MOMENTS OF UNRAMIFIED 2-GROUP EXTENSIONS OF QUADRATIC FIELDS

JACK KLYS

Abstract. We formulate a conjecture about moments of unramified extensions \( L/K \) with \( [K : \mathbb{Q}] = 2 \), \( G(L/K) = H \) and \( G(L/\mathbb{Q}) = G \) for any 2-group \( G \). We prove a formula for the number of such extensions for any fixed quadratic field \( K \) and for any \( G \) belonging to the class of central extensions of \( \mathbb{F}_2^n \) by \( \mathbb{F}_2 \) and use this to prove our conjecture for these extensions. In certain cases we obtain an explicit formula for the \( k \)th moment.

1. Introduction
1.1. Background. For any function \( f(K) \) defined on the set of quadratic fields let

\[
E_k^\pm(f) = \lim_{X \to \infty} \frac{\sum_{K, 0 < \pm D_K < X} f^k(K)}{\sum_{K, 0 < \pm D_K < X} 1}
\]

be the average of \( f^k \) over positive (resp. negative) discriminants.

For any pair of groups \( H \leq G \) with \( [G : H] = 2 \) define

\[
f(K) = |\{L/K \text{ unramified } \exists \phi : G(L/\mathbb{Q}) \cong G, \phi(G(L/K)) = H\}|.
\]

We call any such extension as in the definition of \( f \) a \((G, H)\)-extension. Things have been proven about \( E_k^\pm(f) \) for various pairs of groups \((G, H)\) and variants of \( f \). The Cohen-Lenstra heuristics predict \( E_k^\pm(f) \) for all \( k \) when \( H \) is an abelian \( p \)-group with \( p \) odd and \( G = H \rtimes C_2 \) with \( C_2 \) acting by inversion \([4]\). They are more commonly phrased as a statement about class groups, but can be interpreted in the above way using class field theory. The well known theorem of Davenport-Heilbronn gives \( E_1^\pm(f) \) for \( H \cong \mathbb{Z}/3\mathbb{Z} \) \([5]\). Bhargava computed \( E_1^\pm(f) \) for \((G, H) = (S_n, A_n)\) for \( n = 3, 4, 5 \) \([3]\). The work of Fouvry and Klüners on 4-ranks of class groups of quadratic fields (an extension of the Cohen-Lenstra heuristics to \( p = 2 \)) can be rephrased as computing \( E_k^\pm(f/2^{\omega(D_k)}) \) for \((D_8, C_4)\) for all \( k \) \([6]\).

For any even group \( G \) Wood conjectured that \( E_1^\pm(f) \) is finite (and gave a specific value) when there is a unique conjugacy class of order 2 elements not in \( H \) and infinite otherwise \([10]\). Brandon Alberts and the author investigated the latter case for the pair \((G, H) = (Q_8 \rtimes C_2, C_2)\) by computing a finite value for \( E_k^\pm(f/3^{\omega(D_k)}) \) for all \( k \) (here \( Q_8 \rtimes C_2 \) is the central product of \( D_8 \) and \( C_4 \) along \( C_2 \)) where \( f/3^{\omega(D_k)} \) is normalized precisely to make the moments finite \([1, 2]\). We refer the reader there for a more detailed exposition of all the above results.

In this paper we consider the generalization of this to all 2-groups \((G, H)\). In particular we formulate a conjecture about the asymptotics of \( f^k \) for any 2-groups \((G, H)\) as well as of a refinement of \( f \) (denoted \( f_T \) below). We determine a normalized function
\( f / \epsilon^{\omega(D_k)} \) which we conjecture has finite moments. We prove our conjectures in the case that \( G \) is a central extension of \( \mathbb{F}_2^n \) by \( \mathbb{F}_2 \). Furthermore we explicitly compute \( E_k^\pm (f_T / \epsilon^{\omega(D_k)}) \) in certain cases.

1.2. Conjectures. Let \( G \) be a finite 2-group with \( H \leq G \) a subgroup such that \( [G : H] = 2 \). We will call the pair \((G, H)\) admissible if there exists a \((G, H)\)-extension. This implies \( G \) can be generated by order 2 elements not contained in \( H \). Thus for example any pair \((G, H)\) with \( G \) an abelian 2-group of exponent greater than 2 is not admissible.

Let \( c \) be the number of conjugacy classes of order 2 elements in \( G \) which are not contained in \( H \).

**Conjecture 1.1.** Let \( G \) be a finite 2-group. Let \( H \leq G \) be a subgroup with \( [G : H] = 2 \) such that \((G, H)\) is admissible. Then

\[
E_k^\pm \left( \frac{f}{\epsilon^{\omega(D_k)}} \right) < \infty
\]

for all \( k \) and these moments determine a distribution. Furthermore

\[
\sum_{K, 0 < \pm D_k < X} f^k(K) \sim C(G, H) X (\log X)^{k-1}.
\]

We prove this conjecture for \( G \) which are central extensions of \( \mathbb{F}_2^n \) by \( \mathbb{F}_2 \). The suggestion that \( c \) controls the asymptotics for even groups appeared previously in the work of Wood [10]. She has shown that a suitable modification of the Malle-Bhargava field counting heuristics predicts the above asymptotic for \( k = 1 \) for any even group. She also proved this asymptotic for \( G \) elementary abelian and obtained a lower bound in a function field (see Sections 5, 6 and Theorem 1.2 in [10]).

In fact we will prove a refined conjecture. To state it we first refine the above definition of \( f \). Let \( \Phi(G) \) be the Frattini subgroup of \( G \) and let \( T \) be a generating set of the \( \mathbb{F}_2 \) vector space \( G / \Phi(G) \). We will call \( T \) admissible for \((G, H)\), or say that \((G, H, T)\) is admissible if \( T \) lifts to a generating set of order 2 elements of \( G \) not contained in \( H \).

For any \( L/K \) a \((G, H)\)-extension there is a canonical generating set \( U \) for \( G(L/\mathbb{Q}) / \Phi(G(L/\mathbb{Q})) \) which is not contained in \( G(L/K) \) and lifts to a generating set of order 2 elements (given by projecting the inertia groups). We define

\[
f_T(K) = \left| \{ L/K \text{ unramified} \mid \exists \phi : G(L/\mathbb{Q}) \cong G, \phi(G(L/K)) = H, \phi(U) = T \} \right|
\]

and call such an extension a \((G, H, T)\)-extension.

Let \( c_T \) denote the number of conjugacy classes of order 2 elements in \( G \) which lift an element of \( T \).

With this notation we make the following conjecture.

**Conjecture 1.2.** Let \( G \) be a finite 2-group. Let \( H \leq G \) be a subgroup with \( [G : H] = 2 \) and \( T \) a generating set of \( G / \Phi(G) \) such that \((G, H, T)\) is admissible. Let \( c_T \) be as
defined above. Then

\[ E^\pm_k \left( \frac{f_T}{c_T^{\omega(D_K)}} \right) < \infty \]

for all \( k \) and these moments determine a distribution. Furthermore

\[ \sum_{K,0<\pm D_K<X} f^k_T(K) \sim C(G,H,T) X (\log X)^{c_2^h-1}. \]

1.3. Main results. Let \( G \) be a central extension of \( \mathbb{F}_2^n \) by \( \mathbb{F}_2 \). Suppose \((G,H,T)\) is admissible.

**Theorem 1.3.** Let \( G \) be a central extension of \( \mathbb{F}_2^n \) by \( \mathbb{F}_2 \) and let \((G,H,T)\) be admissible. Suppose \( G \) is not elementary abelian. Then Conjectures 1.1 and 1.2 are true.

We now define the following additional condition on \( T \).

**A.1** There do not exist \( x_i, x_j, x_k \in G \) lifting elements in \( T \), such that \([x_i, x_j] \neq 1, [x_j, x_k] \neq 1 \) and \([x_i, x_k] = 1 \).

The property in [A.1] is equivalent to \( \langle x_i, x_j, x_k \rangle \cong (C_2 \times C_4) \rtimes_{-1} C_2 \) with \( C_2 \times C_4 \subset H \) and \( C_2 \) acting by inversion (see Lemma 4.6). This condition is independent of chosen lift. In this case we compute the moments explicitly.

We need some more notation to state the next theorem. For any admissible generating set \( T \) with \(|T| = r \), and any set of lifts \( \{x_1, \ldots, x_r\} \) let \( r_1 = |\{x_i \mid x_i \notin Z(G)\}| \) and \( r_2 = r - r_1 \). Furthermore consider the graph with vertices \( \{1, \ldots, r_1\} \) where \( i,j \) are connected if \( x_i \) and \( x_j \) do not commute in \( G \) and let \( C_1, \ldots, C_s \) be the connected components. Let \( s_2 \) be the number of connected components of size 2 and \( s_1 = s - s_2 \). Let \( C_{s+1} = \{r_1 + 1, \ldots, r\} \). These quantities are also independent of chosen lifts. Let \( Aut_{H,T}G \leq AutG \) be the subgroup preserving the sets \( H \) and \( T \).

We remark that we prove the following theorem only for odd discriminants but the proofs in the other cases are analogous and the final answer is expected to be the same (in the real and imaginary cases respectively).

