{char}}\}$. In case T is not a subset of $S' - \{i_{\mathrm{char}}\}$, we define F_T in the same way, except that j runs up to n_m instead of $n_{|T|+1}$ in the definitions of $F_{T,1}$ and $F_{T,2}$. Having constructed the map F_T, we will now verify that C_T^{acc} satisfies property (d).

Verification of property (d)

Let $\bar{x} \in C_T^{\mathrm{acc}}$, so that $\bar{x} \in C_T$ and $F_T(\bar{x}) = 0$. In particular $F_{T,3}(\bar{x}) = 0$, so equation (8.28) holds. Therefore it remains to establish that $\bar{x}$ satisfies equations (8.24), (8.25), (8.26) and (8.27), which is equivalent to showing that $\psi(\bar{x}, j) = 0$ for all $1 \le j \le n_{|T|+1}$. In case $|T| = 1$, this follows from our choice of variable indices. So henceforth we will assume that $|T| > 1$.

In order to show that $\psi(\bar{x}, j) = 0$, we first observe that $L(\psi(\bar{x}, j))\mathbb{Q}(\sqrt{x})/\mathbb{Q}(\sqrt{x})$ is an unramified extension for every $x \in \bar{x}(\varnothing)$. Indeed, this is a consequence of the vanishing of $F_{T',3}(\bar{y})$ for all $\varnothing \subset T' \subset T$ and all $\bar{y} \in \bar{x}(T')$: it is at this point that we make essential use of the assumption $|T| > 1$.

Next we claim that $\psi(\bar{x}, j) \in V_{a,2}$. Let $x \in \bar{x}(\varnothing)$ and let $p = \pi_i(x)$ for some $i \in [r]$. We have to show that $\mathrm{Up}_{\mathbb{Q}(\sqrt{x})/\mathbb{Q}}(p)$ splits completely in $L(\psi(\bar{x}, j))\mathbb{Q}(\sqrt{x})/\mathbb{Q}(\sqrt{x})$. In case $i \in [r] - T$, we have already established this, while for $i \in T$ this follows from the vanishing of $F_{T,1}(\bar{x})$. This establishes the claim.

We are now ready to prove that $\psi(\bar{x}, j) = 0$. Indeed, since $\psi(\bar{x}, j) \in V_{a,2}$, we can write $\psi(\bar{x}, j)$ as a linear combination of R and the elements w_k. But $F_{T,2}(\bar{x}) = 0$ implies that $\psi(\bar{x}, j)$ vanishes on $\sigma_{\pi_{i_0}(x)}$ for all $x \in \bar{x}(\varnothing)$, so $\psi(\bar{x}, j)$ must in fact be a linear combination of the elements w_k. Using once more that $F_{T,2}(\bar{x}) = 0$ and the definition of the injection $f : [n_2] \to [r] - S - \{1\}$, we conclude that $\psi(\bar{x}, j) = 0$.

So far we have constructed an additive system $\mathfrak{A}$ satisfying properties (a) and (d) such that $|A_T| \le 2^{(n_{\max}+10)(n_{\max}+2m+10)}$. We will now show that this implies properties (b) and (c), and we will do so case by case.

Verification of property (b) **and** (c) **in case** I

We start with case I. Take $\bar{x} \in C(\mathfrak{A})$. If $\bar{x} \in C(\mathfrak{A})$ is degenerate, then property (b) and (c) hold. So suppose that $\bar{x}$ is not degenerate. By definition of $C(\mathfrak{A})$, it follows that

$$\bar{x}(S - \{i\}) \cap C^{\mathrm{acc}}_{S-\{i\}} \neq \varnothing.$$

Fix for every $i \in S$ an element $\bar{z}_i$ in the intersection $\bar{x}(S - \{i\}) \cap C^{\mathrm{acc}}_{S-\{i\}}$. Then there exists a unique $x_0 \in \bar{x}(\varnothing)$ such that $x_0 \notin \bar{z}_i(\varnothing)$ for all i. For all $x_1 \in \bar{x}(\varnothing)$ with $x_1 \neq x_0$, we see that there exists $i \in S$ such that $x_1 \in \bar{z}_i(\varnothing)$. In particular, we deduce that $x_1 \in C^{\mathrm{acc}}_{\varnothing}$. Therefore it is enough to show that $x_0 \in C^{\mathrm{acc}}_{\varnothing}$ to conclude that $\mathfrak{A}$ is $(2^{(n_{\max}+10)(n_{\max}+2m+10)}, S)$-acceptable, i.e. property (b) holds.

To start, we see that $x_0 \in X(a)$. We will show that

$$\mathrm{Art}_{i,x_0} = \mathrm{Art}_i$$

for all $2 \leq i < m$ by induction on i. Since $i < m$ and $|S| = m + 1$, we can pick a subset T of S such that $|T| = i$ and T does not contain i_{Cheb} or i_{char}. We apply Theorem 5.10 to any element $\bar{y}$ in $\bar{x}(T)$ containing x_0. Since $\bar{z}_j \in C^{\mathrm{acc}}_{S-\{j\}}$ for all $j \in T$, it follows that

$$(\bar{y}(\varnothing), (\psi_{|T|}(x, w_k))_{x \in \bar{y}(\varnothing) - \{x_0\}}, \chi(w_k))$$

is a minimal triple for all $1 \leq k \leq n_{|T|}$, where $\chi(w_k) = \psi_1(x, w_k)$ for any choice of $x \in \bar{y}(\varnothing)$. We emphasize that $\psi_1(x, w_k)$ does not depend on the choice of $x \in \bar{y}(\varnothing)$ by our choice of variable indices and our choice of T. Now take an element $b \in A_{|T|}$. If there does not exist $l \in T$ with $\pi_l(b) = 1$, then we deduce from Theorem 5.10 that

