Abstract. We show that there are order of magnitude $H^2(\log H)^2$ monic quartic polynomials with integer coefficients having box height at most $H$ whose Galois group is $D_4$. Further, we prove that the corresponding number of $V_4$ and $C_4$ quartics is $O(H^2\log H)$. Finally, we show that the count for $A_4$ quartics is $O(H^{2.95})$. Our work establishes that irreducible non-$S_4$ quartics are less numerous than reducible quartics.

1. Introduction

We consider monic quartic polynomials
\begin{equation}
f(X) = X^4 + aX^3 + bX^2 + cX + d \tag{1.1}
\end{equation}
with integer coefficients. Recall that the Galois group $G_f$ of $f$ is the Galois group of its splitting field. As $G_f$ acts on the roots of $f$, it can be embedded into $S_4$ (the symmetric group on four elements). The enumeration of polynomials with prescribed Galois group is a long-studied topic. Van der Waerden [23] showed that a generic polynomial has full Galois group, and a popular objective has been to sharpen his bound on the size of the exceptional set, which for quartics is
\[
E_4(H) := \# \{(a, b, c, d) \in \mathbb{Z}^4 \cap [-H, H]^4 : G_f \not\cong S_4\}.
\]

It was thought that the second author [8] had essentially solved this problem a decade ago, asserting the estimate
\[
E_4(H) \ll \varepsilon H^{3+\varepsilon}. \tag{1.2}
\]
However, we have discovered an error in Eq. (7) therein, which appears to damage the argument beyond repair—see [11] for the correct expressions. To our knowledge, the strongest unconditional bound to date is $E_4(H) \ll \varepsilon H^{2+\sqrt{2}+\varepsilon}$, obtained in [10]. Note that the inequality (1.2) is known conditionally [26, Theorem 1.4].

We prove unconditionally that if only irreducible polynomials are considered then the exponent can be reduced below 3.

Theorem 1.1. The number of monic, irreducible non-$S_4$ quartic polynomials (1.1) with $a, b, c, d \in \mathbb{Z} \cap [-H, H]$ is $O_\varepsilon(H^{2.947+\varepsilon})$.

Note that $2^{\frac{5}{2}} + \frac{1}{\sqrt{5}} \approx 2.947$. It has long been known that the number of monic reducible quartics up to box height $H$ is $16(\zeta(3) + \frac{1}{6})H^3 + O(H^2\log H)$, see [1, 22]. In light of this, Theorem 1.1 shows that non-$S_4$ irreducible quartics are less numerous than reducible quartics. Not only does Theorem 1.1 recover (1.2), but it establishes the following asymptotic formula for $E_4(H)$.

2010 Mathematics Subject Classification. 11R32 (primary); 11H06, 11C08, 11G35, 11R45 (secondary).

Key words and phrases. Galois theory, determinant method.
Theorem 1.2. We have the asymptotic formula

\[ E_4(H) = 16\left(\zeta(3) + \frac{1}{6}\right)H^3 + O\left(H^{\frac{5}{2} + \frac{1}{\sqrt{5}} + \varepsilon}\right). \]

We know that \( f \) is irreducible if and only if \( G_f \) acts transitively on its roots. In this case there are five possibilities for \( G_f \), namely \( S_4, A_4, D_4, V_4 \) and \( C_4 \), see [16]. Here \( D_4 \) is the dihedral group of order 8, and \( A_4, V_4 \) are respectively the alternating and Klein four groups. As usual \( C_4 \) is the cyclic group of order 4. We write \( S_H \) for the set of monic, irreducible quartics with coefficients in \( \mathbb{Z} \cap [-H, H] \), and for \( G \in \{ S_4, A_4, D_4, V_4, C_4 \} \) we define

\[ N_G = N_G(H) = \# \{ f \in S_H : G_f \simeq G \}. \]

We ascertain the order of magnitude for the number of \( D_4 \) quartics.

Theorem 1.3. We have

\[ N_{D_4} \asymp H^2 (\log H)^2. \]

In addition, we show that \( V_4 \) and \( C_4 \) quartics are less numerous.

Theorem 1.4. We have

\[ N_{V_4} + N_{C_4} \ll H^2 \log H. \]

Finally, to complete the proof of Theorem 1.1 we establish the following upper bound for \( A_4 \) quartics.

Theorem 1.5. We have

\[ N_{A_4} \ll \varepsilon H^{\frac{5}{2} + \frac{1}{\sqrt{5}} + \varepsilon}. \]

We searched the literature for constructions that imply lower bounds for these quantities. Working from [19], one obtains \( N_{A_4} \gg H \), see [6.2]. We can deduce from [21, §12] and [6, Theorem 2.1] that \( N_{C_4} \gg H \); the latter cited result is based on a quantitative version of Hilbert’s irreducibility theorem. We can construct a family of quartics that implies a sharper lower bound for \( N_{V_4} \) than what we were able to find in the literature: the construction given in [6.1] shows that \( N_{V_4} \gg H^{3/2} \).

We summarise our state of knowledge as follows:

\[
\begin{align*}
N_{S_4} &= 16H^4 + O(H^3) \\
N_{D_4} &\asymp H^2 (\log H)^2 \\
H^{3/2} &\ll N_{V_4} \ll H^2 \log H \\
H &\ll N_{C_4} \ll H^2 \log H \\
H &\ll N_{A_4} \ll \varepsilon H^{\frac{5}{2} + \frac{1}{\sqrt{5}} + \varepsilon}.
\end{align*}
\]

The story is still far from complete. We expect that in time asymptotic formulas will emerge for every \( N_G(H) \). Below we provide the values of \( N_G(100) \), evaluated using the C programming language (for the code, see Appendix B).
This suggests that the upper bounds for $A_4, V_4$ and $C_4$ quartics may be far from the truth.

We remark that our counting problem differs substantially from the corresponding problem for quartic fields, for which Cohen, Diaz y Diaz and Olivier [5] showed that in some sense a positive proportion of quartic fields have Galois group $D_4$. For an explanation of why the results are consistent, see [26, Remark 5.1].

One might wish to consider the analogous problem in degree $n \in \{3, 5, 6, 7, \ldots\}$. For $G \leq S_n$, let us write $N_{G,n} = N_{G,n}(H)$ for the number of monic, integer polynomials, with coefficients bounded by $H$ in absolute value, whose Galois group is isomorphic to $G$. The second author showed in [9] that

$$N_{G,n} \ll_{n,\varepsilon} H^{n-1 + \frac{1}{|S_n:G|} + \varepsilon},$$

and in [10] that

$$N_{A_n,n} \ll_{n,\varepsilon} H^{n-2 + \sqrt{2} + \varepsilon}.$$  

The latter article established that the number of non-$S_n$ monic polynomials of degree $n$ is $O_{n,\varepsilon}(H^{n-2 + \sqrt{2} + \varepsilon})$, breaking a record previously held by van der Waerden [23], Knobloch [17], Gallagher [12] and Zywina [27]. We plan to embark on a detailed analysis of the quintic case in future work. Note that even the cubic problem has not been fully resolved: it seems that Lefton’s 1979 upper bound

$$N_{A_3,3} \ll_{\varepsilon} H^{2 + \varepsilon}$$

remains unsurpassed to this day [18]. We witness that Theorem 7.1 of Rivin’s preprint [20] sharpens the inequality (1.3) to $N_{G,n} \ll_{n,\varepsilon} H^{n-1 + \varepsilon}$ when $n \geq 12$ and $G \not\in \{S_n, A_n\}$.

As far as we are aware, the present article is the first instance of the order of magnitude of $N_{G,n}$ being obtained, for $G \not\cong S_n$, and also the first instance of showing that non-$S_n$ polynomials of degree $n$ are dominated by reducibles. In view of this, we presently offer a brief description of the ideas that enable us to succeed on these two fronts.

