Orbital exponential sums for prehomogeneous vector spaces

Takashi Taniguchi and Frank Thorne

July 26, 2016

Abstract

Let (G, V) be a prehomogeneous vector space, let $\mathcal{O}$ be any $G(\mathbb{F}_q)$-invariant subset of $V(\mathbb{F}_q)$, and let Φ be the characteristic function of $\mathcal{O}$. In this paper we develop a method for explicitly and efficiently evaluating the Fourier transform $\widehat{\Phi}$, based on combinatorics and linear algebra. We then carry out these computations in full for each of five prehomogeneous vector spaces, including the 12-dimensional space of pairs of ternary quadratic forms. Our computations reveal that these Fourier transforms enjoy a great deal of structure, and sometimes exhibit more than square root cancellation on average.

These Fourier transforms naturally arise in analytic number theory, where explicit formulas (or upper bounds) lead to *sieve level of distribution* results for related arithmetic sequences. We describe some examples, and in the companion paper [TT] we develop a new method to do so, designed to exploit the particular structure of these Fourier transforms.

1 Introduction

Our results are best illustrated by example. Let $V = \mathrm{Sym}^3(2)$ be the space of binary cubic forms, together with an action of $G := \mathrm{GL}(2)$ given by

$$(g \circ f)(u, v) = \frac{1}{\det(g)} f((u, v)g). \tag{1}$$

The pair (G, V) is *prehomogeneous*: over an algebraically closed field k, the action of $G(k)$ on $V(k)$ has a Zariski open orbit – here the locus of points $v \in V$ with $\mathrm{Disc}(v) \neq 0$. Any binary cubic form is determined up to a scalar multiple by its roots in $\mathbb{P}^1(k)$, and prehomogeneity is equivalent to the fact that $\mathrm{PGL}(2)$ acts triply transitively on $\mathbb{P}^1$.

If k is any field with $\mathrm{char}(k) \neq 3$, then (as we will explain later) there is a bilinear form $[-,-] : V(k) \times V(k) \to k$ for which $[gv, g^{-T}v'] = [v, v']$ for all $v, v' \in V(k)$ and $g \in G(k)$. Here $g^{-T} \in G(k)$ is the inverse of the transpose of g. If further $k = \mathbb{F}_q$ is a *finite* field of characteristic p and $\Phi : V(\mathbb{F}_q) \to \mathbb{C}$ is any function, we define its Fourier transform $\widehat{\Phi} : V(\mathbb{F}_q) \to \mathbb{C}$ by

$$\widehat{\Phi}(v') = q^{-4} \sum_{v \in V(\mathbb{F}_q)} \Phi(v) \exp\left(2\pi\sqrt{-1} \cdot \frac{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}([v, v'])}{p}\right). \tag{2}$$

The following elementary result is the prototype for the kind of result we are after:

Proposition 1 *Let $w_q : V(\mathbb{F}_q) \to \mathbb{C}$ be the counting function of the number of roots of $v \in V(\mathbb{F}_q)$ in $\mathbb{P}^1(\mathbb{F}_q)$. Then, assuming that $\mathrm{char}(\mathbb{F}_q) \neq 3$, we have*

$$\widehat{w_q}(v) = \begin{cases} 1 + q^{-1} & v = 0, \\ q^{-1} & v \neq 0 \text{ and } v \text{ has a triple root in } \mathbb{P}^1(\mathbb{F}_q), \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

Work of Davenport and Heilbronn [DH71] connected this (G, V) to counting problems involving cubic fields and 3-torsion in the class groups of imaginary quadratic fields, and formulas of a similar shape to (3) appeared in subsequent works including the following:

1. The function $w_p(v)$ appears in Bhargava, Shankar, and Tsimerman's [BST13, (80)-(83)] proof of negative secondary terms in the Davenport-Heilbronn theorem. These authors proved and applied the weaker result [BST13, (80)-(83)] that $|w_p(v)| \ll p^{-1}$ for all $v \neq 0$.

2. Related functions, defined over $V(\mathbb{Z}/p^2\mathbb{Z})$, appear in the authors' [TT13a, TT13b] (independent) proof of these same secondary terms. Coarse bounds did not suffice for our methods, and we obtained exact formulas, but by rather laborious methods.

3. As we will shortly describe, Belabas and Fouvry proved [BF99, Corollaire 2] that there are infinitely many cubic fields whose discriminant is fundamental and divisible by at most 7 prime factors. They relied on similar exponential sum estimates which are proved in [BF99, Section 3].

Our aim was to develop a simple and generalizable method for proving exact formulas of this shape. In this paper, we will describe our method and compute the Fourier transforms of the characteristic functions of each of the $G(\mathbb{F}_q)$-orbits on each of the following prehomogeneous vector spaces:

- $V = \mathrm{Sym}^3(2)$, the space of binary cubic forms; $G = \mathrm{GL}_2$.
- $V = \mathrm{Sym}^2(2)$, the space of binary quadratic forms; $G = \mathrm{GL}_1 \times \mathrm{GL}_2$.
- $V = \mathrm{Sym}^2(3)$, the space of ternary quadratic forms; $G = \mathrm{GL}_1 \times \mathrm{GL}_3$.
- $V = 2 \otimes \mathrm{Sym}^2(2)$, the space of pairs of binary quadratic forms; $G = \mathrm{GL}_2 \times \mathrm{GL}_2$.
- $V = 2 \otimes \mathrm{Sym}^2(3)$, the space of pairs of ternary quadratic forms; $G = \mathrm{GL}_2 \times \mathrm{GL}_3$.

We thus obtain Fourier transform formulas for any G-invariant function Φ, i.e. one which satisfies $\Phi(gv) = \Phi(v)$ for all $g \in G(\mathbb{F}_q)$ and $v \in V(\mathbb{F}_q)$. We exclude finitely many field characteristics in each case, but otherwise our results are completely general. Our formulas for (G, V) above are respectively given in Theorems 9, 13, 16, 19 and 23. We have worked out some additional cases as well, but we leave the details for subsequent papers.

A sample result (in addition to the simpler Proposition 1) is as follows:

Theorem 2 *For a finite field $\mathbb{F}_q$ of characteristic not equal to 2, let $V(\mathbb{F}_q) := \mathbb{F}_q^2 \otimes \mathrm{Sym}^2(\mathbb{F}_q^3)$ be the space of pairs of ternary quadratic forms, and write $\Psi_q \colon V(\mathbb{F}_q) \to \{0, 1\}$ for the characteristic function of those $x \in V(\mathbb{F}_q)$ which are singular.*

Then, we have

$$\widehat{\Psi_q}(x) = \begin{cases} q^{-1} + 2q^{-2} - q^{-3} - 2q^{-4} - q^{-5} + 2q^{-6} + q^{-7} - q^{-8} & x \in \mathcal{O}_0, \\ q^{-3} - q^{-4} - 2q^{-5} + 2q^{-6} + q^{-7} - q^{-8} & x \in \mathcal{O}_{D1^2}, \\ 2q^{-4} - 5q^{-5} + 3q^{-6} + q^{-7} - q^{-8} & x \in \mathcal{O}_{D11}, \\ q^{-4} - 3q^{-5} + 2q^{-6} + q^{-7} - q^{-8} & x \in \mathcal{O}_{C\mathrm{s}}, \\ -q^{-5} + q^{-6} + q^{-7} - q^{-8} & x \in \mathcal{O}_{D2}, \mathcal{O}_{D\mathrm{ns}}, \mathcal{O}_{C\mathrm{ns}}, \mathcal{O}_{B11}, \mathcal{O}_{B2}, \\ -q^{-6} + 2q^{-7} - q^{-8} & x \in \mathcal{O}_{1^2 1^2}, \\ q^{-6} - q^{-8} & x \in \mathcal{O}_{2^2}, \\ q^{-7} - q^{-8} & x \in \mathcal{O}_{1^4}, \mathcal{O}_{1^3 1}, \mathcal{O}_{1^2 11}, \mathcal{O}_{1^2 2}, \\ -q^{-8} & x \in \mathcal{O}_{1111}, \mathcal{O}_{112}, \mathcal{O}_{22}, \mathcal{O}_{13}, \mathcal{O}_4. \end{cases} \tag{4}$$

The sets on the right are defined, and their cardinalities computed, in Proposition 21. (An element $x \in V(\mathbb{F}_q)$ is *singular* if it belongs to any of the orbits listed before the last line; see the introduction to Section 7 for a more intrinsic definition.)

We can see at once that the sizes of $\widehat{\Psi_q}(x)$ and the orbits $\mathcal{O}$ containing x are inversely correlated. For example those $\mathcal{O}$ with a D in their subscript consist of pairs (A, B) of doubled forms satisfying $\lambda A + \mu B = 0$ for some $\lambda, \mu \in \mathbb{F}_q$, and there are only $O(q^7)$ such pairs.

In particular, on average, we obtain better than square root cancellation:

Corollary 3 *We have the L_1-norm bound*

$$\sum_{x \in V(\mathbb{F}_q)} |\widehat{\Psi_q}(x)| \ll q^4.$$

We mention two other papers to which are results are related:

1. In an important paper [FK01], Fouvry and Katz obtained *upper bounds* for related exponential sums in a much more general context. As a special case, let Y be a (locally closed) subscheme of $\mathbb{A}^n_{\mathbb{Z}}$, and consider the exponential sum (2) with $V = \mathbb{A}_{\mathbb{Z}}$, $q = p$ prime, and Φ the characteristic function of $Y(\mathbb{F}_p)$. Fouvry and Katz produce a filtration of subschemes $\mathbb{A}^n_{\mathbb{Z}} \supseteq X_1 \supseteq \cdots \supseteq X_j \supseteq \cdots \supseteq X_n$ of increasing codimension, so that successively weaker upper bounds hold on each $(\mathbb{A}^n_{\mathbb{Z}} - X_j)(\mathbb{F}_p)$. Our Proposition 1 and Theorem 2 illustrate a similar structure, with substantially smaller values than the general bounds proved by Fouvry-Katz.

   As an interesting application ([FK01, Corollary 1.3]), they prove that there are infinitely many primes $p \equiv 1 \pmod 4$ for which $p + 4$ is squarefree and not the discriminant of a cubic field.

2. Denef and Gyoja [DG98] studied the sum (2), in the non-G-invariant case defined by $\Phi(v) = \chi(\mathrm{Disc}(v))$, where χ is a nontrivial Dirichlet character modulo p, so that Φ is relatively invariant and supported on the nonsingular orbits. In this setting, Denef and Gyoja proved that the Fourier transform of $\Phi(v)$ is equal to $\chi^{-1}(\mathrm{Disc}(v))$ times a factor independent of v. Their result has a shape reminiscent to that of Sato's [Sat90] fundamental theorem of prehomogeneous vector spaces (over $\mathbb{C}$).

   In some cases where χ is of small order their result excludes singular v, depending on the Sato-Bernstein polynomial of (G, V). When the quadratic character does define a G-invariant function we can recover these cases of their results. The case $\mathrm{Sym}^2(2)$ is particularly interesting, as Denef-Gyoja does not guarantee that $\widehat{\Phi}(v) = 0$ for singular v. Indeed, in Remark 14 we compute that this is not true (and in fact $2 \otimes \mathrm{Sym}^2(2)$ provides another such example).

Both of these papers are quite long and invoke the machinery of sheaf cohomology. Our methods are much simpler, as we demonstrate by now giving a complete proof of Proposition 1. Write $\langle n \rangle := \exp(2\pi i \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(n)/p)$, and write Φ_q for the characteristic function of the orbit (1^3): those nonzero elements of $V(\mathbb{F}_q)$ which have a triple root. By Fourier inversion, it suffices to compute the Fourier transform of the right side of (3), and thus to compute $\widehat{\Phi_q}$.

Using the facts that (1^3) is a single $\mathrm{GL}_2(\mathbb{F}_q)$-orbit, and that our bilinear form (defined by (11)) is $\mathrm{SL}_2(\mathbb{F}_q)$-invariant, we compute that

$$q^4 \widehat{\Phi_q}(y) = \frac{1}{q^2 - q} \sum_{g \in \mathrm{SL}_2(\mathbb{F}_q)} \sum_{t \in \mathbb{F}_q^\times} \langle [g \cdot (t,0,0,0), y] \rangle = \frac{1}{q^2 - q} \sum_{g \in \mathrm{SL}_2(\mathbb{F}_q)} \sum_{t \in \mathbb{F}_q^\times} \langle [(t,0,0,0), g^T y] \rangle$$

The inner sum is equal to $q - 1$ if $[1:0] \in \mathbb{P}^1(\mathbb{F}_q)$ is a root of $g^T y$, and -1 if it is not. For each root α of y, counted with multiplicity, $[1:0]$ will be a root of $g^T y$ for $\frac{|\mathrm{SL}_2(\mathbb{F}_q)|}{q+1} = q^2 - q$ elements $g \in \mathrm{SL}_2(\mathbb{F}_q)$, so that

$$q^4 \widehat{\Phi_q}(y) = \frac{1}{q^2 - q} \cdot (q^2 - q) \cdot \Big(q w_q(x) - (q+1) \Big).$$

Proposition 1 now follows easily.

Similar ideas can easily be applied to compute characteristic functions of other orbits. Generally, the idea is to consider subspaces $W \subseteq V$ defined by the vanishing of some of the coordinates (whose orthogonal complements are also so defined); as in the above example, the number of elements in $W \cap \mathcal{O}$ and $W^{\perp} \cap \mathcal{O}$ for various G-orbits $\mathcal{O}$ can be computed via elementary geometric considerations, and these counts determine the Fourier transforms. This is the basic principle which we will develop and apply to obtain all of our Fourier transform formulas.

Sieve Applications. Typically (and in the papers described above), exponential sum bounds lead to *level of distribution estimates*, which in turn lead to sieve applications. Typically a sieve involves the following:

- A set of objects being sieved. For example, with any of the (G, V) studied in this paper, one might consider the set of $G(\mathbb{Z})$-equivalence classes of $x \in V(\mathbb{Z})$ with $0 < |\operatorname{Disc}(x)| < X$.
- For each prime p, a notion of an object being 'bad at p'. Often this means simply that $p \mid \operatorname{Disc}(x)$. In works [BBP10, Bha05, Bha10, BST13, DH71, ST14, TT13b] on counting number fields, 'bad at p' is taken to mean that the ring R corresponding to x is nonmaximal at p, i.e. that $R \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is nonmaximal as a cubic ring over $\mathbb{Z}_p$.

A typical aim of sieve methods is to fix a large set of primes $\mathcal{P}$ and estimate the number of objects x which are not bad at any $p \in \mathcal{P}$. To carry this out one generally needs, for squarefree integers q, estimates for the number of x bad at each prime divisor of q. Loosely speaking, we say that our sieve has *level of distribution* $\alpha > 0$ if we can usefully bound the sum over $q < X^{\alpha}$ of the resulting error terms.

Positive levels of distribution for the nonmaximal definition of 'bad' have led to power saving error terms in certain counting functions for maximal orders, and thus also for the number fields containing them. Sieving for divisibility leads instead to estimates for almost-prime discriminants of number fields, and in our companion paper [TT] we obtain such an application:

Theorem 4 *There is an absolute constant $C > 0$ such that for each $X > 0$, there exist $\geq (C + o_X(1)) \frac{X}{\log X}$ quartic fields K whose discriminant is fundamental, bounded above by X, and has at most 8 prime factors.*

Our methods are closely related to those of Belabas and Fouvry [BF99], who proved [BF99, Corollaire 2] the same for *cubic* fields. (They formulated their result in terms of the 2-torsion in the class group of the quadratic resolvent; see (1.1) of their paper.) They pointed out that a weighted sieve would reduce their 7 to 4, and we will separately recover their result and further reduce this 4 to 3.

The basic heuristic of [TT] is that L_1-norm bounds such as Corollary 3, trivially obtained as consequences of the results of this paper, should lead to corresponding levels of distribution, and in [TT] we develop a geometric method which approaches this heuristic. Most of our work in [TT] is carried out in a general setting, adaptable to other representations (G, V) and to other sieve applications.

Zeta functions. Another motivation for our work is that the exponential sums being studied arise as coefficients of the functional equations of the associated Sato-Shintani zeta functions. These zeta functions can be used to prove sieve estimates (see e.g. [TT13a, TT13b]), and are also of intrinsic interest – especially when it can then be proved that the functional equations assume a particularly nice form. In Corollary 12 (of this paper) we present an application of this type.

Organization of the paper. We begin in Section 2 by giving the necessary background and assumptions. Our method applies to any $\mathbb{F}_q$-linear representation V of a finite group G, for which there exists a symmetric bilinear form which behaves nicely (see Assumption 1) with respect to the G-action. *There is no assumption that (G, V) is prehomogeneous*, although our method was designed to exploit features typical for prehomogeneous vector spaces.

We define (see (8)) a matrix M which carries all the necessary information concerning our Fourier transforms. We then prove Proposition 5, our main technical input, and explain how it reduces the problem

of determining M to the combinatorial task of counting $W \cap \mathcal{O}_i$ for all $G(\mathbb{F}_q)$-orbits $\mathcal{O}_i$ on V, for a large number of subspaces W.

In the next five sections we treat the prehomogeneous representations $\mathrm{Sym}^3(2)$, $\mathrm{Sym}^2(2)$, $\mathrm{Sym}^2(3)$, $2 \otimes \mathrm{Sym}^2(2)$, and $2 \otimes \mathrm{Sym}^2(3)$ in turn. We describe each representation, determine the $G(\mathbb{F}_q)$-orbits on $V(\mathbb{F}_q)$ (in each case excluding a 'bad' characteristic), carry out the combinatorial problem described above, and determine the matrix M. In the latter three cases embeddings of the previously considered representations will be relevant, so that these sections are not independent of the previous ones.

Finally, in Appendix A we explain why bilinear forms satisfying Assumption 1 exist in a general setting which includes each of the five (G, V) treated here. This seems to be 'well known', but the constructions are usually presented without proof in the related literature and we hope that a complete presentation will be useful to the reader.