**Theorem 1.4.** Let \( G \) be a central extension of \( \mathbb{F}_2^n \) by \( \mathbb{F}_2 \) and let \((G,H,T)\) be admissible. Suppose \( G \neq D_8 \) and \( G \) is not elementary abelian. Suppose \( T \) satisfies (A.1). Then summing over odd discriminants

\[ E^\pm_k \left( \frac{f_T}{c_T^{\omega(D_K)}} \right) = \left( \frac{2^{s_1+2s_2-r+n+1}}{|Aut_{H,T}G|} \sum_{m \equiv a(2)} \sum_{m_1=0,1(4)} \prod_{i=1}^{s+1} \left( \frac{|C_i|}{m_i} \right) \right)^k \]

where \( a = 0,1 \) in the +, - cases respectively. Thus the values of the function \( f_T(K)/c_T^{\omega(D_K)} \) determine a point-mass distribution supported at

\[ \frac{2^{s_1+2s_2-r+n+1}}{|Aut_{H,T}G|} \sum_{m \equiv a(2)} \sum_{m_1=0,1(4)} \prod_{i=1}^{s+1} \left( \frac{|C_i|}{m_i} \right). \]
The case $G = D_8$ is not covered by our proof (the precise point where this comes up is the proof of Proposition 4.7) but is already solved. The pair $(D_8, C_4)$ is the above mentioned work of Fouvry and Klüners [6] and the pair $(D_8, C_2 \times C_2)$ is not admissible.

The condition (A.1) is imposed to make the highly combinatorial proofs more manageable, and we do not expect that it is a crucial obstruction.

1.4. **Plan of the proof.** In Section 3 we prove a formula for the number of $(G, H, T)$-extensions of any quadratic field (see Theorem 3.5). In Sections 4 and 5 we prove Theorem 1.3. The method developed by Fouvry and Klüners [6] and its extension in [2] show that the asymptotics are controlled by maximal unlinked sets (see 4.2 for the definition). Determining these sets is a crucial part of the proof and is done in Section 4. In Section 6 we prove Theorem 1.4 by extending the computations in [2].

1.5. **Acknowledgements.** The author would like to thank Brandon Alberts, Jacob Tsimerman and Melanie Wood for their helpful comments on the final drafts.

2. **Preliminaries**

Let $K = \mathbb{Q}(\sqrt{d})$. Let $G$ be a central extension of $\mathbb{F}_2^n$ by $\mathbb{F}_2$ and let $L$ be an unramified extension of $K$ with $\phi : G(L/\mathbb{Q}) \cong G$ such that $\phi(G(L/K)) = H$. We want to define a canonical (up to multiplication by the distinguished central element) generating of $G(L/\mathbb{Q})$.

Let $L^g = L \cap K^{gen}$ where $K^{gen} = \mathbb{Q}(\sqrt{q_1}, \ldots, \sqrt{q_r})$ and the $q_i$ are prime discriminants with $\prod q_i = d$. It is easy to show that $L^g = K(\sqrt{d_1}, \ldots, \sqrt{d_n})$ where $d_i \mid d$ and are independent modulo $(\mathbb{Q}^*)^2$.

It is clear that $G(L^g/\mathbb{Q}) \cong C_2^n$ and we can pick the isomorphism such that the standard basis element $e_i \in C_2^n$ projects nontrivially onto $G_i = G(K\sqrt{d_i}/\mathbb{Q})$. For any prime $p \mid d$ in $L$ let $I_p \subset G$ be the inertia group.

For each $1 \leq i \leq n$ pick some prime $p_i \mid d_i$ and such that $I_{p_i}$ projects onto $e_i$ and let $I_{p_i} = \langle y_i \rangle$. Let $\langle a \rangle$ be the distinguished central subgroup of $G$ of order 2. Note this implies there are only two choices for $y_i$ and they are off by a multiple of $a$.

**Definition 2.1.** We call $L/K$ a $(G, H, T)$-extension if there exists an isomorphism $\phi : G(L/\mathbb{Q}) \cong G$ such that $\phi(G(L/K)) = H$ and $\phi(U) = T$.

Let $c_T$ denote the number of conjugacy classes of order 2 elements in $G$ which lift an element of $T$.

3. **The formula**

The main goal of this section is to obtain a formula for the function $f_T(K)$ which gives the number of $(G, H, T)$-extensions of a quadratic field $K$ for any fixed admissible $(G, H, T)$.

First we define a notion which will be helpful to this end, using ideas of Lemmermeyer from [8]. The field $L$ can be written as $L = L^g(\sqrt{\mu})$ for some $\mu \in L^g$. Then since
$L/L^g$ is a Kummer extension we see that $\mu^{e_ie_j} / 2 = \mu$ in $L^g$. Let $\alpha^{g}_{ij} = \mu^{e_ie_j-1}$. Then $(\alpha^{g}_{ij})^{1+e_ie_j} = \mu^{(e_ie_j-1)(e_ie_j+1)} = 1$. Hence $\alpha^{1+e_ie_j} = \pm 1$. Define $S(\mu) \in \mathbb{F}_2$ by

$$S(\mu)_{ij} = \begin{cases} 1 & \text{if } \alpha^{1+e_ie_j} = -1 \\ 0 & \text{if } \alpha^{1+e_ie_j} = +1. \end{cases}$$

Lemma 3.1. $y_i$ and $y_j$ commute in $G$ if and only if $S(\mu)_{ij} = 0$.

Proof. Since the $y_i$ have order 2 we have $[y_i, y_j] = (y_iy_j)^2$. We have $\sqrt{\mu^{e_ie_j}} = \alpha_{ij}\sqrt{\mu}$ and hence $\sqrt{1 + a + b\sqrt{\mu}} = a + \alpha_{ij}^{1+e_ie_j} b\sqrt{\mu}$ for $a, b \in L^g$. Thus $y_iy_j$ has order 2 if and only if $\alpha_{ij}^{1+e_ie_j} = 1$ and the result follows.

This lemma in particular shows that the group $G$ is determined by the choice of $e_i$'s along with $S(\mu)$ (up to permutation of the entries) since $G$ is generated by the $y_i$ which by definition have order 2, and $S(\mu)$ encodes the relations between them. Then it is clear that $S(\mu) = 0$ in $\mathbb{F}_2^{e_i}$ if and only if $G = C^{n+1}_2$.

Lemma 3.2. Suppose $L$ and $L'$ are both $(G,H,T)$-extensions with $L = L^g (\sqrt{\mu})$ and $L' = L^g (\sqrt{\nu})$. Then $\mu \overset{2}{=} \nu \delta$ for some $\delta \in \mathbb{Z}$ a fundamental discriminant such that $\delta | d$. Conversely for any fundamental discriminant $\delta \in \mathbb{Z}$ such that $\delta | d$ we have that $L^g (\sqrt{\delta\mu})$ is a $(G,H,T)$-extension.

Proof. Let $M = LL'$ and let $L''$ be the third quadratic extension of $L^g$ contained in $M$, so $L'' = L^g (\sqrt{\mu\nu})$. Let $\beta_{ij}^2 = \nu^{e_ie_j-1}$. Then $(\alpha_{ij} \beta_{ij})^2 = (\mu\nu)^{e_ie_j-1}$. Hence $S(\mu\nu)_{ij} = S(\mu)_{ij} + S(\nu)_{ij}$.

Let $\varphi : G(L/Q) \cong G(L'/Q)$ such that $\varphi|_{G(L^g/Q)} = id$ (note such an isomorphism always exists). From the existence of $\varphi$ we see that $S(\mu)_{ij} = S(\nu)_{ij}$ for all $i, j$, and thus $G(L''/Q) \cong C^{n+1}_2$. This implies $\mu\nu \overset{2}{=} \delta \in \mathbb{Z}$ and $\delta$ can be chosen to be a fundamental discriminant. Since $L$ and $L'$ are unramified over $K = Q (\sqrt{\mu})$ so is $L''$, and hence $\delta | d$.

Now suppose $\delta \in \mathbb{Z}$ is a fundamental discriminant such that $\delta | d$. From the definitions it is clear that $S(\mu) = S(\delta\mu)$ and hence there is a $\varphi : G(L^g (\sqrt{\delta\mu})/Q) \cong G(L^g (\sqrt{\mu})/Q)$ such that $\varphi|_{G(L^g/Q)} = id$. This implies $L^g (\sqrt{\delta\mu})$ is a $(G,H,T)$-extension.

Proposition 3.3. If there exists a quadratic extension $L$ of $K (\sqrt{d_1}, \ldots, \sqrt{d_n})$ which is unramified over $K$ with $G(L/Q) \cong G$ then there are exactly $2^{w(\delta)-n}$ such extensions.