Our methods begin with classical criteria [16] involving the discriminant and cubic resolvent of a monic, irreducible quartic polynomial (1.1). When the Galois group is $D_4, V_4$ or $C_4$, the cubic resolvent has an integer root, which we introduce as an extra variable $x$. Changing variables to use $e = b - x$ instead of $b$, we obtain the astonishing symmetry (2.3), which we believe is new. For emphasis, the identity is

$$(x^2 - 4d) \cdot (a^2 - 4e) = (xa - 2c)^2.$$  

Using ideas from the geometry of numbers and diophantine approximation leads to the upper bound

$$N_{D_4} + N_{V_4} + N_{C_4} \ll H^2(\log H)^2.$$  

\[1.4\]
The proof then motivates a construction that implies the matching lower bound

\[ N_{D_4} + N_{V_4} + N_{C_4} \gg H^2 \log^2 H. \]  

(1.5)

The analysis described above roughly speaking provides an approximate parametrisation of the \( D_4, V_4 \) and \( C_4 \) quartics, by certain variables \( u, v, w, x, a \), where \( a \) is as in (1.1). To show that \( N_{V_4} \) and \( N_{C_4} \) satisfy the stronger upper bound \( O(H^2 \log H) \), we use an additional piece of information in each case; this takes the form of an equation \( y^2 = P_{u,v,w,a}(x) \), where \( P_{u,v,w,a} \) is a polynomial and \( y \) is an additional variable. We require upper bounds for the number of integer solutions to this diophantine equation in \((x, y)\), and these bounds need to be uniform in the coefficients. We are able to ascertain that the curve defined is absolutely irreducible, which enables us to apply a Bombieri–Pila [2] style of result by Vaughan [24, Theorem 1.1].

Our study of \( A_4 \) quartics begins with the standard fact that the discriminant is in this case a square—see, for instance, the Kappe–Warren criterion [16]. Deviating from previous work on this topic, we employ the invariant theory of \( GL_2 \) actions on binary quartic forms (or, equivalently, unary quartic polynomials), see [1]. The discriminant can then be written as \( (4I^3 - J^2)/27 \), where

\[ I = 12d - 3ac + b^2, \quad J = 72bd + 9abc - 27c^2 - 27a^2d - 2b^3. \]  

(1.6)

Our strategy is first to count integer solutions \((I, J, y)\) to

\[ 4I^3 - J^2 = 27y^2, \]  

(1.7)

and then to count integer solutions \((a, b, c, d)\) to (1.6). In the latter step, we require upper bounds that are uniform in the coefficients. Further manipulations lead us to an affine surface \( Y_{I,J} \), which we show to be absolutely irreducible. A result stated by Browning [3, Lemma 1], which he attributes to Heath-Brown and Salberger, then enables us to cover the integer points on the surface by a family of curves. By showing that \( Y_{I,J} \) contains no lines, and using this fact nontrivially, we can then decompose each curve in the family into irreducible curves of degree greater than or equal to 2, and finally apply Bombieri–Pila [2].

The miracle that our exponent for \( N_{A_4} \) is lower than 3 comes about because the degree of \( Y_{I,J} \) exceeds 4; this is carefully arranged. For us \( Y_{I,J} \) has degree 5, but more sophisticated manoeuvres would have provided us with a degree 6 surface, leading in principle to an even lower exponent of roughly 2.91. However, in that case the calculations to show that there are no lines would have been substantially more involved. Having reduced the exponent below the key threshold of 3, we have decided not to pursue this minor improvement.

We organise thus. In §2 we establish (1.4), and in §3 we prove the complementary lower bound (1.5). In §4 we establish Theorem 1.4, thereby also completing the proof of Theorem 1.3. In §5 we prove Theorem 1.2, thereby also completing the proof of Theorem 1.1. Finally, in §6 we show that \( N_{V_4} \gg H^{3/2} \) and \( N_{A_4} \gg H \). The first appendix contains a proof of Lemma 4.1, for which we claim no originality. The second appendix contains the C code used to compute the values of \( N_G(100) \), for \( G \in \{S_4, A_4, D_4, V_4, C_4\} \). We adopt the convention that \( \varepsilon \) denotes an arbitrarily small positive constant, whose value is allowed to change between occurrences. We use Vinogradov and Bachmann–Landau notation throughout, with the implicit constants being allowed to depend on \( \varepsilon \). We write \( #S \) for the cardinality of a set \( S \). If \( g \) and \( h \) are positive-valued, we write \( g \asymp h \) if \( g \ll h \ll g \).
Throughout $H$ denotes a positive real number, sufficiently large in terms of $\varepsilon$. Let $\mu(\cdot)$ be the Möbius function.

SC was supported by EPSRC Programme Grant EP/J018260/1, by an Oberwolfach Leibniz Graduate Students grant, and by the National Science Foundation under Grant No. DMS-1440140 while in residence at the Mathematical Sciences Research Institute in Berkeley, California, during the Spring 2017 semester. Both authors thank the Mathematisches Forschungsinstitut Oberwolfach for excellent working conditions. Both authors thank the Fields Institute for funding, and for favourable working conditions. SC thanks Henning Bostelmann for IT support. We thank Victor Beresnevich, Manjul Bhargava, Tim Browning, John Cremona, Samir Siksek, Frank Thorne, and most of all Stanley Xiao for helpful discussions.

2. A remarkable symmetry

In this section, we establish (1.4). A well-known criterion [16, Theorem 1] tells us that if $f$ is irreducible then $G_f$ is isomorphic to $D_4, V_4$ or $C_4$ if and only if the cubic resolvent
\[ r(X) = r(X; a, b, c, d) = X^3 - bX^2 + (ac - 4d)X - (a^2 d - 4bd + c^2) \]
has a rational root. As $r$ is monic, any rational root of $r$ is an integer. Moreover, if $f \in S_H$ and $r(x) = 0$ then $|x| \leq 8H$. The proposition below therefore implies (1.4).

**Proposition 2.1.** Write $R(H)$ for the number of integer solutions $(x, a, b, c, d) \in [-8H, 8H] \times [-H, H]^4$ to the equation
\[ r(x; a, b, c, d) = 0. \] (2.1)

Then
\[ R(H) \ll H^2 (\log H)^2. \]

We set about proving this. Multiplying (2.1) by 4, we obtain
\[ (x^2 - 4d) \cdot (a^2 - 4(b - x)) = (xa - 2c)^2. \] (2.2)

Change variables, replacing $b - x$ by $e$, so that (2.2) becomes
\[ (x^2 - 4d) \cdot (a^2 - 4e) = (xa - 2c)^2, \] (2.3)

with $|e| \leq 9H$. Observe that the equation (2.3) exhibits a great deal of symmetry. We need to count integer solutions $(x, a, c, d, e)$ with
\[ |a|, |c|, |d| \leq H, \quad |x| \leq 8H, \quad |e| \leq 9H. \]

We begin with the case in which both sides of (2.3) are 0. For each $c$ there are at most $\tau(2c)$ choices of $(x, a)$. Therefore, by an average divisor function estimate, the number of choices of $(x, a, c)$ is $O(H \log H)$. Having chosen $x, a, c$ with $xa = 2c$, there are then $O(H)$ possible $(d, e)$. We conclude that the number of solutions for which $xa = 2c$ is $O(H^2 \log H)$. It remains to treat solutions for which $xa \neq 2c$. 5
Write $x^2 - 4d = uv^2$ with $u \in \mathbb{Z} \setminus \{0\}$ squarefree and $v \in \mathbb{N}$. This forces $a^2 - 4e = uw^2$ and $xa - 2c = \pm uvw$ for some $w \in \mathbb{N}$. Our strategy will be to upper bound the number of lattice points $(u, v, w, x, a)$ with $u \neq 0$ in the region defined by $|x|, |a| \leq 8H$ and

$$|x^2 - uv^2| \leq 36H \quad (2.4)$$

$$|a^2 - uw^2| \leq 36H \quad (2.5)$$

$$\min\{|xa - uvw|, |xa + uvw|\} \leq 2H. \quad (2.6)$$

At most two values of $(c, d, e)$ are then determined by $(u, v, w, x, a)$.

For the case $u < 0$, choose $p = -u$ in the range $1 \leq p \ll H$. Then (2.4) implies $x^2 + pv^2 \ll H$, which has $O(H/\sqrt{p})$ solutions $(x, v)$. Similarly there are $O(H/\sqrt{p})$ choices of $(a, w)$. As

$$\sum_{1 \leq p \ll H} H^2/p \ll H^2 \log H,$$

we find that the total contribution from this case is $O(H^2 \log H)$.