Notation. For the convenience of the reader we describe some commonly used notation. We work with a finite field $\mathbb{F}_q$ of characteristic p, and V will always denote a finite dimensional $\mathbb{F}_q$-linear representation of a finite group G. The G-orbits on $\mathbb{F}_q$ will be labeled either $\mathcal{O}_1$, $\mathcal{O}_2$, etc. when we emphasize their ordering with respect to the matrix M, or using descriptive labels such as $\mathcal{O}_{D1^2}$ and $\mathcal{O}_{1111}$ when we emphasize their arithmetic properties. These labels will be introduced separately in each section.

If $g \in \mathrm{GL}_n$, then $g^{-T} \in \mathrm{GL}_n$ is the inverse of the transpose of g, and if $g = (g_1, \dots, g_r) \in \mathrm{GL}_{n_1} \times \cdots \times \mathrm{GL}_{n_r}$, we write $g^{-T} = (g_1^{-T}, \dots, g_r^{-T})$.

Some additional notation used in our orbit counting (e.g., $W_{[i,j]}$, $W_{[i,j]}^{\times}$, Y) is introduced and explained in Section 6.

2 The basic setup

In this section we formalize our method. We start by describing the common features of our representation over $\mathbb{F}_q$ which are necessary to make the method work; we then formulate several basic results which we apply in the course of our proofs. Specifically, our aim in this section is to establish Proposition 5, which is the primary tool for our exponential sum computations.

Let V be a (finite dimensional) vector space over $\mathbb{F}_q$. Let V^* be the dual space, i.e., the set of linear forms on V. For $x \in V$ and $y \in V^*$, we write $[x, y] := y(x) \in \mathbb{F}_q$ for the natural pairing between V and V^*. For $x \in V$ and $y \in V^*$, let

$$\langle x, y \rangle := \exp\left(2\pi\sqrt{-1} \cdot \frac{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}([x,y])}{p}\right) \in \mathbb{C}_1^{\times}.$$

Here $\mathbb{C}_1^{\times} = \{z \in \mathbb{C}^{\times} \mid |z| = 1\}$. Then $V \ni x \mapsto \langle x, y \rangle \in \mathbb{C}_1^{\times}$ is a group homomorphism. The fundamental underlying principle for the present (finite) Fourier analysis is that V^* is canonically identified with the group of additive characters on V, via $V^* \ni y \mapsto \langle \cdot, y \rangle \in \mathrm{Hom}(V, \mathbb{C}_1^{\times})$. Let $\mathcal{F}_V$ and $\mathcal{F}_{V^*}$ be the space of $\mathbb{C}$-valued functions on V and V^*, respectively. There are special $\mathbb{C}$-linear isomorphisms between them; the Fourier transforms

$$\mathcal{F}_V \ni \phi \longmapsto \widehat{\phi} \in \mathcal{F}_{V^*}; \qquad \widehat{\phi}(y) = |V|^{-1} \sum_{x \in V} \phi(x) \langle x, y \rangle$$

and

$$\mathcal{F}_{V^*} \ni \psi \longmapsto \widehat{\psi} \in \mathcal{F}_V; \qquad \widehat{\psi}(x) = |V|^{-1} \sum_{y \in V^*} \psi(y) \langle x, y \rangle.$$

By the orthogonality relation we have $\widehat{\widehat{\phi}}(x) = |V|^{-1}\phi(-x)$, which is the Fourier inversion formula in this case. For a subspace W of V, let $W^{\perp} \subset V^*$ be the subspace of its annihilators in the dual space. Let ϕ_W and $\psi_{W^{\perp}}$ respectively be their indicator functions. It is easy to see that

$$\widehat{\phi_W} = \frac{|W|}{|V|} \cdot \psi_{W^{\perp}}. \tag{5}$$

If a finite group G acts on V, then the action is naturally inherited by $\mathcal{F}_V$: for $g \in G$ and $\phi \in \mathcal{F}_V$, defining $g\phi \in \mathcal{F}_V$ by $(g\phi)(x) = \phi(g^{-1}x)$ defines a $\mathbb{C}$-linear representation of G. Let $\mathcal{F}_V^G \subset \mathcal{F}_V$ be the subspace of G-invariant functions on V. If $\mathcal{O}_1, \dots, \mathcal{O}_r$ are all the distinct G-orbits in V, then their respective indicator functions $e_1, \dots, e_r \in \mathcal{F}_V^G$ form a basis of $\mathcal{F}_V^G$. As is common, the averaging operator

$$\mathrm{av}\colon \mathcal{F}_V \longrightarrow \mathcal{F}_V^G; \qquad \phi \longmapsto \mathrm{av}(\phi) := |G|^{-1} \sum_{g \in G} g\phi$$

is useful for our analysis. If ϕ_x is the indicator function of a point $x \in V$, then $\mathrm{av}(\phi_x) = e_i/|\mathcal{O}_i|$, where $x \in \mathcal{O}_i$. Hence if ϕ_X is the indicator function of a subset $X \subset V$, then since $\phi_X = \sum_{x \in X} \phi_x$ we have

$$\mathrm{av}(\phi_X) = \sum_{1 \le i \le r} \frac{|\mathcal{O}_i \cap X|}{|\mathcal{O}_i|} \cdot e_i. \tag{6}$$

We now assume that the action of G on V is $\mathbb{F}_q$-linear. Given any automorphism $G \ni g \mapsto g^\iota \in G$ of order 1 or 2 (as will be discussed shortly), we consider the action of G on V^* defined by $[x, gy] = [(g^\iota)^{-1}x, y]$. It is easy to see that this action is well-defined and $\mathbb{F}_q$-linear, and that the action thus defined on V^{**} is equivariant with respect to the canonical isomorphism $V \to V^{**}$. We thus have a $\mathbb{C}$-linear representation of G on $\mathcal{F}_{V^*}$, the subspace of G-invariant functions $\mathcal{F}_{V^*}^G$, and the averaging operator $\mathrm{av}\colon \mathcal{F}_{V^*} \to \mathcal{F}_{V^*}^G$ as well.

For the Fourier transform, we immediately see that

$$\widehat{g\phi} = g^\iota \widehat{\phi}, \qquad g \in G, \phi \in \mathcal{F}_V. \tag{7}$$

In particular, if ϕ is G-invariant, then so is $\widehat{\phi}$. Thus we have a $\mathbb{C}$-linear isomorphism

$$\mathcal{F}_V^G \longrightarrow \mathcal{F}_{V^*}^G; \qquad \phi \longmapsto \widehat{\phi}.$$

Our goal is to understand this Fourier transform between $\mathcal{F}_V^G$ and $\mathcal{F}_{V^*}^G$ explicitly. By looking at their dimensions, we see that V and V^* have the same number of G-orbits. Let $\mathcal{O}_1^*, \dots, \mathcal{O}_r^*$ be the all G-orbits in V^*, and $e_i^* \in \mathcal{F}_{V^*}^G$ be the indicator function of $\mathcal{O}_i^*$. Let $M \in \mathrm{M}_r(\mathbb{C})$ be the representation matrix of the Fourier transformation with respect to the basis $e_1, \dots, e_r \in \mathcal{F}_V^G$ and $e_1^*, \dots, e_r^* \in \mathcal{F}_{V^*}^G$. By definition,

$$M = [a_{ij}] \quad \text{where} \quad \widehat{e_j} = \sum_i a_{ij} e_i^*, \tag{8}$$

and we wish to determine this matrix M.

By (7), we have $\widehat{\mathrm{av}(\phi)} = \mathrm{av}(\widehat{\phi})$. Let W be any subspace of V and put $\phi = \phi_W$. Then by (5) and (6), we have the following simple formula, which is particularly useful:

$$\sum_{1 \le i \le r} \frac{|\mathcal{O}_i \cap W|}{|\mathcal{O}_i|} \cdot \widehat{e_i} = \frac{|W|}{|V|} \sum_{1 \le i \le r} \frac{|\mathcal{O}_i^* \cap W^\perp|}{|\mathcal{O}_i^*|} \cdot e_i^*. \tag{9}$$

We now consider the following assumption on the representation (G, V), which is satisfied by all of the cases we will study in later sections. (We will be required to assume that the characteristic of $\mathbb{F}_q$ is not one of finitely many 'bad' primes, depending on the particular (G, V).)

Assumption 1 *There is an involution $G \ni g \mapsto g^\iota \in G$ and a non-degenerate symmetric bilinear form $V \times V \ni (x, y) \to b(x, y) \in \mathbb{F}_q$, such that $b(gx, g^\iota y) = b(x, y)$.*

By non-degeneracy the map $\theta\colon V \ni y \mapsto b(\cdot, y) \in V^*$ is an $\mathbb{F}_q$-linear isomorphism. We consider the representation of V^* with respect to the involution ι. Then θ preserves the action of G. We identify V^* with V via θ. Hence the pairing on V and $V^* = V$ is given by $[x, y] = b(x, y)$, and this satisfies $[gx, g^\iota y] = [x, y]$. The Fourier transform is now an automorphism on $\mathcal{F}_V$ or on $\mathcal{F}_V^G$. We put $\mathcal{O}_i^* = \mathcal{O}_i$ and thus $e_i^* = e_i$. We summarize our argument into the following.

Proposition 5 *Let V be a finite dimensional representation of a group G over $\mathbb{F}_q$, satisfying Assumption 1. Then for any subspace W of V, we have*

$$\sum_{1\le i\le r} \frac{|\mathcal{O}_i \cap W|}{|\mathcal{O}_i|} \cdot \widehat{e_i} = \frac{|W|}{|V|} \sum_{1\le i\le r} \frac{|\mathcal{O}_i \cap W^\perp|}{|\mathcal{O}_i|} \cdot e_i. \tag{10}$$

We can now precisely explain our strategy for determining M: given (G, V), we compute the vectors $(|\mathcal{O}_i \cap W|)_i$ and $(|\mathcal{O}_i \cap W^\perp|)_i$ for many subspaces W. Eventually these vectors will span $\mathbb{R}^r$, after which basic linear algebra finishes off the computation.

We have not attempted to prove in general that the vectors $(|\mathcal{O}_i \cap W|)_i$ span $\mathbb{R}^r$, but in practice this does not seem to be an issue.

Before ending this section, we prove an additional lemma on the matrix M. This lemma is logically not necessary, but we find it quite convenient to check our computation.

Lemma 6 *1. We have $|\mathcal{O}_i|a_{ij} = |\mathcal{O}_j|a_{ji}$. Namely, if we put $S = \mathrm{diag}(|\mathcal{O}_i|)$, then SM is symmetric.*

2. Suppose that x and $-x$ lie in the same G-orbit for each $x \in V$. Then $M^2 = |V|^{-1}E_r$, where E_r is the identity matrix.

Proof: For (1), first note that $\widehat{\phi_x}(y) = |V|^{-1}\langle x, y\rangle = \widehat{\phi_y}(x)$ for all $x, y \in V$. Hence we also have

$$\widehat{\mathrm{av}(\phi_x)}(y) = \frac{1}{|G|}\sum_{g\in G} \widehat{g\phi_x}(y) = \frac{1}{|G|}\sum_{g\in G} \widehat{\phi_{gx}}(y) = \frac{1}{|G|}\sum_{g\in G} \widehat{\phi_y}(gx) = \mathrm{av}(\widehat{\phi_y})(x) = \widehat{\mathrm{av}(\phi_y)}(x).$$

If $x \in \mathcal{O}_j$ and $y \in \mathcal{O}_i$, then since $\mathrm{av}(\phi_x) = |\mathcal{O}_j|^{-1}e_j$ we have

$$\widehat{\mathrm{av}(\phi_x)}(y) = |\mathcal{O}_j|^{-1}\widehat{e_j}(y) = |\mathcal{O}_j|^{-1}\sum_k a_{kj}e_k(y) = |\mathcal{O}_j|^{-1}a_{ij},$$

and similarly $\widehat{\mathrm{av}(\phi_y)}(x) = |\mathcal{O}_i|^{-1}a_{ji}$. For (2), by assumption $\phi(-x) = \phi(x)$ if $\phi \in \mathcal{F}_V^G$. Thus $M^2 = |V|^{-1}E_r$ is simply the Fourier inversion. □

In successive sections, we obtain M in Theorems 9, 13, 16, 19 and 23 for each of the cases. We double checked our computation by confirming that M's in the theorems all satisfy Lemma 6.

We used PARI/GP [PG14] to carry out the necessary linear algebra. In each case we have embedded our source code, together with the matrix M in machine-readable format, as a comment immediately following the theorem statement in the LaTeX source for this file, which may be freely downloaded from the arXiv. The source code is also available on the second author's website (link).

3 $\mathrm{Sym}^3(2)$

We first handle the space of binary cubic forms, as we described in the introduction. In this case the matrix M was determined previously by Mori [Mor10], and so here we give a second proof.

Let $V = \mathrm{Sym}^3(\mathbb{F}_q^2)$ be the space of binary cubic forms in variables u and v, let $G = \mathrm{GL}_2(\mathbb{F}_q)$, and consider the usual 'twisted action' of G on V, given by

$$(g \circ x)(u, v) = (\det g)^{-1}x((u, v)g).$$

We write an element of V as $x = x(u, v) = au^3 + bu^2v + cuv^2 + dv^3 = (a, b, c, d)$. Let $\mathrm{Disc}(x) = b^2c^2 + 18abcd - 4ac^3 - 4b^3d - 27a^2d^2$ be the discriminant of x. Then $\mathrm{Disc}(gx) = (\det g)^2\,\mathrm{Disc}(x)$. We say that x is singular if $\mathrm{Disc}(x) = 0$, or equivalently if x has a multiple root in $\mathbb{P}^1$.

The following orbit description is well known. For a proof, see, e.g., [Wri85, Section 2] or [TT13a, Section 5.1].

Proposition 7 *The action of G on V consists of six orbits, of which three are singular. We label them with the usual symbols*

$$(0), (1^3), (1^2 1), (111), (21), (3),$$

where here $(0) = \{0\}$, and for the remaining orbits the symbol indicates the degrees and multiplicities of the irreducible factors of any representative form x. The following table lists a representative, the number of zeros in $\mathbb{P}^1(\mathbb{F}_q)$ of any element in the orbit, and the size of the orbit:

Orbit name	Representative	Zeros	Orbit size
$\mathcal{O}_{(0)} = \mathcal{O}_1$	0	$q+1$	1
$\mathcal{O}_{(1^3)} = \mathcal{O}_2$	v^3	1	q^2-1
$\mathcal{O}_{(1^2 1)} = \mathcal{O}_3$	uv^2	2	$q(q^2-1)$
$\mathcal{O}_{(111)} = \mathcal{O}_4$	$uv(u-v)$	3	$\frac{1}{6}(q^2-1)(q^2-q)$
$\mathcal{O}_{(21)} = \mathcal{O}_5$	$v(u^2+a_2uv+b_2v^2)$	1	$\frac{1}{2}(q^2-1)(q^2-q)$
$\mathcal{O}_{(3)} = \mathcal{O}_6$	$u^3+a_3u^2v+b_3uv^2+c_3v^3$	0	$\frac{1}{3}(q^2-1)(q^2-q)$

Here $u^2+a_2u+b_2$ and $u^3+a_3u^2+b_3u+c_3 \in \mathbb{F}_q[u]$ are respectively any irreducible quadratic and cubic polynomials.

We now assume that $p \neq 3$. We define a symmetric bilinear form[1] on V by

$$[x, x'] := aa' + bb'/3 + cc'/3 + dd'. \tag{11}$$

Then we have $[gx, g^{-T}x'] = [x, x']$ and so (G, V) satisfies Assumption 1.

The following table describes the counts of elements in each orbit for a variety of subspaces W_i.

Subspace	$\mathcal{O}_{(0)}$	$\mathcal{O}_{(1^3)}$	$\mathcal{O}_{(1^2 1)}$	$\mathcal{O}_{(111)}$	$\mathcal{O}_{(21)}$	$\mathcal{O}_{(3)}$
$W_0 = \{(0,0,0,0)\}$	1					
$W_1 = \{(0,0,0,*)\}$	1	$q-1$				
$W_2^\perp = W_2 = \{(0,0,*,*)\}$	1	$q-1$	$q(q-1)$			
$W_3 = \{(0,*,*,0)\}$	1		$2(q-1)$	$(q-1)^2$		
$W_3^\perp = \{(*,0,0,*)\}$	–	–	–	–	–	–
$(q \equiv 1 \pmod 3)$	1	$2(q-1)$		$\frac{1}{3}(q-1)^2$		$\frac{2}{3}(q-1)^2$
$(q \equiv 2 \pmod 3)$	1	$2(q-1)$			$(q-1)^2$	
$W_1^\perp = \{(0,*,*,*)\}$	1	$\lvert\mathcal{O}_{(1^3)}\rvert/(q+1)$	$2\lvert\mathcal{O}_{(1^2 1)}\rvert/(q+1)$	$3\lvert\mathcal{O}_{(111)}\rvert/(q+1)$	$\lvert\mathcal{O}_{(21)}\rvert/(q+1)$	
$V = \{(*,*,*,*)\}$	1	$\lvert\mathcal{O}_{(1^2)}\rvert$	$\lvert\mathcal{O}_{(1^2 1)}\rvert$	$\lvert\mathcal{O}_{(111)}\rvert$	$\lvert\mathcal{O}_{(21)}\rvert$	$\lvert\mathcal{O}_{(3)}\rvert$

Here, the notation $\{(0,0,*,*)\}$ (for example) means the subspace of binary cubic forms whose first two coefficients are zero and whose latter two is arbitrary.

Remark 8 *Note that (for example) we don't literally have $W_2^\perp = W_2$; rather, these two spaces $W_2 = \{(0,0,*,*)\}$ and $W_2^\perp = \{(*,*,0,0)\}$ are $\mathrm{GL}_2(\mathbb{F}_q)$-equivalent and so the intersections with each $\mathcal{O}_i$ have the same size. Similarly the subspace listed for $W_1^\perp$ is in fact a $\mathrm{GL}_2(\mathbb{F}_q)$-transformation of $W_1^\perp = \{(*,*,*,0)\}$, and in general we will (if the transformations are obvious) apply such transformations in our listings of subspaces without further comment.*

The counts above are for the most part trivial to verify, and so we only describe a few cases explicitly. The subspace $W_1^\perp$ consists of those forms having $[1:0]$ as a zero; since $\mathrm{GL}_2(\mathbb{F}_q)$ acts transitively on $\mathbb{P}^1(\mathbb{F}_q)$, we have that $\frac{|W_1^\perp \cap \mathcal{O}_i|}{|\mathcal{O}_i|} \cdot (q+1)$ is equal to the number of zeros of any $x \in \mathcal{O}_i$ in $\mathbb{P}^1(\mathbb{F}_q)$.

