TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 370, Number 4, April 2018, Pages 2537–2561
http://dx.doi.org/10.1090/tran/7089
Article electronically published on November 28, 2017

TRACES OF HECKE OPERATORS AND REFINED WEIGHT ENUMERATORS OF REED-SOLOMON CODES

NATHAN KAPLAN AND IAN PETROW

Abstract. We study the quadratic residue weight enumerators of the dual projective Reed-Solomon codes of dimensions 5 and $q-4$ over the finite field $\mathbb{F}_q$. Our main results are formulas for the coefficients of the quadratic residue weight enumerators for such codes. If $q=p^v$ and we fix v and vary p, then our formulas for the coefficients of the dimension $q-4$ code involve only polynomials in p and the trace of the q^{th} and $(q/p^2)^{\text{th}}$ Hecke operators acting on spaces of cusp forms for the congruence groups $\mathrm{SL}_2(\mathbb{Z}), \Gamma_0(2)$, and $\Gamma_0(4)$. The main tool we use is the Eichler-Selberg trace formula, which gives along the way a variation of a theorem of Birch on the distribution of rational point counts for elliptic curves with prescribed 2-torsion over a fixed finite field.

1. Introduction

The main goal of this paper is to show how traces of Hecke operators for the congruence subgroups $\mathrm{SL}_2(\mathbb{Z}), \Gamma_0(2)$ and $\Gamma_0(4) \cong \Gamma(2)$ enter into formulas for certain weight enumerators attached to classical and projective Reed-Solomon codes. We study a refinement of the Hamming weight enumerator, which we call the *quadratic residue weight enumerator*. We prove a variation of the MacWilliams theorem for it, which follows in a straightforward way from the analogous MacWilliams theorem for the complete weight enumerator.

Projective and classical Reed-Solomon codes are maximum distance separable, which means that their Hamming weight enumerators are completely understood. We compute the quadratic residue weight enumerator of the 5-dimensional projective Reed-Solomon code, which leads directly to the corresponding weight enumerator of the 5-dimensional classical Reed-Solomon code of length q over the finite field $\mathbb{F}_q$. By applying our version of the MacWilliams theorem we deduce formulas for individual coefficients of the quadratic residue weight enumerator of the projective Reed-Solomon code of dimension $q-4$ and for the corresponding classical Reed-Solomon code. One of the main points of this paper is to demonstrate that there are interesting cases in which refined weight enumerators can be computed explicitly, giving additional information about rational point count distributions for varieties coming from well-studied codes. This addresses a particular case of Research Problem 11.2 of [18] about refined weight enumerators of Reed-Solomon codes.

This paper fits into a literature about how weight enumerators of algebraically constructed codes can be expressed in terms of number-theoretic functions. For a

Received by the editors September 25, 2015, and, in revised form, July 15, 2016.
2010 *Mathematics Subject Classification.* Primary 11T71; Secondary 11F25, 11G20, 94B27.
The second author was partially supported by Swiss National Science Foundation grant 200021-137488 and an AMS-Simons Travel Grant.

©2017 American Mathematical Society

broad overview of these types of connections, focusing on codes and exponential sums over finite fields, see the survey of Hurt [10]. Most directly related to our work is the detailed analysis of Zetterberg and Melas codes given in [9, 23]. These codes are related to certain families of genus one curves over finite fields, and the Eichler-Selberg trace formula for $\Gamma_1(4)$ is the main tool in the proofs. While these earlier families are considered only in characteristic 2 and 3, we consider codes in all characteristics not equal to 2, and every isomorphism class of an elliptic curve over $\mathbb{F}_q$ contributes to the refined weight enumerators that we consider. In [22], Schoof notes that the appearance of Hecke operators acting on cusp forms for $\Gamma_1(4)$ in the formulas for these weight enumerators is "probably related" to the fact that the curves in the families considered have a rational point of order 4, but does not give a "direct connection". In our analysis of the quadratic residue weight enumerator the connection to rational 2-torsion points on elliptic curves is made much more explicit.

We also note that the quadratic residue weight enumerator has appeared previously, for example in Section 5.8 of [20], where it is used to study Hermitian self-dual codes over $\mathbb{F}_9$. However, we are unaware of any previous work connecting the coefficients of this weight enumerator to number theory.