It remains to deal with the case $u > 0$. Arguing by symmetry, it suffices to count solutions for which

$$u > 0, \quad x, a \geq 0, \quad 1 \leq w \leq v. \quad (2.7)$$

Now (2.6) is equivalent to

$$|xa - uvw| \leq 2H. \quad (2.8)$$

Choose $u$ and $v$ to begin with, so that $uv^2 \ll H^2$. First suppose $uv^2 \leq 40H$. Then $x, a \ll \sqrt{H}$, so the contribution from this case is bounded above by a constant times

$$H \sum_{v \leq \sqrt{40H}} \sum_{u \leq 40H/v^2} \sum_{w \leq v} 1 \ll H^2 \log H.$$

This is more than adequate, so in the sequel we assume that $uv^2 > 40H$.

Now (2.4) implies that $x \asymp v\sqrt{u}$. There are $v$ choices of $w$, and since

$$|x - v\sqrt{u}| \leq \frac{36H}{x + v\sqrt{u}} \ll \frac{H}{v\sqrt{u}}$$

there are $O(1 + \frac{H}{v\sqrt{u}}) = O(\frac{H}{v\sqrt{u}})$ choices of $x$. Using (2.8), observe that

$$x(a - w\sqrt{u}) + w\sqrt{u}(x - v\sqrt{u}) = xa - uvw \ll H.$$

As $w \leq v$, we now have

$$a - w\sqrt{u} \ll \frac{H}{v\sqrt{u}} + w\sqrt{u}\frac{|x^2 - uv^2|}{(x + v\sqrt{u})^2} \ll \frac{H}{v\sqrt{u}}.$$  

In particular, there are $O(1 + \frac{H}{v\sqrt{u}}) = O(\frac{H}{v\sqrt{u}})$ possibilities for $a$. We obtain the upper bound

$$\sum_{1 \leq u, v \ll H^2} v \left(\frac{H}{v\sqrt{u}}\right)^2 \leq H^2 \sum_{1 \leq u, v \ll H^2} \frac{1}{uv} \ll H^2 (\log H)^2,$$

completing the proof.

6
3. A construction

In this section, we establish (1.5). Our construction is motivated by the previous section. Let \( \delta \) be a small positive constant. We shall choose positive integers

\[
x, a, u, w \equiv 12 \mod 18, \quad v \equiv 4 \mod 6
\]

with \( u \) squarefree, in the ranges

\[
1 \leq u \leq H^{2-2\delta} \quad \delta^{-1}\sqrt{H} \leq \frac{1}{2}v\sqrt{u} \leq w\sqrt{u} \leq v\sqrt{u} \leq \delta^2H \\
v\sqrt{u} < x \leq v\sqrt{u} + \frac{\delta H}{v\sqrt{u}} \\
w\sqrt{u} < a \leq w\sqrt{u} + \frac{\delta H}{v\sqrt{u}}.
\]

Let us now bound from below the number of choices \((u, v, w, x, a)\). If we choose \(u, v \in \mathbb{N}\) with \(u \leq H^{2-2\delta}\), \(v \geq 99\) and

\[
2\delta^{-1}\sqrt{H} \leq v\sqrt{u} \leq \delta^2H,
\]

then the number of choices for \((w, x, a)\) is bounded below by a constant times \(v(\frac{H}{v\sqrt{u}})^2 = \frac{H^2}{uv}\). Thus, the number of possible choices of \((x, a, u, v, w)\) is bounded below by a constant times

\[
X(H) := H^2 \sum_{u \in U} u^{-1} \sum_{v \in V(u)} v^{-1},
\]

where

\[
U = \{ u \in \mathbb{N} : |\mu(u)| = 1, \ u \equiv 12 \mod 18, \ u \leq H^{2-2\delta} \}
\]

and

\[
V(u) = \{ v \geq 99 : v \equiv 4 \mod 6, \ 2\delta^{-1}\sqrt{H} \leq v\sqrt{u} \leq \delta^2H \}.
\]

We compute that

\[
X(H) = H^2 \sum_{u \in U} u^{-1} \sum_{v \in V(u)} v^{-1} \gg H^2 \log H \sum_{u \in U} u^{-1}.
\]

Observe that the conditions

\[
u \equiv 12 \mod 18, \quad |\mu(u)| = 1\]

on \( u \) are equivalent to the conditions

\[
r \equiv 5 \mod 6, \quad |\mu(r)| = 1
\]

on \( r = u/6 \). It thus follows from work of Hooley [13, Theorem 3] that

\[
\# \{ u \in U : u \leq t \} = c_0 t + O(\sqrt{t}),
\]

for some constant \( c_0 > 0 \). Partial summation now gives

\[
\sum_{u \in U} u^{-1} \sim c_1 \log H,
\]

where \( c_1 = c_1(\delta) = (2 - 2\delta)c_0 \), so in particular \( X(H) \gg H^2(\log H)^2 \).
Given such a choice of \((u, v, w, x, a)\), define \(b, c, d \in \mathbb{Z}\) by

\[
4d = x^2 - uv^2, \quad 4(b - x) = a^2 - uw^2, \quad 2c = xa - uwv.
\]

We claim that the polynomial \(f\) defined by (1.1) lies in \(\mathcal{S}_H\), and that \(G_f\) is isomorphic to \(D_4, V_4\) or \(C_4\). We now confirm this claim.

Plainly \(|a| \leq H\). Moreover, since

\[
4d = x^2 - uv^2 = (x - v\sqrt{u})(x + v\sqrt{u}),
\]

we have

\[
0 < 4d \leq \frac{\delta H}{v\sqrt{u}}(2v\sqrt{u} + \frac{\delta H}{v\sqrt{u}}) < H,
\]

and similarly \(0 < 4(b - x) < H\). Now the triangle inequality gives \(|b| \leq x + H/4 < H\).

Finally, we check that

\[
0 < 2c = xa - uwv \leq \left(v\sqrt{u} + \frac{\delta H}{v\sqrt{u}}\right)\left(w\sqrt{u} + \frac{\delta H}{v\sqrt{u}}\right) - uwv < H.
\]

We have shown that \(|a|, |b|, |c|, |d| \leq H\).

Since \(x, a\) and \(u\) are divisible by 3, we have \(a \equiv b \equiv c \equiv d \equiv 0 \mod 3\). Furthermore

\[
4d = x^2 - uv^2 \equiv -3v^2 \mod 9,
\]

so \(9 \nmid d\). Thus, by Eisenstein’s criterion, the polynomial (1.1) is irreducible. Hence \(f \in \mathcal{S}_H\). Moreover, since \(x \in \mathbb{Z}\) is a root of the cubic resolvent of \(f\), we know from [16, Theorem 1] that \(G_f\) is isomorphic to \(D_4, V_4\) or \(C_4\).

Finally, we verify that the number of distinct polynomials \(f(X)\) arising from this construction is at least a constant times \(H^2(\log H)^2\). We achieve this by showing that a polynomial \(f(X)\) occurs for at most three different choices of \((u, v, w, x, a)\). Suppose the quadruple \((a, b, c, d)\) is obtained via this construction. Then \(x\) is a root of the cubic resolvent of \(f\), so there are at most three possibilities for \(x\). Since \(u, v, w \in \mathbb{N}\) with \(u\) squarefree, the equations

\[
x^2 - 4d = uv^2, \quad a^2 - 4(b - x) = uw^2
\]

now determine the triple \((u, v, w)\). Thus, a quadruple \((a, b, c, d)\) can be obtained from \((u, v, w, x, a)\) in at most three ways via our construction, and so we’ve constructed at least a constant times \(H^2(\log H)^2\) polynomials in this way. This completes the proof of (1.5).