For $W_3^\perp$, let $x = (a,0,0,d) = au^3 + dv^3 \in W_3^\perp$ with $ad \neq 0$. Then x is non-singular, with a zero in $\mathbb{P}^1(\mathbb{F}_q)$ if and only if $\frac{d}{a} \in (\mathbb{F}_q^\times)^3$. If $q \equiv 2 \mod 3$, then $(\mathbb{F}_q^\times)^3 = \mathbb{F}_q^\times$, so that every x has a root in $\mathbb{F}_q$. Moreover,

[1] In the literature the alternating form $[x, x']^\sim = da' - cb'/3 + bc'/3 - ad'$ is sometimes introduced and used instead of our $[x, x']$; see for example Shintani [Shi72]. Since $[\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right] x, x'] = [x, x']^\sim$, these two bilinear forms are essentially the same. Here we choose this $[x, x']$ because it is more similar to the forms associated to other representations in later sections.

the quotient of any two roots of x is a third root of unity, hence not in $\mathbb{F}_q$, so that we have $x \in \mathcal{O}_{(21)}$ for all $(q-1)^2$ forms x. If $p \equiv 1 \mod 3$, then $(\mathbb{F}_q^\times)^3$ is the index three subgroup of $\mathbb{F}_q^\times$, there are $\frac{2}{3}(q-1)^2$ irreducible $x \in \mathcal{O}_{(3)}$, and the remaining $\frac{1}{3}(q-1)^2$ forms x all factor completely and are in $\mathcal{O}_{(111)}$.

We now use Proposition 5 to determine M. We verify by inspection that the vectors $(|W \cap \mathcal{O}_i|)_i$ for $W \in \{W_0, W_1, W_2, W_3, W_1^\perp, V\}$ are linearly independent, and that this set together with $W_3^\perp$ is closed under taking duals. The linear algebra is not difficult to carry out by hand, but we used PARI/GP [PG14] for this purpose. We therefore obtain the matrix M, with a different proof than that previously given by Mori.

Theorem 9 (Mori [Mor10]) *Suppose $q \neq 3$. We have*

$$M = \frac{1}{q^4}\begin{bmatrix} 1 & q^2-1 & q^3-q & (q^2-1)(q^2-q)/6 & (q^2-1)(q^2-q)/2 & (q^2-1)(q^2-q)/3 \\ 1 & -1 & q^2-q & q(q-1)(2q-1)/6 & -q(q-1)/2 & -q(q^2-1)/3 \\ 1 & q-1 & q^2-2q & -3q(q-1)/6 & -q(q-1)/2 & 0 \\ 1 & 2q-1 & -3q & q(5\pm q)/6 & -q(-1\pm q)/2 & q(-1\pm q)/3 \\ 1 & -1 & -q & -q(-1\pm q)/6 & q(1\pm q)/2 & -q(-1\pm q)/3 \\ 1 & -q-1 & 0 & q(-1\pm q)/6 & -q(-1\pm q)/2 & q(2\pm q)/3 \end{bmatrix},$$

where the signs $\pm$ appearing in right-lower 3-by-3 entries are according as $q \equiv \pm 1 \pmod 3$.

We derive two formulas as corollaries to Theorem 9. The first one below was previously given and used in [TT13a] to establish an analogue of the Ohno-Nakagawa formula for the 'divisible zeta function'. In a companion paper [TT], we use this to study almost-prime cubic field discriminants.

Corollary 10 *For a finite field $\mathbb{F}_q$ of characteristic not equal to 3, write $\Psi_q(x)$ for the characteristic function of singular binary cubic forms over $\mathbb{F}_q$. We have*

$$\widehat{\Psi_q}(x) = \begin{cases} q^{-1}+q^{-2}-q^{-3} & x = 0, \\ q^{-2}-q^{-3} & x \neq 0, \mathrm{Disc}(x) = 0 \\ -q^{-3} & \mathrm{Disc}(x) \neq 0, \end{cases} \tag{12}$$

This is immediate from Theorem 9, because $\Psi_q = e_1 + e_2 + e_3$ and thus $\widehat{\Psi_q} = \widehat{e_1} + \widehat{e_2} + \widehat{e_3}$. Another consequence of Theorem 9 is an explicit formula of the Fourier transform of $\psi(\mathrm{Disc}(x))$, where ψ is the quadratic character on $\mathbb{F}_q$. This result is contained within Denef and Gyoja's main theorem [DG98] and in this case we obtain a simpler proof.

Corollary 11 *Assume $p \neq 2$, and let $\psi\colon \mathbb{F}_q^\times \to \{\pm 1\}$ be the quadratic character. We use the usual convention $\psi(0) = 0$. We have*

$$\frac{1}{q^4}\sum_{x \in V} \psi\left(\mathrm{Disc}(x)\right) \exp\left(2\pi\sqrt{-1} \cdot \frac{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}([x,y])}{p}\right) = \frac{1}{q^2} \cdot \psi\left(\mathrm{Disc}^*(y)\right), \tag{13}$$

where $\mathrm{Disc}^*(y) = -\mathrm{Disc}(y)/27$ is the normalized invariant for the dual space V^*.

Proof: If $x \in V$ is non-singular, then $\psi\left(\mathrm{Disc}(x)\right) = 1$ or -1 according as $x \in \mathcal{O}_{(111)} \cup \mathcal{O}_{(3)}$ or $x \in \mathcal{O}_{(2)}$. Hence $\psi\left(\mathrm{Disc}(\cdot)\right) = e_4 - e_5 + e_6$ and the left hand side of (13) is $(\widehat{e_4} - \widehat{e_5} + \widehat{e_6})(y)$. By Theorem 9, we have

$$\widehat{e_4} - \widehat{e_5} + \widehat{e_6} = \pm q^{-2}\left(e_4 - e_5 + e_6\right) = \pm q^{-2} \cdot \psi\left(\mathrm{Disc}(\cdot)\right)$$

where the sign is according as $q \equiv \pm 1 \pmod 3$. Since $\psi(-27) = \psi(-3) = \pm 1$, where again the sign is according as $q \equiv \pm 1 \pmod 3$, we have the result. $\square$

We illustrate an application of this formula to the functional equation of the Shintani zeta function. Let $n \neq 1$ be a square-free integer coprime to 6, and ψ be the unique primitive quadratic Dirichlet charter

modulo n. By the Chinese remainder theorem, the similar formula for (13) is true for ψ. For each sign, we define

$$\xi_{\pm}(s,\psi) := \sum_{\substack{x \in \mathrm{GL}_2(\mathbb{Z})\backslash \mathrm{Sym}^3(\mathbb{Z}^2) \\ \pm \mathrm{Disc}(x) > 0}} \frac{\psi(\mathrm{Disc}(x))}{|\mathrm{Stab}(x)|} |\mathrm{Disc}(x)|^{-s}.$$

This is a quadratic twist of the zeta function introduced and studied by Shintani [Shi72]. Note that we put $\psi(\mathrm{Disc}(x)) = 0$ if $\mathrm{Disc}(x)$ is not coprime to n. It is shown in [TT13a] that these Dirichlet series $\xi_{\pm}(s,\psi)$ enjoy analytic continuation as entire functions to the whole complex plane and satisfy functional equations. Corollary 11 may then be applied to describe this functional equation explicitly. Write

$$\xi_{\mathrm{add}}(s,\psi) := 3^{1/2}\xi_+(s,\psi) + \xi_-(s,\psi),$$
$$\xi_{\mathrm{sub}}(s,\psi) := 3^{1/2}\xi_+(s,\psi) - \xi_-(s,\psi),$$

and

$$\Lambda_{\mathrm{add}}(s,\psi) := \left(\frac{432n^4}{\pi^4}\right)^{s/2} \Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s}{2}+\frac{1}{2}\right)\Gamma\left(\frac{s}{2}-\frac{1}{12}\right)\Gamma\left(\frac{s}{2}+\frac{1}{12}\right)\xi_{\mathrm{add}}(s,\psi),$$
$$\Lambda_{\mathrm{sub}}(s,\psi) := \left(\frac{432n^4}{\pi^4}\right)^{s/2} \Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s}{2}+\frac{1}{2}\right)\Gamma\left(\frac{s}{2}+\frac{5}{12}\right)\Gamma\left(\frac{s}{2}+\frac{7}{12}\right)\xi_{\mathrm{sub}}(s,\psi).$$

Then similarly to [Ohn97, TT13a], Corollary 11 combined with Datskovsky-Wright's diagonalization [DW86] and Nakagawa's dual identity [Nak98] enables us to write the functional equation of $\xi_{\pm}(s,\psi)$ in a self dual form:

Corollary 12 *We have*

$$\Lambda_{\mathrm{add}}(s,\psi) = \Lambda_{\mathrm{add}}(1-s,\psi), \qquad \Lambda_{\mathrm{sub}}(s,\psi) = \Lambda_{\mathrm{sub}}(1-s,\psi).$$

4 $\mathrm{Sym}^2(2)$

We now turn our attention to the easier case of binary quadratic forms. Let $V = \mathrm{Sym}^2(\mathbb{F}_q^2)$ be the space of binary quadratic forms in variables u and v, together with the action of $G = \mathrm{GL}_1(\mathbb{F}_q) \times \mathrm{GL}_2(\mathbb{F}_q)$ given by

$$(g_1, g_2) \cdot x(u,v) = g_1 x((u,v)g_2). \tag{14}$$

We write an element of V as $x = x(u,v) = au^2 + buv + cv^2 = (a,b,c)$. We let $\mathrm{Disc}(x) = b^2 - 4ac$, and say x is singular if $\mathrm{Disc}(x) = 0$. As usual, we identify x with the two-by-two symmetric matrix $A = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$, with $\mathrm{Disc}(x) = -4 \det A$. Then the action of the $\mathrm{GL}_2(\mathbb{F}_q)$ part is given by $(g_2, A) \mapsto g_2 A g_2^T$, while the $\mathrm{GL}_1(\mathbb{F}_q)$ part acts by scalar mulitplication.

Let $p \neq 2$. V consists of four G orbits, which we enumerate as follows. (Rank is the rank as a symmetric matrix of any element in the orbit.)

Symbol	Orbit name	Representative	Rank	Orbit size
(0)	$\mathcal{O}_{(0)} = \mathcal{O}_1$	0	0	1
(1^2)	$\mathcal{O}_{(1^2)} = \mathcal{O}_2$	v^2	1	q^2-1
(11)	$\mathcal{O}_{(11)} = \mathcal{O}_3$	uv	2	$\frac{1}{2}q(q^2-1)$
(2)	$\mathcal{O}_{(2)} = \mathcal{O}_4$	$u^2 - lv^2$	2	$\frac{1}{2}q(q-1)^2$

Here $l \in \mathbb{F}_q^{\times}$ denotes an arbitrary non-square element. The proof is elementary and we omit the details. Note that the factor of GL_1 is included to ensure that the G-orbits of v^2 and lv^2 coincide.

We define a symmetric bilinear form on V by

$$[x, x'] := aa' + bb'/2 + cc'. \tag{15}$$

Then we have $[gx, g^{-T}x'] = [x, x']$ and so (G, V) satisfies Assumption 1.

The counts of the $W \cap \mathcal{O}_i$ for the following subspaces W are immediately verified:

Subspace	$\mathcal{O}_{(0)}$	$\mathcal{O}_{(1^2)}$	$\mathcal{O}_{(11)}$	$\mathcal{O}_{(2)}$
$\{(0,0,0)\}$	1			
$\{(0,0,*)\}$	1	$q-1$		
$\{(0,*,0)\}$	1		$q-1$	
$\{(0,*,*)\}$	1	$q-1$	q^2-q	
$\{(*,0,*)\}$	1	$2q-2$	$\frac{(q-1)^2}{2}$	$\frac{(q-1)^2}{2}$
$\{(*,*,*)\}$	1	$\lvert\mathcal{O}_{(1^2)}\rvert$	$\lvert\mathcal{O}_{(11)}\rvert$	$\lvert\mathcal{O}_{(2)}\rvert$

Therefore by Proposition 5, we immediately obtain the following. (We in fact do not require the above counts for $\{(0,*,0)\}$ and $\{(*,0,*)\}$.)

Theorem 13 *Suppose $p \neq 2$. We have*

$$M = \frac{1}{q^3} \cdot \begin{bmatrix} 1 & q^2-1 & \frac{1}{2}q(q^2-1) & \frac{1}{2}q(q-1)^2 \\ 1 & -1 & \frac{1}{2}(q^2-q) & -\frac{1}{2}(q^2-q) \\ 1 & q-1 & -q & 0 \\ 1 & -(q+1) & 0 & q \end{bmatrix}.$$

We can now provide an example where a complete analogue of Corollary 11 is not guaranteed by Denef-Gyoja, and indeed is not true:

Remark 14 *Let ψ be the quadratic character on $\mathbb{F}_q^\times$. Then since $\psi(\mathrm{Disc}(\cdot)) = e_3 - e_4$, its Fourier transform is*

$$\widehat{e_3} - \widehat{e_4} = (q^{-1} - q^{-2})(e_1 + e_2) - q^{-2}(e_3 + e_4).$$

This function does not vanish on the singular set.

5 $\mathrm{Sym}^2(3)$

Now, let $V = \mathrm{Sym}^2(\mathbb{F}_q^3)$ be the space of ternary quadratic forms in variables u, v and w, together with the action of $G = \mathrm{GL}_1(\mathbb{F}_q) \times \mathrm{GL}_3(\mathbb{F}_q)$ given by

$$(g_1, g_3) \cdot x(u, v, w) = g_1 x((u, v, w)g_3).$$

We write an element of V as

$$x = x(u, v, w) = au^2 + buv + cuw + dv^2 + evw + fw^2 = (a, b, c, d, e, f).$$

We again assume $p \neq 2$. As in the previous section, we identify V as the space of symmetric matrices of size three. Hence x is identified with $A = \begin{bmatrix} a & b/2 & c/2 \\ b/2 & d & e/2 \\ c/2 & e/2 & f \end{bmatrix}$. We define $\mathrm{Disc}(x) = -4\det(A)$, and say x is singular if $\mathrm{Disc}(x) = 0$.

Proposition 15 *Assume $p \neq 2$, and let $l \in \mathbb{F}_q^\times$ denote an arbitrary non-square element. The action of G on V has five orbits, of which four are singular. For each orbit, the table below lists orbital representatives,*

the number of zeros in $\mathbb{P}^2(\mathbb{F}_q)$ and the rank as a symmetric matrix of any element in the orbit, and the size of the orbit.

Symbol	Orbit name	Representative	Zeros	Rank	Orbit size
(0)	$\mathcal{O}_{(0)} = \mathcal{O}_1$	0	q^2+q+1	0	1
(1^2)	$\mathcal{O}_{(1^2)} = \mathcal{O}_2$	u^2	$q+1$	1	q^3-1
(11)	$\mathcal{O}_{(11)} = \mathcal{O}_3$	uv	$2q+1$	2	$q(q^3-1)\frac{q+1}{2}$
(2)	$\mathcal{O}_{(2)} = \mathcal{O}_4$	$u^2 - lv^2$	1	2	$q(q^3-1)\frac{q-1}{2}$
ns	$\mathcal{O}_{\text{ns}} = \mathcal{O}_5$	$u^2 - vw$	$q+1$	3	$(q^5-q^2)(q-1)$

Here $l \in \mathbb{F}_q^\times$ is a non-square element.

Proof: This is well known (see e.g. [Elk13]), and for the sake of completeness we include a proof.

To prove that there are five orbits, start with an arbitrary $x \in V$ and complete the square to get rid of any off-diagonal terms. If x is not G-equivalent to one of the first four representatives it must be of the form $\lambda_1 u^2 - \lambda_2 v^2 - \lambda_3 w^2$ with $\lambda_1\lambda_2\lambda_3 \neq 0$, and indeed with $\lambda_1 = 1$ after multiplying by $\lambda_1^{-1} \in \mathrm{GL}_1(\mathbb{F}_q)$. Now, if λ_2 or λ_3 is a square element, then this form is visibly equivalent to $u^2 - vw$. Otherwise, by a suitable $\mathrm{GL}_3(\mathbb{F}_q)$ translation we may assume that $\lambda_2 = \lambda_3$. Moreover, for each $\alpha \in \mathbb{F}_q^\times$ we have that $y^2 + z^2$ is equivalent to $(v+\alpha w)^2 + (w - \alpha v)^2 = (1+\alpha^2)(v^2+w^2)$; as $1+\alpha^2$ cannot be a square element for every α, we see that $\lambda_2(v^2+w^2)$ is equivalent to v^2+w^2.

We moreover see that the orbits are all distinct, for example from the counts of $\mathbb{F}_q$-rational zeros, together with the observation that u^2 and $u^2 - vw$ are clearly not G-equivalent.

The first two orbit sizes are very easy to compute; the next two are most easily computed by observing that the stabilizer size is $p^3 - p^2$ times the analogous stabilizer size in $\mathrm{Sym}^2(2)$, as any $g_3 \in \mathrm{GL}_3$ in the stabilizer may send w to any $a_1u + a_2v + a_3w$ with $a_3 \neq 0$. The final orbit size is most easily computed by subtracting the first four orbit sizes from q^6. □

We define a symmetric bilinear form on V by

$$[x, x'] := aa' + bb'/2 + cc'/2 + dd' + ee'/2 + ff'. \tag{16}$$

Then we have $[gx, g^{-T}x'] = [x, x']$ and so (G, V) satisfies Assumption 1.

We come now to the computations of $|W \cap \mathcal{O}_i|$ for suitable W. In the table below, we write $\times\alpha$ as a shorthand for $\alpha|\mathcal{O}_i|$.