$$\mathrm{Art}_{i,x_0}(b, w_k) = \mathrm{Art}_i(b, w_k).$$

Now suppose that there exists $l \in T$ with $\pi_l(b) = 1$. By our choice of variable indices, we see that there does not exist $l \in T$ with $\pi_l(b + R) = 1$. Therefore it follows from the previous case that

$$\mathrm{Art}_{i,x_0}(b + R, w_k) = \mathrm{Art}_i(b + R, w_k).$$

But Theorem 5.10 yields

$$\mathrm{Art}_{i,x_0}(R, w_k) = \mathrm{Art}_i(R, w_k),$$

so $\mathfrak{A}$ is $(2^{(n_{\max}+10)(n_{\max}+2m+10)}, S)$-acceptable in case I.

We will now show that property (c) holds in case I. Let $\bar{x} \in C(\mathfrak{A})$ and let $\bar{y} \in \bar{x}(S - \{i_{\mathrm{Cheb}}\})$. It follows from Theorem 5.10 and Theorem 5.11 that

$$\sum_{y \in \bar{y}(\varnothing)} \mathrm{Art}_{m,y}(v_l, w_k) = \begin{cases} 0 & \text{if } k \neq j_2 \\ \displaystyle\sum_{\substack{1 \leq i \leq r \\ \pi_i(v_l)=1}} \phi_{\pi_{S'-\{i_{\mathrm{char}}\}}(\bar{x}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{x}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{x}))}(\mathrm{Frob}(\pi_i(\bar{y}))) & \text{if } k = j_2 \end{cases}$$

for all $1 \leq k, l \leq n_m$, where we impose the additional condition $l \neq j_2$ if $j_2 \leq d_m$. Now suppose that $l = j_2$ with $j_2 \leq d_m$. Then Theorem 5.10, applied to the cube $\bar{y} \in \bar{x}(S - \{i_{\mathrm{char}}\})$, gives

$$\sum_{y \in \bar{y}(\varnothing)} \mathrm{Art}_{m,y}(v_{j_2}, w_k) = 0$$

for all $1 \leq k \leq n_m$, where we impose that $k \neq j_1$ if $j_1 \leq d_m$. Using the above equations for both choices of $\bar{y}$, we obtain the identity

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(v_l, w_k) = 0 \tag{8.30}$$

for all pairs (l, k) satisfying $(l, k) \notin \{(j_1, j_2), (j_2, j_1)\}$ if $j_1, j_2 \leq d_m$ and all pairs $(l, k) \neq (j_1, j_2)$ otherwise. We also get the identity

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(v_{j_1}, w_{j_2}) = \phi_{\pi_{S'-\{i_{\mathrm{char}}\}}(\bar{x}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{x}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{x}))}(\mathrm{Frob}(\mathrm{pr}_1(\pi_{i_{\mathrm{Cheb}}}(\bar{x})))) +$$

$$\phi_{\pi_{S'-\{i_{\mathrm{char}}\}}(\bar{x}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{x}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{x}))}(\mathrm{Frob}(\mathrm{pr}_2(\pi_{i_{\mathrm{Cheb}}}(\bar{x})))). \tag{8.31}$$

We now apply part (ii) of Theorem 5.10 to a cube $\bar{y} \in \bar{x}(S - \{i_{\mathrm{Cheb}}\})$. This yields

$$\sum_{y \in \bar{y}(\varnothing)} \mathrm{Art}_{m,y}(R, w_k) = 0 \tag{8.32}$$

if $k \neq j_2$. Similarly, part (ii) of Theorem 5.10 gives for $\bar{y} \in \bar{x}(S - \{i_{\mathrm{char}}\})$

$$\sum_{y \in \bar{y}(\varnothing)} \mathrm{Art}_{m,y}(R, w_{j_2}) = 0. \tag{8.33}$$

Adding up equation (8.32) and equation (8.33) for the two choices of $\bar{y}$, we conclude that

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(R, w_k) = 0 \tag{8.34}$$

for all $1 \leq k \leq n_m$. Equation (8.30, (8.31) and (8.34) and the shape of F imply that

$$(\Sigma F')(\bar{x}) = \phi_{\pi_{S'-\{i_{\mathrm{char}}\}}(\bar{x}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{x}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{x}))}(\mathrm{Frob}(\mathrm{pr}_1(\pi_{i_{\mathrm{Cheb}}}(\bar{x})))) +$$

$$\phi_{\pi_{S'-\{i_{\mathrm{char}}\}}(\bar{x}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{x}))\mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{x}))}(\mathrm{Frob}(\mathrm{pr}_2(\pi_{i_{\mathrm{Cheb}}}(\bar{x}))))$$

as desired.

Verification of property (b) and (c) in case II

We will now deal with case II. We will start with property (b) and adapt the notation from case I. So let $\bar{x} \in C(\mathfrak{A})$ and let x_0 be the element of $\bar{x}(\varnothing)$ not in any of the $\bar{z}_i(\varnothing)$ (for the definition of $\bar{z}_i$, see case I). We have to show that

$$\mathrm{Art}_{i,x_0} = \mathrm{Art}_i$$

for all $2 \leq i < m$. Since $|S| = m$ in this case, we can find a subset T of S with $|T| = i$ and $i_{\mathrm{Cheb}} \notin T$. Take $\bar{y} \in \bar{x}(T)$. Then

$$(\bar{y}(\varnothing), (\psi_{|T|}(x, w_k))_{x \in \bar{y}(\varnothing) - \{x_0\}}, \chi(w_k))$$

is a minimal triple for all $1 \leq k \leq n_{|T|}$. Proceeding as in case I gives

$$\mathrm{Art}_{i,x_0} = \mathrm{Art}_i.$$

Our next task is to verify property (c) in case II. Take $\bar{x} \in C(\mathfrak{A})$. By construction of the variable indices, we know that

$$F = \sum_{\substack{1 \leq j_3 \leq n_m+1 \\ 1 \leq j_4 \leq n_m}} c_{j_3,j_4} F_{j_3,j_4}, \quad c_{j_3,j_4} \in \mathbb{F}_2,$$

where c_{j_3,j_4} satisfies

- $c_{j_3,j_4} = c_{j_4,j_3}$ for all $1 \leq j_3, j_4 \leq n_m$;