1.1. **Reed-Solomon codes and weight enumerators.** Projective Reed-Solomon codes are constructed by evaluating each element of the $\mathbb{F}_q$-vector space of homogeneous polynomials of degree h in two variables at an affine representative of each of the $q+1$ $\mathbb{F}_q$-rational points of $\mathbb{P}^1$. More precisely, take the standard choice of affine representatives $(1, a)$ where $a \in \mathbb{F}_q$ together with $(0, 1)$ under some fixed ordering $p_1, \dots, p_{q+1}$, and consider the evaluation map defined by

$$f \mapsto (f(p_1), \dots, f(p_{q+1})) \in \mathbb{F}_q^{q+1}.$$

For $h \leq q$ the image of this map is an $(h+1)$-dimensional linear subspace of $\mathbb{F}_q^{q+1}$ called the *projective Reed-Solomon code*, or sometimes the doubly extended Reed-Solomon code, of order h. A key observation is that a different choice of affine representatives gives an equivalent code, i.e., the same up to scaling and permuting coordinates. We denote this code by $C_{1,h}$. Choosing a different ordering of the points also gives an equivalent code. Puncturing such a code at one point, that is, deleting a fixed coordinate from each codeword, gives the classical, or affine, Reed-Solomon code of length q.

One reason why Reed-Solomon codes have received so much attention is that their minimal distance is as large as possible given their length and dimension. The *Hamming distance* on $\mathbb{F}_q^n$ between $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ is defined

$$d(x, y) \stackrel{\text{def}}{=} \#\left\{i \in [1, n] \;\; \textit{such that } x_i \neq y_i\right\},$$

and the *weight*, $\mathrm{wt}(x)$, of x is the number of non-zero coordinates of x. That is, $\mathrm{wt}(\cdot)$ is a norm on $\mathbb{F}_q^n$, and the Hamming distance is the induced metric. The *minimal distance* of a code C is $\min_{c_1 \neq c_2 \in C} d(c_1, c_2)$. For a linear code, the minimal distance is equal to the minimal weight of a non-zero codeword. The Singleton bound [18, Ch. 1, Thm. 9] states that the maximum size of a code $C \subseteq \mathbb{F}_q^n$ with minimum distance d is $q^{n-(d-1)}$. A code for which equality holds is called *maximal distance separable* or *MDS*. A non-zero degree h form on $\mathbb{P}^1$ vanishes at no more than h distinct $\mathbb{F}_q$-rational points, implying that for $h \leq q$ the code $C_{1,h}$ has minimum distance $q + 1 - h$ and is therefore MDS.

In order to analyze rational point count distributions for families of varieties, we would like to have a deeper understanding of the associated codes beyond their minimal distances. The *Hamming weight enumerator* of C is a homogeneous polynomial in two variables that keeps track of the number of codewords of C of each weight. Given a code $C \subset \mathbb{F}_q^n$ we define

$$W_C(X,Y) \stackrel{\text{def}}{=} \sum_{c \in C} X^{n-\text{wt}(c)} Y^{\text{wt}(c)} = \sum_{i=0}^{n} A_i X^{n-i} Y^i,$$

where $A_i = \#\{c \in C \ : \ \text{wt}(c) = i\}$. The discussion above shows that the weight enumerator of $C_{1,h}$ does not depend on the choice of affine representatives. The weight enumerator of an MDS code of length n over $\mathbb{F}_q$ is uniquely determined and easily computed. See Corollary 5 of Chapter 11 of [18].

We study a refinement of the Hamming weight enumerator that carries additional information about the non-zero coordinates of codewords. The *quadratic residue weight enumerator* of $C \subset \mathbb{F}_q$ is defined by

$$\text{QR}_C(X,Y,Z) \stackrel{\text{def}}{=} \sum_{c \in C} X^{n-\text{wt}(c)} Y^{\text{res}(c)} Z^{\text{nres}(c)} = \sum_{\substack{i,j,k \geq 0 \\ i+j+k=q+1}} A_{i,j,k} X^i Y^j Z^k,$$

where $\text{res}(c)$ denotes the number of coordinates of c that are non-zero squares in $\mathbb{F}_q$, $\text{nres}(c)$ denotes the number of coordinates that are not squares, and $A_{i,j,k}$ denotes the number of codewords $c \in C$ with $\text{res}(c) = j$ and $\text{nres}(c) = k$. When h is even $\text{QR}_{C_{1,h}}(X,Y,Z)$ is well-defined since choosing a different affine representative for a projective point corresponds to multiplying the corresponding coordinate of each codeword by the same non-zero quadratic residue.