Subspace	$\mathcal{O}_{(0)}$	$\mathcal{O}_{(1^2)}$	$\mathcal{O}_{(11)}$	$\mathcal{O}_{(2)}$	$\mathcal{O}_{\text{ns}}$
$W_0 = \{(0,0,0,0,0,0)\}$	1				
$W_1 = \{(0,0,0,0,0,*)\}$	1	$q-1$			
$W_2 = \{(0,0,0,*,0,*)\}$	1	$2q-2$	$\frac{(q-1)^2}{2}$	$\frac{(q-1)^2}{2}$	
$W_3 = \{(0,0,*,*,*,*)\}$	1	q^2-1	$\frac{1}{2}q(3q^2-2q-1)$	$\frac{1}{2}q(q-1)^2$	$q^2(q-1)^2$
$W_1^\perp = \{(0,*,*,*,*,*)\}$	1	$\times\frac{q+1}{q^2+q+1}$	$\times\frac{2q+1}{q^2+q+1}$	$\times\frac{1}{q^2+q+1}$	$\times\frac{q+1}{q^2+q+1}$
$W_2^\perp = \{(0,*,*,0,*,*)\}$	1	$\times\frac{q+1}{q^2+q+1}\cdot\frac{q}{q^2+q}$	$\times\frac{2q+1}{q^2+q+1}\cdot\frac{2q}{q^2+q}$	0	$\times\frac{q+1}{q^2+q+1}\cdot\frac{q}{q^2+q}$
$V = \{(*,*,*,*,*,*)\}$	1	$\times 1$	$\times 1$	$\times 1$	$\times 1$

The map

$$du^2 + euv + fv^2 \longmapsto 0u^2 + 0uv + 0uw + dv^2 + evw + fw^2$$

is an embedding $\mathrm{Sym}^2(2) \to \mathrm{Sym}^2(3)$, and as $a = b = c = 0$ for W_0, W_1, and W_2 the counts coincide with those previously given for $\mathrm{Sym}^2(2)$. For W_3, let $x = cuw + dv^2 + evw + fw^2 \in W_3$. This is non-singular if and only if $cd \neq 0$. Hence there are $q^2(q-1)^2$ elements of $\mathcal{O}_{\text{ns}}$. The count for $c = 0$ follows from the whole of $\mathrm{Sym}^2(2)$, and for $d = 0$ follows immediately. For $W_1^\perp$ and $W_2^\perp$, we are counting the number of elements of each $\mathcal{O}_i$ with, respectively, having $[1:0:0]$ as a zero, and having $[1:0:0]$ and $[0:1:0]$ as zeros. As $\mathrm{GL}_3(\mathbb{F}_q)$ acts 4-transitively on $\mathbb{P}^2(\mathbb{F}_q)$, the proportion of elements of each $\mathcal{O}_i$ in $W_1^\perp$ and $W_2^\perp$ is respectively

$\frac{\#Z_x(\mathbb{F}_q)}{\#\mathbb{P}^2(\mathbb{F}_q)}$ and $\frac{\#Z_x(\mathbb{F}_q)(\#Z_x(\mathbb{F}_q)-1)}{\#\mathbb{P}^2(\mathbb{F}_q)(\#\mathbb{P}^2(\mathbb{F}_q)-1)}$ for any $x \in \mathcal{O}_i$ where $Z_x \subset \mathbb{P}^2$ is the conic defined by x, and these quantities $\#Z_x(\mathbb{F}_q)$ were enumerated above.

The above vectors span $\mathbb{R}^5$, and as before by Proposition 5 we conclude:

Theorem 16 *We have*

$$M = \frac{1}{q^6}\begin{bmatrix} 1 & q^3-1 & q(q+1)(q^3-1)/2 & q(q-1)(q^3-1)/2 & q^2(q-1)(q^3-1) \\ 1 & -1 & q(q+1)(q^2-1)/2 & -q(q-1)(q^2+1)/2 & -q^2(q-1) \\ 1 & q^2-1 & q(q^2-2q-1)/2 & q(q-1)^2/2 & -q^2(q-1) \\ 1 & -q^2-1 & q(q^2-1)/2 & q(q^2+1)/2 & -q^2(q-1) \\ 1 & -1 & -q(q+1)/2 & -q(q-1)/2 & q^2 \end{bmatrix}.$$

6 $2 \otimes \mathrm{Sym}^2(2)$

Next we investigate the space V of pairs of binary quadratic forms. As before, we assume $p \neq 2$. Let $V := \mathbb{F}_q^2 \otimes \mathrm{Sym}^2(\mathbb{F}_q^2)$ be the space of pairs of binary quadratic forms. We write an element of V as follows:

$$x = (A, B) = (au^2 + buv + cv^2, du^2 + euv + fv^2) = \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} \tag{17}$$

Here, $A = \left[\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} d & e/2 \\ e/2 & f \end{smallmatrix}\right]$ are the symmetric matrices representing the respective binary quadratic forms. Let $G_1 = G_2 = \mathrm{GL}_2(\mathbb{F}_q)$ and $G := G_1 \times G_2$. The group action of G is defined by

$$\left(\left[\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right], g_2\right) \circ (A, B) = (\alpha g_2 A g_2^T + \beta g_2 B g_2^T, \gamma g_2 A g_2^T + \delta g_2 B g_2^T).$$

To investigate this representation, it is useful to associate to each $x \in V$ its *quadratic resolvent* $r_x \in \mathrm{Sym}^2(\mathbb{F}_q^2)$, defined by

$$r_x(u, v) := -4 \det(Au + Bv) = (bu + ev)^2 - 4(au + dv)(cu + fv).$$

Then we can see easily from the definition that $r_{(g_1,g_2)\circ x} = (\det g_2)^2 (g_1 \circ r_x)$, where the action of $g_1 \in \mathrm{GL}_2(\mathbb{F}_q)$ on $\mathrm{Sym}^2(\mathbb{F}_q)$ is as in (the $\mathrm{GL}_2(\mathbb{F}_q)$ component of) (14).

We first study its orbit decomposition.

Proposition 17 *Assume $p \neq 2$. There are seven orbits over $\mathbb{F}_q$. For each orbit, the following table lists orbital representatives, the rank, the label of the quadratic resolvent of any element in the orbit, and the size of the orbit. Here the* rank *of $x = (A, B) \in V$ is the rank of the matrix in* (17).

Orbit name	Representative	Rank	Resolvent	Orbit size
$\mathcal{O}_{(0)} = \mathcal{O}_1$	$(0, 0)$	0	(0)	1
$\mathcal{O}_{D1^2} = \mathcal{O}_2$	$(0, v^2)$	1	(0)	$(q-1)(q+1)^2$
$\mathcal{O}_{D11} = \mathcal{O}_3$	$(0, uv)$	1	(1^2)	$q(q-1)(q+1)^2/2$
$\mathcal{O}_{D2} = \mathcal{O}_4$	$(0, u^2 - lv^2)$	1	(1^2)	$q(q-1)^2(q+1)/2$
$\mathcal{O}_{Cs} = \mathcal{O}_5$	(v^2, uv)	2	(1^2)	$q(q^2-1)^2$
$\mathcal{O}_{B11} = \mathcal{O}_6$	(v^2, u^2)	2	(11)	$(q^3-q)^2/2$
$\mathcal{O}_{B2} = \mathcal{O}_7$	$(uv, u^2 + lv^2)$	2	(2)	$(q^2-q)^2(q^2-1)/2$

Here $l \in \mathbb{F}_q$ is a non-square element.

Remark 18 *The subscripts D and C indicate respectively that x is doubled (i.e., rank 1) or has a common component. The subscript B (binary) is chosen to be consistent with the quartic case $V = 2 \otimes \mathrm{Sym}^2(3)$.*

Proof: We first show that any $x = (A, B) = \left[\begin{smallmatrix} a & b & c \\ d & e & f \end{smallmatrix}\right] \in V$ is G-equivalent to one of the seven elements above. We write $x \sim x'$ if $x, x' \in V$ are in the same G-orbit. If A and B are linearly dependent, then by

the action of G_1, we may let $A = 0$. By our results for $\mathrm{Sym}^2(2)$, x is equivalent to one of the first four elements. So suppose A and B are linearly independent. If the left side 2-by-2 matrix $\left[\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right]$ of x is invertible (as a matrix), then by a G_1 translation, we can move x to $\left[\begin{smallmatrix} 0 & 1 & c' \\ 1 & e' & f' \end{smallmatrix}\right]$. By a G_2 translation, we move this to $\left[\begin{smallmatrix} 0 & 1 & 0 \\ 1 & e'' & f'' \end{smallmatrix}\right]$ and then again by G_1 we further erase e'', and thus assume $x = (uv, u^2 + fv^2)$. Observe that $(uv, u^2 + fv^2) \sim (tuv, u^2 + ft^2v^2) \sim (uv, u^2 + ft^2v^2)$ for $t \in \mathbb{F}_q^\times$, $(uv, u^2 + fv^2) \sim (uv, u^2 + lv^2)$ if f is non-square. If f is square, $(uv, u^2 + fv^2) \sim (uv, u^2 + v^2)$ and is further $\sim (u^2 + v^2 + 2uv, u^2 + v^2 - 2uv) \sim (v^2, u^2)$. Suppose $\left[\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right]$ is not invertible (it cannot be zero). By G_1, we may let x be either $\left[\begin{smallmatrix} 0 & 0 & c \\ 0 & 1 & f \end{smallmatrix}\right]$ or $\left[\begin{smallmatrix} 0 & 0 & c \\ 1 & e & f \end{smallmatrix}\right]$. In the latter case we use $\left[\begin{smallmatrix} 1 & 0 \\ -e/2 & 1 \end{smallmatrix}\right] \in G_2$ to move it to $\left[\begin{smallmatrix} 0 & 0 & c \\ 1 & 0 & f' \end{smallmatrix}\right]$. Since A and B are independent, $c \neq 0$ and so x is equivalent to $\left[\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right] = (v^2, uv)$ or $\left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right] = (v^2, u^2)$, respectively.

We next prove that the seven elements are in different orbits. We compare their ranks and the quadratic resolvent: if $x, y \in V$ are in the same orbit, then $\mathrm{rank}(x) = \mathrm{rank}(y)$ and also $r_x, r_y \in \mathrm{Sym}^2(\mathbb{F}_q^2)$ are of the same type. To conclude it is enough to check that $(0, v^2)$ and $(0, u^2 - lv^2)$ are not in the same orbit. Our assertion follows from the results of $\mathrm{Sym}^2(2)$, because $x = (0, B)$ and $x' = (0, B)$ with $B \neq 0$, $B' \neq 0$ are in the same G-orbit iff $B, B' \in \mathrm{Sym}^2(\mathbb{F}_q^2)$ lie in the same $\mathrm{GL}_1(\mathbb{F}_q) \times \mathrm{GL}_2(\mathbb{F}_q)$-orbit.

Thus we have shown that there are exactly seven orbits, and the orbit counts will be proved later in this section. □

Writing the symmetric bilinear form (15) on $\mathrm{Sym}^2(\mathbb{F}_q^2)$ by $[A, A']'$, we define a symmetric bilinear form on V by

$$[(A, B), (A', B')] = [A, A']' + [B, B']'.$$

Then we have $[gx, g^{-T}x'] = [x, x']$ (recall that $(g_1, g_2)^T := (g_1^T, g_2^T)$) and so (G, V) satisfies Assumption 1.

We come now to our orbit counts. Anticipating the more difficult computations in the quartic case, we introduce a new method for the computations which enables us to work inductively (and rather systematically). By subtracting the results of previously handled computations, we may assume that certain of the coordinates are nonzero, and then apply G-transformations to obtain a map to a set Y for which the $|Y \cap \mathcal{O}_i|$ are more easily counted. For $X \subset V$, we find it convenient to use the same symbol X to denote the vector $(X \cap \mathcal{O}_i)_i \in \mathbb{R}^7$. For example,

$$(X \cup Y) = X + Y - (X \cap Y)$$

is an identity in the vector space $\mathbb{R}^7$, representing the inclusion-exclusion principle.

For $i, j \in \{0, 1, 2, 3\}$, let $W_{[i,j]}$ be the subspace consisting of pairs of forms (A, B) such that the last i entries of A and the last j entries of B are arbitrary, and other entries are 0. For example,

$$W_{[0,0]} = \{0\}, \quad W_{[1,3]} = \left\{ \begin{bmatrix} 0 & 0 & * \\ * & * & * \end{bmatrix} \right\}, \quad W_{[2,2]} = \left\{ \begin{bmatrix} 0 & * & * \\ 0 & * & * \end{bmatrix} \right\}, \quad W_{[3,3]} = \left\{ \begin{bmatrix} * & * & * \\ * & * & * \end{bmatrix} \right\} = V.$$

Of course some coordinate subspaces of V, such as $\{\left[\begin{smallmatrix} 0 & 0 & * \\ * & * & 0 \end{smallmatrix}\right]\}$, are not of this form, but here it suffices to consider only such subspaces. We count $W_{[i,j]} \cap \mathcal{O}_k$ for all $0 \leq i \leq j \leq 3$ (there are ten of them), because we need this result when studying $2 \otimes \mathrm{Sym}^2(3)$ in the next section. (However, as we observe when proving Theorem 19, counts for a certain seven of $W_{[i,j]}$ are enough to determine A.) Note that $\eta \cdot W_{[i,j]}^\perp = W_{[3-j,3-i]}$ where $\eta = (\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]) \in G$, so that $W_{[i,j]}^\perp = W_{[3-j,3-i]}$ (not literally as subspaces of V, but rather as in the sense described previously).

If $1 \leq i < j$, then let $W_{[i,j]}^\times$ be the elements in $W_{[i,j]}$ whose first $*$'s are non-zero in each row. For example,

$$W_{[1,2]}^\times = \left\{ \begin{bmatrix} 0 & 0 & c \\ 0 & e & * \end{bmatrix} \;\middle|\; c, e \neq 0 \right\}, \qquad W_{[1,3]}^\times = \left\{ \begin{bmatrix} 0 & 0 & c \\ d & * & * \end{bmatrix} \;\middle|\; c, d \neq 0 \right\}.$$

Then by inclusion-exclusion,

$$W_{[i,j]} = W_{[i,j]}^\times + W_{[i-1,j]} + W_{[i,j-1]} - W_{[i-1,j-1]}. \tag{18}$$

If $2 \le i = j$, then let $W^{\times}_{[i,i]}$ be the elements x in $W_{[i,i]}$ whose leftmost 2-by-2 matrix $\left[\begin{smallmatrix} * & * \\ * & * \end{smallmatrix}\right]$ of x is invertible. For example,

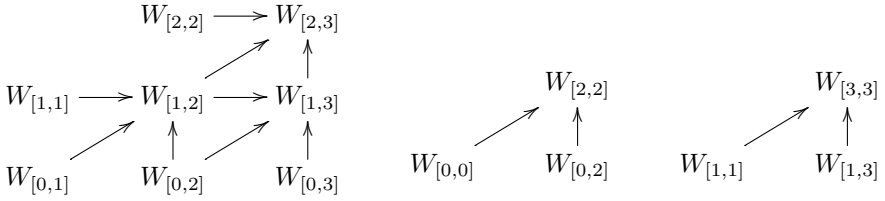
$$W^{\times}_{[2,2]} = \left\{ \begin{bmatrix} 0 & b & c \\ 0 & e & f \end{bmatrix} \;\middle|\; bf - ce \neq 0 \right\}, \qquad W^{\times}_{[3,3]} = \left\{ \begin{bmatrix} a & b & * \\ d & e & * \end{bmatrix} \;\middle|\; ae - bd \neq 0 \right\},$$

Then in this case we have

$$W_{[i,i]} = W^{\times}_{[i,i]} + (q+1) \cdot W_{[i-2,i]} - q \cdot W_{[i-2,i-2]}. \tag{19}$$

To verify this, let $W'_{[i,i]}$ denote the subset of $W_{[i,i]}$ whose leftmost two-by-two matrix M is of rank 1, and $W'_{[i-2,i]} = W'_{[i,i]} \cap W_{[i-2,i]}$; it suffices to describe an orbit preserving map $W'_{[i,i]} \to W'_{[i-2,i]}$ which is precisely $(q+1)$-to-one. This is most easily described as a bijection $\mathbb{P}^1(\mathbb{F}_q) \times W'_{[i-2,i]} \to W'_{[i,i]}$: we map $([\mu : 1], x)$ to $(\left[\begin{smallmatrix} 1 & \beta \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]) \cdot x$ and $([1 : 0], x)$ to $(\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]) \cdot x$.

Hence provided that we have counted for smaller i and j, our count of each $W_{[i,j]}$ is reduced to that of $W^{\times}_{[i,j]}$, by (18) or (19). Our induction process may be illustrated in the following diagram:



At the beginning we need to know the counts for $W_{[0,j]}$ for all j and $W_{[1,1]}$. The former is contained in our results for $\mathrm{Sym}^2(2)$, while the latter is trivial. We have:

Subspace	$\mathcal{O}_0$	$\mathcal{O}_{D1^2}$	$\mathcal{O}_{D11}$	$\mathcal{O}_{D2}$	$\mathcal{O}_{Cs}$	$\mathcal{O}_{B11}$	$\mathcal{O}_{B2}$
$W_{[0,0]}$	1						
$W_{[0,1]}$	1	$q-1$					
$W_{[0,2]}$	1	$q-1$	$q(q-1)$				
$W_{[0,3]}$	1	q^2-1	$\frac{1}{2}q(q^2-1)$	$\frac{1}{2}q(q-1)^2$			
$W_{[1,1]}$	1	q^2-1					

We now examine $W^{\times}_{[1,2]}, W^{\times}_{[1,3]}, W^{\times}_{[2,2]}, W^{\times}_{[2,3]}$ and $W^{\times}_{[3,3]}$. For $W^{\times}_{[1,3]}$, we have

$$W^{\times}_{[1,3]} = (q-1)^2 \cdot \left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & * & * \end{smallmatrix}\right] = q^2(q-1)^2 \cdot \left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right] \tag{20}$$

so that all of these elements are in $\mathcal{O}_{B11}$. The reduction (20) is proved as follows. There is a bijection $\mathbb{F}_q^{\times} \times \mathbb{F}_q^{\times} \times \{\left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & * & * \end{smallmatrix}\right]\} \to W^{\times}_{[1,3]}$, given by $(\lambda, \mu, \left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & a & b \end{smallmatrix}\right]) \to (\left[\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]) \cdot \left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & a & b \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 & 0 & \lambda \\ \mu & \mu a & \mu b \end{smallmatrix}\right]$, and this yields the first equality. Then, there is a bijection $\mathbb{F}_q \times \{\left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & * \end{smallmatrix}\right]\} \to \{\left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & * & * \end{smallmatrix}\right]\}$, given by $(\lambda, \left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & a \end{smallmatrix}\right]) \to (\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right]) \cdot \left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & a \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 2\lambda & \lambda^2 + a \end{smallmatrix}\right]$. Finally, there is a bijection $\mathbb{F}_q \times \{\left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right]\} \to \{\left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & * \end{smallmatrix}\right]\}$, given by $(\lambda, \left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right]) \to (\left[\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]) \cdot \left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & \lambda \end{smallmatrix}\right]$.