- $c_{j_3,j_4} = 0$ if $n_m \geq j_3 > d_m$ or $n_m \geq j_4 > d_m$;

- $c_{n_m+1,j_2} = 1$.

We deduce from Theorem 5.10 that

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(v_l, w_k) = \left\{ \begin{array}{ll} 0 & \text{for all } l \neq j_2 \text{ and all } k \neq j_2 \text{ if } j_2 \leq d_m \\ 0 & \text{for all } k \neq j_2 \text{ if } j_2 > d_m. \end{array} \right.$$

Let $\bar{y} \in \bar{x}(S - \{i_{\mathrm{Cheb}}\})$. Theorem 5.2 implies that

$$\sum_{y \in \bar{y}(\varnothing)} \mathrm{Art}_{m,y}(R, w_k) = \sum_{\substack{1 \leq i \leq r \\ \pi_i(w_k)=1}} \phi_{\pi_{S'}(\bar{x});-1}(\mathrm{Frob}(\pi_i(\bar{y}))).$$

Therefore we get

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(R, w_k) = 0 \tag{8.35}$$

if $k \neq j_2$ and

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(R, w_k) = \phi_{\pi_{S'}(\bar{x});-1}(\mathrm{Frob}(\mathrm{pr}_1(\pi_{i_{\mathrm{Cheb}}}(\bar{x})))) + \phi_{\pi_{S'}(\bar{x});-1}(\mathrm{Frob}(\mathrm{pr}_2(\pi_{i_{\mathrm{Cheb}}}(\bar{x}))))$$

$$\tag{8.36}$$

if $k = j_2$. Now suppose that $j_2 \leq d_m$. Then, since $m \geq 3$, we apply Theorem 5.6 twice to obtain

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(w_{j_2}, w_{j_2}) = 0. \tag{8.37}$$

Since we are working with pairings valued in $\mathbb{F}_2$, we have the identity

$$\mathrm{Art}_{m,x}(v_l, w_{j_2}) + \mathrm{Art}_{m,x}(w_{j_2}, v_l) = \mathrm{Art}_{m,x}(v_l, v_l) + \mathrm{Art}_{m,x}(w_{j_2}, w_{j_2}) + \mathrm{Art}_{m,x}(v_l + w_{j_2}, v_l + w_{j_2})$$

for all $l \leq d_m$. Six applications of Theorem 5.6 show that

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(v_l, w_{j_2}) + \mathrm{Art}_{m,x}(w_{j_2}, v_l) = 0 \tag{8.38}$$

for all $l \leq d_m$. It follows from equations (8.35), (8.36), (8.37), (8.38) and the properties of c_{j_3,j_4} that

$$(\Sigma F')(\bar{x}) = \phi_{\pi_{S'}(\bar{x});-1}(\mathrm{Frob}(\mathrm{pr}_1(\pi_{i_{\mathrm{Cheb}}}(\bar{x})))) + \phi_{\pi_{S'}(\bar{x});-1}(\mathrm{Frob}(\mathrm{pr}_2(\pi_{i_{\mathrm{Cheb}}}(\bar{x}))))$$

as desired.

Verification of property (b) **and** (c) **in case** III

We will now treat case III. Let us verify property (b) first. In case III we can expand F as

$$F = \sum_{\substack{1 \leq j_3 \leq n_m+1 \\ 1 \leq j_4 \leq n_m}} c_{j_3,j_4} F_{j_3,j_4}, \quad c_{j_3,j_4} \in \mathbb{F}_2,$$

where c_{j_3,j_4} satisfies

- $c_{j_3,j_4} = c_{j_4,j_3}$ for all $1 \leq j_3, j_4 \leq n_m$;

- $c_{j_3,j_4} = 0$ if $j_3 > d_m$ or $j_4 > d_m$;

- $c_{n_m+1,k} = 0$ for all $1 \leq k \leq n_m$;

- $c_{j_2,j_2} = 1$.

Take $\bar{x} \in C(\mathfrak{A})$ and define x_0 to be the unique element of $\bar{x}(\varnothing)$ outside of all the $\bar{z}_i(\varnothing)$. Again we have to show that

$$\mathrm{Art}_{i,x_0} = \mathrm{Art}_i$$

for all $2 \leq i < m$. Because $|S| = m$, there exists a subset T of S with $|T| = i$ and $i_{\mathrm{Cheb}} \notin T$. Fix a choice of $\bar{y} \in \bar{x}(T)$ containing x_0. We now apply Theorem 5.10 to the minimal triple

$$(\bar{y}(\varnothing), (\psi_{|T|}(x, w_k))_{x \in \bar{y}(\varnothing)-\{x_0\}}, \chi(w_k))$$

for $k \neq j_2$ and the minimal triple

$$(\bar{y}(\varnothing), (\psi_{|T|}(x, w_{j_2} + R))_{x \in \bar{y}(\varnothing)-\{x_0\}}, \chi(w_{j_2} + R)),$$

where $\chi(w_{j_2} + R) = \psi_1(y, w_{j_2} + R)$ for any choice of $y \in \bar{y}(\varnothing)$. Note that this does not depend on the choice of y precisely by our choice of variable indices. This gives property (b).