Proof. If $L = K (\sqrt{d_1}, \ldots, \sqrt{d_n}) (\sqrt{\mu})$ then by Lemma 3.2 every other such extension is of the form $L^g (\sqrt{\delta\mu})$ for some fundamental discriminant $\delta | d$. Define the $\mathbb{F}_2$ vector space $V = \langle q_1, \ldots, q_{w(\delta)} \rangle / \langle q_1^2, \ldots, q_{w(\delta)}^2 \rangle$ where the $q_i$ are the divisors of $d$ which are prime fundamental discriminants or one of $\{-4, \pm 8\}$. Then the number of such extensions which are distinct is the size of the vector space $V/ \langle d_1, \ldots, d_n \rangle$, which is clearly $2^{w(\delta)-n}$ (recall the $d_i$ are all independent mod $Q^{*2}$). □
For \(a, b \in \mathbb{Q}\) let \((a, b)\) denote the cyclic algebra in \(\text{Br}(\mathbb{Q})\) defined by
\[
(a, b) = K\langle u, v \rangle / \langle u^2 = a, v^2 = b, uv = -vu \rangle.
\]
Recall that there is an injection
\[
\text{inv} : \text{Br}(\mathbb{Q}) \hookrightarrow \prod_v \text{Br}(\mathbb{Q}_v) = \prod_v \mathbb{Q}/\mathbb{Z}.
\]
Since \((a, b)\) has order 2 we can view each factor of the image of \(\text{inv}\) as lying in \(\frac{1}{2}\mathbb{Z}/\mathbb{Z}\). Identify this group with \((\pm 1)\). Denote by \((a, b)_v\) the Hilbert symbol at \(v\). Then the crucial property we will need is
\[
\text{inv}_v((a, b)) = (a, b)_v.
\]

We will use the following theorem, stated as Theorem 1.2 in [9].

**Theorem 3.4 (Embedding Criterion [9]).** Let \(K = F(\sqrt{d_1}, \ldots, \sqrt{d_n})\), where the \(d_i\)'s are elements of \(F^*\) independent modulo \(F^*\). Let \(G = \text{Gal}(K/F)\), and consider a non-split central extension \(G^*\) of \(\mathbb{F}_2\) by \(G\). Let \(t_1, \ldots, t_n\) generate \(G\), where \(x_i\sqrt{d_j} = (-1)^{\delta(i,j)}\sqrt{d_j}\) and let \(x_1, \ldots, x_n\) be any set of preimages of \(t_1, \ldots, t_n\) in \(G^*\). Define \(c_{ij} = 1\) if \([x_i, x_j] \neq 1\) and 0 otherwise for \(i \neq j\) and \(c_{ii} = 1\) if \(x_i^2 \neq 1\).

There exists a Galois extension \(L/F, K \subset L\) such that \(\text{Gal}(L/F) \cong G^*\) and the surjection \(G^* \twoheadrightarrow G\) is the natural surjection of Galois groups, if and only if
\[
\prod_{i \leq j} (d_i, d_j)^{c_{ij}} = 1 \in \text{Br}(F).
\]

We will call a set of \(n\) fundamental discriminants \(d_i \mid d\) independent modulo \(\mathbb{Q}^*\) an independent set of factors and identify two distinct sets if their span is equal in \(\mathbb{Q}^*/\mathbb{Q}^*\). Let \(D\) denote the set of all independent sets of factors.

Let \(\text{Aut}_{H,T,G}\) be the subgroup of \(\text{Aut}G\) preserving the set \(H\) and the set \(T\). Finally let \(S_i = \{1 \leq j \leq r \mid [x_i, x_j] \neq 1\}\).

**Theorem 3.5.** Suppose \((G, H, T)\) is admissible. Let \(T = \{t_1, \ldots, t_r\}\). Then
\[
f_T(d) = \frac{1}{2^n |\text{Aut}_{H,T,G}|} \sum_{d = d_1 \cdots d_r} \prod_{i=1}^r \prod_{p|d_i} \left(1 + \left(\prod_{j \in S_i} \frac{d_j}{p}\right)\right)
\]
where the sum is over factorizations into coprime fundamental discriminants.

**Proof.** Let \(d_1', \ldots, d_n'\) be an independent set of factors. Let \(t_1', \ldots, t_n'\) be a basis for \(G/\Phi(G)\). Let \(S_i' = \{1 \leq j \leq n \mid [x_i, x_j] \neq 1\}\). By Theorem 3.4 there exists a \((G, H, T)\)-extension \(L/\mathbb{Q}\) with \(L^g = K(\sqrt{d_1'}, \ldots, \sqrt{d_n'})\) if and only if
\[
\prod_{j < i, j \in S_i'} (d_i', d_j') = 1
\]
in \(\text{Br}(\mathbb{Q})\). By the discussion preceding this theorem this is equivalent to the condition that
\[
\prod_{j < i, j \in S_i'} (d_i', d_j')_v = 1 \quad \text{for all places } v \text{ of } \mathbb{Q}.
\]
This is trivially satisfied for $p \nmid d'$.

Let $\alpha_i(p) = \text{ord}_p d'_i$, and let $\alpha_{i,j}(p) = \alpha_i(p) \alpha_j(p)$. Note the property of the Hilbert symbol $(d'_i, d'_j)_v = (d'_j, d'_i)_v$. Then the condition at odd $p$ becomes

$(-1)^{\frac{p-1}{2}} \sum_{j < i, j \in S'_i} \alpha_{i,j}(p) \left( \frac{\prod_{j < i, j \in S'_i} (d'_j/p^{\alpha_j(p)})^{\alpha_i(p)} (d'_i/p^{\alpha_i(p)})^{\alpha_j(p)}}{p} \right) = 1$

and at $p = 2$ becomes

$-\sum_{j < i, j \in S'_i} \alpha_{i,j}(2) \left( \frac{d'_i}{d'_j} \right)^{2-1} \sum_{j < i, j \in S'_i} \alpha_{i,j}(2) \left( \frac{d'_j}{d'_i} \right)^{2-1} = 1$.

Since we can choose the $d'_1, \ldots, d'_n$ such that at most one is divisible by 2, and a fundamental discriminant is congruent to 1 mod 4 if it is odd, the last condition reduces to, for some fixed $i$

$-\sum_{j \in S'_i} \alpha_{i,j}(2) \left( \frac{d'_j}{d'_i} \right)^{2-1} = \left( \frac{\prod_{j \in S'_i} d'_j}{2} \right)$

Thus the existence of such an extension is equivalent to

$(3.1) \prod_{p|d} \left( 1 + (-1)^{\frac{p-1}{2}} \sum_{j < i, j \in S'_i} \alpha_{i,j}(p) \left( \frac{\prod_{j < i, j \in S'_i} (d'_j/p^{\alpha_j(p)})^{\alpha_i(p)} (d'_i/p^{\alpha_i(p)})^{\alpha_j(p)}}{p} \right) \right) \neq 0$

and if $2 | d$ additionally

$1 + \left( \frac{\prod_{j \in S'_i} d'_j}{2} \right) \neq 0$.

By Proposition 3.3 if such an extension $L/\mathbb{Q}$ exists, there are exactly $2^{\omega(d) - n}$ such extensions intersecting $K^{gen}$ at $L^g$. Hence for any independent set of factors $\{d'_1 \cdots d'_n\} \in \mathcal{D}$ the formula (3.1) divided by $2^n$ gives the number of relevant extensions of $K(\sqrt{d_1}, \ldots, \sqrt{d_n})$.

We rewrite the formula (3.1) further. Write $t_i = \sum_{j \in U_i} t'_j$ for $i = 1, \ldots, r$. This implies that there exists a coprime factorization $d = \prod_{i=1}^r d'_i$ such that $d'_j = \prod_{i,j \in U_i} d_i$ for each $1 \leq j \leq n$. There is a bijective correspondence between independent sets of factors and such coprime factorizations.

Since each $x_i$ has order 2 this implies that the number of subsets $\{j_1, j_2\} \subset U_i$ satisfying $[x_{j_1}, x_{j_2}] \neq 1$ is even. Note that for $1 \leq i \leq n \alpha_i(p) = 1$ if and only if $p | d_j$ and $i \in U_j$ for some $1 \leq j \leq r$. This combined with the previous fact implies that $\sum_{j < i, j \in S'_i} \alpha_{i,j}(p)$ is even.
Now we partition the product over \( p \mid d \) in (3.1) by the \( d_i \). Let \( 1 \leq i \leq r \) and \( p \mid d_i \) with \( p \) odd. Recall this implies \( \alpha_j (p) = 1 \) for all \( j \in U_i \). Fix \( j \). Then

\[
\prod_{k \in S_j'} \left( \frac{d_j'/p^{\alpha_j(p)}}{d_k'/p^{\alpha_k(p)}} \right)^{\alpha_j(p)} = \prod_{k \in S_j' \cap U_i} \left( \frac{d_j'/p^{\alpha_j(p)}}{d_k'/p^{\alpha_k(p)}} \right)^{\alpha_j(p)} \times \prod_{k \in S_j' \setminus U_i} \left( \frac{d_k'/p^{\alpha_k(p)}}{d_j'/p^{\alpha_j(p)}} \right)^{\alpha_j(p)} = \left( \frac{d_j'/p^{\alpha_j(p)}}{p} \right)^{|S_j' \cap U_i|} \cdot a
\]

for some \( a \). Hence considering the contribution for each \( j \) we see that for any \( l \neq i \) the power of \( d_l \) in the factor corresponding to \( d_i \) in (3.1) will be \( \sum_{j \in U_l} |S_j' \cap U_i| \) which is odd exactly when \( x_l \) and \( x_i \) do not commute. Thus this factor is

\[
\prod_{p \mid d_i} \left( 1 + \left( \frac{\prod_{j \in S_i} d_j}{p} \right) \right).
\]

Now suppose \( p \mid d_i \) and \( p = 2 \). Recall we fixed some \( i \) such that \( 2 \mid d_i' \) and \( 2 \nmid d_j' \) for \( j \neq i \). By construction of the \( d_1, \ldots, d_r \) this implies that if \( 2 \mid d_i \) then \( d_i = d_i' \). Thus the above formula also holds for \( p = 2 \).