Put together these three bijections prove (20); note that each factor of $\mathbb{F}_q$ or $\mathbb{F}_q^{\times}$ determined an element of $G(\mathbb{F}_q)$. Each of these three steps illustrates a reduction which we will use quite frequently in our analysis, and we will usually leave similar such verifications to the reader.

For $W^{\times}_{[3,3]}$, we can similarly prove that

$$W^{\times}_{[3,3]} = (q^2-1)(q^2-q) \cdot \left[\begin{smallmatrix} 0 & 1 & * \\ 1 & 0 & * \end{smallmatrix}\right] = (q^2-1)(q^2-q) \cdot \left[\begin{smallmatrix} 0 & 1 & 0 \\ 1 & * & * \end{smallmatrix}\right] = q(q^2-1)(q^2-q) \cdot \left[\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 0 & * \end{smallmatrix}\right];$$

the second equality may be verified by observing that for each $\lambda \in \mathbb{F}_q$ $(\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right])$ gives a bijective map from $\left[\begin{smallmatrix} 0 & 1 & -\lambda \\ 1 & 0 & * \end{smallmatrix}\right]$ to $\left[\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 2\lambda & * \end{smallmatrix}\right]$.

The element $\left[\begin{smallmatrix}0&1&0\\1&0&f\end{smallmatrix}\right]$ is, according as f is zero, a quadratic residue or a quadratic non-residue, in $\mathcal{O}_{Cs}$, $\mathcal{O}_{B11}$ or $\mathcal{O}_{B2}$, respectively. The remaining cases are treated similarly and easily. We summarize our argument in the following table. In each row the orbit counts for $W^\times$ are equal to the multiplier times those for Y, and those for Y are listed in the middle columns.

Subset	Y	$\mathcal{O}_{Cs}$	$\mathcal{O}_{B11}$	$\mathcal{O}_{B2}$	multiplier
$W^\times_{[1,2]}$	$\left[\begin{smallmatrix}0&0&1\\0&1&0\end{smallmatrix}\right]$	1			$\times q(q-1)^2$
$W^\times_{[1,3]}$	$\left[\begin{smallmatrix}0&0&1\\1&0&0\end{smallmatrix}\right]$		1		$\times q^2(q-1)^2$
$W^\times_{[2,2]}$	$\left[\begin{smallmatrix}0&0&1\\0&1&0\end{smallmatrix}\right]$	1			$\times(q^2-1)(q^2-q)$
$W^\times_{[2,3]}$	$\left[\begin{smallmatrix}0&1&0\\1&0&*\end{smallmatrix}\right]$	1	$\frac{q-1}{2}$	$\frac{q-1}{2}$	$\times q^2(q-1)^2$
$W^\times_{[3,3]}$	$\left[\begin{smallmatrix}0&1&0\\1&0&*\end{smallmatrix}\right]$	1	$\frac{q-1}{2}$	$\frac{q-1}{2}$	$\times q(q^2-1)(q^2-q)$

As a conclusion, we have the following counts:

Subspace	$\mathcal{O}_0$	$\mathcal{O}_{D1^2}$	$\mathcal{O}_{D11}$	$\mathcal{O}_{D2}$	$\mathcal{O}_{Cs}$	$\mathcal{O}_{B11}$	$\mathcal{O}_{B2}$
$W_{[1,2]}$	1	q^2-1	$q(q-1)$		$q(q-1)^2$		
$W_{[1,3]}$	1	$2q^2-q-1$	$\frac{1}{2}q(q^2-1)$	$\frac{1}{2}q(q-1)^2$	$q(q-1)^2$	$(q-1)^2q^2$	
$W_{[2,2]}$	1	q^2-1	$q(q^2-1)$		$(q^2-1)(q^2-q)$		
$W_{[2,3]}$	1	$2q^2-q-1$	$\frac{1}{2}q(3q^2-2q-1)$	$\frac{1}{2}q(q-1)^2$	$(q-1)^2(2q^2+q)$	$\frac{1}{2}q^2(q-1)^2(q+1)$	$\frac{1}{2}q^2(q-1)^3$
$W_{[3,3]}$	1	$(q-1)(q+1)^2$	$\frac{1}{2}q(q-1)(q+1)^2$	$\frac{1}{2}q(q-1)^2(q+1)$	$q(q^2-1)^2$	$\frac{1}{2}(q^3-q)^2$	$\frac{1}{2}(q^2-q)^2(q^2-1)$

We now deduce M. The vectors $(W\cap\mathcal{O}_i)_i\in\mathbb{R}^7$ for

$$W = W_{[0,0]}, W_{[1,1]}, W_{[0,2]}, W_{[0,3]}, W_{[1,3]}, W_{[2,2]}, W_{[3,3]}$$

span $\mathbb{R}^7$. We have:

Theorem 19 *The matrix q^6M is given by*

$$\begin{bmatrix}
1 & (q-1)(q+1)^2 & (q-1)(q+1)^2q/2 & (q-1)^2q(q+1)/2 & (q+1)^2q(q-1)^2 & (q+1)^2q^2(q-1)^2/2 & (q-1)^3q^2(q+1)/2\\
1 & q^2-q-1 & q(2q+1)(q-1)/2 & -q(q-1)/2 & (q^2-q-1)q(q-1) & -q^2(q-1)(q+1)/2 & -q^2(q-1)^2/2\\
1 & (2q+1)(q-1) & q(q^2-2q-1)/2 & q(q-1)^2/2 & -(q-1)(q+1)q & q^2(q-1)^2/2 & -q^2(q-1)^2/2\\
1 & -q-1 & (q-1)(q+1)q/2 & (q^2+1)q/2 & -(q-1)(q+1)q & -q^2(q-1)(q+1)/2 & q^2(q-1)(q+1)/2\\
1 & q^2-q-1 & -(q+1)q/2 & -q(q-1)/2 & q & -q^2(q-1)/2 & q^2(q-1)/2\\
1 & -q-1 & q(q-1)/2 & -q(q-1)/2 & -q(q-1) & q^2 & 0\\
1 & -q-1 & -(q+1)q/2 & (q+1)q/2 & (q+1)q & 0 & -q^2
\end{bmatrix}.$$

7 $2\otimes\mathrm{Sym}^2(3)$

We come now to the prehomogeneous vector space $(\mathrm{GL}_2\times\mathrm{GL}_3, 2\otimes\mathrm{Sym}^2(3))$, which we call the 'quartic case' because (roughly speaking) it parametrizes quartic fields [WY92] and rings [Bha04]. We assume that $p\neq 2$ in the argument, in which case there are 20 orbits over $\mathbb{F}_q$.

We write an element of $V=\mathbb{F}_q^2\otimes\mathrm{Sym}^2(\mathbb{F}_q^3)$ as follows:

$$x=(A,B)=\begin{bmatrix}a&b&c&d&e&f\\a'&b'&c'&d'&e'&f'\end{bmatrix},$$

where A, B are the ternary quadratic forms

$$A=au^2+buv+cuw+dv^2+evw+fw^2,\quad B=a'u^2+b'uv+c'uw+d'v^2+e'vw+f'w^2.$$

We also regard A and B as the three-by-three symmetric matrices representing the forms. Let $G_1=\mathrm{GL}_2(\mathbb{F}_q)$, $G_2=\mathrm{GL}_3(\mathbb{F}_q)$ and $G:=G_1\times G_2$. We consider the group action of G given by

$$\left(\left[\begin{smallmatrix}\alpha&\beta\\\gamma&\delta\end{smallmatrix}\right], g_2\right)\circ(A,B)=(\alpha g_2Ag_2^T+\beta g_2Bg_2^T, \gamma g_2Ag_2^T+\delta g_2Bg_2^T).$$

The *cubic resolvent* $r_x \in \mathrm{Sym}^3(\mathbb{F}_q^2)$ and the discriminant $\mathrm{Disc}(x)$ of $x \in V$ are respectively defined by

$$r_x(u,v) := -4\det(Au+Bv) \in \mathrm{Sym}^3(\mathbb{F}_q^2),$$
$$\mathrm{Disc}(x) := \mathrm{Disc}(r_x),$$

and as before we say x is singluar if $\mathrm{Disc}(x) = 0$. Then $r_{(g_1,g_2)\circ x} = \det g_1 (\det g_2)^2 (g_1 \circ r_x)$, and thus $\mathrm{Disc}(g \circ x) = (\det g_1)^6 (\det g_2)^8 \mathrm{Disc}(x)$.

Writing the symmetric bilinear form (16) on $\mathrm{Sym}^2(\mathbb{F}_q^3)$ by $[A, A']'$, we define a symmetric bilinear form on V by

$$[(A,B),(A',B')] = [A,A']' + [B,B']'.$$

Then we have $[gx, g^{-T}x'] = [x,x']$ and so (G,V) satisfies Assumption 1.

7.1 Orbit description

The aim of this subsection is to give an orbit description over $\mathbb{F}_q$. Note first that the non-singular orbits are known by Wright-Yukie [WY92], where they showed that the set of non-singular orbits corresponds bijectively to the set of isomorphism classes of etale quartic algebras of $\mathbb{F}_q$. Hence there are five of them. Moreover, they gave a natural geometric interpretation of this result. An $x = (A,B)$ determines two conics in $\mathbb{P}^2(\overline{\mathbb{F}}_q)$, and x is non-singular if and only if they are of complete intersection. Thus to a non-singular x, we attach one of the symbols (1111), (112), (22), (13) or (4), identifying the degrees of the residue fields at the points of intersections. It is clear that elements in a non-singular orbit posses the same symbol, and they actually showed that elements having the same symbol lie in the same orbit. This gives a satisfactory description of the non-singular orbits. We denote these orbits respectively by $\mathcal{O}_{1111}$, $\mathcal{O}_{112}$, $\mathcal{O}_{22}$, $\mathcal{O}_{13}$ and $\mathcal{O}_4$.

Bhargava [Bha04, Lemma 21] described many of the singular orbits and computed their cardinalities, and we will build upon his work as well.

To classify singular orbits, it is useful to think of certain "higher singular" conditions of $x = (A,B)$, described as follows:

(D) A and B are linearly dependent;

(C) A and B share a common linear factor;

(B) After a change of variables, A and B can be written as a pair of binary quadratic forms (each in the same two variables).

In other words, the G-orbit of x contains an element in the subspace

$$W_{(\mathrm{D})} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & * \end{bmatrix}, \quad W_{(\mathrm{C})} = \begin{bmatrix} 0 & 0 & * & 0 & * & * \\ 0 & 0 & * & 0 & * & * \end{bmatrix}, \quad W_{(\mathrm{B})} = \begin{bmatrix} 0 & 0 & 0 & * & * & * \\ 0 & 0 & 0 & * & * & * \end{bmatrix},$$

respectively. Geometrically, x is of type (D) if $A = 0$ and $B = 0$ are identical conics so they are doubled; x is of type (C) if $A = 0$ and $B = 0$ are both reducible conics sharing a common line; x is of type (B) if $A = 0$ and $B = 0$ are both reducible as conics over $\overline{\mathbb{F}}_q$ and pass through a single common point. (These conditions are not mutually exclusive, and should be interpreted a bit loosely; for example the doubled zero conic belongs to all three subspaces.)

We will prove that if x is singular but not of type (D), (C) or (B), then two conics $A = 0$ and $B = 0$ intersect with each other in exactly four points counting multiplicities, and that the state of intersection is a complete invariant for those orbits. There are six types, and we attach symbols (1^4), (1^31), (1^21^2), (2^2), (1^211) or (1^22). Hence we denote these respective six orbits by $\mathcal{O}_{1^4}$, $\mathcal{O}_{1^31}$, $\mathcal{O}_{1^21^2}$, $\mathcal{O}_{2^2}$, $\mathcal{O}_{1^211}$ and $\mathcal{O}_{1^22}$, after we have the assertion.

We prove:

Lemma 20 *Singular elements are either of type* (D), (C) *or* (B), *or G-equivalent to one of the six elements below. Here, $l \in \mathbb{F}_q^\times$ is a non-square element.*

$$(w^2, uw+v^2), (vw, uw+v^2), (w^2, u^2-v^2), (w^2, u^2-lv^2), (v^2-w^2, uw), (v^2-lw^2, uw).$$

The symbols of these six elements are (1^4), (1^31), (1^21^2), (2^2), (1^211) *or* (1^22), *respectively.*

Proof: Suppose $x = (A, B)$ is singular. Then since r_x is a singular binary cubic form, we may assume that the coefficients of u^3 and u^2v of r_x are both zero. Thus in particular $\det(A) = 0$ and hence $\mathrm{rank}(A) \leq 2$.

1. If $\mathrm{rank}(A) = 0$, then x is of type (D).
2. Let $\mathrm{rank}(A) = 1$. Then by GL_3, we may assume that $A = w^2$. Let $B = au^2+buv+cuw+dv^2+evw+fw^2$. We look at $B(u, v, 0) = au^2 + buv + dv^2 \in \mathrm{Sym}^2(\mathbb{F}_q^2)$.
   (a) If $au^2 + buv + dv^2$ is a zero form, then x is of type (C).
   (b) Suppose $au^2 + buv + dv^2$ is non-zero but singular. By a linear change of u and v, we may assume $a = b = 0$ and $d = 1$, and thus $(A, B) = (w^2, v^2 + w(cu + ev + fw))$.
      i. If $c = 0$, then x is of type (B).
      ii. If $c \neq 0$, we may replace $cu + ev + fw$ with u via GL_3, and thus $(A, B) = (w^2, v^2 + uw)$.
   (c) Suppose $au^2 + buv + dv^2$ is non-singular. By a linear change of u and v, we may assume $b = 0$, and hence $ad \neq 0$. Then
   $$B = au^2 + cuw + dv^2 + evw + fw^2 = a(u + \tfrac{c}{2a}w)^2 + d(v + \tfrac{e}{2d}w)^2 + *w^2.$$
   Replacing $u + \frac{c}{2a}w$ with u and $v + \frac{e}{2d}w$ with v via GL_3, and further eliminating the w^2-term using $A = w^2$, we have $x = (w^2, au^2 + dv^2)$. Since $ad \neq 0$, this is equivalent to one of the middle two in the list.
3. Let $\mathrm{rank}(A) = 2$. Using the GL_3 action, Proposition 15 allows us to assume that $A = av^2 + bvw + cw^2$. Since the u^2v term of r_x vanishes, B is of the form $B = duv + euw + fv^2 + gvw + hw^2$.
   (a) If $d = e = 0$, then x is of type (B).
   (b) If $(d, e) \neq (0, 0)$, then by a linear change of v and w, we may assume that $(d, e) = (0, 1)$.
      i. Suppose $a = 0$. Then $A = w(bv + cw)$. Since $\mathrm{rank}(A) = 2$, we have $b \neq 0$ and hence may replace $bv+cw$ with v via GL_3. So $A = vw$. On the other hand, since $B = fv^2+w(u+gv+hw)$, we may replace $u + gv + hw$ with u and thus $B = fv^2 + uw$.
         A. If $f = 0$, then $x = (vw, uw)$ is of type (C).
         B. If $f \neq 0$, then replace u with fu and we have $B = f(v^2 + uw) \sim v^2 + uw$.
      ii. Suppose $a \neq 0$. We may assume $a = 1$. We can eliminate b and f and thus may assume $(A, B) = (v^2 + cw^2, w(u + gv + hw))$. This lies in the orbit of $(v^2 + cw^2, uw)$ since we can replace $u + gv + hw$ with u via GL_3. This is equivalent to the one of the last two in the list.

This finishes the proof. □

We now give our orbit description, extending [Bha04, Lemma 21]. To describe the orbit sizes, we write

$$s(a, b, c, d) := (q-1)^a q^b (q+1)^c (q^2+q+1)^{d/2},$$

where d is always even. Note that its degree as a polynomial in q is $a + b + c + d$.