As for property (c), take $\bar{x} \in C(\mathfrak{A})$ and take $\bar{y} \in \bar{x}(S - \{i_{\mathrm{Cheb}}\})$. Theorem 5.7 yields

$$\sum_{y \in \bar{y}(\varnothing)} \mathrm{Art}_{m,y}(w_{j_2}, w_{j_2}) = \sum_{\substack{1 \leq i \leq r \\ \pi_i(w_{j_2}+R)=1}} \phi_{\pi_{S'}(\bar{x});-1}(\mathrm{Frob}(\pi_i(\bar{y}))).$$

We conclude that

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(w_{j_2}, w_{j_2}) = \phi_{\pi_{S'}(\bar{x});-1}(\mathrm{Frob}(\mathrm{pr}_1(\pi_{i_{\mathrm{Cheb}}}(\bar{x})))) + \phi_{\pi_{S'}(\bar{x});-1}(\mathrm{Frob}(\mathrm{pr}_2(\pi_{i_{\mathrm{Cheb}}}(\bar{x})))).$$

$$(8.39)$$

Take some $l \leq d_m$ satisfying $l \neq j_2$. Using Theorem 5.6 twice, we obtain

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(v_l, v_l) = 0. \tag{8.40}$$

Following the argument that led to equation (8.39), we show in a completely analogous fashion that

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(v_l + w_{j_2}, v_l + w_{j_2}) =$$

$$\phi_{\pi_{S'}(\bar{x});-1}(\mathrm{Frob}(\mathrm{pr}_1(\pi_{i_{\mathrm{Cheb}}}(\bar{x})))) + \phi_{\pi_{S'}(\bar{x});-1}(\mathrm{Frob}(\mathrm{pr}_2(\pi_{i_{\mathrm{Cheb}}}(\bar{x})))) \quad (8.41)$$

for all $l \leq d_m$ with $l \neq j_2$. Recalling the identity

$$\mathrm{Art}_{m,x}(v_l, w_{j_2}) + \mathrm{Art}_{m,x}(w_{j_2}, v_l) = \mathrm{Art}_{m,x}(v_l, v_l) + \mathrm{Art}_{m,x}(w_{j_2}, w_{j_2}) + \mathrm{Art}_{m,x}(v_l + w_{j_2}, v_l + w_{j_2}),$$

we get from equations (8.39), (8.40) and (8.41)

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(v_l, w_{j_2}) + \mathrm{Art}_{m,x}(w_{j_2}, v_l) = 0. \tag{8.42}$$

If we take k and l both not equal to j_2, then we have the equality

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(v_l, w_k) + \mathrm{Art}_{m,x}(w_k, v_l) = 0 \tag{8.43}$$

as a consequence of Theorem 5.10. From the shape of F and equations (8.39), (8.42) and (8.43), we conclude that

$$(\Sigma F')(\bar{x}) = \phi_{\pi_{S'}(\bar{x}); -1}(\mathrm{Frob}(\mathrm{pr}_1(\pi_{i_{\mathrm{Cheb}}}(\bar{x})))) + \phi_{\pi_{S'}(\bar{x}); -1}(\mathrm{Frob}(\mathrm{pr}_2(\pi_{i_{\mathrm{Cheb}}}(\bar{x})))),$$

which finishes the proof of property (c) in case III.

Verification of property (b) and (c) in case IV

Finally, we deal with case IV. In case IV we can expand F as

$$F = \sum_{\substack{1 \leq j_3 \leq n_m + 1 \\ 1 \leq j_4 \leq n_m}} c_{j_3, j_4} F_{j_3, j_4}, \quad c_{j_3, j_4} \in \mathbb{F}_2,$$

where c_{j_3, j_4} satisfies

- $c_{j_3, j_4} = c_{j_4, j_3}$ for all $1 \leq j_3, j_4 \leq n_m$;
- $c_{j_3, j_4} = 0$ if $j_3 > d_m$ or $j_4 > d_m$;
- $c_{n_m + 1, k} = 0$ for all $1 \leq k \leq n_m$;
- $c_{k,k} = 0$ for all $1 \leq k \leq d_m$;
- $c_{j_1, j_2} = 1$.

Suppose that we are given $\bar{x} \in C(\mathfrak{A})$. Then let x_0 be the unique element of $\bar{x}(\varnothing)$ outside of all the $\bar{z}_i(\varnothing)$. For property (b), we need to establish that

$$\mathrm{Art}_{i, x_0} = \mathrm{Art}_i$$

for all $2 \leq i < m$. We will proceed as in case III. Because $|S| = m$, we may and will choose a subset T of S with $|T| = i$ and $i_{\mathrm{Cheb}} \notin T$. Take $\bar{y} \in \bar{x}(T)$ containing x_0. Now we are in the position to apply Theorem 5.10 to the minimal triple

$$(\bar{y}(\varnothing), (\psi_{|T|}(x, w_k))_{x \in \bar{y}(\varnothing) - \{x_0\}}, \chi(w_k))$$

for $k \neq j_2$ and the minimal triple

$$(\bar{y}(\varnothing), (\psi_{|T|}(x, w_{j_2} + R))_{x \in \bar{y}(\varnothing) - \{x_0\}}, \chi(w_{j_2} + R)),$$

where $\chi(w_{j_2} + R) = \psi_1(y, w_{j_2} + R)$ for any choice of $y \in \bar{y}(\varnothing)$. This yields property (b) in case IV.