A main result (Theorem 4) of this paper is the computation of $\text{QR}_{C_{1,4}}(X,Y,Z)$ by a slight refinement of the methods of [5] and [21]. The coefficients of this weight enumerator solve an enumerative problem about elliptic curves. The coefficient $A_{i,j,k}$ is equal to the number of homogeneous quartic polynomials $f_4(x,y)$ such that the variety defined by $w^2 = f_4(x,y)$ has exactly $i + 2j$ $\mathbb{F}_q$-rational points, i of which come from roots of f_4. This is related to counting elliptic curves over $\mathbb{F}_q$ with a specified number of rational points and a specified number of rational 2-torsion points. See Section 2.1 for details.

In order to give the statement of our main result we introduce one additional important concept from coding theory, the dual code of a linear code. Given $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{F}_q^n$ we define a non-degenerate symmetric bilinear pairing $\mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ by

$$\langle x, y \rangle \stackrel{\text{def}}{=} \sum_{i=1}^{n} x_i y_i \in \mathbb{F}_q$$

and the *dual code* of a linear code C to be

$$C^{\perp} \stackrel{\text{def}}{=} \left\{ y \in \mathbb{F}_q^n \ \mid \ \langle x, y \rangle = 0 \ \forall \ x \in \mathbb{F}_q^n \right\}.$$

The MacWilliams theorem [18, Ch. 5, Thm. 13] says that the weight enumerator of C determines the weight enumerator of $C^{\perp}$.

Theorem 1 (MacWilliams)**.** *Let $C \subseteq \mathbb{F}_q^n$ be a linear code. Then*

$$W_{C^{\perp}}(X,Y) = \frac{1}{|C|} W_C(X + (q-1)Y, X - Y).$$

It is well known that the dual of an MDS code is MDS and moreover that the dual of a Reed-Solomon code is also a Reed-Solomon code. More specifically, for $h \leq q$, $C_{1,h}^{\perp} = C_{1,q-h-1}$. See [18, Ch. 11, Thm. 2] for details.

1.2. **Main results.** We use our computation of the quadratic residue weight enumerator of $C_{1,4}$ combined with a variation of the MacWilliams theorem to show that the coefficients of the quadratic residue weight enumerator of $C_{1,q-5}$ can be expressed in terms of traces of Hecke operators acting on spaces of cusp forms for the congruence subgroups $\mathrm{SL}_2(\mathbb{Z}), \Gamma_0(2)$, and $\Gamma_0(4)$. Let $\mathbb{Q}[x]$ denote the polynomial ring. Let v, R, N be integers, $v, N \geq 1$ and $R \geq 0$. Let $M_{v,R}(N)$ denote the set of functions on odd v^{th} prime powers $q = p^v$ of the form

$$\sum_{\substack{k=2 \\ k \equiv 0 \pmod 2}}^{2R+2} \left(g_{k,1}(p) \mathrm{tr}_{\Gamma_0(N),k} T_q + g_{k,2}(p) \mathrm{tr}_{\Gamma_0(N),k} T_{q/p^2} \right),$$

where each $g_{k,1}, g_{k,2} \in \mathbb{Q}[x]$ and we interpret $\mathrm{tr}_{\Gamma_0(N),k} T_{q/p^2}$ as 0 unless $p^3 \mid q$. We also let M_v denote the set of functions on odd v^{th} prime powers $q = p^v$ of the form $g(p)$ for some $g \in \mathbb{Q}[x]$. Note that the $M_{v,R}(N)$ and M_v have the structure of $\mathbb{Q}[x]$-modules. In what follows, all sums of modules take place within the $\mathbb{Q}[x]$-module of *all* functions on odd v^{th} prime powers.