Proposition 21 *Assume $p \neq 2$. The action of G on V has twenty orbits, of which fifteen are singular. For each orbit, the table below lists an orbital representative, the type of the resolvent, and the number of rational common zeros in $\mathbb{P}^2(\mathbb{F}_q)$, of any element in the orbit, and the size of the orbit:*

Orbit	Representative	Resolvent	Common zeros	Orbit size
$\mathcal{O}_0$	$(0,0)$	(0)	q^2+q+1	1
$\mathcal{O}_{D1^2}$	$(0,w^2)$	(0)	$q+1$	$s(1,0,1,2)$
$\mathcal{O}_{D11}$	$(0,vw)$	(0)	$2q+1$	$s(1,1,2,2)/2$
$\mathcal{O}_{D2}$	$(0,v^2-lw^2)$	(0)	1	$s(2,1,1,2)/2$
$\mathcal{O}_{D\mathrm{ns}}$	$(0,u^2-vw)$	(1^3)	$q+1$	$s(2,2,1,2)$
$\mathcal{O}_{C\mathrm{s}}$	(w^2,vw)	(0)	$q+1$	$s(2,1,2,2)$
$\mathcal{O}_{C\mathrm{ns}}$	(vw,uw)	(0)	$q+2$	$s(2,3,1,2)$
$\mathcal{O}_{B11}$	(w^2,v^2)	(0)	1	$s(2,2,2,2)/2$
$\mathcal{O}_{B2}$	(vw,v^2+lw^2)	(0)	1	$s(3,2,1,2)/2$
$\mathcal{O}_{1^4}$	$(w^2,uw+v^2)$	(1^3)	1	$s(3,2,2,2)$
$\mathcal{O}_{1^31}$	$(vw,uw+v^2)$	(1^3)	2	$s(3,3,2,2)$
$\mathcal{O}_{1^21^2}$	(w^2,u^2-v^2)	(1^21)	2	$s(2,4,2,2)/2$
$\mathcal{O}_{2^2}$	(w^2,u^2-lv^2)	(1^21)	0	$s(3,4,1,2)/2$
$\mathcal{O}_{1^211}$	(v^2-w^2,uw)	(1^21)	3	$s(3,4,2,2)/2$
$\mathcal{O}_{1^22}$	(v^2-lw^2,uw)	(1^21)	1	$s(3,4,2,2)/2$
$\mathcal{O}_{1111}$	$(uw-vw,uv-vw)$	(111)	4	$s(4,4,2,2)/24$
$\mathcal{O}_{112}$	$(vw,u^2-v^2-lw^2)$	(12)	2	$s(4,4,2,2)/4$
$\mathcal{O}_{22}$	$(vw,u^2-lv^2-lw^2)$	(111)	0	$s(4,4,2,2)/8$
$\mathcal{O}_{13}$	$(uw-v^2,B_3)$	(3)	1	$s(4,4,2,2)/3$
$\mathcal{O}_4$	$(uw-v^2,B_4)$	(12)	0	$s(4,4,2,2)/4$

Here B_3 and B_4 in the last two rows are $B_3 = uv+a_3v^2+b_3vw+c_3w^2$ and $B_4 = u^2+a_4uv+b_4v^2+c_4vw+d_4w^2$, where $X^3+a_3X^2+b_3X+c_3$ and $X^4+a_4X^3+b_4X^2+c_4X+d_4$ are respectively irreducible cubic and quartic polynomials over $\mathbb{F}_q$ (and as before $l \in \mathbb{F}_q^\times$ is a non-square element).

Proof: If x is of type (D), then by the orbit description of $\mathrm{Sym}^2(3)$, x is equivalent to one of the first five elements in the table. If x is of type (B), then by the orbit description of $2 \otimes \mathrm{Sym}^2(2)$, x is equivalent to either one of the first four elements in the table, or to (w^2,vw), (w^2,v^2) or (vw,v^2+lw^2). If x is of type (C), then x is equivalent to either $(0,0)$, $(0,w^2)$, $(0,vw)$, (w^2,vw) or (vw,uw). Hence by Lemma 20 and the result of [WY92] mentioned above, any element in V is equivalent to one of the twenty elements in the table.

We confirm that their orbits are all different. This is immediate, except for the possibility that (w^2,v^2) and (vw,v^2+lw^2) may lie the same orbit, by comparing the three invariants rank, resolvent, and the number of common zeros in $\mathbb{P}^2$. We show that $(w^2,v^2) \sim (vw,v^2-w^2)$ and (vw,u^2+lw^2) are not in the same orbit.

We embed $W = 2 \otimes \mathrm{Sym}^2(2)$ into $V = 2 \otimes \mathrm{Sym}^2(3)$ via $\left[\begin{smallmatrix} a & b & c \\ d & e & f \end{smallmatrix}\right] \mapsto \left[\begin{smallmatrix} 0 & 0 & 0 & a & b & c \\ 0 & 0 & 0 & d & e & f \end{smallmatrix}\right]$, and regard it as a subspace. Let $y = \left[\begin{smallmatrix} 0 & 1 & 0 \\ d & e & f \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & d & e & f \end{smallmatrix}\right]$ and suppose $g \circ y \in W$ for a $g = (g_1,g_2) \in G$. Since W is invariant under G_1, we have $(1,g_2) \circ y \in W$ as well. Let $g_2 = \begin{bmatrix} h & \alpha & \beta \\ i & j & k \\ l & m & n \end{bmatrix}$. We claim that $\alpha = \beta = 0$. The first row of y is the ternary quadratic form vw, and it is transformed by g_2 to $(\alpha u + jv + mw)(\beta u + kv + nw)$. Since this form involves only the variables v and w, we have $\alpha\beta = \alpha k + \beta j = \alpha n + \beta m = 0$. If $\alpha \neq 0$, then $\beta = k = n = 0$ and so g_2 is not invertible. Hence $\alpha = 0$. Similarly, we have $\beta = 0$.

This shows that elements of the form $\left[\begin{smallmatrix} 0 & 1 & 0 \\ d & e & f \end{smallmatrix}\right]$ are G-equivalent in V if and only if they are $\mathrm{GL}_2 \times \mathrm{GL}_2$-equivalent in W, and thus the difference of the orbits is asserted.

We count the orbit sizes. Note that the argument above also gives an expression of the stabilizers of $\left[\begin{smallmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & d & e & f \end{smallmatrix}\right]$ in G in terms of the stabilizers of $\left[\begin{smallmatrix} 0 & 1 & 0 \\ d & e & f \end{smallmatrix}\right]$ in $\mathrm{GL}_2 \times \mathrm{GL}_2$. Namely, if $g = (g_1,g_2) \in G$ stabilizes $y = \left[\begin{smallmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & d & e & f \end{smallmatrix}\right]$, then g_2 must be of the form $\begin{bmatrix} h & 0 & 0 \\ i & j & k \\ l & m & n \end{bmatrix}$, and for such a $g = (g_1,g_2)$, we immediately find that g stabilizes y if and only if $(g_1, \left[\begin{smallmatrix} j & k \\ m & n \end{smallmatrix}\right]) \in \mathrm{GL}_2 \times \mathrm{GL}_2$ stabilizes $\left[\begin{smallmatrix} 0 & 1 & 0 \\ d & e & f \end{smallmatrix}\right]$. Therefore, the orbit sizes of $\mathcal{O}_{C\mathrm{s}}$,

$\mathcal{O}_{B11}$ and $\mathcal{O}_{B2}$ in V are multiplied by q^2+q+1 to those of in W. Each of the orbits $\mathcal{O}_{D1^2}$, $\mathcal{O}_{D11}$, $\mathcal{O}_{D2}$ and $\mathcal{O}_{D\mathrm{ns}}$ consisting of doubled conics is in bijection with a pair $(\mathcal{O},\gamma)$ where $\mathcal{O}$ is a $\mathrm{GL}_1\times\mathrm{GL}_3$ orbit in $\mathrm{Sym}^2(3)$ and $\gamma\in\mathbb{P}^1$, so that the orbit sizes are deduced from those for $\mathrm{Sym}^2(3)$. To compute the orbit size of $\mathcal{O}_{C\mathrm{ns}}$, we determine the stabilizers of $x=(vw,uw)$. Suppose $g=(g_2,g_3)$ stabilizes x. Let g_3 translates u,v,w to l_1,l_2,l_3 respectively; these are independent ternary linear forms. Also let $g_2^{-1}=\left[\begin{smallmatrix}\alpha&\beta\\ \gamma&\delta\end{smallmatrix}\right]$. Then $gx=x$ means $(l_2l_3,l_1l_3)=((\alpha v+\beta u)w,(\gamma v+\delta u)w)$. Thus l_3 must coincide with w up to scaling, and therefore l_1,l_2 are linear forms in u and v. Now it is easy to see that $\mathrm{Stab}(x)=\left\{\left(\left[\begin{smallmatrix}a&c\\ b&d\end{smallmatrix}\right]^{-1},\left[\begin{smallmatrix}a&b&\\ c&d&\\ &&e\end{smallmatrix}\right]\right)\right\}\cong\mathrm{GL}_1\times\mathrm{GL}_2$; we conclude $|\mathcal{O}_{C\mathrm{ns}}|=|G|/|\mathrm{Stab}(x)|=|\mathrm{GL}_3|/|\mathrm{GL}_1|$.

The orbit sizes of the latter eleven orbits are determined in [Bha04, Lemma 21].

Finally, we compute the resolvents. Except for the last one, this follows by rather easy case by case computation. For $x=(vw-u^2,B_4)$, we find that

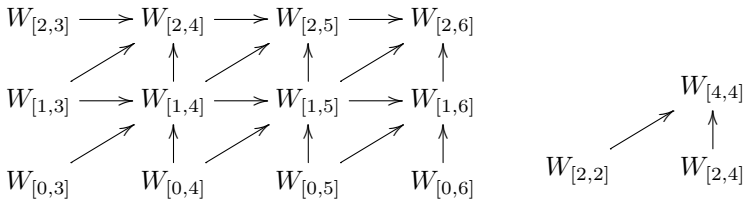
$$r_x(u,1)=u^3-b_4u^2+(a_4c_4-4d_4)u-(a_4^2d_4-4b_4d_4+c_4^2)$$

is the cubic resolvent of the polynomial $Q(u)=u^4-a_4u^3+b_4u^2-c_4u+d_4$ and thus $\mathrm{Disc}(r_x)=\mathrm{Disc}(Q)$. Since $\mathrm{Disc}(r_x)=\mathrm{Disc}(Q)\equiv\mathrm{Disc}(\mathbb{F}_{q^4}/\mathbb{F}_q)\pmod{(\mathbb{F}_q^\times)^2}$ is not a square in $\mathbb{F}_q$, $r_x\in\mathrm{Sym}^3(\mathbb{F}_q^2)$ is of type (12). This finishes the proof. □

7.2 Counting elements in subspaces

We now demonstrate our counts. For $i,j\in\{0,1,2,3,4,5,6\}$, let $W_{[i,j]}$ be the subspace consisting of pairs of forms (A,B) such that the last i entries of A and the last j entries of B are arbitrary, and other entries are 0. We largely follow the method in the previous section. We define $W^\times_{[i,j]}$ for $i<j$ and $i=j$ in the same way; then (18) and (19) remains true, and we argue inductively. Note also that the counts of $W_{[i,j]}$ for $i,j\le 3$ are obtained in the previous section, while the counts of $W_{[0,j]}$ for $4\le j\le 6$ are obtained in Section 5. For $X\subset V$, we use the same symbol X to denote $(X\cap\mathcal{O}_i)_i\in\mathbb{R}^{20}$.

(I) We first count $W_{[1,4]},W_{[1,5]},W_{[1,6]},W_{[2,4]},W_{[2,5]},W_{[2,6]}$ and $W_{[4,4]}$ by the same method as in the previous section. The following diagram illustrates our induction process:



We have previously counted $W_{[0,3]},W_{[1,3]},W_{[2,3]},W_{[0,4]},W_{[0,5]},W_{[0,6]},W_{[2,2]}$, and now analyze $W^\times_{[i,j]}$ for the seven subspaces mentioned above. The following two tables give the summary of our counts:

Subset	Y	$\mathcal{O}_{C\mathrm{s}}$	$\mathcal{O}_{C\mathrm{ns}}$	$\mathcal{O}_{B11}$	$\mathcal{O}_{1^4}$	$\mathcal{O}_{1^31}$	$\mathcal{O}_{1^21^2}$	$\mathcal{O}_{2^2}$	$\mathcal{O}_{1^211}$	multiplier
$W^\times_{[1,4]}$	$\left[\begin{smallmatrix}0&0&0&0&0&1\\0&0&1&*&0&0\end{smallmatrix}\right]$	1			$q-1$					$\times q^2(q-1)^2$
$W^\times_{[1,5]}$	$\left[\begin{smallmatrix}0&0&0&0&0&1\\0&1&0&0&0&0\end{smallmatrix}\right]$						1			$\times q^4(q-1)^2$
$W^\times_{[1,6]}$	$\left[\begin{smallmatrix}0&0&0&0&0&1\\1&0&0&*&*&0\end{smallmatrix}\right]$			1	$q-1$		$\frac{q(q-1)}{2}$	$\frac{q(q-1)}{2}$		$\times q^3(q-1)^2$
$W^\times_{[2,4]}$	$\left[\begin{smallmatrix}0&0&0&0&1&0\\0&0&1&*&0&0\end{smallmatrix}\right]$		1			$q-1$				$\times q^3(q-1)^2$
$W^\times_{[2,5]}$	$\left[\begin{smallmatrix}0&0&0&0&1&0\\0&1&*&0&0&*\end{smallmatrix}\right]$		1			$q-1$			$q(q-1)$	$\times q^3(q-1)^2$

Subset	Y	$\mathcal{O}_{1^21^2}$	$\mathcal{O}_{1^211}$	$\mathcal{O}_{1^22}$	$\mathcal{O}_{1111}$	$\mathcal{O}_{112}$	$\mathcal{O}_{22}$	multiplier
$W^\times_{[2,6]}$	$\left[\begin{smallmatrix}0&0&0&0&1&0\\1&0&0&*&0&*\end{smallmatrix}\right]$	1	$q-1$	$q-1$	$\frac{(q-1)^2}{4}$	$\frac{(q-1)^2}{2}$	$\frac{(q-1)^2}{4}$	$\times q^4(q-1)^2$
$W^\times_{[4,4]}$	$\left[\begin{smallmatrix}0&0&0&1&0&*\\0&0&1&0&0&0\end{smallmatrix}\right]$	1	$\frac{q-1}{2}$	$\frac{q-1}{2}$				$\times q^3(q^2-1)(q^2-q)$

As with $2 \otimes \mathrm{Sym}^2(2)$, the counts for each $W^\times$ are equal to the relevant multiplier times those for the associated Y. These reductions are obtained in a very similar manner to those for $2 \otimes \mathrm{Sym}^2(2)$ and so we limit ourselves to an outline of the necessary steps in the more difficult cases.

- $Y_{[1,4]} \ni \left[\begin{smallmatrix} 0&0&0&0&0&0&1\\ 0&0&1&a&0&0&\end{smallmatrix}\right] = (w^2, uw+av^2)$ is in $\mathcal{O}_{C\mathrm{s}}$ if $a = 0$; otherwise, $(w^2, uw+av^2) \sim (w^2, uw+v^2) \in \mathcal{O}_{1^4}$, as was listed in our table of orbital representatives.

- $Y_{[1,5]} \ni \left[\begin{smallmatrix} 0&0&0&0&0&1\\ 0&1&0&0&0&0\end{smallmatrix}\right] = (w^2, uv)$ is in $\mathcal{O}_{1^2 1^2}$. (The reduction, slightly more complicated than previous ones, is most easily verified in the order $\left[\begin{smallmatrix} 0&0&0&0&0&1\\ 0&1&*&*&*&*\end{smallmatrix}\right] = q\left[\begin{smallmatrix} 0&0&0&0&0&1\\ 0&1&0&*&*&*\end{smallmatrix}\right] = q^3\left[\begin{smallmatrix} 0&0&0&0&0&1\\ 0&1&0&0&0&*\end{smallmatrix}\right] = q^4\left[\begin{smallmatrix} 0&0&0&0&0&1\\ 0&1&0&0&0&0\end{smallmatrix}\right]$.)

- $Y_{[1,6]} \ni \left[\begin{smallmatrix} 0&0&0&0&0&1\\ 1&0&0&-a&b&0\end{smallmatrix}\right] = (w^2, u^2 - av^2 + bvw)$ is in $\mathcal{O}_{B11}$ if $a = b = 0$ and is in $\mathcal{O}_{1^4}$ if $a = 0$ but $b \neq 0$. If $a \neq 0$, a routine intersection multiplicity computation establishes that it is either in $\mathcal{O}_{1^2 1^2}$ or in $\mathcal{O}_{2^2}$ according as a is a quadratic residue or non-residue.

- $Y_{[2,4]} \ni \left[\begin{smallmatrix} 0&0&0&0&1&0\\ 0&0&1&a&0&0\end{smallmatrix}\right] = (vw, uw + av^2)$ is in $\mathcal{O}_{C\mathrm{ns}}$ if $a = 0$ and is in $\mathcal{O}_{1^3 1}$ elsewhere. (The reduction may be verified in the order $\left[\begin{smallmatrix} 0&0&0&0&1&*\\ 0&0&1&*&*&*\end{smallmatrix}\right] = q\left[\begin{smallmatrix} 0&0&0&0&1&0\\ 0&0&1&*&*&*\end{smallmatrix}\right] = q^3\left[\begin{smallmatrix} 0&0&0&0&1&0\\ 0&0&1&*&0&0\end{smallmatrix}\right]$.)

- $Y_{[2,5]} \ni \left[\begin{smallmatrix} 0&0&0&0&1&0\\ 0&1&a&0&0&b\end{smallmatrix}\right] = (vw, uv + w(au + bw))$ is in $\mathcal{O}_{C\mathrm{ns}}$ if $a = b = 0$ and is in $\mathcal{O}_{1^3 1}$ if $a = 0$ but $b \neq 0$. If $a \neq 0$, we see that it has three rational zeros $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(b : 0 : -a)$, and thus is in $\mathcal{O}_{1^2 11}$. ($(1 : 0 : 0)$ is the double zero.)

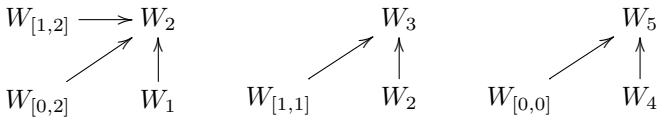
- $Y_{[2,6]} \ni \left[\begin{smallmatrix} 0&0&0&0&1&0\\ 1&0&0&-a&0&-b\end{smallmatrix}\right] = (vw, u^2 - av^2 - bw^2)$ has four common zeros $(\pm\sqrt{a} : 1 : 0), (\pm\sqrt{b} : 0 : 1)$. The multiplicity and rationality are determined by whether a and b are respectively zero, a quadratic residue, or a quadratic non-residue, and we have the counts. (The reduction may be verified in the order $\left[\begin{smallmatrix} 0&0&0&0&1&*\\ 1&*&*&*&*&*\end{smallmatrix}\right] = q\left[\begin{smallmatrix} 0&0&0&0&1&0\\ 1&*&*&*&*&*\end{smallmatrix}\right] = q^3\left[\begin{smallmatrix} 0&0&0&0&1&0\\ 1&0&0&*&*&*\end{smallmatrix}\right] = q^4\left[\begin{smallmatrix} 0&0&0&0&1&0\\ 1&0&0&*&0&*\end{smallmatrix}\right]$.)