It remains to deal with property (c). Let l and k be distinct and bounded by d_m. If $\{l, k\} = \{j_1, j_2\}$, then Theorem 5.10 yields (applied to the character $\chi(w_{j_2} + v_{j_1} + R)$)

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(w_{j_2} + v_{j_1}, w_{j_2} + v_{j_1}) = 0.$$

Now suppose that $\{l, k\} \neq \{j_1, j_2\}$. It follows from Theorem 5.6 and Theorem 5.7 that

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(w_k + v_l, w_k + v_l) = 0$$

if $j_2 \notin \{k, l\}$ and

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(w_k + v_l, w_k + v_l) =$$

$$\phi_{\pi_{S'}(\bar{x}); -1}(\mathrm{Frob}(\mathrm{pr}_1(\pi_{i_{\mathrm{Cheb}}}(\bar{x})))) + \phi_{\pi_{S'}(\bar{x}); -1}(\mathrm{Frob}(\mathrm{pr}_2(\pi_{i_{\mathrm{Cheb}}}(\bar{x}))))$$

otherwise. Furthermore, we deduce from Theorem 5.6 and Theorem 5.7 that

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(w_k, w_k) = 0$$

if $k \neq j_2$ and

$$\sum_{x \in \bar{x}(\varnothing)} \mathrm{Art}_{m,x}(w_{j_2}, w_{j_2}) = \phi_{\pi_{S'}(\bar{x}); -1}(\mathrm{Frob}(\mathrm{pr}_1(\pi_{i_{\mathrm{Cheb}}}(\bar{x})))) + \phi_{\pi_{S'}(\bar{x}); -1}(\mathrm{Frob}(\mathrm{pr}_2(\pi_{i_{\mathrm{Cheb}}}(\bar{x})))).$$

Using the identity

$$\mathrm{Art}_{m,x}(v_l, w_k) + \mathrm{Art}_{m,x}(w_k, v_l) = \mathrm{Art}_{m,x}(v_l, v_l) + \mathrm{Art}_{m,x}(w_k, w_k) + \mathrm{Art}_{m,x}(v_l + w_k, v_l + w_k)$$

once more, this shows that

$$(\Sigma F')(\bar{x}) = \phi_{\pi_{S'}(\bar{x}); -1}(\mathrm{Frob}(\mathrm{pr}_1(\pi_{i_{\mathrm{Cheb}}}(\bar{x})))) + \phi_{\pi_{S'}(\bar{x}); -1}(\mathrm{Frob}(\mathrm{pr}_2(\pi_{i_{\mathrm{Cheb}}}(\bar{x}))))$$

as desired.

End of proof

The final step of the proof is very similar to the proof of Proposition 8.5 in Smith [42]. Let $\sigma \in \mathrm{Gal}(M_\circ(Z)M(Z)/M_\circ(Z))$. Define $X_i(a, Q, M_\circ(Z), \sigma)$ to be the subset of $p \in X_i(a, Q, M_\circ(Z))$ such that $\mathrm{Frob}(p) = \sigma$. This is well-defined, since $\mathrm{Gal}(M_\circ(Z)M(Z)/M_\circ(Z))$ is a central subgroup of $\mathrm{Gal}(M_\circ(Z)M(Z)/\mathbb{Q})$. We apply the Chebotarev density theorem [42, Proposition 6.5] to the extension $L(Q)M_\circ(Z)M(Z)/\mathbb{Q}$ to deduce that

$$|X_i(a, Q, M_\circ(Z), \sigma)| = \frac{|X_i(a, Q, M_\circ(Z))|}{2^{(M_{\mathrm{box}}-1)|S'|}} \cdot \left(1 + O(e^{-k_{\mathrm{gap}}})\right) \tag{8.44}$$

for $i > k_{\text{gap}}$, where we deal with potential Siegel zeroes by appealing to [23] and where we used Lemma 6.7 and Lemma 6.10 to compute the size of $\mathrm{Gal}(M_\circ(Z)M(Z)/M_\circ(Z))$.

Given an element
$$Q_{\text{post}} \in \prod_{\substack{i \in [r] - [k_{\text{gap}}] \\ i \neq i_{\text{Cheb}}}} X_i(a, Q, M_\circ(Z)),$$

we define $\widetilde{Z}(Q_{\text{post}})$ to be the subset of $x \in \widetilde{Z}$ such that $\pi_{[r]-[k_{\text{gap}}]-\{i_{\text{Cheb}}\}}(x) = Q_{\text{post}}$. We call Q_{post} unevenly distributed over the Chebotarev classes if there exists an element $\sigma \in \mathrm{Gal}(M_\circ(Z)M(Z)/M_\circ(Z))$ such that

$$\left| |X_{i_{\text{Cheb}}}(a, Q \times Q_{\text{post}}, M_\circ(Z), \sigma)| - \frac{|X_{i_{\text{Cheb}}}(a, Q \times Q_{\text{post}}, M_\circ(Z))|}{2^{(M_{\text{box}}-1)|S'|}} \right| \geq$$
$$\frac{|X_{i_{\text{Cheb}}}(a, Q \times Q_{\text{post}}, M_\circ(Z))|}{e^{0.5k_{\text{gap}}} \cdot 2^{(M_{\text{box}}-1)|S'|}},$$

and we call Q_{post} evenly distributed otherwise. The sets $\widetilde{Z}(Q_{\text{post}})$ cover $\widetilde{Z}$, and we will make one more reduction step by reducing to the sets $\widetilde{Z}(Q_{\text{post}})$ with Q_{post} evenly distributed over the Chebotarev classes. To complete this reduction step, we need to bound

$$\left| \sum_{Q_{\text{post}} \text{ uneven}} \sum_{x \in X(a, Q, \{\mathrm{Art}_k\}_{2 \leq k < m}) \cap \widetilde{Z}(Q_{\text{post}})} \iota(F(\mathrm{Art}_{m,x})) \right| \leq$$
$$|Z| \cdot |X_{i_{\text{Cheb}}}(a, Q, M_\circ(Z))| \cdot \sum_{Q_{\text{post}} \text{ uneven}} 1. \quad (8.45)$$