Theorem 2. *Let v be a fixed positive integer. For fixed non-negative integers j and k consider the coefficient $A_{q+1-j-k,j,k}$ of $\mathrm{QR}_{C_{1,q-5}}(X,Y,Z)$ as a function on v^{th} powers of odd primes, $q=p^v$. For each fixed residue class of $q \pmod 4$, $A_{q+1-j-k,j,k}$ is given by polynomials in p and traces of Hecke operators. More precisely, for each fixed v, j, k and $\epsilon \in \{\pm 1\}$, there exists*

$$h \in M_v + M_{v,\lfloor \frac{j+k}{2} \rfloor}(1) + M_{v,\lfloor \frac{j+k-2}{2} \rfloor}(2) + M_{v,\lfloor \frac{j+k-3}{2} \rfloor}(4)$$

such that $A_{q+1-j-k,j,k} = h(q)$ for all v^{th} powers of odd primes $q = p^v$ satisfying $q \equiv \epsilon \pmod 4$.

Example 1. When $q = p \equiv 1 \pmod 4$ is a prime we find

$$\begin{aligned}
&\mathrm{QR}_{C_{1,q-5}}(X,Y,Z) \\
&= X^{q+1} + (q-1)^2 q(q+1) \Bigg(\frac{1}{23040}(q^2 - 6q + 53)(q-3) X^{q-5} \left(Y^6 + Z^6\right) \\
&\quad + \frac{1}{1536}(q-1)(q-3)(q-5) X^{q-5} \left(Y^4 Z^2 + Y^2 Z^4\right) \\
&\quad + \frac{1}{645120} \left(q^5 - 20q^4 + 120q^3 - 860q^2 + 6154q - 13005 - 35 \mathrm{tr}_{\Gamma_0(4),6} T_q\right) X^{q-6} \left(Y^7 + Z^7\right) \\
&\quad + \frac{1}{92160}(q^5 - 20q^4 + 160q^3 - 660q^2 + 1274q - 765 + 5 \mathrm{tr}_{\Gamma_0(4),6} T_q) X^{q-6} \left(Y^6 Z + Y Z^6\right) \\
&\quad + \frac{1}{30720}(q^5 - 20q^4 + 160q^3 - 660q^2 + 1274q - 765 + 5 \mathrm{tr}_{\Gamma_0(4),6} T_q) X^{q-6} \left(Y^5 Z^2 + Y^2 Z^5\right) \\
&\quad + \frac{1}{18432}(q^5 - 20q^4 + 152q^3 - 508q^2 + 714q - 333 - 3 \mathrm{tr}_{\Gamma_0(4),6} T_q) X^{q-6} \left(Y^4 Z^3 + Y^3 Z^4\right) \\
&\quad + O(X^{q-7}) \Bigg).
\end{aligned}$$

Example 2. When $q = p \equiv 3 \pmod 4$ is a prime ≥ 7 we find

$$\begin{aligned}
&\mathrm{QR}_{C_{1,q-5}}(X,Y,Z) \\
&= X^{q+1} + (q-1)^2 q(q+1)\Bigg(\frac{1}{3840}(q+1)(q-3)(q-7)X^{q-5}\left(Y^5Z + YZ^5\right) \\
&\quad + \frac{1}{1152}(q^2-6q+17)(q-3)X^{q-5}Y^3Z^3 \\
&\quad + \frac{1}{645120}(q^5 - 20q^4 + 120q^3 - 20q^2 - 566q - 405 - 35\mathrm{tr}_{\Gamma_0(4),6}T_q)X^{q-6}\left(Y^7 + Z^7\right) \\
&\quad + \frac{1}{92160}(q^5 - 20q^4 + 160q^3 - 540q^2 + 314q + 1035 + 5\mathrm{tr}_{\Gamma_0(4),6}T_q)X^{q-6}\left(Y^6Z + YZ^6\right) \\
&\quad + \frac{1}{30720}(q^5 - 20q^4 + 160q^3 - 540q^2 + 314q + 1035 + 5\mathrm{tr}_{\Gamma_0(4),6}T_q)X^{q-6}\left(Y^5Z^2 + Y^2Z^5\right) \\
&\quad + \frac{1}{18432}(q^5 - 20q^4 + 152q^3 - 628q^2 + 1674q - 2133 - 3\mathrm{tr}_{\Gamma_0(4),6}T_q)X^{q-6}\left(Y^4Z^3 + Y^3Z^4\right) \\
&\quad + O(X^{q-7})\Bigg).
\end{aligned}$$

Remarks.