4. \(V_4\) and \(C_4\) quartics

In this section we prove Theorem 1.4 and thereby also establish Theorem 1.3. From [2] we know that if \(f \in \mathcal{S}_H\) and \(G_f\) is isomorphic to \(V_4\) or \(C_4\) then, with \(O(H^2 \log H)\) exceptions, there exist integers \(u, v, w > 0\) and \(x \in [-8H, 8H]\) such that

\[
d = \frac{x^2 - uv^2}{4}, \quad b = x + \frac{a^2 - uw^2}{8}, \quad c = \frac{xa \pm uwv}{2}.
\]

(4.1)
4.1. $V_4$ quartics. Since $V_4$ is a subgroup of $A_4$, the discriminant $\Delta$ of $f$ is a square [14 §4.8]. We have the standard formula [11 §14.6]

\[
\Delta = -128b^2d^2 - 4a^2c^3 + 16b^4d - 4b^3c^2 - 27a^4d^2 + 18abc^3 \\
+ 144a^2bd^2 - 192acd^2 + a^2b^2c^2 - 4a^2b^3d - 6a^2c^2d \\
+ 144bc^2d + 256d^3 - 27c^4 - 80ab^2cd + 18a^3bcd.
\]

We make the substitutions (4.1) using the software Mathematica [25], obtaining the factorisation

\[
\frac{64\Delta}{u^2(2v^2 \pm avw + w^2x)^2} = a^4 - 64uv^2 \mp 32auvw - 2a^2uw^2 \\
+ u^2w^4 - 16a^2x - 16uw^2x + 64x^2.
\] (4.2)

Note that the denominator of the left hand side is nonzero, for the irreducibility of $f$ implies that $\Delta \neq 0$. We now equate the right hand side with $y^2$, for some $y \in \mathbb{Z}$. Given $u, v, w, a$, the integer point $(x, y)$ must lie on one of the two curves $C_{u,v,w,a}^\pm$ defined by

\[
(8x - (a^2 + uw^2))^2 - (4a^2uw^2 + 64u^2w^2 \mp 32auvw) = y^2.
\] (4.3)

Therefore $N_{V_4}$ is bounded above, up to a multiplicative constant, by $H^2 \log H$ plus the number of sextuples $(u, v, w, x, a, y) \in \mathbb{N}^3 \times \mathbb{Z}^3$ satisfying $|x|, |a| \leq 8H$, (2.4), (2.5), (2.6) and $(x, y) \in C_{u,v,w,a}^+ \cup C_{u,v,w,a}^-$. 

We first consider the contribution from $(u, v, w, a)$ for which $C_{u,v,w,a}^\pm$ is reducible over $\overline{\mathbb{Q}}$. In this case

\[
(8x - (a^2 + uw^2))^2 - (4a^2uw^2 + 64u^2w^2 \mp 32auvw)
\]

is a square in $\overline{\mathbb{Q}}[x]$, so

\[
4a^2uw^2 + 64u^2w^2 \mp 32auvw = 0.
\]

As $u \neq 0$ we now have $(aw \pm 4v)^2 = 0$, so

\[
aw = \mp 4v. \tag{4.4}
\]

(1) For the case $uw^2 \leq 40H$, we first choose $u \in [1, 40H]$, then there are $O(\sqrt{H/u})$ choices of $w$, and by (2.5) there are $O(\sqrt{H})$ possibilities for $a$. This then determines at most two possible $v$, via (4.4). Since

\[
|x| - v\sqrt{u} \ll \frac{H}{|x| + v\sqrt{u}},
\]

there are now $O(1 + H/\sqrt{u}) = O(H/\sqrt{u})$ choices of $x$. The contribution from this case is therefore bounded above by a constant times

\[
\sum_{u \leq 40H} \sqrt{\frac{H}{u}} \sqrt{H} \frac{H}{\sqrt{u}} \ll H^2 \log H.
\]

(2) If instead $uw^2 > 40H$, then $|a| \asymp w\sqrt{u}$, so from (4.4) we have

\[
v \gg |aw| \gg w^2\sqrt{u}.
\]
Start by choosing $u, w$ for which $40H < uw^2 \ll H^2$. There are then

$$O\left(1 + \frac{H}{w \sqrt{u}}\right) = O\left(\frac{H}{w \sqrt{u}}\right)$$

possible $a$, since

$$|a| - w \sqrt{u} \ll \frac{H}{|a| + w \sqrt{u}},$$

and then $v$ is determined by (4.4) in at most two ways. Now

$$|x| - v \sqrt{u} \ll \frac{H}{v \sqrt{u}},$$

so the number of possibilities for $x$ is bounded above by a constant times

$$1 + \frac{H}{v \sqrt{u}} \ll \frac{H}{v \sqrt{u}} \ll \frac{H}{w^2 u}. $$

Thus, the contribution from this case is bounded above by a constant times

$$\sum_{uw^2 \ll H^2} \frac{H}{w \sqrt{u}} \cdot \frac{H}{w^2 u} \ll H^2.$$

We have shown that there are $O(H^2 \log H)$ sextuples

$$(u, v, w, x, a, y) \in \mathbb{N}^3 \times \mathbb{Z}^3$$

satisfying $|x|, |a| \leq 8H$, (2.4), (2.5), (2.6) and (4.3) such that $C_{u, v, w, a}^\pm$ is reducible over $\mathbb{Q}$.

It remains to address the situation in which $C_{u, v, w, a}^\pm$ is absolutely irreducible. We will ultimately apply Vaughan’s uniform count for integer points on curves of this shape [24, Theorem 1.1].

Suppose $w \leq v$ and $uv^2 \leq 40H$. Then $x, a \ll \sqrt{H}$, so the number of solutions is bounded above by a constant times

$$H \sum_{v \leq \sqrt{40H}} \sum_{w \leq 40H/v^2} \sum_{u \leq v} 1 \ll H^2 \log H. $$

Similarly, if $v \leq w$ and $uw^2 \leq 40H$ then there are $O(H^2 \log H)$ solutions.

Next, we consider the scenario in which $w \leq v$ and $uv^2 > 40H$. Using (2.4), this implies that

$$x^2 > \frac{1}{10} uv^2,$$

so $|x| > \frac{1}{4} v \sqrt{u}$. Using (2.6), we have

$$||x|(|a| - w \sqrt{u}) + w \sqrt{u} |x| - v \sqrt{u}| = ||xa| - uvw| \leq 2H. $$

As $|x| > \frac{1}{4} v \sqrt{u}$ and $w \leq v$, we now have

$$||a| - w \sqrt{u}| \leq \frac{2H + w \sqrt{u} |x| - v \sqrt{u}|}{|x|} \leq \frac{8H}{v \sqrt{u}} + 4|x| - v \sqrt{u}|.$$

Since

$$||x| - v \sqrt{u}| = \frac{|x^2 - uv^2|}{|x| + v \sqrt{u}|} \leq \frac{36H}{v \sqrt{u}}. $$

(4.5)
we arrive at the inequality
\[ |a| - w\sqrt{u} \ll \frac{H}{v\sqrt{u}}. \]
In particular, given \( u, v, w \) there are
\[ O\left(1 + \frac{H}{v\sqrt{u}}\right) = O\left(\frac{H}{v\sqrt{u}}\right) \]
possibilities for \( a \).
Choose \( u, v, w \in \mathbb{N} \) and \( a \in \mathbb{Z} \) such that \( C_{u,v,w,a}^\pm \) is absolutely irreducible. Note (4.5), and put \( L = \frac{36H}{v\sqrt{u}} + 1 \). Now [24, Theorem 1.1] reveals that (4.3) has \( O\left(L^{1/2}\right) \) solutions \((x, y)\), with an absolute implied constant. As \( w \leq v \), the number of solutions is therefore bounded by a constant multiple of
\[
\sum_{uv^2 \ll H^2} v \frac{H}{v\sqrt{u}} \sqrt{\frac{H}{v\sqrt{u}}} \ll H^{3/2} \sum_{u \ll H^2} u^{-3/4} \sum_{v \ll H/\sqrt{u}} v^{-1/2} \ll H^2 \sum_{u \ll H^2} u^{-1} \ll H \log H.
\]

The final case, wherein \( v \leq w \) and \( uw^2 > 40H \), is very similar to the previous one. We have considered all cases, and conclude that
\[ N_{C_4} \ll H^2 \log H. \]

4.2. \( C_4 \) quartics. We require the following result from an expository note written by Keith Conrad [7, Corollary 4.3]. This is a variant of the Kappe–Warren criterion [16, Theorem 1 (iv)], and we provide a proof—claiming no originality—in the appendix.

**Lemma 4.1.** Let \( f \) be a monic, irreducible quartic polynomial given by (1.1), with \( a, b, c, d \in \mathbb{Z} \) and \( G_f \simeq C_4 \). Then the cubic resolvent \( r(X) \) has a unique integer root \( t \), and \((t^2 - 4d)\Delta \) is a perfect square.

**Remark 4.2.** In [7], one also has \((a^2 - 4(b - t))\Delta \) being a square, for \( C_4 \) quartics. By our identity (2.2), this is equivalent to \((t^2 - 4d)\Delta \) being a square, unless one of the two terms vanishes. The latter can occur.