We say that an element
$$Q_{j,\text{post}} \in \prod_{\substack{i \in [j] - [k_{\text{gap}}] \\ i \neq i_{\text{Cheb}}}} X_i(a, Q, M_\circ(Z))$$

is an evenly distributed candidate if the following two conditions are satisfied

- $j - 1 > k_{\text{gap}}$ implies that $\pi_{[j-1]-[k_{\text{gap}}]}(Q_{j,\text{post}})$ is an evenly distributed candidate;

- $j \neq i_{\text{Cheb}}$ implies that

$$\left| \sum_{p \in X_{i_{\text{Cheb}}}(a, Q \times Q_{j-1,\text{post}}, M_\circ(Z), \sigma)} \left(\frac{p}{\pi_j(Q_{j,\text{post}})} \right) \right| \leq \frac{|X_{i_{\text{Cheb}}}(a, Q \times Q_{j-1,\text{post}}, M_\circ(Z), \sigma)|}{|X_{k_{\text{gap}}+1}(a, Q, M_\circ(Z))|^{1/100}}$$

    for all $\sigma \in \mathrm{Gal}(M_\circ(Z)M(Z)/M_\circ(Z))$.

If $Q_{\text{post}} = Q_{r,\text{post}}$ is an evenly distributed candidate, then equation (8.44) and a direct computation show that Q_{post} is evenly distributed over the Chebotarev classes provided that we take N_0 sufficiently large. We will now repeatedly apply the large sieve, as for example presented in [42, Proposition 6.6]. This yields that the number of Q_{post}, that are not evenly distributed candidates, is bounded by

$$\frac{\prod_{\substack{i \in [r] - [k_{\text{gap}}] \\ i \neq i_{\text{Cheb}}}} |X_i(a, Q, M_\circ(Z))|}{|X_{k_{\text{gap}}+1}(a, Q, M_\circ(Z))|^{1/100}}$$

if we take N_0 sufficiently large. In particular, we conclude that equation (8.45) is upper bounded by

$$\frac{|Z| \cdot \prod_{i \in [r] - [k_{\text{gap}}]} |X_i(a, Q, M_\circ(Z))|}{|X_{k_{\text{gap}}+1}(a, Q, M_\circ(Z))|^{1/100}}.$$

Note that Proposition 7.6 allows us to calculate the size of $X(a, Q) \cap \widetilde{Z}$. Then we see that

$$\frac{|Z| \cdot \prod_{i \in [r] - [k_{\text{gap}}]} |X_i(a, Q, M_\circ(Z))|}{|X_{k_{\text{gap}}+1}(a, Q, M_\circ(Z))|^{1/100}} \leq \frac{|X(a, Q) \cap \widetilde{Z}|}{|X_{k_{\text{gap}}+1}(a, Q, M_\circ(Z))|^{1/1000}},$$

which fits in the error term. Therefore it suffices to show that there exists $A > 0$ such that

$$\left| \sum_{x \in X(a, Q, \{\text{Art}_k\}_{2 \leq k < m}) \cap \widetilde{Z}(Q_{\text{post}})} \iota(F(\text{Art}_{m,x})) \right| \leq \frac{A \cdot |X(a, Q) \cap \widetilde{Z}(Q_{\text{post}})|}{(\log \log \log \log N)^{\frac{100c}{m6^m}}} \tag{8.46}$$

for every Q_{post} evenly distributed over the Chebotarev classes.

We are now ready to use our combinatorial results from Section 6. We remark that the space

$$X(a, Q) \cap \widetilde{Z}(Q_{\text{post}})$$

is just the product

$$Z \times X_{i_{\text{Cheb}}}(a, Q \times Q_{\text{post}}, M_\circ(Z)).$$

We now formally apply Proposition 6.6 to the product set $Z \times [M_{\text{box}}]$ and

$$a = 2^{(n_{\max}+10)(n_{\max}+2m+10)}, \quad \epsilon = \frac{1}{(\log \log \log \log N)^{\frac{100c}{m6^m}}}.$$

We observe that $\epsilon < a^{-1}$ and $\log M_{\text{box}} \geq A_{\text{Comb}} \cdot 6^{m+1} \cdot \log \epsilon^{-1}$ by definition of c.

Denote by $g_0 \in \text{Add}(Z \times [M_{\text{box}}], S)$ the function guaranteed by Proposition 6.6. Here we implicitly index the space $Z \times [M_{\text{box}}]$ by S in the obvious way. To primes $p_1, \ldots, p_{M_{\text{box}}}$ we associate the element $g_{p_1, \ldots, p_{M_{\text{box}}}} \in \text{Add}(Z \times [M_{\text{box}}], S)$ by mapping a cube $(\bar{z}, (i, j)) \in \text{Cube}(Z \times [M_{\text{box}}], S)$ to

$$\phi_{\pi_{S'-\{i_{\text{char}}\}}(\bar{z}); \text{pr}_1(\pi_{i_{\text{char}}}(\bar{z}))\text{pr}_2(\pi_{i_{\text{char}}}(\bar{z}))}(\text{Frob}(p_i)) + \phi_{\pi_{S'-\{i_{\text{char}}\}}(\bar{z}); \text{pr}_1(\pi_{i_{\text{char}}}(\bar{z}))\text{pr}_2(\pi_{i_{\text{char}}}(\bar{z}))}(\text{Frob}(p_j))$$