(1) The above formulas match with an explicit brute-force computation of $\mathrm{QR}_{C_{1,q-5}}(X,Y,Z)$ for small values of q.
(2) There are actions of $\mathrm{PGL}_2(\mathbb{F}_q)$ and of $\mathbb{F}_q^*$ on non-zero codewords of $C_{1,q-5}$, so it is clear up to factors of 2 or 3 that $(q-1)^2q(q+1)$ divides all of the quadratic residue weight enumerator coefficients after the first.
(3) The denominators in the above example arise essentially only from the trinomial coefficients produced by the quadratic MacWilliams theorem. If sufficiently motivated one could understand them completely.
(4) The proof of Theorem 2 (see the end of Section 3) also gives other types of formulas, e.g., the case where one fixes p and varies v; however, the formulas involved are less aesthetically pleasing.

Similar ideas can be used to show analogous results for the weight enumerators of classical Reed-Solomon codes of dimension $q-5$. The dual of the Reed-Solomon code of dimension 5 and length q over $\mathbb{F}_q$ is the Reed-Solomon code of dimension $q-5$ and length q, which we denote $C'_{1,q-5}$.

Example 3. Let $a(q)$ be the q^{th} Fourier coefficient of $\eta^{12}(2z)$, the unique normalized Hecke eigenform of weight 6 for $\Gamma_0(4)$.

When $q \geq 11$ is a prime congruent to 1 modulo 4, the $X^{q-7}Y^7$ coefficient of $\mathrm{QR}_{C'_{1,q-5}}(X,Y,Z)$ is

$$\begin{aligned}
&\frac{1}{645120}(q-6)q(q-1)^2(q^5 - 20q^4 + 120q^3 - 860q^2 + 6154q - 13005) \\
&\qquad - \frac{1}{18432}(q-6)q(q-1)^2 a(q).
\end{aligned}$$

When $q \geq 7$ is a prime congruent to 3 modulo 4, the $X^{q-7}Y^7$ coefficient of $\mathrm{QR}_{C'_{1,q-5}}(X,Y,Z)$ is

$$\begin{aligned}
&\frac{1}{645120}(q-6)q(q+1)(q-1)^2(q^4 - 21q^3 + 141q^2 - 161q - 405) \\
&\qquad - \frac{1}{18432}(q-6)q(q-1)^2 a(q).
\end{aligned}$$

Note that up to factors of 2 or 3 that $q(q-1)^2$ divides all of the coefficients of $\mathrm{QR}_{C'_{1,q-5}}(X,Y,Z)$ after the first since there is an action on non-zero codewords by the subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$ fixing a point of $\mathbb{P}^1(\mathbb{F}_q)$, as well as an action of $\mathbb{F}_q^*$ by scaling.

The results of Section 3 can also be used to give exact formulas for certain sums involving rational point counts for families of elliptic curves over a fixed finite field.

Example 4. Let p be an odd prime. For $a, b \in \mathbb{F}_p$, let $E_{a,b}$ denote the projective curve $y^2z = x(x^2 + axz + bz^2)$. We define

$$S'_3(p) = \sideset{}{'}\sum_{a,b\in\mathbb{F}_p} \left(\#E_{a,b}(\mathbb{F}_p) - (p+1)\right)^6,$$

where the symbol $\sum'$ indicates that we only sum over pairs (a,b) such that $E_{a,b}$ defines an elliptic curve. Then

$$S'_3(p) = (p-1)(p+1)\left(5p^3 - 10p^2 - 8p - 2\right) - \frac{1}{2}(p-1)\mathrm{tr}_{\Gamma_0(4),8}T_p.$$

Birch gives similar formulas for sums taken over all elliptic curves over $\mathbb{F}_p$ in [2].