- $Y_{[4,4]} \ni \left[\begin{smallmatrix} 0&0&0&1&0&-a\\ 0&0&1&0&0&0\end{smallmatrix}\right] = (v^2 - aw^2, uw)$ is in $\mathcal{O}_{1^2 1^2}$, $\mathcal{O}_{1^2 11}$ or $\mathcal{O}_{1^2 2}$ according as a is zero, a quadratic residue, or a quadratic non-residue.

(II) Secondly, again by the same method, we count for the following five subspaces

$$W_1 := \left[\begin{smallmatrix} 0&0&0&0&0&0\\ 0&0&*&0&*&*\end{smallmatrix}\right], \quad W_2 := \left[\begin{smallmatrix} 0&0&0&0&0&*\\ 0&0&*&0&*&*\end{smallmatrix}\right], \quad W_3 := \left[\begin{smallmatrix} 0&0&*&0&*&*\\ 0&0&*&0&*&*\end{smallmatrix}\right] \quad \text{and} \quad W_4 := \left[\begin{smallmatrix} 0&0&0&0&0&0\\ 0&0&0&*&0&*\end{smallmatrix}\right], \quad W_5 := \left[\begin{smallmatrix} 0&0&0&*&0&*\\ 0&0&0&*&0&*\end{smallmatrix}\right]$$

with the following steps:



Our result is:

Subspace	$\mathcal{O}_0$	$\mathcal{O}_{D1^2}$	$\mathcal{O}_{D11}$	$\mathcal{O}_{C\mathrm{s}}$	$\mathcal{O}_{C\mathrm{ns}}$
$W_1 = \left[\begin{smallmatrix} 0&0&0&0&0&0\\ 0&0&*&0&*&*\end{smallmatrix}\right]$	1	$q-1$	$q(q^2-1)$		
$W_2 = \left[\begin{smallmatrix} 0&0&0&0&0&*\\ 0&0&*&0&*&*\end{smallmatrix}\right]$	1	q^2-1	$q(q^2-1)$	$(q^2-1)(q^2-q)$	
$W_3 = \left[\begin{smallmatrix} 0&0&*&0&*&*\\ 0&0&*&0&*&*\end{smallmatrix}\right]$	1	q^2-1	$q(q^2-1)(q+1)$	$q(q^2-1)^2$	$q^2(q^2-1)(q^2-q)$

Subspace	$\mathcal{O}_0$	$\mathcal{O}_{D1^2}$	$\mathcal{O}_{D11}$	$\mathcal{O}_{D2}$	$\mathcal{O}_{B11}$
$W_4 = \left[\begin{smallmatrix} 0&0&0&0&0&0\\ 0&0&0&*&0&*\end{smallmatrix}\right]$	1	$2(q-1)$	$\frac{1}{2}(q-1)^2$	$\frac{1}{2}(q-1)^2$	
$W_5 = \left[\begin{smallmatrix} 0&0&0&*&0&*\\ 0&0&0&*&0&*\end{smallmatrix}\right]$	1	$2(q^2-1)$	$\frac{1}{2}(q-1)(q^2-1)$	$\frac{1}{2}(q-1)(q^2-1)$	$(q^2-1)(q^2-q)$

The counts for W_1 and W_4 are immediate. To work as before, we define $W_2^\times$, $W_3^\times$ and $W_5^\times$ in the same way:

$$W_2^\times := \left\{\left[\begin{smallmatrix} 0&0&0&0&0&0&a\\ 0&0&b&0&0&c&d\end{smallmatrix}\right] \mid a, b \neq 0\right\},$$

and

$$W_3^\times := \left\{ \left[\begin{smallmatrix} 0&0&a&0&b&c \\ 0&0&d&0&e&f \end{smallmatrix}\right] \;\middle|\; ae-bd\neq 0 \right\}, \quad W_5^\times := \left\{ \left[\begin{smallmatrix} 0&0&0&a&0&b \\ 0&0&0&c&0&d \end{smallmatrix}\right] \;\middle|\; ad-bc\neq 0 \right\}.$$

Then in this case we immediately see that $W_2^\times \subset \mathcal{O}_{C\mathrm{s}}$, $W_3^\times \subset \mathcal{O}_{C\mathrm{ns}}$ and $W_5^\times \subset \mathcal{O}_{B11}$, and thus we have the table.

(III) Thirdly, we count for

$$W_{[5,5]} = \left[\begin{smallmatrix} 0&*&*&*&*&* \\ 0&*&*&*&*&* \end{smallmatrix}\right] \qquad \text{and} \qquad W_6 := \left[\begin{smallmatrix} 0&*&0&*&*&* \\ 0&*&0&*&*&* \end{smallmatrix}\right].$$

For these subspaces, we are counting the number of elements of each $\mathcal{O}_i$ with, respectively, having $[0:0:1]$ as a common zero, and having $[0:1:0]$ and $[0:0:1]$ as common zeros. Let n_i be the number of common zeros of any $x \in \mathcal{O}_i$. Then we have

$$|W_{[5,5]} \cap \mathcal{O}_i| = \frac{n_i}{p^2+p+1}|\mathcal{O}_i|,$$
$$|W_6 \cap \mathcal{O}_i| = \frac{n_i(n_i-1)}{(p^2+p+1)(p^2+p)}|\mathcal{O}_i|.$$

(IV) Finally, we study

$$W_7 := \left[\begin{smallmatrix} 0&0&0&*&*&* \\ *&*&*&0&0&0 \end{smallmatrix}\right].$$

We work directly for this case. Let $x = \left[\begin{smallmatrix} 0&0&0&a&b&c \\ d&e&f&0&0&0 \end{smallmatrix}\right] = (av^2+bvw+cw^2, u(du+ev+fw))$.

- Let $e=f=0$. Then according as $av^2+bvw+cw^2 \in \mathrm{Sym}^2(2)$ is of type $(0),(1^2),(11),(2)$, x is in $\mathcal{O}_0$, $\mathcal{O}_{D1^2}$, $\mathcal{O}_{D11}$, $\mathcal{O}_{D2}$ if $d=0$ and in $\mathcal{O}_{D1^2}$, $\mathcal{O}_{B11}$, $\mathcal{O}_{1^21^2}$, $\mathcal{O}_{2^2}$ if $d\neq 0$.
- Suppose $(e,f)\neq(0,0)$. The subset consists of such x has a (q^2-1)-to-1 map to $Y = \{\left[\begin{smallmatrix} 0&0&0&a&b&c \\ d&0&1&0&0&0 \end{smallmatrix}\right]\}$. We assume $x = (av^2+bvw+cw^2, u(du+w)) \in Y$.
  - Let $a=0$. Then according as $b=c=0$, $b=0$ but $c\neq 0$, $b\neq 0$, x is in $\mathcal{O}_{D11}$, $\mathcal{O}_{C\mathrm{s}}$, $\mathcal{O}_{C\mathrm{ns}}$ if $d=0$ and in $\mathcal{O}_{D11}$, $\mathcal{O}_{B11}$, $\mathcal{O}_{1^211}$ if $d\neq 0$.
  - Let $a\neq 0$. Then according as $av^2+bvw+cw^2$ is of type $(1^2),(11),(2)$, x is in $\mathcal{O}_{1^21^2}$, $\mathcal{O}_{1^211}$, $\mathcal{O}_{1^22}$ if $d=0$ and in $\mathcal{O}_{1^21^2}$, $\mathcal{O}_{1111}$, $\mathcal{O}_{22}$ if $d\neq 0$.

As a result, the number of elements of W_7 in the twenty orbits are respectively counted as

$$1, q^2+q-2, \tfrac{3}{2}(q^3-q), \tfrac{1}{2}q(q-1)^2, 0, (q-1)(q^2-1), (q^2-q)(q^2-1), (q^2-q)(q^2-1), 0,$$
$$0, 0, \tfrac{1}{2}(q^3-q)(2q^2-q-1), \tfrac{1}{2}q(q-1)^3, \tfrac{3}{2}(q^3-q)(q-1)^2, \tfrac{1}{2}(q^3-q)(q-1)^2,$$
$$\tfrac{1}{2}(q^3-q)(q-1)^3, 0, \tfrac{1}{2}(q^3-q)(q-1)^3, 0, 0,$$

where the ordering of the orbits are as in Proposition 21.

Proposition 22 *The vectors* $(|W\cap\mathcal{O}_i|)_i$ *for*

$$W = W_{[0,0]}, W_{[6,6]}; W_{[1,1]}, W_{[5,5]}; W_{[0,4]}, W_{[2,6]}; W_{[0,5]}, W_{[1,6]}; W_{[1,4]}, W_{[2,5]};$$
$$W_{[2,2]}, W_{[4,4]}; W_{[3,3]}, W_3; W_5, W_6; W_{[0,6]}; W_{[1,5]}; W_{[2,4]}; W_7$$

span $\mathbb{R}^{20}$.

Proof: With the twenty vectors ordered as in the table below, one checks one column at a time that the span of the vectors $(|W\cap\mathcal{O}_i|)_i$ for those W listed in the first j columns, includes the characteristic functions of those orbits $\mathcal{O}$ listed beneath them. Since all twenty orbits appear in the table, this gives the proposition.

Subspace added	$W_{[0,0]}$	$W_{[1,1]}$	$W_{[0,4]}, W_{[0,5]}, W_{[0,6]}$	$W_{[2,2]}$	W_3	W_5	$W_{[3,3]}$	
Spanned	$\mathcal{O}_0$	$\mathcal{O}_{D1^2}$	$\mathcal{O}_{D11}, \mathcal{O}_{D1^2}, \mathcal{O}_{D\mathrm{ns}}$	$\mathcal{O}_{C\mathrm{s}}$	$\mathcal{O}_{C\mathrm{ns}}$	$\mathcal{O}_{B11}$	$\mathcal{O}_{B2}$	

$W_{[1,4]}$	$W_{[1,5]}$	$W_{[1,6]}$	$W_{[2,4]}$	$W_{[2,5]}$	$W_{[4,4]}$	$W_{[2,6]}, W_6, W_7$	$W_{[5,5]}$	$W_{[6,6]} = V$
$\mathcal{O}_{1^4}$	$\mathcal{O}_{1^2 1^2}$	$\mathcal{O}_{2^2}$	$\mathcal{O}_{1^3 1}$	$\mathcal{O}_{1^2 11}$	$\mathcal{O}_{1^2 2}$	$\mathcal{O}_{1111}, \mathcal{O}_{112}, \mathcal{O}_{22}$	$\mathcal{O}_{13}$	$\mathcal{O}_4$

For those W listed singly this verification is immediate. For the two groupings of three, we need (and can easily check) that the 3-by-3 matrices obtained from the tables

	$\mathcal{O}_{D11}$	$\mathcal{O}_{D2}$	$\mathcal{O}_{D\mathrm{ns}}$
$W_{[0,4]}$	$\frac{1}{2}q(3q^2-2q-1)$	$\frac{1}{2}q(q-1)^2$	$q^2(q-1)^2$
$W_{[0,5]}$	$\frac{1}{2}q(q^2-1)(2q+1)$	$\frac{1}{2}q(q-1)^2$	$q^2(q-1)(q^2-1)$
$W_{[0,6]}$	$\frac{1}{2}q(q+1)(q^3-1)$	$\frac{1}{2}q(q-1)(q^3-1)$	$q^2(q-1)(q^3-1)$

and

	$\mathcal{O}_{1111}$	$\mathcal{O}_{112}$	$\mathcal{O}_{22}$
$W_{[2,6]}$	$\frac{1}{4}q^4(q-1)^4$	$\frac{1}{2}q^4(q-1)^4$	$\frac{1}{4}q^4(q-1)^4$
W_6	$\frac{12s(4,4,2,2)}{24(p^2+p+1)(p^2+p)}$	$\frac{2s(4,4,2,2)}{4(p^2+p+1)(p^2+p)}$	0
W_7	$\frac{1}{2}(q^3-q)(q-1)^3$	0	$\frac{1}{2}(q^3-q)(q-1)^3$

are invertible. □

Theorem 23 *We have an explicit formula of M. (For typesetting reasons it is given on p. 27, after the bibliography.)*

Acknowledgments

We would like to thank Jan Denef, Yasuhiro Ishitsuka, Kentaro Mitsui, Arul Shankar, Ari Shnidman, Nicolas Templier, and Kota Yoshioka for helpful comments.

This material is based upon work supported by the National Science Foundation under Grant No. DMS-1201330, by the National Security Agency under a Young Investigator Grant, by the JSPS KAKENHI Grant Numbers JP24654005, JP25707002, and by JSPS Joint Research Project with CNRS.

A Invariance of bilinear forms

In this section, we describe a general principle to construct invariant bilinear forms and apply it to show the invariance of the bilinear forms we introduced in this paper.

Let V be a vector space over a field K, with a linear action of a group G. Suppose a bilinear form $[\cdot,\cdot]$ on V and an involution $g \mapsto g^\iota$ on G such that $[gx, g^\iota y] = [x, y]$ hold for all $x, y \in V$ and $g \in G$ are given. Let us consider the outer tensor representation of $\tilde{G} = \mathrm{GL}_n(K) \times G$ on $\tilde{V} = K^n \otimes V$. We regard $\tilde{V}$ as the space of n-tuples of elements in V, and define a bilinear form on it by

$$[x, y]_{\tilde{V}} := \sum_i [x_i, y_i], \qquad x = (x_i), y = (y_i) \in \tilde{V}.$$

Then we have

$$[gx, g^\iota y]_{\tilde{V}} = [x, y]_{\tilde{V}}$$

for all $x, y \in \tilde{V}$ and $g \in \tilde{G}$, where $g^\iota := (g_1^{-T}, g_2^\iota)$ for $g = (g_1, g_2)$. To confirm this, since $(g_1, g_2) = (g_1, 1)(1, g_2)$ and the assertion for $g = (1, g_2)$ is obvious, we may assume $g = (g_1, 1)$. Let $g_1 = (g_{ij}) \in \mathrm{GL}_n(K)$ and

$g_1^{-1} = (h_{ij})$. Then

$$[gx, g^t y]_{\tilde{V}} = \sum_{i,j,k} [g_{ij}x_j, h_{ki}y_k] = \sum_{j,k} [x_j, y_k] \sum_i h_{ki}g_{ij} = \sum_{j,k} [x_j, y_k]\delta_{k,j} = \sum_i [x_i, y_i] = [x, y]_{\tilde{V}},$$

as desired. We also note that if the bilinear form on V is symmetric, then so is the bilinear form on $\tilde{V}$.

We consider the space $n \otimes n = K^n \otimes K^n$ with the action of $\mathrm{GL}_n(K) \times \mathrm{GL}_n(K)$. Let $e_1, \ldots, e_n \in K^n$ be the standard basis of K^n. Then the bilinear form on $n \otimes n$, constructed from the one dimensional trivial representation $(\{\mathrm{id}\}, K)$ with $[x, y] = xy$ as above, is given by

$$[x, y] := \sum_{i,j} x_{ij}y_{ij}$$

for

$$x = \sum_{i,j} x_{ij} e_i \otimes e_j, \quad y = \sum_{i,j} y_{ij} e_i \otimes e_j.$$

Hence this satisfies

$$[gx, g^{-T} y] = [x, y],$$

where $g^{-T} = (g_1^{-T}, g_2^{-T})$ for $g = (g_1, g_2) \in \mathrm{GL}_n(K) \times \mathrm{GL}_n(K)$, and is symmetric.

Let $\mathrm{Sym}_2(n)$ and $\mathrm{Sym}^2(n)$ be the symmetric subspace and symmetric quotient of $n \otimes n$, respectively[2]. The single $\mathrm{GL}_n(K)$ acts on $n \otimes n$ through its diagonal embedding $g \mapsto (g, g)$, and this action is inherited to the actions of $\mathrm{GL}_n(K)$ on $\mathrm{Sym}_2(n)$ and $\mathrm{Sym}^2(n)$. Namely, the linear maps

$$\mathrm{Sym}_2(n) \hookrightarrow n \otimes n \twoheadrightarrow \mathrm{Sym}^2(n)$$

are $\mathrm{GL}_n(K)$-equivariant. Now assume that the characteristic of K is not two. Then the composition of the two maps is an isomorphism. If we identify $\mathrm{Sym}^2(n)$ with $\mathrm{Sym}_2(n)$ via this isomorphism, we have a bilinear form on $\mathrm{Sym}^2(n) = \mathrm{Sym}_2(n)$ by restricting the bilinear form on $n \otimes n$. It is symmetric and satisfies

$$[gx, g^{-T} y] = [x, y],$$

for $x, y \in \mathrm{Sym}^2(n)$ and $g \in \mathrm{GL}_n(K)$.

The space $\mathrm{Sym}^2(n)$ is canonically identified with the space of quadratic forms in variables $v_1, \ldots, v_n$; the monomial $v_i v_j \in \mathrm{Sym}^2(n)$ is the image of $e_i \otimes e_j \in n \otimes n$, and $\mathrm{GL}_n(K)$ acts by the linear change of the variables $v_1, \ldots, v_n$. The inverse image of

$$x(v_1, \ldots, v_n) = \sum_{i \le j} x_{ij} v_i v_j \in \mathrm{Sym}^2(n)$$

in $\mathrm{Sym}_2(n)$ via the isomorphism above is

$$\sum_i x_{ii} \cdot e_i \otimes e_i + \sum_{i<j} \frac{x_{ij}}{2} \cdot (e_i \otimes e_j + e_j \otimes e_i),$$

so the bilinear form on $\mathrm{Sym}^2(n)$ is given by

$$[x, y] := \sum_i x_{ii}y_{ii} + \frac{1}{2} \sum_{i<j} x_{ij}y_{ij}$$

for

$$x = \sum_{i \le j} x_{ij} v_i v_j, \quad y = \sum_{i \le j} y_{ij} v_i v_j,$$

[2]By definition, $\mathrm{Sym}_2(n)$ is the subspace of $n \otimes n$ invariant under the flip $x \otimes y \mapsto y \otimes x$, and $\mathrm{Sym}^2(n)$ is the quotient of $n \otimes n$ by the subspace which is generated by elements of the form $x \otimes y - y \otimes x$.

and this satisfies $[gx, g^{-T}y] = [x, y]$ for $g \in \mathrm{GL}_n(K)$.