This proves the theorem. \( \square \)

**Remark 3.6.** Note that if \( S_i \) is empty then \( \left( \frac{\prod_{j \in S_i} d_j}{p} \right) = 1 \) so the formula can be written

\[
(3.2) \quad f_T (d) = \frac{1}{2^{|\text{Aut}_{H,T} G|}} \sum_{d = d_1 \cdots d_r} 2^{\omega(\Pi_{i, S_i \neq \emptyset} d_i)} \prod_{i, S_i \neq \emptyset} \prod_{p \mid d_i} \left( 1 + \left( \frac{\prod_{j \in S_i} d_j}{p} \right) \right).
\]

**4. Asymptotic Analysis of the Formula**

We will now look at the growth of the function (3.2) as \( d \) ranges over all odd fundamental discriminants. First we will make some heuristic considerations to see what kind of behaviour to expect. If we expect the legendre symbol to take each value \( \pm 1 \) with probability \( 1/2 \) then the expected value of \( \prod_{i, S_i \neq \emptyset} \prod_{p \mid d_i} \left( 1 + \left( \frac{\prod_{j \in S_i} d_j}{p} \right) \right) \) is

\[
\frac{1}{2^{\omega(\Pi_{i, S_i \neq \emptyset} d_i)}} \sum_{d = d_1 \cdots d_r} 2^{\omega(\Pi_{i, S_i \neq \emptyset} d_i)} \left( 1 - \frac{1}{2^{\omega(\Pi_{i, S_i \neq \emptyset} d_i)}} \right) 0 = 1.
\]
Let \( r_1 = |\{ i \mid S_i \neq \emptyset \}| \) and \( r_2 = r - r_1 \). Hence on average we expect

\[
2^n |\text{Aut}_{H,T}G| f_T (d) = \sum_{d=d_1 \cdots d_r} 2^\omega(\prod_{i,s_i=a} d_i)
\]

\[
= \sum_{i=0}^{\omega(d)} 2^i \left( \omega (d) \right) r_2^i r_1^{\omega(d) - i}
\]

\[
= r_1^{\omega(d)} \sum_{i=0}^{\omega(d)} \left( \frac{2r_2}{r_1} \right)^i \left( \omega (d) \right) i
\]

\[
= r_1^{\omega(d)} \left( 1 + \frac{2r_2}{r_1} \right)^{\omega(d)}
\]

\[
= (r_1 + 2r_2)^{\omega(d)}.
\]

Thus we expect \( \sum_{d < X} f_T (d) \sim C(G, H, T) X (\log X)^{r_1 + 2r_2 - 1} \) for some constant \( C(G, H, T) \).

We will show that this is the case.

We give an interpretation of the quantity \( r_1 + 2r_2 \).

**Lemma 4.1.** Let \( c_T \) be the number of conjugacy classes in \( G \) of the set \( \{ x_i, x_i a \mid i = 1, \ldots, r \} \). Let \( r_1 = |\{ i \mid S_i \neq \emptyset \}| \) and \( r_2 = r - r_1 \). Then \( c_T = r_1 + 2r_2 \).

**Proof.** If \( S_i = \emptyset \) then \( x_i \) commutes with all the \( x_j \). Hence \( x_i \in Z(G) \) and there are the two conjugacy classes \( \{ x_i \} \) and \( \{ x_i a \} \) (recall \( a \) is the distinguished central element of order 2). If \( S_i \neq \emptyset \) then there is the conjugacy class \( \{ x_i, x_i a \} \).

**4.1. The quadratic form.** Define a quadratic form on \( \mathbb{F}_2^n \) by

\[
Q(u) = \sum_{i<j} a_{ij} u_i u_j
\]

where \( a_{ij} = 1 \) if \( [x_i, x_j] \neq 1 \) and 0 otherwise. It has an associated symmetric bilinear form \( B(u, v) = Q(u + v) + Q(u) + Q(v) \) on \( \mathbb{F}_2^n \times \mathbb{F}_2^n \). Alternately \( B(u, v) = u^T A v \) where \( A \) is the symmetric matrix given by \( A_{ij} = a_{ij} \) as defined above. It is easy to see by explicit computation that for any \( x = \prod_{i=1}^n x_i^{u_i} \) in \( G \) with \( u \in \mathbb{F}_2^n \), \( x \) has order 2 if and only if \( Q(u) = 0 \). Furthermore if \( y = \prod_{i=1}^n x_i^{v_i} \) and \( u, v \) have disjoint supports then \( [x, y] = 1 \) if and only if \( B(u, v) = 0 \).

**Lemma 4.2.** Let \( x = \prod_{i=1}^n x_i^{u_i} \) and \( y = \prod_{i=1}^n x_i^{v_i} \). Then \( [x, y] = 1 \) if and only if \( B(u, v) = 0 \).
Proof. Write \( u = u' + z \) and \( v = v' + z \), where the support of \( u', v' \) are disjoint. Then \([x, y] = 1\) if and only if

\[
0 = \sum_{i,j=0}^{n} a_{ij}v'_i z_j + \sum_{i,j=0}^{n} a_{ij}v'_i u'_j + \sum_{i,j=0}^{n} a_{ij}u'_i z_j
\]

\[
= v'^T Az + v'^T Au' + u'^T Az
\]

\[
= B(u',v') + B(u',z) + B(v',z) + B(z,z)
\]

\[
= B(u,v).
\]

\( \square \)

We collect some facts regarding quadratic forms in characteristic 2. We can decompose \( \mathbb{F}_2^n = V \oplus R \oplus R_0 \), where \( R \oplus R_0 = \mathbb{F}_2^{n \perp} \) and \( Q(R_0) = 0 \). Hence \( Q \) is non-degenerate on \( V \) and it is easy to see that \( \dim R = 0 \) or 1.

We call a subspace \( W \subset \mathbb{F}_2^n \) totally singular for \( Q \) if \( Q(W) = 0 \).

Proposition 14.6 from [7] states that if \( Q \) is nondegenerate, given any totally singular space there exists another one disjoint from it. We extend this result to the case when \( Q \) degenerate and \( \ker Q \mid R_{n \perp} = 0 \). In the above notation this means \( \mathbb{F}_2^n = V \oplus R \). Let \( p_R \) be the projection onto \( R \).

Lemma 4.3. Let \( Q \) be a quadratic form on \( \mathbb{F}_2^n \) and let \( R = \mathbb{F}_2^{n \perp} \). Suppose \( \ker Q \mid R = 0 \). Given any totally singular subspace \( W \) there exists another one \( W' \) of the same size such that \( W \cap W' \subset \langle u \rangle \) with \( p_R (u) \neq 0 \).

Proof. As noted above we have \( \mathbb{F}_2^n = V \oplus R \). Note the subspace \( W_0 = W \cap V \) has index 2 in \( W \).

We can apply Proposition 14.6 from [7] to \( W_0 \) to obtain a totally singular subspace \( W_1 \subset V \) of the same size such that \( W_0 \cap W_1 = 0 \). Furthermore \( W_0 \) has basis \( \{u_1, \ldots, u_k\} \) and \( W_1 \) has basis \( \{v_1, \ldots, v_k\} \) and \( H_i = \langle u_i, v_i \rangle \) is hyperbolic, meaning \( B(u_i, v_i) = 1 \), and \( B(H_i, H_j) = 0 \) for \( i \neq j \).

Let \( u \in W \setminus W_0 \). If we let \( v \) be the element obtained by applying to \( u \) the transposition exchanging \( u_i \) and \( v_i \) for all \( i \) then by symmetry \( v \in W_1 \) (taken in \( \mathbb{F}_2^n \)) and \( Q(v) = 0 \) and \( p_R (v) \neq 0 \). Note that \( u = v \) is possible. Then \( W' = \langle W_1, v \rangle \) satisfies the desired properties. \( \square \)

4.2. Maximal unlinked sets. Define a set of elements \( F = \{w, v_w | w \in \mathbb{F}_2^n\} \). We define \( u, v \in F \) to be linked if \( u = u_w \) and \( v = v_z \) and \( B(w, z) = 1 \). Otherwise we say \( u \) and \( v \) are unlinked. Define \( L(u, v) = 0 \) if they are unlinked and 1 if they are linked. For \( u, v \in F_k \) let \( L_k(u, v) = \sum_{i=1}^{k} L(u_i, v_i) \) and define them to be unlinked if \( L_k(u, v) = 0 \) and linked otherwise. Additionally for any subsets \( F_1 \subset F \) and \( V \subset \mathbb{F}_2^n \) we say \( F_1 \) is supported on \( V \) if every element of \( F_1 \) is of the form \( u_w \) or \( v_w \) for some \( w \in V \). Let \( s(F_1) \) be the support of \( F_1 \).
For each \( i = 1, \ldots, r \) let \( d_i = D_{2i-1}D_{2i} \). Let \( U = \{1, \ldots, 2r\} \). Note that the formula (3.2) can be expanded as

\[
f_T(d) = \frac{1}{2^n |\text{Aut}_{H,T}G|} \sum_{d = 1}^{n} \prod_{u,v \in U} \left( \frac{D_u}{D_v} \right)^{\Phi(u,v)}
\]

where \( \Phi(u,v) \in \mathbb{F}_2 \). That is \( \Phi(u,v) = 1 \) if the symbol \( \left( \frac{D_u}{D_v} \right) \) appears in the expression and 0 otherwise. For \( u, v \in U^k \) define \( \Phi_k(u,v) = \sum_{i=1}^{k} \Phi(u_i, v_i) \). Then we define \( u, v \in U^k \) to be unlinked if

\[
\Phi_k(u, v) + \Phi_k(v, u) = 0.
\]

For any \( 1 \leq i \leq r \), if \( x_i = \prod_{j=1}^{n} x_j^{w_j} \) define a mapping \( \varphi : U \longrightarrow F \) by

\[
2i - 1 \mapsto u_w, \quad 2i \mapsto v_w.
\]

Then it is easy to see that \( \Phi_k = L \circ \varphi \).