We follow a similar strategy to the one that we used for \( V_4 \). The root of the cubic resolvent is \( x \), so \((x^2 - 4d)\Delta \) is a perfect square. Observe from (4.1) that \( x^2 - 4d = uv^2 \). Factorising the right hand side of (4.2), we thus obtain
\[
up\left((8x - (a^2 + uw^2))^2 - 4u(aw \pm 4v)^2\right) = y^2,
\]
for some \( y \in \mathbb{Z} \). Given \( u, v, w, a \), this defines a pair of curves \( Z_{u,v,w,a}^\pm \). As \( u \neq 0 \), the curve \( Z_{u,v,w,a}^\pm \) is absolutely irreducible if and only if the curve \( C_{u,v,w,a}^\pm \) defined in (4.3) is absolutely irreducible. The remainder of the proof can be taken almost verbatim from §4.1.

We conclude that
\[ N_{C_4} \ll H^2 \log H, \]
and this completes the proof of Theorem 1.3. In light of (1.4) and (1.5), we have also completed the proof of Theorem 1.3.
5. $A_4$ quartics

In this section, we establish Theorem 1.5. We use the criterion [16] Theorem 1], which in particular asserts that $A_4$ quartics have square discriminant. It remains to show that the diophantine equation

$$\text{disc}(X^4 + aX^3 + bX^2 + cX + d) = y^2$$

has $O(H^{5/2 + \varepsilon})$ integer solutions for which $|a|, |b|, |c|, |d| \leq H$ and $y \in \mathbb{Z} \setminus \{0\}$. We have the standard formula [1]

$$\Delta := \text{disc}(X^4 + aX^3 + bX^2 + cX + d) = \frac{4I^3 - J^2}{27},$$

where $I$ and $J$ are as defined in (1.6). The idea now is to count integer triples $(I, J, y)$ solving (1.7) with $I \ll H^2$ and $y \neq 0$, and to then count quadruples of integers $(a, b, c, d) \in [-H, H]^4$ corresponding via (1.6) to a given $(I, J, y)$. Each integer $I \ll H^2$ defines via (1.7) a quadratic polynomial in $(J, y)$ with nonzero discriminant. Thus, by [18, Lemma 2], the diophantine equation (1.7) admits $O(H^{2+\varepsilon})$ solutions $(I, J, y)$ with $I \ll H^2$. It therefore remains to show that if $4I^3 - J^2 \neq 0$ then there are $O(H^{1+\varepsilon})$ integer quadruples $(a, b, c, d) \in [-H, H]^4$ satisfying (1.6).

First we deal with the case $a = 0$. In this case (1.6) becomes

$$I = 12d + b^2, \quad J = 72bd - 27c^2 - 2b^3,$$

so

$$c^2 = -\frac{1}{27}(8b^3 - 6Ib + J). \quad (5.1)$$

Given $I$ and $J$, the right hand side has an odd degree in $b$, and is therefore not a square in $\mathbb{Q}[b]$. Hence (5.1) defines an absolutely irreducible curve in $b, c$, and so by [24, Theorem 1.1] there are $O(H^{1/2})$ solutions $(b, c) \in (\mathbb{Z} \cap [-H, H])^2$. As $d = (I - b^2)/12$ in this case, we conclude that there are $O(H^{1/2})$ integer quadruples $(a, b, c, d) \in \{0\} \times [-H, H]^3$ satisfying (1.6). We may therefore assume in the sequel that $a \neq 0$.

Fix $I, J$ for which $4I^3 \neq J^2$. Substituting $c = \frac{b^2 + 12d - I}{3a}$ into the expression (1.6) for $J$ yields

$$72a^2bd + 3a^2b(b^2 + 12d - I) - 3(b^2 + 12d - I)^2 - 27a^4d - 2a^2b^3 - a^2J = 0. \quad (5.2)$$

This defines an affine surface $Y_{I, J}$ in the variables $a, b, d$. It remains to show that there are $O(H^{1+\varepsilon})$ integer solutions $(a, b, d) \in [-H, H]^3$ to (5.2).

**Lemma 5.1.** The affine surface $Y_{I, J}$ contains no rational lines.

**Proof.** A line has the form

$$\mathcal{L} = \{((\alpha, \beta, \delta) + t(A, B, D) : t \in \mathbb{Q}\}$$

for some $(\alpha, \beta, \delta) \in \mathbb{Q}^3$ and some $(A, B, D) \in \mathbb{Q}^3 \setminus \{0\}$. There are three types of line to consider:

I. $\mathcal{L} = \{(0, \beta, \delta) + t(1, B, D) : t \in \mathbb{Q}\}$

II. $\mathcal{L} = \{(\alpha, 0, \delta) + t(0, 1, D) : t \in \mathbb{Q}\}$

III. $\mathcal{L} = \{(\alpha, \beta, 0) + t(0, 0, 1) : t \in \mathbb{Q}\}$. 

12
**Case I.** Substituting \((a, b, d) = (0, \beta, \delta) + t(1, B, D)\) into (5.2) yields
\[
72t^2(\beta + Bt)(\delta + Dt) + 3t^2(\beta + Bt)((\beta + Bt)^2 + 12(\delta + Dt) - I) \\
- 3((\beta + Bt)^2 + 12(\delta + Dt) - I)^2 - 27t^4(\delta + Dt) - 2t^2(\beta + Bt)^3 - t^2J = 0. \tag{5.3}
\]
Regarding this as a polynomial in \(t\), and equating constant coefficients, yields
\[
\beta^2 + 12\delta - I = 0. \tag{5.4}
\]
Dividing (5.3) by \(t^2\) now gives
\[
72(\beta + Bt)(\delta + Dt) + 3t(\beta + Bt)(2\beta B + 12D + B^2t) \\
- 3(2\beta B + 12D + B^2t)^2 - 27t^2(\delta + Dt) - 2(\beta + Bt)^3 - J = 0.
\]
Now equate \(t^j\) coefficients for \(j = 3, 2, 0\), obtaining
\[
B^3 - 27D = 0 \tag{5.5}
\]
\[
-3B^4 + 3\beta B^2 - 27\delta + 108BD = 0 \tag{5.6}
\]
\[
-J - 12\beta^2B^2 - 2\beta^3 + 72\beta\delta - 144\beta BD - 432D^2 = 0. \tag{5.7}
\]
From (5.4) and (5.5) we have
\[
\delta = \frac{I - \beta^2}{12}, \quad D = \frac{B^3}{27}.
\]
Substituting these into (5.6) yields
\[
-3B^4 + 3\beta B^2 - \frac{9}{4}(I - \beta^2) + 4B^4 = 0,
\]
and so
\[
9\beta^2 + (12B^2)\beta + (4B^4 - 9I) = 0.
\]
Therefore
\[
I \geq 0, \quad \beta = Z - \frac{2}{3}B^2, \quad Z = \pm \sqrt{I}.
\]
Next, we substitute
\[
\beta = Z - \frac{2}{3}B^2, \quad \delta = \frac{Z^2 - \beta^2}{12}, \quad D = \frac{B^3}{27}
\]
into (5.7). After some simplification, checked using the computer algebra package *Mathematica* [25], we obtain
\[
-J - 2Z^3 = 0.
\]
Now \(J^2 = 4I^3\), contrary to hypothesis. We conclude that \(Y_{I,J}\) has no lines of Type I.

**Case II.** Substituting \((a, b, d) = (\alpha, 0, \delta) + t(0, 1, D)\) into (5.2) yields a quartic in \(t\), which cannot vanish identically. This case provides no lines.

**Case III.** Substituting \((a, b, d) = (\alpha, \beta, t)\) into (5.2) yields a quadratic in \(t\), which cannot vanish identically. This case provides no lines.