in case I and

$$\phi_{\bar{z}; -1}(\text{Frob}(p_i)) + \phi_{\bar{z}; -1}(\text{Frob}(p_j))$$

in case II, III or IV. Our goal is now to partition $X_{i_{\text{Cheb}}}(a, Q \times Q_{\text{post}}, M_\circ(Z))$ as

$$X_{i_{\text{Cheb}}}(a, Q \times Q_{\text{post}}, M_\circ(Z)) = L \cup \bigcup_{i=1}^{t} A_i, \tag{8.47}$$

where each $A_i = \{p_{i,1}, \ldots, p_{i,M_{\text{box}}}\}$ is an ordered set (so it comes with a map $[M_{\text{box}}] \to A_i$) of size M_{box} satisfying

$$g_{p_{i,1}, \ldots, p_{i,M_{\text{box}}}} = g_0$$

and where $|L|$ is small.

To this end pick any element $p_1 \in X_{i_{\mathrm{Cheb}}}(a, Q \times Q_{\mathrm{post}}, M_\circ(Z))$. We claim that we can find $p_2, \ldots, p_{M_{\mathrm{box}}}$ with

$$g_{p_1, \ldots, p_{M_{\mathrm{box}}}} = g_0.$$

So fix $2 \leq j \leq M_{\mathrm{box}}$ and consider the additive function

$$g_0(\bar{z}, (1, j)) - \phi_{\pi_{S' - \{i_{\mathrm{char}}\}}(\bar{z}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{z})) \mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{z}))}(\mathrm{Frob}(p_1)) \in \mathrm{Add}(Z, S')$$

in case I and consider the additive function

$$g_0(\bar{z}, (1, j)) - \phi_{\bar{z}; -1}(\mathrm{Frob}(p_1)) \in \mathrm{Add}(Z, S')$$

in case II, III or IV. By Lemma 6.9 and Lemma 6.10, there exists a unique element $\sigma \in \mathrm{Gal}(M_\circ(Z)M(Z)/M_\circ(Z))$ such that

$$g_0(\bar{z}, (1, j)) - \phi_{\pi_{S' - \{i_{\mathrm{char}}\}}(\bar{z}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{z})) \mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{z}))}(\mathrm{Frob}(p_1)) =$$
$$\phi_{\pi_{S' - \{i_{\mathrm{char}}\}}(\bar{z}); \mathrm{pr}_1(\pi_{i_{\mathrm{char}}}(\bar{z})) \mathrm{pr}_2(\pi_{i_{\mathrm{char}}}(\bar{z}))}(\sigma)$$

in case I and

$$g_0(\bar{z}, (1, j)) - \phi_{\bar{z}; -1}(\mathrm{Frob}(p_1)) = \phi_{\bar{z}; -1}(\sigma)$$

in case II, III or IV. Now pick p_j such that $\mathrm{Frob}(p_j) = \sigma$. Note that σ implicitly depends on our choice of p_1. In fact, σ is a fixed linear shift of $\mathrm{Frob}(p_1)$. Using additivity in the last coordinate, we directly check that

$$g_{p_1, \ldots, p_{M_{\mathrm{box}}}} = g_0.$$

Since Q_{post} is evenly distributed in the Chebotarev classes, we can repeatedly use the above procedure to get a partition as in equation (8.47) with

$$|L| \leq \frac{|X_{i_{\mathrm{Cheb}}}(a, Q \times Q_{\mathrm{post}}, M_\circ(Z))|}{e^{0.25 k_{\mathrm{gap}}}}$$

provided that we take N_0 sufficiently large. From this, we obtain that

$$\left| \sum_{x \in X(a, Q, \{\mathrm{Art}_k\}_{2 \leq k < m}) \cap \widetilde{Z}(Q_{\mathrm{post}}) \cap (Z \times L)} \iota(F(\mathrm{Art}_{m,x})) \right| \leq \frac{|Z| \cdot |X_{i_{\mathrm{Cheb}}}(a, Q \times Q_{\mathrm{post}}, M_\circ(Z))|}{e^{0.25 k_{\mathrm{gap}}}}.$$
(8.48)

Let $\mathfrak{A}_i$ be the additive system on $Z \times [M_{\mathrm{box}}]$ obtained by restricting $\mathfrak{A}$ to $Z \times A_i$ and then using the map $[M_{\mathrm{box}}] \to A_i$ (coming from the fact that A_i was an ordered set). By properties (b) and (c) of $\mathfrak{A}$, it follows that $\mathfrak{A}_i$ is (a, S)-acceptable and that

$$(\Sigma F')(\bar{x}) = g_0(\bar{x})$$

for all $\bar{x} \in C(\mathfrak{A}_i)$. By the defining property of g_0, see Proposition 6.6, this implies that

$$\left| \sum_{x \in X(a, Q, \{\mathrm{Art}_k\}_{2 \leq k < m}) \cap \widetilde{Z}(Q_{\mathrm{post}}) \cap (Z \times A_i)} \iota(F(\mathrm{Art}_{m,x})) \right| \leq \epsilon \cdot |Z \times A_i|.$$
(8.49)

Equation (8.46) now falls as a consequence of equations (8.47), (8.48) and (8.49), which completes the proof. $\qquad \square$

References

[1] M. Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math. (2)* 162:1031-1063, 2005.

[2] M. Bhargava. The density of discriminants of quintic rings and fields. *Ann. of Math. (2)* 172:1559-1591, 2010.

[3] M. Bhargava, A. Shankar and J. Tsimerman. On the Davenport-Heilbronn theorems and second order terms. *Invent. Math.* 193:439-499, 2013.