**Theorem 4.4.** The size of a maximal unlinked set in \( U \) is \( c_T \).

**Proof.** Decompose \( \mathbb{F}_n^2 = V \oplus R \oplus R_0 \), where \( R \oplus R_0 = \mathbb{F}_n^{\perp} \) and \( Q(R_0) = 0 \). Let \( Y = V \oplus R \).

Suppose \( U \subset F \) is a maximal unlinked set supported on \( U \). Let \( s(U) = s(U) \cap (Y + z) \) for any \( z \in R_0 \) (recall \( s(U) \) is the support of \( U \)). Let \( U_z = U \cap \{u_w, v_w \mid w \in s(U) \} \). Define \( U_z + z = \{u_{w+z} \mid u_w \in U_z\} \cup \{v_{w+z} \mid v_w \in U_z\} \). Then \( U_z + z \) is an unlinked set in \( Y \). We will show that for any unlinked set \( U' \) with \( s(U') \subset Y \) we have \( |U'| \leq |s(U')| \).

Then since \( s(U) \cap R_0 \) is in bijective correspondence with elements of \( T \) which are not central and \( |s(U) \cap R_0| = \sum_{z \in R_0} |s(U) \cap \{z\}| \) the result follows.

First let \( U \) be a maximal unlinked with \( s(U) = \{w_1, \ldots, w_r\} \subset Y \setminus H \). Then let \( \{w_1, \ldots, w_m\} \subset \{w_1, \ldots, w_r\} \) be exactly the elements of degree 0 (in the subgraph on \( \{w_1, \ldots, w_r\} \)). Then either \( u_w \in U \) or \( v_w \in U \) for all \( w \in \{w_{m+1}, \ldots, w_r\} \). Furthermore

\[
\{w_1, \ldots, w_m\} = \{w \in Y \mid u_w \text{ and } v_w \in U\}.
\]

Next we show that \( m \leq s(U) - r' \) which will imply that

\[
|U| = (r' - m) + 2m
\]

\[
\leq s(U).
\]

By Lemma 4.2 \( B(w_i, w_j) = 0 \) for all \( i, j \) and clearly \( Q(w_i) = 0 \) for all \( i \). The set \( \{w_1, \ldots, w_m\} \) can be extended to a totally singular subspace \( W \) of \( Y \) whose size is maximal among all containing \( \{w_1, \ldots, w_m\} \).

If \( \dim V \oplus R \) is even then \( R = 0 \). If \( \dim V \oplus R \) is odd then \( R = \langle z \rangle \) and \( Q(z) = 1 \). Let \( p_R \) be the projection onto \( R \). Note the subspace \( \{x \in W \mid p_R(x) = 0\} \) has index 2 in \( W \). By Lemma 4.3 there exists a subspace \( W' \subset Y \) such that \( W \cap W' \subset \langle w \rangle \) for some \( w \) with \( p_R(w) \neq 0 \).

First suppose \( w \notin \{w_1, \ldots, w_m\} \). Let \( W_0 \subset W' \) be the set of all elements \( w \) such that \( B(w_i, w) = 1 \) for some \( i = 1, \ldots, m \). If \( |W_0| < m \) then \( W_1 = (W' \setminus W_0) \cup \{w_1, \ldots, w_m\} \) is a strictly larger totally singular space containing \( \{w_1, \ldots, w_m\} \). If \( |W_0 \setminus H| < m \) then
Lemma 4.6. Let $\con{\mathbb{T}}$ restriction on the generating set Maximal unlinked sets, the special case.

Proof. Let $x \in \{w_1, \ldots, w_m\}$ apply the above argument to $\{w_1, \ldots, w_m\} \setminus w$. Then it is clear there exists some $w' \in Y \setminus H$ such that $B(w, w') = 1$ and since $w \in W'$ this implies $w' \not\in W'$. Thus $|W_0 \setminus H| \geq m$. Since $\mathcal{U}$ is maximal unlinked this implies $(W_0 \setminus H) \cap \{w_1, \ldots, w_m\} = \emptyset$. Thus $m \leq s(\mathcal{U}) - r'$ as desired.

If $\mathcal{U}$ is a maximal unlinked set in $Y \cap H$ the argument is identical. This proves the theorem. □

Proposition 4.5. The size of a maximal unlinked set in $U^k$ is $c_T^k$.

Proof. As in Theorem 1.4 decompose $\mathbb{F}_2^n = V \oplus R \oplus R_0$, where $R \oplus R_0 = \mathbb{F}_2^k$ and $Q(R_0) = 0$. Let $Y = V \oplus R$. Let $q$ be the projection onto the last coordinate. We will show that an unlinked set $\mathcal{U}'$ with $s(q(\mathcal{U}')) \subset Y$ has $|\mathcal{U}'| \leq s(q(\mathcal{U}')) \cdot c_T^{k-1}$. Then the result will follow by summing over all cosets of $Y$ in $\mathbb{F}_2^n$ as before.

We prove this by induction on $k$. The base case is Theorem 1.4.

Let $\mathcal{U} \subset F^{k-1} \times s^{-1}(Y)$ be an unlinked set with $s(q(\mathcal{U})) = \{w_1, \ldots, w_r\} \subset Y \setminus H$ (in the case $\{w_1, \ldots, w_r\} \subset Y \cap H$ the proof is identical). Without loss of generality assume that $\{w_1, \ldots, w_m\} \subset \{w_1, \ldots, w_r\}$ are exactly the elements of degree 0 (in the subgraph on $\{w_1, \ldots, w_r\}$).

Let $\mathcal{U}_i = \{u \in \mathcal{U} | u_k = i\}$ for any $i \in s^{-1}(\{w_1, \ldots, w_r\})$. Let $b_w = |\mathcal{U}_{uw}| + |\mathcal{U}_{uw}'|$ for any $w \in \{w_1, \ldots, w_r\}$. Let $p$ be the projection onto the first $k - 1$ coordinates. Let $X_i = p(\mathcal{U}_i)$. It is easy to see that $X_i$ is an unlinked set for all $i$. It is clear that $|X_i| \leq c_T^{k-1}$ for all $i$. Hence $b_w \leq 2c_T^{k-1}$ for each $w \in \{w_1, \ldots, w_r\}$. Furthermore for each $w \in \{w_{r+1}, \ldots, w_r\}$ it is easy to show that $b_w \leq c_T^{k-1}$. By completing $\{w_1, \ldots, w_m\}$ to a totally singular space and using the same argument as in Theorem 1.4 we see there exist at least $m$ distinct elements $w$ with $b_w = 0$ which implies that $r' + m \leq r$. It follows that

$$\sum_{i=1}^{r'} b_{w_i} \leq \sum_{1}^{m} 2c_T^{k-1} + \sum_{m+1}^{r'} c_T^{k-1} = s(q(\mathcal{U})) c_T^{k-1}.$$ 

This completes the proof. □

4.3. Maximal unlinked sets, the special case. We now describe the additional restriction on the generating set $T$ required in the statement of Theorem 1.4.

A.1 There do not exist $x_i, x_j, x_k \in G$ lifting elements in $T$, such that $[x_i, x_j] \neq 1, [x_j, x_k] \neq 1$ and $[x_i, x_k] = 1$.

It has the following alternate description.

Lemma 4.6. Let $x_i, x_j, x_k \in G$ be lifts of elements in $T$. These elements satisfy the relations $[x_i, x_j] \neq 1, [x_j, x_k] \neq 1$ and $[x_i, x_k] = 1$ if and only if $\langle x_i, x_j, x_k \rangle \cong (C_2 \times C_4) \times_{-1} C_2$ with $C_2 \times C_4 \subset H$ and $C_2 \cap H = \{1\}$ and $C_2$ acting by inversion.
Proof. Suppose \( x_i, x_j, x_k \) satisfy the relations. Then \( \langle x_i, x_j, x_k \rangle \cong C_2 \times C_4 \) and \( x_k \cong C_2 \) acts as required. Since \( x_i, x_j, x_k \notin H \) they all project non-trivially to \( G/H \cong C_2 \) and hence \( x_i, x_j, x_k \in H \).

Conversely if \( \langle x_i, x_j, x_k \rangle \cong (C_2 \times C_4) \rtimes_{-1} C_2 \) then we can assume without loss of generality \( x_i = (1, 0, 1), x_j = (0, 1, 1) \) and \( x_k = (0, 0, 1) \) since these are all of the order 2 elements not in \( H \). Then the relations are satisfied. \( \square \)

For the remainder of this subsection we will assume \( T \) satisfies \([A.1]\). Note this condition is independent of chosen lift.