Having checked all cases, we find that \(Y_{I,J}\) contains no rational lines. \(\Box\)

**Lemma 5.2.** The affine surface \(Y_{I,J}\) is absolutely irreducible.
Proof. Observe that $Y_{I,J}$ is the zero locus of the polynomial
\[ g(a, b, d) = c_2 d^2 + c_1(a, b)d + c_0(a, b), \]
where
\[ c_2 = -432, \quad c_1(a, b) = 108a^2b - 72(b^2 - I) - 27a^4 \]
\[ c_0(a, b) = a^2b^3 - 3a^2bI - 3(b^2 - I)^2 - a^2J. \]
Assume for a contradiction that $Y_{I,J}$ is not absolutely irreducible. Then there exist polynomials $g_0(a, b)$ and $h_0(a, b)$, defined over $\mathbb{Q}$, for which
\[ c_2 d^2 + c_1(a, b)d + c_0(a, b) = (d + g_0(a, b))(c_2d + h_0(a, b)). \]
Now
\[ c_1(a, b) = c_2g_0(a, b) + h_0(a, b) \quad (5.8) \]
and
\[ c_0(a, b) = g_0(a, b)h_0(a, b). \quad (5.9) \]
From (5.8) we have
\[ \max\{\deg_a(g_0), \deg_a(h_0)\} \geq \deg_a(c_1) = 4. \]
This violates (5.9), since $\deg_a(c_0) = 2$. This contradiction confirms that $Y_{I,J}$ is absolutely irreducible. \hfill \Box

Finally, we complete the proof of Theorem 1.5. By [3, Lemma 1], there exist polynomials $g_1, \ldots, g_J \in \mathbb{Z}[a, b, d]$ with $J \ll H^{\frac{3}{2} + \varepsilon}$, and a finite set of points $Z \subseteq Y_{I,J}$ such that
1. Each $g_j$ is coprime to $g$, and has degree $O(1)$
2. $|Z| \ll H^{\frac{3}{2} + \varepsilon}$
3. For $(a, b, d) \in Y_{I,J} \cap (\mathbb{Z} \cap [-H, H]^3 \setminus Z$ there exists $j \leq J$ for which
   \[ g(a, b, d) = g_j(a, b, d) = 0. \]
Next, we let $G(a, b, d) \in \mathbb{Z}[a, b, d]$ be coprime to $g$, and count solutions to
\[ g(a, b, d) = G(a, b, d) = 0. \quad (5.10) \]
Our first task is to show that $F(a, b) = 0$ for some nonzero polynomial $F$. One can take $F$ to be the resultant of $g$ and $G$ in the variable $d$, however in our setting we can easily perform the elimination explicitly, as we now explain. From $g(a, b, d) = 0$ we have
\[ d^2 = -c_2^{-1}c_1(a, b)d - c_2^{-1}c_0(a, b). \quad (5.11) \]
We substitute this repeatedly into $G(a, b, d) = 0$, and stop when the degree in $d$ is at most 1. To describe each step of the process more precisely, regard $G(a, b, d)$ as a polynomial in $d$ with coefficients in $\mathbb{Z}[a, b]$, and if $D = \deg_d(G) \geq 2$ then replace $d^D$ by
\[ d^{D-2}(-c_2^{-1}c_1(a, b)d - c_2^{-1}c_0(a, b)). \]
We always obtain something relatively prime to $g$, and in particular we do not end up with the zero polynomial. We finally obtain
\[ G_1(a, b)d = G_2(a, b), \]
for some relative prime polynomials \( G_1, G_2 \) with integer coefficients. Thus, for each solution \((a, b, d)\) to (5.10), we have \( F(a, b) = 0 \), where

\[
F(a, b) = c_2 G_2(a, b)^2 + c_1(a, b)G_2(a, b)G_1(a, b) + c_0(a, b)G_1(a, b)^2
\]
is not the zero polynomial.

Observe that \( F(a, b) = 0 \) if and only if we have \( F(a, b) = 0 \) for some irreducible factor \( F(a, b) \in \mathbb{Q}[a, b] \) of \( F(a, b) \). So let \( F(a, b) \in \mathbb{Q}[a, b] \) be an irreducible factor of \( F(a, b) \). If \( F(a, b) \) is nonlinear, then Bombieri–Pila [2] gives

\[
\# \{(a, b) \in (\mathbb{Z} \cap [-H, H])^2 : F(a, b) = 0 \} \ll H^{\frac{3}{2} + \varepsilon}.
\]

Then \( d \) is determined by (5.11) in at most two ways, so the number of solutions \((a, b, d)\) counted in this case is \( O(H^{\frac{3}{2} + \varepsilon}) \).

Suppose instead that \( F(a, b) \) is linear. Now

\[
\alpha a + \beta b + \gamma = 0,
\]
for some \((\alpha, \beta, \gamma) \in (\mathbb{Q}^2 \setminus \{(0, 0)\}) \times \mathbb{Q}\). If \( \beta \neq 0 \) then substitute \( b = -\beta^{-1}(\alpha a + \gamma) \) into (5.11), giving

\[
d^2 + P_1(a)d + P_0(a) = 0,
\]
where

\[
P_i(a) = c_2^{-1}c_i(a, \beta^{-1}(\alpha a + \gamma)) \in \mathbb{Q}[a] \quad (i = 1, 0).
\]

Factorise the left hand side over \( \mathbb{Q} \), and let \( P(a, d) \in \mathbb{Q}[a, d] \) be an irreducible factor. Note that \( P(a, d) \) is nonlinear, for if it were linear then \( P(a, d) = F(a, b) = 0 \) would define a rational linear subvariety of \( Y_{I,J} \), of dimension greater than or equal to 1, violating Lemma [5.1] Now Bombieri–Pila yields

\[
\# \{(a, d) \in (\mathbb{Z} \cap [-H, H])^2 : P(a, d) = 0 \} \ll H^{\frac{3}{2} + \varepsilon}.
\]

If \( \beta = 0 \) then substitute \( a = -\gamma/\alpha \) into (5.11) and apply essentially the same reasoning.

In both cases, the number of integer solutions \((a, b, d)\) to (5.10) \([-H, H]^3 \) is \( O(H^{\frac{3}{2} + \varepsilon}) \). We conclude that

\[
|Y_{I,J} \cap (\mathbb{Z} \cap [-H, H])^3| \ll J H^{\frac{3}{2} + \varepsilon} + H^{\frac{3}{2} + \varepsilon} \ll H^{\frac{1}{2} + \frac{1}{2} + 2\varepsilon}.
\]

This concludes the proof of Theorem 1.5. Theorems 1.3, 1.4 and 1.5 imply Theorem 1.1.

6. LOWER BOUNDS

6.1. Construction for \( V_4 \). Consider

\[
f(X) = X^4 + bX^2 + t^2,
\]
where \( b, t \in \mathbb{N} \) with \( b \equiv 0 \mod 4, \quad t \equiv 1 \mod 4 \)
and

\[
\frac{1}{2}H \leq b \leq H, \quad t \leq \sqrt{H}.
\]

Observe that the cubic resolvent

\[
r(X) = X^3 - bX^2 - 4t^2X + 4bt^2 = (X - b)(X - 2t)(X + 2t)
\]

15
splits into linear factors over the rationals. If we can show that \( f \) is irreducible over \( \mathbb{Q} \), then it will follow from [16] Theorem 1 that \( G_f \simeq V_4 \).

Plainly \( f(x) > 0 \) whenever \( x \in \mathbb{R} \), so \( f(X) \) has no rational roots, and therefore no linear factors. Suppose for a contradiction that \( f(X) \) is reducible. Then by Gauss’s lemma

\[
f(X) = (X^2 + pX + q)(X^2 + rX + s),
\]

for some \( p, q, r, s \in \mathbb{Z} \). Considering the \( X^3 \) coefficient of \( f \) gives \( r = -p \).

We begin with the case \( p \neq 0 \). Then considering the \( X \) coefficient of \( f \) gives \( s = q \). Now

\[
X^4 + bX^2 + t^2 = (X^2 + pX + q)(X^2 - pX + q) = X^4 + (2q - p^2)X^2 + q^2,
\]

so \( q = \pm t \) and \( 2q - b = p^2 \geq 0 \). This is impossible, since

\[
b \geq H/2 > 2\sqrt{H} \geq 2t = |2q|.
\]

It remains to consider the case \( p = 0 \). Now

\[
X^4 + bX^2 + t^2 = (X^2 + q)(X^2 + s),
\]

so

\[
q + s = b, \quad qs = t^2.
\]

In particular \( b^2 - 4t^2 \) is a square, which is impossible because

\[
b^2 - 4t^2 \equiv 12 \mod 16.
\]

Both cases led to a contradiction. Therefore \( f \) is irreducible, and we conclude that \( G_f \simeq V_4 \).

Our construction shows that \( N_{V_4} \gg H^{3/2} \).

6.2. Construction for \( A_4 \). We use a construction motivated by [19] Theorem 1.1]. Consider the family of quartic polynomials

\[
f(X) = f_{u,v}(X) = X^4 + 18v^2X^2 + 8uvX + u^2.
\]

Observe that \( f(X) \) is irreducible in \( \mathbb{Z}[X,u,v] \), as \( f_{1,0}(X) = X^4 + 1 \) is irreducible in \( \mathbb{Z}[X] \).