The projective Reed-Solomon codes $C_{1,h}$ fit into a broader class of projective Reed-Muller codes. One analogously defines $C_{n,h}$ by evaluating each homogeneous degree h form on $\mathbb{P}^n$ at each of the $(q^{n+1}-1)/(q-1)$ $\mathbb{F}_q$-rational points of $\mathbb{P}^n$. For $n > 1$ these codes are not MDS, and their Hamming weight enumerators are generally quite hard to compute. For example, the weight enumerators from codes from quadrics in $\mathbb{P}^n$, $C_{n,2}$, are computed in [8], along with the weight enumerator from codes coming from plane cubics, $C_{2,3}$, and from cubic surfaces, $C_{3,3}$. The $C_{2,3}$ case is most similar to the results of this paper. The weight enumerator is given in terms of the sizes of isogeny classes of elliptic curves over $\mathbb{F}_q$, and the results of Birch described in Section 3 show that the coefficients of the weight enumerator of $C_{2,3}^{\perp}$ can be expressed in terms of traces of Hecke operators acting on cusp forms for $\mathrm{SL}_2(\mathbb{Z})$. One of the interesting aspects of our main result is that by treating rational 2-torsion points differently we also get contributions from the congruence subgroups $\Gamma_0(2)$ and $\Gamma_0(4)$.

Projective Reed-Solomon and Reed-Muller codes give examples of a more general construction of codes from evaluating polynomials at the $\mathbb{F}_q$-rational points of projective varieties. This evaluation construction has been extensively studied by Tsfasman and Vlăduţ, Lachaud, Sørensen, and others [14, 24, 25]. For much more information, particularly focusing on codes from higher-dimensional varieties, see the survey of Little [17].

2. Weight enumerators of codes from genus one curves

This section has two parts. In the first we compute the quadratic residue weight enumerator $\mathrm{QR}_{C_{1,4}}(X,Y,Z)$ of the 5-dimensional projective Reed-Solomon code. In the second we give a variation of the classical MacWilliams theorem for this quadratic residue weight enumerator.

2.1. The quadratic residue weight enumerator of $C_{1,4}$.

For non-negative integers i, j, k with $i + j + k = q + 1$ let $A_{i,j,k}$ be the number of homogeneous quartics $f_4(x,y)$ that have i $\mathbb{F}_q$-rational roots and such that the variety defined by

$w^2 = f_4(x,y)$ has exactly $i+2j$ $\mathbb{F}_q$-points. We define the quadratic residue weight enumerator to be

$$\mathrm{QR}_{C_{1,4}}(X,Y,Z) \stackrel{\mathrm{def}}{=} \sum_{\substack{i,j,k\geq 0\\ i+j+k=q+1}} A_{i,j,k}X^iY^jZ^k.$$

We compute these coefficients by building slightly on work of Deuring on elliptic curves over a fixed finite field [5].

We first consider quartics $f_4(x,y)$ that have a double root. In this case, $w^2 = f_4(x,y)$ is singular, and counting points on this variety is elementary. We then compute $\mathrm{QR}_{C_{1,4}}(X,X^2,1)$, which gives the rational point count distribution for the family of varieties being considered, but does not distinguish between points that come from $\mathbb{F}_q$-rational roots of $f_4(x,y)$ and points of $\mathbb{P}^1(\mathbb{F}_q)$ at which $f_4(x,y)$ takes a non-zero quadratic residue value. Finally, we consider elliptic curves with a given number of points and prescribed 2-torsion structure to compute $\mathrm{QR}_{C_{1,4}}(X,Y,Z)$.

Proposition 1. *Let* $\mathrm{QR}^{\mathrm{sing}}_{C_{1,4}}(X,Y,Z)$ *denote the contribution to* $\mathrm{QR}_{C_{1,4}}(X,Y,Z)$ *from quartics* $f_4(x,y)$ *that do not have distinct roots over* $\overline{\mathbb{F}}_q$. *Then* $\mathrm{QR}^{\mathrm{sing}}_{C_{1,4}}(X,Y,Z)$ *is given by*

$$\begin{aligned} & X^{q+1} + \frac{(q-1)(q+1)}{2}X(Y^q+Z^q) + (q-1)q(q+1)X^2Y^{\frac{q-1}{2}}Z^{\frac{q-1}{2}} \\ + \ & \frac{(q-1)q(q+1)}{4}X^2(Y^{q-1}+Z^{q-1}) + \frac{(q-1)^2q(q+1)}{4}X^3(Y^{\frac{q-1}{2}}Z^{\frac{q-3}{2}} + Y^{\frac{q-3}{2}}Z^{\frac{q-1}{2}}) \\ + \ & \frac{(q-1)^2q(q+1)}{4}X(Y^{\frac{q+1}{2}}Z^{\frac{q-1}{2}} + Y^{\frac{q-1}{2}}Z^{\frac{q+1}{2}}) + \frac{(q-1)^2q}{4}(Y^{q+1}+Z^{q+1}). \end{aligned}$$