Without loss of generality we can assume \( i \in \{1, \ldots, r_1\} \) satisfies \( S_i \neq \emptyset \). For each \( i = 1, \ldots, r \) let \( d_i = D_{2i-1}D_{2i} \). Consider the graph with vertices \( \{1, \ldots, r_1\} \) where \( i, j \) are connected if \( x_i \) and \( x_j \) do not commute in the group \( G \). Let \( C_1, \ldots, C_s \) be the connected components of this graph. By the assumption that \( T \) satisfies \([A.1]\) each component \( C_i \) is a fully connected graph.

For \( 1 \leq j \leq s \) we let

\[
A_j = \{2i - 1 \mid 1 \leq i \leq r_1, i \in C_j\},
\]

\[
B_j = \{2i \mid 1 \leq i \leq r_1, i \in C_j\}
\]

and if \( C_j = \{i_1, i_2\} \) we additionally let

\[
A'_j = \{2i_1 - 1, 2i_1\},
\]

\[
B'_j = \{2i_2 - 1, 2i_2\}
\]

(if \( |C_j| > 2 \) we define these to be empty for notational convenience). Also we let

\[
C = \{2i - 1, 2i \mid i = r_1 + 1, \ldots, r\}.
\]

Let \( U_j = A_j \cup B_j \cup A'_j \cup B'_j \) and let \( U = \bigcup_{j=1}^{s} U_j \cup C \).

For \( k = 1 \) it is easy to verify the following description of linked indices. If \( i_1 \in C_j \) and \( u = 2i_1 - 1 \) (that is \( u \in A_j \)) then \( u \) is linked with every \( 2i_2 \) with \( i_2 \in C_j \) and \( i_2 \neq i_1 \). It is unlinked with every other element of \( U \). Similarly \( u = 2i_1 \) (that is \( u \in B_j \)) is linked with every \( 2i_2 - 1 \) with \( i_2 \in C_j \) and \( i_2 \neq i_1 \) and unlinked with everything else. Every element of \( C \) is unlinked with everything.

Consider the set of subsets of \( U \),

\[
\mathcal{T} = \left\{ \bigcup_{j=1}^{s} W_j \cup C \mid W_j = A_j, B_j, A'_j, B'_j \right\}.
\]

**Proposition 4.7.** The maximal unlinked sets in \( U^k \) are exactly the elements \( t \in \mathcal{T}^k \) and they have size \( c_T^k \).

**Proof.** It is clear that any \( t \in \mathcal{T}^k \) is an unlinked set of size \( c_T^k \). We prove the converse by induction on \( k \).

The case \( k = 1 \) is straightforward. Suppose the statement is true for \( k - 1 \). Let \( U \) be a maximal unlinked set in \( U^k \). We can write it as a disjoint union

\[
U = \bigcup_{j=1}^{s} U_j \cup U_C
\]
where
\[ \mathcal{U}_j = \{ u \in \mathcal{U} \mid u_k \in U_j \}, \]
\[ \mathcal{U}_C = \{ u \in \mathcal{U} \mid u_k \in C \}. \]

Let \( p \) be the projection onto the first \( k-1 \) coordinates. By the same proof as of Lemma 17 in [2] we have \(|\mathcal{U}_j| \leq c_T^{k-1} |C_j|\) and \(|\mathcal{U}_C| \leq c_T^{k-1} |C|\) and \( \mathcal{U} \) is maximal if and only if there is equality for all \( j \) and \( C \).

Fix \( 1 \leq j \leq s \). We will now show that \( \mathcal{U}_j = p(\mathcal{U}_j) \times W_j \) for some \( W_j \in \{ A_j, B_j, A'_j, B'_j \} \).

We consider two cases.

First suppose \( |C_j| \geq 2 \). Then using the same proof as of Lemma 17 of [2] with small modifications shows that \( \mathcal{U}_j = p(\mathcal{U}_j) \times W_j \) where \( W_j = A_j \) or \( B_j \) and \( p(\mathcal{U}_j) \) is a maximal unlinked set in \( U^{k-1} \). Thus \( p(\mathcal{U}_j) \) is equal for all such \( j \).

Now suppose \( |C_j| = 2 \). Without loss of generality assume \( C_j = \{1, 2\} \) so \( A_j = \{1, 3\} \), \( B_j = \{2, 4\} \), \( A'_j = \{1, 2\} \), \( B'_j = \{3, 4\} \). Then write \( \mathcal{U}_j = \bigcup_{i=1}^{s} \mathcal{U}_{j,i} \) where
\[ \mathcal{U}_{j,i} = \{ u \in \mathcal{U}_j \mid u_k = i \} \]

and suppose without loss of generality \( \mathcal{U}_{j,i} \neq \emptyset \) for all \( i \) otherwise the result follows by the arguments in Lemma 17 of [2]. Then \( p \) is injective on \( \mathcal{U}_j \). By arguments similar to the first case we obtain four sets
\[ X_i = p(\mathcal{U}_{j,i}) \]
such that each element of \( \mathcal{X} = \{ X_1 \cup X_2, X_1 \cup X_3, X_2 \cup X_4, X_3 \cup X_4 \} \) is an unlinked set, and every element of \( X_1 \) is linked with every element of \( X_4 \), and similarly for \( X_2 \) and \( X_3 \). Since \( \mathcal{U} \) is maximal, by the above we must have equality \(|\mathcal{U}_j| = 2c_T^{k-1}\) so the elements of \( \mathcal{X} \) are maximal unlinked sets which must all be distinct. Then since there is at least one other non-empty \( \mathcal{U}_j \) or \( \mathcal{U}_C \) we have that \( p(\mathcal{U}_j) = \bigcup_i X_i \) is unlinked with \( p(\mathcal{U}_j) \) or \( p(\mathcal{U}_C) \) respectively, which contradicts the maximality the distinct elements of \( \mathcal{X} \). Thus \( \mathcal{U}_j = p(\mathcal{U}_j) \times W_j \) for some \( W_j \in \{ A_j, B_j, A'_j, B'_j \} \).

Applying the induction hypothesis shows that
\[ |\mathcal{U}| = \sum_{j=1}^{s} |p(\mathcal{U}_j)| |W_j| + |p(\mathcal{U}_C)| 2r_2 \]
\[ = c_T^{k-1} \left( \sum_{j=1}^{s} |W_j| + 2r_2 \right) \]
\[ = c_T^{k-1} (r_1 + 2r_2) \]
\[ = c_T^{k-1} \frac{r_1}{r_2} \]
Thus \( \mathcal{U} \) is an element of \( T^k \). This completes the proof.

In each case the size of a maximal unlinked set is \( c_T^{k-1} \). It is also clear from the proposition that there are \((2^n 4^{r_2})^k\) maximal unlinked sets where \( s_1 \) is the number of \( C_j \) with \(|C_j| > 2 \) and \( s_2 \) is the number of \( C_j \) with \(|C_j| = 2 \).
4.4. The asymptotic. We define some notation for the next theorem.

**Theorem 4.8.** For any positive \( k \in \mathbb{Z} \) the sum of the \( k \)th power of \( f_T(d) / c_T(d) \) over positive (resp. negative) fundamental discriminants is

\[
\sum_{d < X} \frac{f_T(d)^k}{c_T(d)} = \frac{1}{2^{c_T + kr} \text{Aut}_H(T(G)) \Gamma_k} \frac{4}{\pi^2} X + o(X)
\]

for some \( \Gamma_k \) not depending on \( X \).

If the sum is restricted to odd discriminants then

\[
\Gamma_k = \sum_N \gamma(N)
\]

where where \( N \) ranges over all sets of the form \( N = \bigcup_{j=1}^k N_j \) with \( N_j \subset \{1, \ldots, r\} \) where \( |N_j| \) is even (resp. odd) and

\[
\gamma(N) = \sum_{\mathcal{U}} \prod_{(h_u)_{u \in \mathcal{U}}} (-1)^{\Phi_k(u,v) \frac{h_u - 1}{2}} \prod_u (-1)^{\lambda^N_N(u) \frac{h_u - 1}{2}}
\]

where the first sum is over maximal unlinked sets \( \mathcal{U} \subset U^k \), and the second sum is over tuples of congruence conditions \( h_u \equiv \pm 1 \mod 4 \) for each \( u \in \mathcal{U} \) satisfying \( \prod_{u \in \mathcal{U}} h_u \equiv 1 \mod 4 \).