[4] V. Blomer. A note on the negative Pell equation. *From arithmetic to zeta-functions*, 31-40, Springer, Cham, 2016.

[5] N. Boston, M.R. Bush and F. Hajir. Heuristics for p-class towers of real quadratic fields. *J. Inst. Math. Jussieu* 20(4):1429-1452, 2021.

[6] N. Boston and M.M. Wood. Nonabelian Cohen-Lenstra Heuristics over Function Fields. *Compos. Math.* 153(7):1372-1390, 2017.

[7] B. Breen, I. Varma, J. Voight, appendix with N. Elkies. On unit signatures and narrow class groups of odd degree abelian number fields. *arXiv preprint*, 1910.00449.

[8] S. Chan, P. Koymans, D.Z. Milovic and C. Pagano. On the negative Pell equation. *arXiv preprint*, 1908.01752.

[9] H. Cohen and H.W. Lenstra. Heuristics on class groups of number fields. Number theory, Noordwijkerhout 1983, *Lecture Notes in Math., Springer, Berlin*, 1984, 33-62.

[10] J, Corsman. Rédei symbols and governing fields. *ProQuest LLC, Ann Arbor*, MI, 2007. PhD thesis-McMaster University (Canada).

[11] J.E. Cremona and R.W.K. Odoni. Some density results for negative Pell equations; an application of graph theory. *J. London Math. Soc. (2)* 39:16-28, 1989.

[12] B. Datskovsky and D.J. Wright. Density of discriminants of cubic extensions. *J. Reine Angew. Math.* 386:116-138, 1988.

[13] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields, II. *Proc. Roy. Soc. Lond. A* 322:405-420, 1971.

[14] P.G.L. Dirichlet. Einige neue Sätze über unbestimmte Gleichungen. *Abh. K. Preuss. Akad. d. Wiss.* 649-664, 1834.

[15] J. Ellenberg, A. Venkatesh and C. Westerland. Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields. *Ann. of Math. (2)* 183:729-786, 2016.

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

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

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

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

[20] J.B. Friedlander, H. Iwaniec, B. Mazur and K. Rubin. The spin of prime ideals. *Invent. math.* 193:697-749, 2013.

[21] F. Gerth. The 4-class ranks of quadratic fields. *Invent. Math.* 77:498-515, 1984.

[22] D.R. Heath-Brown. The size of Selmer groups for the congruent number problem, II. *Invent. Math.* 118:331-370, 1994.

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

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

[25] J. Klys. The distribution of p-torsion in degree p cyclic fields. *Algebra Number Theory* 14:815-854, 2020.

[26] P. Koymans and D.Z. Milovic. Joint distribution of spins. *Duke Math. J.* 170:1723-1755, 2021.

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

[28] P. Koymans and C. Pagano. Higher genus theory. *Int. Math. Res. Not.*, To Appear, DOI: 10.1093/imrn/rnaa196.

[29] P. Koymans and C. Pagano. Higher Rédei reciprocity and integral points on conics. *arXiv preprint*, 2005.14157.

[30] P. Koymans and C. Pagano. A sharp upper bound for the 2-torsion of class groups of multiquadratic fields. *Mathematika*, To Appear, arXiv:2009.08399.

[31] R.J. Lemke Oliver, J. Wang and M.M. Wood. The average size of 3-torsion in class groups of 2-extensions. *arXiv preprint*, 2110.07712.

[32] M. Lipnowski, W. Sawin and J. Tsimerman. Cohen–Lenstra heuristics and bilinear pairings in the presence of roots of unity. *arXiv preprint*, 2007.12533.

[33] Y. Liu, M.M. Wood and D. Zureick-Brown. A predicted distribution for Galois groups of maximal unramified extensions. *arXiv preprint*, 1907.05002.

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

[35] H.L. Montgomery and R.C. Vaughan. Multiplicative number theory. I. Classical theory. *Cambridge Studies in Advanced Mathematics,* 97. Cambridge University Press, Cambridge, 2007.

[36] A. Morgan and A. Smith. The Cassels–Tate pairing for finite Galois modules. *arXiv preprint*, 2103.08530.

[37] T. Nagell. Über die Lösbarkeit der Gleichung $x^2 - Dy^2 = -1$. *Arkiv för Mat. Astr. Fysik* B 23:1-5, 1932.

[38] L. Rédei. Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. *J. reine angew. Math.* 171:131-148, 1935.

[39] L. Rédei. Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper. *J. reine angew. Math.* 180:1-43, 1939.

[40] L. Rédei and H. Reichardt. Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers. *J. reine angew. Math.* 170:69-74, 1934.

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

[42] A. Smith. 2^∞-Selmer Groups, 2^∞-class groups, and Goldfeld's conjecture. *arXiv preprint*, 1702.02325v2.

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

[44] P. Stevenhagen. Redei reciprocity, governing fields, and negative Pell. *Math. Proc. Camb. Philos. Soc.*, To Appear, DOI: 10.1017/S0305004121000335.

[45] T. Taniguchi and F. Thorne. Secondary terms in counting functions for cubic fields. *Duke Math. J.* 162:2451-2508, 2013.

[46] M. Watkins. Distribution of the 2-Selmer rank under twisting. `http://magma.maths.usyd.edu.au/~watkins/papers/Smith2Selmer.pdf`, retrieved 19 April 2021.

[47] M. Watkins. Notes on 4-Selmer and 8-class ranks. `http://magma.maths.usyd.edu.au/~watkins/papers/Smith4Selmer.pdf`, retrieved 19 April 2021.

[48] M.M. Wood. Nonabelian Cohen-Lenstra moments. With an appendix by the author and Philip Matchett Wood. *Duke Math. J.* 168(3):377–427, 2019.