Similarly, the composition

$$\mathrm{Sym}_3(2) \hookrightarrow 2 \otimes 2 \otimes 2 \twoheadrightarrow \mathrm{Sym}^3(2)$$

is an isomorphism if the characteristic of K is not three. The symmetric bilinear form on the space of binary cubic forms $\mathrm{Sym}^3(2)$ induced from $\mathrm{Sym}_3(2) \subset 2 \otimes 2 \otimes 2$ is

$$[x, y] = x_1y_1 + \frac{1}{3}x_2y_2 + \frac{1}{3}x_3y_3 + x_4y_4$$

for

$$x(u, v) = x_1u^3 + x_2u^2v + x_3uv^2 + x_4v^3, \quad y(u, v) = y_1u^3 + y_2u^2v + y_3uv^2 + y_4v^3,$$

and this satisfies $[gx, g^{-T}y] = [x, y]$ for $g \in \mathrm{GL}_2(K)$.

Thus we in particular have shown that the symmetric bilinear forms we introduced for the spaces $\mathrm{Sym}^2(2)$, $\mathrm{Sym}^2(3)$, $2 \otimes \mathrm{Sym}^2(2)$, $2 \otimes \mathrm{Sym}^2(3)$ and $\mathrm{Sym}^3(2)$ all satisfy $[gx, g^{-T}y] = [x, y]$.

References

[BBP10] Karim Belabas, Manjul Bhargava, and Carl Pomerance. Error estimates for the Davenport-Heilbronn theorems. *Duke Math. J.*, 153(1):173–210, 2010.

[BF99] K. Belabas and E. Fouvry. Sur le 3-rang des corps quadratiques de discriminant premier ou presque premier. *Duke Math. J.*, 98(2):217–268, 1999.

[Bha04] Manjul Bhargava. Higher composition laws. III. The parametrization of quartic rings. *Ann. of Math. (2)*, 159(3):1329–1360, 2004.

[Bha05] Manjul Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math. (2)*, 162(2):1031–1063, 2005.

[Bha10] Manjul Bhargava. The density of discriminants of quintic rings and fields. *Ann. of Math. (2)*, 172(3):1559–1591, 2010.

[BST13] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman. On the Davenport-Heilbronn theorems and second order terms. *Invent. Math.*, 193(2):439–499, 2013.

[DG98] Jan Denef and Akihiko Gyoja. Character sums associated to prehomogeneous vector spaces. *Compositio Math.*, 113(3):273–346, 1998.

[DH71] 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.

[DW86] Boris Datskovsky and David J. Wright. The adelic zeta function associated to the space of binary cubic forms. II. Local theory. *J. Reine Angew. Math.*, 367:27–75, 1986.

[Elk13] N. Elkies. *The rationality of conics over finite fields (And an introduction to rational normal curves and classical Goppa codes)*, 2013. Lecture notes, available at `http://www.math.harvard.edu/~elkies/M256.13/conicfq.pdf`.

[FK01] E. Fouvry and N. Katz. A general stratification theorem for exponential sums, and applications. *J. Reine Angew. Math.*, 540:115–166, 2001.

[Mor10] Shingo Mori. Orbital Gauss sums associated with the space of binary cubic forms over a finite field. *RIMS Kôkyûroku*, 1715:32–36, 2010.

[Nak98] Jin Nakagawa. On the relations among the class numbers of binary cubic forms. *Invent. Math.*, 134(1):101–138, 1998.

[Ohn97] Yasuo Ohno. A conjecture on coincidence among the zeta functions associated with the space of binary cubic forms. *Amer. J. Math.*, 119(5):1083–1094, 1997.

[PG14] The PARI Group. *PARI/GP version* `2.8.0`. Bordeaux, 2014. Available from `http://pari.math.u-bordeaux.fr/`.

[Sat90] Mikio Sato. Theory of prehomogeneous vector spaces (algebraic part)—the English translation of Sato's lecture from Shintani's note. *Nagoya Math. J.*, 120:1–34, 1990. Notes by Takuro Shintani, Translated from the Japanese by Masakazu Muro.

[Shi72] Takuro Shintani. On Dirichlet series whose coefficients are class numbers of integral binary cubic forms. *J. Math. Soc. Japan*, 24:132–188, 1972.

[ST14] Arul Shankar and Jacob Tsimerman. Counting S_5-fields with a power saving error term. *Forum Math. Sigma*, 2:e13, 8, 2014.

[TT] Takashi Taniguchi and Frank Thorne. *Levels of distribution for sieve problems in prehomogeneous vector spaces*. In preparation.

[TT13a] Takashi Taniguchi and Frank Thorne. Orbital L-functions for the space of binary cubic forms. *Canad. J. Math.*, 65(6):1320–1383, 2013.

[TT13b] Takashi Taniguchi and Frank Thorne. Secondary terms in counting functions for cubic fields. *Duke Math. J.*, 162(13):2451–2508, 2013.

[Wri85] David J. Wright. The adelic zeta function associated to the space of binary cubic forms. I. Global theory. *Math. Ann.*, 270(4):503–534, 1985.

[WY92] David J. Wright and Akihiko Yukie. Prehomogeneous vector spaces and field extensions. *Invent. Math.*, 110(2):283–314, 1992.

Theorem *The matrix $q^{12}M$ of Theorem 23 is as follows, with $[abc] := (q-1)^a q^b (q+1)^c$ and $\phi_2 := q^2+q+1$:*

$$\left[\begin{array}{cccccccccc}
1 & [101]\phi_2 & \frac{1}{2}[112]\phi_2 & \frac{1}{2}[211]\phi_2 & [221]\phi_2 & [212]\phi_2 & [231]\phi_2 & \frac{1}{2}[222]\phi_2 & \frac{1}{2}[321]\phi_2 & [322]\phi_2 \\
1 & d_1 & \frac{1}{2}[111]c_8 & -\frac{1}{2}[111] & [120]d_1 & [111]d_1 & [232] & -\frac{1}{2}[122] & -\frac{1}{2}[221] & -[222] \\
1 & [100]c_8 & \frac{1}{2}[010]e_3 & \frac{1}{2}[212] & [120]d_1 & [110]d_{10} & [130]c_3 & \frac{1}{2}[220]c_{12} & \frac{1}{2}[220]c_1 & [221]c_1 \\
1 & -[001] & \frac{1}{2}[113] & \frac{1}{2}[010]e_1 & [120]d_1 & -[112] & [231] & -\frac{1}{2}[121]\phi_2 & \frac{1}{2}[121]c_2 & -[221]\phi_2 \\
1 & d_1 & \frac{1}{2}[011]d_1 & \frac{1}{2}[110]d_1 & [020]e_2 & -[112] & -[131] & -\frac{1}{2}[122] & -\frac{1}{2}[221] & [121] \\
1 & d_1 & \frac{1}{2}[010]d_{10} & -\frac{1}{2}[111] & -[121] & [010]e_4 & [130]c_1 & \frac{1}{2}[120]d_5 & \frac{1}{2}[120]d_2 & -[120]c_1 \\
1 & [102] & \frac{1}{2}[011]c_3 & \frac{1}{2}[211] & -[121] & [111]c_1 & -[030]b_{-2} & \frac{1}{2}[222] & \frac{1}{2}[321] & -[221] \\
1 & -[001] & \frac{1}{2}[110]c_{12} & -\frac{1}{2}[110]\phi_2 & -[121] & [110]d_5 & [231] & -\frac{1}{2}[020]d_3 & -\frac{1}{2}[221] & [121] \\
1 & -[001] & \frac{1}{2}[011]c_1 & \frac{1}{2}[011]c_2 & -[121] & [011]d_2 & [231] & -\frac{1}{2}[122] & -\frac{1}{2}[020]d_4 & [121] \\
1 & -[001] & \frac{1}{2}[011]c_1 & -\frac{1}{2}[110]\phi_2 & [020] & -[010]c_1 & -[130] & \frac{1}{2}[021] & \frac{1}{2}[120] & -[020] \\
1 & c_1 & -\frac{1}{2}[010]a_7 & -\frac{1}{2}[110] & [020] & [010]d_7 & -[030]a_1 & -\frac{1}{2}[121] & -\frac{1}{2}[220] & [120]b_1 \\
1 & c_1 & \frac{1}{2}[010]d_6 & -\frac{1}{2}[110]b_1 & -[120] & [110]c_3 & -2[130] & -\frac{1}{2}[121] & -\frac{1}{2}[220] & -[220] \\
1 & -\phi_2 & \frac{1}{2}[112] & -\frac{1}{2}[010]d_3 & -[120] & -[112] & 0 & \frac{1}{2}[022] & \frac{1}{2}[121] & [121] \\
1 & [100]a_4 & \frac{1}{2}[010]c_6 & \frac{1}{2}[210] & -[120] & [010]d_9 & -[030]a_2 & -\frac{1}{2}[120] & -\frac{1}{2}[120]a_3 & [320] \\
1 & -[001] & \frac{1}{2}[010]c_3 & \frac{1}{2}[010]b_1 & -[120] & [010]d_7 & -[130] & -\frac{1}{2}[120]a_4 & \frac{1}{2}[120] & -[221] \\
1 & c_{10} & \frac{1}{2}[010]c_9 & \frac{1}{2}[110]a_3 & -[020]a_3 & -[010]a_3a_7 & 4[030] & \frac{1}{2}[020]c_{11} & -\frac{1}{2}[120]a_6 & -[020]a_3a_6 \\
1 & c_1 & -\frac{1}{2}[010]a_7 & -\frac{1}{2}[110] & [020] & -[110]a_4 & 2[030] & -\frac{1}{2}[121] & \frac{1}{2}[020]c_4 & [120] \\
1 & -\phi_2 & \frac{1}{2}[110]a_4 & \frac{1}{2}[010]c_7 & -[020]a_3 & -[110]a_4 & 0 & -\frac{1}{2}[020]c_3 & \frac{1}{2}[121] & [021]a_3 \\
1 & -[001] & -\frac{1}{2}[012] & -\frac{1}{2}[111] & [021] & [011] & [030] & \frac{1}{2}[021] & \frac{1}{2}[120] & -[021] \\
1 & -\phi_2 & -\frac{1}{2}[011] & \frac{1}{2}[011] & [020] & [011] & 0 & \frac{1}{2}[022] & -\frac{1}{2}[020]b_1 & -[021]
\end{array}\right.$$

$$\left.\begin{array}{cccccccccc}
[332]\phi_2 & \frac{1}{2}[242]\phi_2 & \frac{1}{2}[341]\phi_2 & \frac{1}{2}[342]\phi_2 & \frac{1}{2}[342]\phi_2 & \frac{1}{24}[442]\phi_2 & \frac{1}{4}[442]\phi_2 & \frac{1}{8}[442]\phi_2 & \frac{1}{3}[442]\phi_2 & \frac{1}{4}[442]\phi_2 \\
[231]c_1 & \frac{1}{2}[141]c_1 & -\frac{1}{2}[240]\phi_2 & \frac{1}{2}[341]a_4 & -\frac{1}{2}[242] & \frac{1}{24}[341]c_{10} & \frac{1}{4}[341]c_1 & -\frac{1}{8}[341]\phi_2 & -\frac{1}{3}[342] & -\frac{1}{4}[341]\phi_2 \\
-[230]a_7 & \frac{1}{2}[140]d_6 & \frac{1}{2}[341] & \frac{1}{2}[240]c_6 & \frac{1}{2}[240]c_3 & \frac{1}{24}[340]c_9 & -\frac{1}{4}[340]a_7 & \frac{1}{8}[440]a_4 & -\frac{1}{3}[342] & -\frac{1}{4}[341] \\
-[231] & -\frac{1}{2}[141]b_1 & -\frac{1}{2}[140]d_3 & \frac{1}{2}[341] & \frac{1}{2}[141]b_1 & \frac{1}{24}[341]a_3 & -\frac{1}{4}[341] & \frac{1}{8}[241]c_7 & -\frac{1}{3}[342] & \frac{1}{4}[242] \\
[131] & -\frac{1}{2}[141] & -\frac{1}{2}[240] & -\frac{1}{2}[241] & -\frac{1}{2}[241] & -\frac{1}{24}[241]a_3 & \frac{1}{4}[241] & -\frac{1}{8}[241]a_3 & \frac{1}{3}[242] & \frac{1}{4}[241] \\
[130]d_7 & \frac{1}{2}[140]c_3 & -\frac{1}{2}[241] & \frac{1}{2}[140]d_9 & \frac{1}{2}[140]d_7 & -\frac{1}{24}[240]a_3a_7 & -\frac{1}{4}[340]a_4 & -\frac{1}{8}[340]a_4 & \frac{1}{3}[241] & \frac{1}{4}[241] \\
-[131]a_1 & -[141] & 0 & -\frac{1}{2}[141]a_2 & -\frac{1}{2}[241] & \frac{1}{6}[241] & \frac{1}{2}[241] & 0 & \frac{1}{3}[241] & 0 \\
-[231] & -\frac{1}{2}[141] & \frac{1}{2}[141] & -\frac{1}{2}[240] & -\frac{1}{2}[240]a_4 & \frac{1}{24}[240]c_{11} & -\frac{1}{4}[341] & -\frac{1}{8}[240]c_3 & \frac{1}{3}[241] & \frac{1}{4}[242] \\
-[231] & -\frac{1}{2}[141] & \frac{1}{2}[141] & -\frac{1}{2}[141]a_3 & \frac{1}{2}[141] & -\frac{1}{24}[241]a_6 & \frac{1}{4}[141]c_4 & \frac{1}{8}[242] & \frac{1}{3}[241] & -\frac{1}{4}[141]b_1 \\
[130]b_1 & -\frac{1}{2}[140] & \frac{1}{2}[140] & \frac{1}{2}[340] & -\frac{1}{2}[241] & -\frac{1}{24}[140]a_3a_6 & \frac{1}{4}[240] & \frac{1}{8}[141]a_3 & -\frac{1}{3}[141] & -\frac{1}{4}[141] \\
[030]d_8 & -[140] & 0 & -\frac{1}{2}[140]a_5 & \frac{1}{2}[140] & \frac{1}{6}[140]a_3 & -\frac{1}{2}[140] & 0 & -\frac{1}{3}[141] & 0 \\
-2[230] & \frac{1}{2}[040]c_5 & -\frac{1}{2}[240] & -[140]a_1 & [140] & \frac{1}{4}[240] & \frac{1}{2}[240] & \frac{1}{4}[240] & 0 & 0 \\
0 & -\frac{1}{2}[141] & \frac{1}{2}[040]b_{-3} & 0 & [141] & 0 & 0 & -\frac{1}{2}[141] & 0 & -\frac{1}{2}[141] \\
-[130]a_5 & -[040]a_1 & 0 & \frac{1}{2}[040]a_8 & \frac{1}{2}[140] & -\frac{1}{2}[140] & -\frac{1}{2}[140] & 0 & 0 & 0 \\
[130] & [040] & [140] & \frac{1}{2}[140] & \frac{1}{2}[040]a_2 & 0 & -\frac{1}{2}[140] & -\frac{1}{2}[140] & 0 & 0 \\
4[030]a_3 & 3[040] & 0 & -6[040] & 0 & \frac{1}{24}[040]b_{23} & -\frac{1}{4}[141] & \frac{1}{8}[141] & \frac{1}{3}[141] & -\frac{1}{4}[141] \\
-2[030] & [040] & 0 & -[040] & -[040] & -\frac{1}{24}[141] & \frac{1}{4}[040]b_3 & -\frac{1}{8}[141] & -\frac{1}{3}[141] & \frac{1}{4}[141] \\
0 & [040] & -2[040] & 0 & -2[040] & \frac{1}{24}[141] & -\frac{1}{4}[141] & \frac{1}{8}[040]b_7 & \frac{1}{3}[141] & -\frac{1}{4}[141] \\
-[031] & 0 & 0 & 0 & 0 & \frac{1}{24}[141] & -\frac{1}{4}[141] & \frac{1}{8}[141] & \frac{1}{3}[040]b_2 & -\frac{1}{4}[141] \\
0 & 0 & -[040] & 0 & 0 & -\frac{1}{24}[141] & \frac{1}{4}[141] & -\frac{1}{8}[141] & -\frac{1}{3}[141] & \frac{1}{4}[040]b_3
\end{array}\right].$$

Here a_i, b_i, c_i, d_i and e_i are irreducible integral polynomials in q, defined by $b_i = b^2 + i$ and

$$\begin{array}{llll}
a_1 = q-2, & c_1 = q^2-q-1, & d_1 = q^3-q-1, & e_1 = q^4+1, \\
a_2 = q-3, & c_2 = q^2-q+1, & d_2 = q^3-q^2+1, & e_2 = q^4-q^3+1, \\
a_3 = 2q-1, & c_3 = q^2-2q-1, & d_3 = q^3-q^2-q-1, & e_3 = q^4+2q^3-2q^2-2q-1, \\
a_4 = 2q+1, & c_4 = q^2+2q-1, & d_4 = q^3+q^2-q+1, & e_4 = 2q^4-2q^3-q^2+q+1. \\
a_5 = 2q-3, & c_5 = q^2-2q+3, & d_5 = q^3-q^2-2q-1, & \\
a_6 = 3q-1, & c_6 = q^2-4q-1, & d_6 = q^3+q^2-3q-1, & \\
a_7 = 3q+1, & c_7 = 2q^2+q+1, & d_7 = q^3-2q^2+q+1, & \\
a_8 = 5q-7, & c_8 = 2q^2+2q+1, & d_8 = q^3-2q^2+2q-2, & \\
 & c_9 = 2q^2-5q-1, & d_9 = q^3-4q^2+q+1, & \\
 & c_{10} = 3q^2-q-1, & d_{10} = 2q^3-q^2-2q-1, & \\
 & c_{11} = 3q^2-2q+1, & & \\
 & c_{12} = 3q^2+3q+1, & &
\end{array}$$