**Proof.** We follow the same procedure as in [6] and [2]. We will outline the key steps along with any modifications.

Let \( \alpha = \text{ord}_2(d) \). First we write

\[
f_T(d) = \frac{1}{2^n} \frac{1}{\text{Aut}_H(T(G))} \sum_{N \subset \{1, \ldots, r\}} \sum_{j=1}^r \sum_{d=2^a} \prod_{D_u, D_v} \Phi(u,v) \prod_u \left( \frac{-1}{D_u} \right)^{\lambda^N(u)}
\]

\[
\times \prod_u \left( \frac{2^a}{D_u} \right)^{\psi_j(u)} \left( 1 + \prod_u \left( \frac{D_u}{2} \right)^{\gamma_j(u)} \right).
\]

where the second sum is over factorizations of \( d \) into positive integers which satisfy the following congruences modulo 4

\[
D_{2i-1} D_{2i} \equiv \begin{cases} 
-1 & i \in N, i \neq j \\
1 & i \notin N, i \neq j \\
1 & i \in N, i = j, \alpha = 2 \\
\pm 1 & i \in N, i = j, \alpha = 3 
\end{cases}
\]

and the functions appearing above are defined

\[
\lambda^N(u) = \begin{cases} 
1 & u = 2i, i \leq r_1, |N \cap S_i| \text{ odd} \\
0 & \text{else}
\end{cases}
\]

\[
\gamma_j(u) = \Phi(u, 2j)
\]
\[ \psi_j(u) = \Phi(2j, u). \]

Note the \( D_u \) were allowed to be negative and divisible by 2 previously, hence we introduce \( \lambda^N \) to keep track of the negative signs and \( \gamma_j, \psi_j \) to keep track of the factor \( 2^\alpha \). Note we are using the expression for \( f_T \) from the statement of Theorem 3.5 and not from Remark 3.6. That is we are not evaluating the Legendre symbols in the factors corresponding to \( d_i \) for \( i > r_1 \).

Taking the \( k \)th power gives

\[
f_T(d)^k = \frac{1}{2^{kn}} \frac{1}{|\text{Aut}_{H,T}(G)|^k} \sum_{\Gamma \subseteq \{1, \ldots, k\}} \sum_N \sum_{J \in \{1, \ldots, \gamma\}} \prod_{D_u, u,v} \left( \prod_u \left( -\frac{1}{D_u} \right)^{\lambda^N(u)} \left( \frac{D_u}{2} \right)^{\gamma_j(u)} \left( \frac{2^\alpha}{D_u} \right)^{\psi_j(u)} \right)
\]

where \( N \) ranges over sets as described in the theorem statement and for each \( 1 \leq j \leq k \) the factorizations satisfy the congruences

\[
\prod_{u,v} D_u D_v \equiv \begin{cases} 
-1 & i \in N, i \neq J_i \\
1 & i \notin N, i \neq J_i \\
1 & i \in N, i = J_i, \alpha = 2 \\
\pm 1 & i \in N, i = J_i, \alpha = 3 
\end{cases}
\]

where the product is over all \( u, v \) with \( u_j = 2i - 1, v_j = 2i \). Note that there are \( kr \) conditions. Furthermore

\[
\lambda^N(u) = \sum_{j=1}^{k} \lambda^N_j(u_j)
\]

\[
\gamma_j(\Gamma)(u) = \sum_{i \in \Gamma} \gamma_j(u_i)
\]

\[
\psi_j(\Gamma)(u) = \sum_{i=1}^{k} \psi_j(u_i).
\]

An analysis of character sums and their cancellation, and a removal of the congruence conditions on the \( D_u \) as in [6] and [2] gives

\[
\sum_{d \leq X} \frac{f_T(d)^k}{ct(d)^k} \leq \frac{1}{2^{kn}} \frac{1}{2^{c_T} |\text{Aut}_{H,T}(G)|^k} \left[ \sum_{\gamma, \Gamma, J} S_{\gamma, \Gamma, J} \right] \left[ \sum_{\gamma, \Gamma, J} \frac{\mu^2(2 \prod D_u)}{ct(\prod D_u)} \right] + o(X)
\]

where the range of the last sum is over factorizations into \( c_T^{k/} \)-tuples of coprime positive integers and

\[
S_{\gamma, \Gamma, J} = \sum_{u,v} \prod_u \left( \frac{D_u}{D_v} \right)^{\Phi_k(u,v)} \prod_u \left( -\frac{1}{D_u} \right)^{\lambda^N(u)} \left( \frac{D_u}{2} \right)^{\gamma_j(u)} \left( \frac{2^\alpha}{D_u} \right)^{\psi_j(u)}
\]
where the sum is over \( U \) which are maximal unlinked sets in \( U^k \). The factor of \( 2^{-c_T^k} \) comes from removing the congruence conditions on the remaining \( c_T^k \) variables. It is easy to see that if \( \alpha = 0 \) then \( \Gamma, J \) are empty and \( S_{N,\Gamma,J} \) reduces to \( \gamma(N) \) as in the statement of the theorem.

Since the number of ways of writing any integer \( x < X \) as a product of \( c_T^k \) integers is \( \omega_{c_T}(x) \) we have

\[
\sum_{(D_u)} \frac{\mu^2(2\prod D_u)}{c_T^k\omega(\prod D_u)} = \left[ \sum_{x < X} \mu^2(2x) \right] + o(X) = \frac{4}{\pi^2}X + o(X)
\]

and the theorem follows. \( \square \)

This proves Conjecture 1.2.

5. Some consequences and remarks

Let \( G \) be a central extension of \( \mathbb{F}_2^n \) by \( \mathbb{F}_2 \) and let \((G,H)\) be admissible. Suppose \( G \) is not elementary abelian. First we complete the proof of Theorem 1.3.

Corollary 5.1. Conjecture 1.1 is true for \((G,H)\).

Proof. Clearly \( f = \sum_{T \text{ admissible}} f_T \). Hence

\[
f^k = \sum_{(j_T), \sum_T j_T = k} \binom{k}{j_T} \prod_T f_T^{j_T}
\]

where the sum if over tuples of nonnegative integers. Following the same proofs as those in Section 4 one can show that the maximal unlinked sets corresponding to the function \( \prod_T f_T^{j_T} \) are of the form \( \prod_T U_T^{j_T} \) with \( U_T \) a maximal unlinked set for \( f_T \), and hence have size \( \prod_T c_T^{j_T} \). Thus it follows from the above proof that

\[
\sum_{d < X} \prod_T f_T^{j_T} \sim C'(\langle j_T \rangle) X\prod_T c_T^{j_T}^{-1}
\]

for some constant \( C'(\langle j_T \rangle) \) or alternately that \( \sum_{d < X} \prod_T f_T^{j_T} \sim C'((j_T)) X (\log X)^{\prod_T c_T^{j_T}^{-1}} \). Thus the only contribution to the main term in \( \sum_{d < X} f^k \) comes from \( (j_T) \) with \( j_T \neq 0 \) if and only if \( c_T = c \) which gives

\[
\sum_{d < X} \prod_T f_T^{j_T} \sim C'(\langle j_T \rangle) X (\log X)^{c^k-1}.
\]

\( \square \)

There remains the question of what the moments of \( f \) are and what distribution they determine. It is evident from the proof of Corollary 5.1 that the \( k \)th moment of
\[ f \text{ will be } \sum_{(j_T), \sum_T j_T = k} \binom{k}{(j_T)} C((j_T)). \]

Computing this would require proofs analogous to those in Section 6 for \( \prod_T f_T^{j_T} \). In Section 6 we compute \( C((j_T)) \) for \( T \) satisfying (A.1). This condition is imposed to make the highly combinatorial proofs more manageable, and we do not expect that it is a crucial obstruction. In particular, in the general case one would require an analogue of Proposition 4.7 and an extension of the computations in Section 6.

6. ANALYSIS OF THE MAIN TERM

Throughout this section we assume \( T \) satisfies (A.1). We now want to analyze the main term in Theorem 4.8.

First we partition \( \gamma(N) \) according to the types of maximal unlinked sets which appear. Without loss of generality assume for \( 1 \leq i \leq s_1 \) that \( |C_i| > 2 \) and for \( s_1 < i \leq s \) that \( |C_i| = 2 \). For any \( t \in \{v, h\}^{s_2} \) let \( \mathcal{U}_t \) denote the set of maximal unlinked sets \( \mathcal{U} \subset U \) which satisfy \( A_i \subset \mathcal{U} \) or \( B_i \subset \mathcal{U} \) if \( t_i = h \) and \( A_i \subset \mathcal{U} \) or \( B_i \subset \mathcal{U} \) if \( t_i = v \). Similarly for \( t \in \prod_k \{v, h\}^{s_2} \) let \( \mathcal{U}_t \) denote the set of maximal unlinked sets \( \mathcal{U} \subset U^k \) which satisfy this condition upon projection to each coordinate. Then let

\[ \gamma_t(N) = \sum_{\mathcal{U} \in \mathcal{U}_t} \left[ \sum \prod_{(h_u) \in \mathcal{U}} (-1)^{\Phi_k(u,v) \frac{h_u-1}{2}} \prod_{u} (-1)^{\lambda^k(u) \frac{h_u-1}{2}} \right] \]

so that \( \gamma(N) = \sum_t \gamma_t(N) \). Define \( t_j(h) = \{1 \leq i \leq s_2 \mid t(j)(i) = h\} \) for each \( 1 \leq j \leq k \).