Next, consider the cubic resolvent of \( f \), given by

\[
r(X) = r_{u,v}(X) = X^3 - 18v^2X^2 - 4u^2X + 8u^2v^2.
\]

This is also irreducible in \( \mathbb{Z}[X,u,v] \), as \( r_{1,1}(X) = X^3 - 18X^2 - 4X + 8 \) is irreducible in \( \mathbb{Z}[X] \). Hence, by Hilbert’s irreducibility theorem [6] Theorem 2.5], almost all specialisations \( u, v \in \mathbb{N} \) with \( u, v \leq \sqrt{H}/5 \) give rise to an irreducible \( f(X) \in \mathbb{Z}[X] \) whose cubic resolvent is also irreducible. Finally, a short calculation reveals that

\[
\text{disc}(f(X)) = (16(27uv^4 + u^3))^2,
\]

so these polynomials have Galois group \( G_f \simeq A_4 \). They are distinct, so \( N_{A_4}(H) \gg H \).
Appendix A. Proof of Lemma 4.1

Here we provide a proof of Lemma 4.1. We claim no originality for this: the lemma was essentially proved by Kappe and Warren [16], and a proof of the precise statement was given by Conrad in an expository note [7, Corollary 4.3].

From [16, Theorem 1], we know that the cubic resolvent \( r(X) \) has a unique rational root \( t \). As \( f \) is monic with integer coefficients, we must have \( t \in \mathbb{Z} \). It remains to show that the integer \( (t^2 - 4d)\Delta \) is a rational square.

From [16, Theorem 1], we also know that the polynomial \( X^2 - tx + d \) splits over \( E \), where \( E \) is the splitting field of \( r(X) \). We first establish that \( E \cong \mathbb{Q}(\sqrt{\Delta}) \). (A.1)

Since \( r(X) \) and \( f(X) \) have the same discriminant \([11, \S 14.6]\), the isomorphism (A.1) is an immediate consequence of the following lemma [7, Theorem 2.6].

**Lemma A.1.** Let \( F(X) \in \mathbb{Q}[X] \) be a separable cubic with discriminant \( \Delta \), and suppose \( F \) has a rational root. Then \( \mathbb{Q}(\sqrt{\Delta}) \) is a splitting field of \( f(X) \) over \( \mathbb{Q} \).

**Proof.** Let \( r \in \mathbb{Q} \) and \( s, t \in \mathbb{Q} \) be the three distinct roots of \( F \). We may assume without loss that \( F \) is monic. Write \( F(X) = (X - r)G(X) \), for some monic rational quadratic polynomial \( G(X) \), and note that \( G(r) \neq 0 \). The quadratic formula yields

\[
\mathbb{Q}(r, s, t) = \mathbb{Q}(s, t) = \mathbb{Q}(\sqrt{\text{disc}(G)}).
\]

As \( F \) and \( G \) are monic, we compute that \( \text{disc}(F) = G(r)^2\text{disc}(G) \), so

\[
\sqrt{\text{disc}(G)} = \pm G(r)^{-1}\sqrt{\text{disc}(F)}.
\]

Therefore

\[
\mathbb{Q}(r, s, t) = \mathbb{Q}(\sqrt{\Delta}).
\]

Note from [16, Theorem 1] that \( r(X) \) does not split into linear factors over \( \mathbb{Q} \), so \( \Delta \) is not a rational square.

We proceed with the proof of Lemma 4.1 armed with the knowledge that \( X^2 - tx + d \) splits over \( \mathbb{Q}(\sqrt{\Delta}) \). The discriminant of this quadratic is \( t^2 - 4d \), therefore \( t^2 - 4d \) is a square in \( \mathbb{Q}(\sqrt{\Delta}) \). A square in \( \mathbb{Q}(\sqrt{\Delta}) \) has the form \( (q_1 + q_2\sqrt{\Delta})^2 \) for some \( q_1, q_2 \in \mathbb{Q} \), and from this we deduce that \( (t^2 - 4d)\Delta \) equals \( q_1^2 \) or \( \Delta q_2^2 \). In the former case the result is proved, so it remains to consider the case in which \( t^2 - 4d \) is a rational square.

Let \( \alpha, \beta, \gamma, \delta \in \mathbb{Q} \) be the roots of \( f \). The cubic resolvent has roots

\[
\alpha\beta + \gamma\delta, \quad \alpha\gamma + \beta\delta, \quad \alpha\delta + \beta\gamma,
\]

see [15, Part I, §10]. Reorder the roots of \( f \), if necessary, so that \( t = \alpha\beta + \gamma\delta \). By Vieta’s formula \( d = \alpha\beta\gamma\delta \), so now we have

\[
t^2 - 4d = (\alpha\beta - \gamma\delta)^2.
\]

As this is a rational square we have \( \alpha\beta - \gamma\delta \in \mathbb{Q} \), and since \( \alpha\beta + \gamma\delta \in \mathbb{Q} \) we now have \( \alpha\beta \in \mathbb{Q} \).

Since \( \alpha\beta + \gamma\delta \) is fixed by \( G_f \), and \( G_f \simeq C_4 \), we must have \( G_f \simeq \langle \sigma \rangle \), where \( \sigma = (\alpha\gamma\beta\delta) \). As \( \alpha\beta \in \mathbb{Q} \), we have \( \gamma\delta = \sigma(\alpha\beta) = \alpha\beta \), and so \( t^2 - 4d = 0 \). Therefore we can also conclude in this case that \( (t^2 - 4d)\Delta \) is a perfect square. This completes the proof of Lemma 4.1.
Appendix B. Code

We used the C programming language to compute the values of $N_C(100)$ provided in the introduction. The code is given below.

```c
#include <stdio.h>
#include <math.h>
#include <stdlib.h>
#define RANGE 100 /* max 100, otherwise not enough space for divisors */
#define TOTAL (2*RANGE+1)*(2*RANGE+1)*(2*RANGE+1)*(2*RANGE+1)

short irred[2*RANGE+1][2*RANGE+1][2*RANGE+1][2*RANGE+1];
int divisors[RANGE*RANGE*RANGE+5*RANGE*RANGE+1][500];

/* short[a,b,c,d]=1 if X^4+a*X^3+b*X^2+c*X+d irreducible otherwise 0
** divisors[i][0]: number of divisors of i (pos. and neg.);
** divisors[i][j]: j-th divisor of i */

void mark(int a, int b, int c, int d) {
    irred[a+RANGE][b+RANGE][c+RANGE][d+RANGE]=0;
}

void generate_irred() {
    /* generate table of all irreducible monic quartic polynomials of height <= H
    ** first all having constant term zero
    ** next those splitting as (X+a)(X^3+b*X^2+c*X+d), where |a| <=H, |d|<=H, |b|,|c|<=2H
    ** finally those splitting as (X^2+a*X+b)(X^2+c*X+d), where |b|, |d| \le H, |a|, |c| \le 2H */
    int a, b, c, d;
    for (a=-RANGE; a<=RANGE; a++)
        for (b=-RANGE; b<=RANGE; b++)
            for (c=-RANGE; c<=RANGE; c++)
                for (d=-RANGE; d<=RANGE; d++)
                    irred[a+RANGE][b+RANGE][c+RANGE][d+RANGE]=d!=0;
    for (a=-RANGE; a<=RANGE; a++)
        for (b=-2*RANGE; b<=2*RANGE; b++)
            for (c=-2*RANGE; c<=2*RANGE; c++)
                for (d=-RANGE; d<=RANGE; d++)
                    if (abs(a+b)<=RANGE && abs(a*b+c)<=RANGE && abs(a*c+d)<=RANGE && abs(a*d)<=RANGE)
                        mark(a+b, a*b+c, a*c+d, a*d);
    for (a=-2*RANGE; a<=2*RANGE; a++)
        for (b=-RANGE; b<=RANGE; b++)
            for (c=-2*RANGE; c<=2*RANGE; c++)
                for (d=-RANGE; d<=RANGE; d++)
                    if (abs(a+c)<=RANGE && abs(b+d+a*c)<=RANGE && abs(a*d+b*c)<=RANGE && abs(b*d)<=RANGE)
                        mark(a+c, b+d+a*c, a*d+b*c, b*d);
}

void generate_divisors() {
    /* generate divisor list, see above; the range covers all potential integer divisors of the
    ** constant term of the cubic resolvent of a monic quartic polynomial of height <=H */
    int i, j, n;
    for (i=1; i<=RANGE*RANGE*RANGE+5*RANGE*RANGE; i++) {
        for (n=0, j=-1; j<i; j++)
            if ((j!=0 && i*Xj)==0) {
                n++; divisors[i][n]=j;
            }
        divisors[i][0]=n;
```
int is_square(long int x) {
    /* returns 1 if x is a square, 0 otherwise */
    long double y;
    y=ceil(sqrt(x));
    return y*y==x;
}