The congruence conditions (4.1) can be encoded as vectors lying in a certain coset of a subspace of \( \mathbb{F}_2^{kT} \). For any tuple \( (h_u) \) corresponding to one of the conditions in (4.1) define the corresponding element \( x \in \mathbb{F}_2^{kT} \) by

\[ x_u = \begin{cases} 1 & \text{if } h_u = -1 \\ 0 & \text{if } h_u = 1. \end{cases} \]

Then there is a matrix \( M_{t,k} \) such that the conditions (4.1) equal a coset of \( \ker M_k \). The definition of \( M_{t,k} \) is analogous to that in [2] (following Proposition 21). We define it recursively as follows. Recall that without loss of generality we assume for \( 1 \leq i \leq s_1 \) that \( |C_i| > 2 \) and for \( s_1 < i \leq s \) that \( |C_i| = 2 \). Let \( \mathbf{0} \) and \( \mathbf{1} \) be vectors of 0’s and 1’s of length \( c_j^{T-1} \). Define a matrix of size

\[ (r_1 - 2t_1(v) + r_2 + t_1(v)) \times c_j^T = (r - t_1(v)) \times c_j^T \]

as

\[ \begin{pmatrix} \mathbf{1} & \cdots & \mathbf{1} \end{pmatrix} \]
and combine any pair of rows corresponding to $|C_l| = 2$ if $t(j)(i) = h$ or any pair $(2l - 1, 2l)$ for $l \geq r_2$. Call the resulting matrix $J$. Then if $j > 1$ we define

$$M_{t,j} = \begin{bmatrix} J & \ldots & M_{t,j-1} \end{bmatrix}$$

which has dimensions $(jr - \sum_{j_0 \leq j} t_{j_0}(v)) \times c_j^d$.

Also using a proof analogous to Lemma 22 from [2] we can compute $\dim \ker M_{t,k}$. It is easy to see that the kernel of each row of $J$ has dimension $2c_T^{j-1} - 1$ or $c_T^{j-1} - 1$ depending on whether it was obtained by combining two rows or not. Then we get

$$\dim \ker M_{t,k} = \sum_{j=1}^{k} [(r_2 + t_j(h)) (2c_T^{j-1} - 1) + (r_1 - 2t_j(h)) (c_T^{j-1} - 1) - c_T^{j-1} + 1]$$

$$= \sum_{j=1}^{k} c_T^{j} + t_j(h) - c_T^{j-1} + 1 - r$$

$$(6.1) \quad = c_T^{k} - k(r - 1) - 1 + \sum_{j=1}^{k} t_j(h).$$

Recall that for $N = \bigcup_{j=1}^{k} N_j$ with $N_j \subset \{1, \ldots, r\}$.

**Proposition 6.1.** Let $a = 0, 1$ in the positive, negative cases respectively. Then

$$\sum_{N} \gamma(N) = 2^{k(s_1 + 2s_2) + c_T^{k} - k(r - 1) - 1} \left( \sum_{m=\alpha(2)}^{r} \sum_{m_i=0,1}^{s+1} \prod_{i=1}^{s+1} \left( \frac{|C_i|}{m_i} \right) \right)^{k}.$$

**Proof.** Let $t \in \prod_{j=1}^{k} \{v, h\}^{s_2}$. Let $B_{t,k} = \{u \mid u_j \in B_i, u_i \in B \cup C \text{ for } l \neq j\}$. By a computation similar to Lemma 22 in [2] we have

$$\gamma_t(N) = \sum_{x \in y + \ker M_{t,k}} \sum_{U \in U_l} (-1)^{\sum_{(u,v)} \Phi_k(u,v)x_u x_v + \sum_u \lambda^N_k(u)x_u}$$

$$= \sum_{x \in y + \ker M_{t,k}} \sum_{U \in U_l} (-1)^{\sum_{(u,v)} \sum_{i=1}^{s+1} \Phi(u_j,v_j)x_u x_v + \sum_u \lambda^N_k(u)x_u}$$

$$= \sum_{x \in y + \ker M_{t,k}} \prod_{j=1}^{k} \prod_{i=1}^{s+1} \left( 1 + (-1)^{\sum_{(u,v)} \Phi(u_j,v_j)x_u x_v + \sum_u \lambda^N_{ij}(u_j)x_u} \right).$$

Now we determine when the expression

$$(6.2) \quad \sum_{(u,v) \in B_{t,j}} \Phi(u, v) x_u x_v + \sum_{u \in B_{t,j}} \lambda^N_{ij}(u) x_u$$

is even or odd. Note that $\Phi(u, v) = 1$ for all $u, v \in B$ if $u \neq v$. 


It follows from (4.1) that for any \( l \) such that \( 2l \in B_i \) we have
\[
\sum_{u \in (B_i \cup C_i)^k, \ u_j=2l} x_u = \begin{cases} 
1 & \text{if } l \in N_j \\
0 & \text{if } i \notin N_j.
\end{cases}
\]
Let \( m_{j,i} = |N_j \cap C_i| \). It follows from this that
\[
\sum_{\{u,v\} \subset B_{i,j}} \Phi (u_j, v_j) x_u x_v = \left( \frac{m_{j,i}}{2} \right)
\]
which is even when \( m_{j,i} \equiv 0, 1 \mod 4 \).
Furthermore for \( 2l \in B_i \) we have
\[
\lambda_{N_j} (2l) = \begin{cases} 
1 & \text{if } |N_j \cap S_l| \text{ odd} \\
0 & \text{else}
\end{cases}
\]
and hence
\[
\sum_{u \in B_{i,j}} \lambda_{N_j} (u_j) x_u = \begin{cases} 
m_{j,i} & \text{if } m_{j,i} \text{ even} \\
0 & \text{else}
\end{cases}
\]
which is always even.

Thus if \( m_{j,i} \equiv 0, 1 \mod 4 \) for all \( i \) and \( j \) then
\[
\gamma_t (N) = \sum_{x \in y + \ker M_{t,k}} 2^{k s_1 + \sum_{j} t_j (v)}
= 2^{k s_1 + \sum_{j} t_j (v) + \dim \ker M_{t,k}}
= 2^{k s_1 + \sum_{j} t_j (v) + c_{2j} - k(r-1) - 1 + \sum_{j} t_j (h)}
= 2^{k s_1 + k s_2 + c_{2j} - k(r-1) - 1}
= 2^{k s + c_{2j} - k(r-1) - 1}
\]
where we are using \( t_j (h) + t_j (v) = s_2 \). If \( m_{j,i} \neq 0, 1 \mod 4 \) then \( \gamma_t (N) = 0 \). Thus we get
\[
\gamma (N) = \sum_t 2^{k s + c_{2j} - k(r-1) - 1}
= 2^{k s_1 + 2 s_2 + c_{2j} - k(r-1) - 1}
\]
Note \( \gamma (N) \) does not depend on \( N \). Let \( a = 0, 1 \) if \( d \) is respectively positive or negative. Then we have
\[
\sum_N \gamma (N) = 2^{k (s_1 + 2 s_2) + c_{2j} - k(r-1) - 1} \sum_{N, \ |N_j| \equiv a(2), \ m_{i,j} \equiv 0, 1(4)} 1
\]
and we compute
\[ \sum_{N_j \equiv a(2), \ \ m_{i,j} \equiv 0,1(4)} 1 = \prod_{j=1}^{k} \sum_{N_j \equiv a(2), \ \ m_{i,j} \equiv 0,1(4)} 1 \]

\[ = \left( \sum_{m \equiv a(2) \ \ m_i \equiv 0,1(4)} \prod_{i=1}^{s+1} \left( \frac{|C_i|}{m_i} \right) \right)^k \]

\[ = Q(a)^k. \]

The outer summation corresponds to choices of possible sizes of the set \( N_j \) and the inner sum to the choices of negative sign for each factor \( d_1, \ldots, d_r \) of \( d \). This completes the proof. \( \square \)

Thus we obtain the \( k \)th moment of the function \( f_T(d) / c_T^{\omega(d)} \) summing over fundamental discriminants

\[ \lim_{X \to \infty} \frac{\sum_{d \leq X} f_T(d)^k}{\sum_{d \leq X} 1} = \frac{2 \cdot 2^{k(s_1+2s_2)+r(r-1)-1}}{2^{s_1+2s_2+n-1}} \cdot \frac{|\text{Aut}_{H,T}(G)|^k}{|\text{Aut}_{H,T}(G)|} \cdot Q(a)^k \]

\[ = \left( \frac{2^{s_1+2s_2+n-1}}{|\text{Aut}_{H,T}(G)|} \cdot Q(a)^k \right)^k. \]

This proves Theorem 1.4.

REFERENCES

[1] Brandon Alberts. Cohen-Lenstra Moments for Some Nonabelian Groups, 2016. Preprint https://arxiv.org/abs/1606.07867.
[2] Brandon Alberts and Jack Klys. The distribution of \( h_8 \)-extensions of quadratic fields. 2016. Preprint https://arxiv.org/abs/1611.05595.
[3] Manjul Bhargava. The geometric sieve and the density of squarefree values of invariant polynomials. 2014. Preprint https://arxiv.org/abs/1402.0031.
[4] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), volume 1068 of Lecture Notes in Math., pages 33–62. Springer, Berlin, 1984.
[5] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. Proc. Roy. Soc. London Ser. A, 322(1551):405–420, 1971.
[6] Étienne Fouvry and Jürgen Klüners. On the 4-rank of class groups of quadratic number fields. Invent. Math., 167(3):455–513, 2007.
[7] Larry C. Grove. Classical groups and geometric algebra, volume 39 of Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2002.
[8] Franz Lemmermeyer. Unramified quaternion extensions of quadratic number fields. J. Théor. Nombres Bordeaux, 9(1):51–68, 1997.
[9] Ján Minác and Tara L. Smith. A characterization of \( C \)-fields via Galois groups. *J. Algebra*, 137(1):1–11, 1991.

[10] Melanie Wood. Nonabelian cohen-lenstra moments. 2016. Preprint 
https://arxiv.org/abs/1702.04644.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TORONTO, CANADA
jack.klys@mail.utoronto.ca