double discr(int a, int b, int c, int d) {
    /* returns the discriminant of X^4+a*X^3+b*X^2+c*X+d */
    double a2, a3, a4, b2, b3, b4, c2, c3, c4, d2, d3;
    a2=a*a; b2=b*b; c2=c*c; d2=d*d;
    a3=a*a2; a4=a2*a2; b3=b*b2; b4=b2*b2; c3=c*c2; c4=c2*c2; d3=d*d2;
    return a2*b2*c2-4*b3*c2-4*a3*c3+18*a*b*c3-27*c4-8*a2*b3*d+16*b4*d+18*a3*b*c*d -
       80*a*b2*c2*d+64*a2*c2*d+144*b*c2*d-27*a4*d2+144*a2*b*d2-128*b2*d2-192*a*c*d2+256*d3;
}

int resolvent_reducible(int a, int b, int c, int d, int *root) {
    /* returns 1 if the cubic resolvent X^3-b*X^2+(ac-4d)X+(a^2d-4bd+c^2) of X^4+a*X^3+b*X^2+c*X+d
    ** is reducible, in which case root will be an integer root of the resolvent;
    ** otherwise return 0, root undefined
    ** Note that for C4 polynomials root is unique */
    int i, x, q, r, ra;
    r=a*a*d-4*b*d+c*c;
    if (r==0) {
        *root=0; return 1;
    }
    q=a*c-4*d;
    ra=abs(r);
    for (i=1; i<=divisors[ra][0]; i++) {
        x=divisors[ra][i];
        if (x*x*x-b*x*x+q*x-r==0) {
            *root=x; return 1;
        }
    }
    return 0;
}

int main() {
    /* Following the criteria in our paper, loop a,b,c,d over the height RANGE, each time compute
    ** the Galois group of X^4+a*X^3+b*X^2+c*X+d and print the resulting statistics */
    long s4=0, a4=0, d4=0, c4=0, v4=0, red=0, disc;
    int a, b, c, d, res_red, root;
    generate_irred();
    generate_divisors();
    for (a=-RANGE; a<=RANGE; a++)
        for (b=-RANGE; b<=RANGE; b++)
            for (c=-RANGE; c<=RANGE; c++)
                for (d=-RANGE; d<=RANGE; d++)
                    if (irred[a+RANGE][b+RANGE][c+RANGE][d+RANGE]) {
                        res_red=resolvent_reducible(a,b,c,d,&root);
                        disc=discr(a,b,c,d);
                        if (is_square(disc))
                            res_red ? v4++ : a4++;
                        else {
                            if (res_red)
is_square((root*root-4*d)*disc) && is_square((a*a-4*(b-root))*disc) ? c4++ : d4++;
else
s4++;
}
else
red++;
printf("Number of \textit{im}
d\textit{reducible}\textit{m}\ polynomials of height at most %d: \%ld\n", RANGE, red);
printf("Number of \textit{S}4\textit{m}\ polynomials of height at most %d: \%ld\n", RANGE, s4);
printf("Number of \textit{A}4\textit{m}\ polynomials of height at most %d: \%ld\n", RANGE, a4);
printf("Number of \textit{D}4\textit{m}\ polynomials of height at most %d: \%ld\n", RANGE, d4);
printf("Number of \textit{V}4\textit{m}\ polynomials of height at most %d: \%ld\n", RANGE, v4);
printf("Number of \textit{C}4\textit{m}\ polynomials of height at most %d: \%ld\n", RANGE, c4);
}

\textbf{References}

[1] M. Bhargava and A. Shankar, \textit{Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves}, Ann. of Math. (2) \textbf{181} (2015), 191–242.
[2] E. Bombieri and J. Pila, \textit{The number of integral points on arcs and ovals}, Duke Math. J. \textbf{59} (1989), 337–357.
[3] T. D. Browning, \textit{Power-free values of polynomials}, Arch. Math. \textbf{96} (2011), 139–150.
[4] R. Chela, \textit{Reducible polynomials}, J. Lond. Math. Soc. \textbf{38} (1963), 183–188.
[5] H. Cohen, F. Diaz y Diaz and M. Olivier, \textit{A survey of discriminant counting}, in Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369 (Springer, Berlin, 2002), 80–94.
[6] S. D. Cohen, \textit{The distribution of Galois groups and Hilbert’s irreducibility theorem}, Proc. Lond. Math. Soc. (3) \textbf{43} (1981), 227–250.
[7] K. Conrad, \textit{Galois groups of cubics and quartics (not in characteristic 2)}, expository note, \url{http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cubicquartic.pdf}
[8] R. Dietmann, \textit{Probabilistic Galois theory for quartic polynomials}, Glasg. Math. J. \textbf{48} (2006), 553–556.
[9] R. Dietmann, \textit{On the distribution of Galois groups}, Mathematika \textbf{58} (2012), 35–44.
[10] R. Dietmann, \textit{Probabilistic Galois theory}, Bull. Lond. Math. Soc. \textbf{45} (2013), 453–462.
[11] D. S. Dummit and R. M. Foote, \textit{Abstract Algebra}, third edition, Wiley and Sons, Hoboken, NJ, 2004.
[12] P. X. Gallagher, \textit{The large sieve and probabilistic Galois theory}, Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), pp. 91–101. Amer. Math. Soc., Providence, RI, 1973.
[13] C. Hooley, \textit{A note on square-free numbers in arithmetic progressions}, Bull. London Math. Soc. \textbf{7} (1975), 133–138.
[14] N. Jacobson, \textit{Basic algebra. I}, second edition, W. H. Freeman and Company, New York, 1985.
[15] I. Kaplansky, \textit{Fields and rings}, second edition, Chicago Lectures in Mathematics, The University of Chicago Press, Chicago, IL–London, 1972.
[16] L.-C. Kappe and B. Warren, \textit{An elementary test for the Galois group of a quartic polynomial}, Amer. Math. Monthly \textbf{96} (1989), 133–137.
[17] H-W. Knobloch, \textit{Die Seltenheit der reduziblen Polynome}, Jber. Deutsch. Math. Verein. \textbf{59} (1956), Abt. 1, 12–19.
[18] P. Lefton, \textit{On the Galois groups of cubics and trinomials}, Acta Arith. \textbf{XXXX} (1979), 239–246.
[19] E. Nart and N. Vila, \textit{Equations with absolute Galois group isomorphic to $A_n$}, J. Number Theory \textbf{16} (1983), 6–13.
[20] I. Rivin, \textit{Galois groups of generic polynomials}, \url{arXiv:1511.06446} 2015.
[21] G. W. Smith, \textit{Some polynomials over $\mathbb{Q}(t)$ and their Galois groups}, Math. Comp. \textbf{69} (2000), 775–796.
[22] W. Specht, \textit{Zur Zahlentheorie der Polynome. II}, Math. Nachr. \textbf{7} (1952), 105–126.
[23] B. L. van der Waerden, \textit{Die Seltenheit der reduziblen Gleichungen und die Gleichungen mit Affekt}, Monatsh. Math. \textbf{43} (1936), 137–147.
[24] R. C. Vaughan, \textit{Integer points on elliptic curves}, Rocky Mountain J. Math. \textbf{44} (2014), 1377–1382.
[25] Wolfram Research, Inc., Mathematica, Version 11.0, Champaign, IL (2016).
[26] S. Wong, Densities of quartic fields with even Galois groups, Proc. Amer. Math. Soc. 133 (2005), 2873–2881.
[27] D. Zywina, Hilbert's irreducibility theorem and the larger sieve, arXiv:1011.6465, 2010.

Department of Mathematics, University of York, Heslington, York YO10 5DD, United Kingdom
E-mail address: sam.chow@york.ac.uk

Department of Mathematics, Royal Holloway, University of London, TW20 0EX Egham, United Kingdom
E-mail address: Rainer.Dietmann@rhul.ac.uk