Proof. There is a small list of factorization types of quartics with a double root. Such a quartic could have a quadruple root, a root of multiplicity three and another rational root, two distinct double roots, or a double root and two other roots. We work out the details of this last case and leave the others as an exercise.

A quartic with a single double root must have its double root at an $\mathbb{F}_q$-rational point. The other two roots can then either be at distinct rational points or be a Galois-conjugate pair of points defined over $\mathbb{F}_{q^2}$. Scaling a quartic by a quadratic residue does not change its contribution to $\mathrm{QR}_{C_{1,4}}(X,Y,Z)$, while scaling by a quadratic non-residue interchanges the number of residue versus non-residue values taken. We write such a quartic as $f(x,y)^2g(x,y)$, where $g(x,y)$ is a quadratic polynomial with distinct roots and $f(x,y)$ is a linear form with an $\mathbb{F}_q$-rational root. The curve $w^2 = g(x,y)$ is a smooth conic, so has $q+1$ rational points. Therefore, $w^2 = f(x,y)g(x,y)$ has either q or $q+2$ $\mathbb{F}_q$-points depending on the value taken by $g(x,y)$ at the rational root of $f(x,y)$. Combining these observations shows that the contribution to $\mathrm{QR}_{C_{1,4}}(X,Y,Z)$ from quartics with a double root and two other distinct roots is

$$\frac{(q-1)^2q(q+1)}{4}\left(X^3(Y^{\frac{q-1}{2}}Z^{\frac{q-3}{2}} + Y^{\frac{q-3}{2}}Z^{\frac{q-1}{2}}) + X(Y^{\frac{q+1}{2}}Z^{\frac{q-1}{2}} + Y^{\frac{q-1}{2}}Z^{\frac{q+1}{2}})\right).$$

□

We now turn to $\mathrm{QR}_{C_{1,4}}(X,X^2,1)$. We first compute the number of times that a particular isomorphism class of an elliptic curve arises as an equation of the form $w^2 = f_4(x,y)$.

Proposition 2. *Let E be an elliptic curve defined over $\mathbb{F}_q$. The number of homogeneous quartic polynomials $f_4(x,y)$ such that $w^2 = f_4(x,y)$ gives a curve isomorphic to E is*

$$(q-1)\frac{|\mathrm{PGL}_2(\mathbb{F}_q)|}{|\mathrm{Aut}_{\mathbb{F}_q}(E)|} = \frac{(q-1)^2 q(q+1)}{|\mathrm{Aut}_{\mathbb{F}_q}(E)|}.$$

Proof. We will phrase this as a double counting argument. Suppose we begin with an elliptic curve E with $\#E(\mathbb{F}_q) = q+1-t$. There are exactly $q+1-t$ choices of a degree two divisor class on E. Riemann-Roch implies that such a divisor has a 2-dimensional space of sections. Choosing a basis for this space of sections gives a degree 2 map to $\mathbb{P}^1$. Taking the inverse image of a point in $\mathbb{P}^1(\mathbb{F}_q)$ recovers the divisor class. The branch points of this map are the roots of this quartic.

Now we consider how many maps take a particular equation of the form $w^2 = f_4(x,y)$ to the underlying elliptic curve E. We can recover E with a distinguished identity element and a degree 2 divisor class D directly from this equation. Now we take a map that forgets D, taking (E,D) to E, and note that it is defined only up to an automorphism of E defined over $\mathbb{F}_q$. Since an automorphism must fix the identity element of E, we multiply $|\mathrm{Aut}_{\mathbb{F}_q}(E)|$ by the number of possible choices of the identity element, $q+1-t$. Therefore, given E there are

$$\frac{(q+1-t)(q-1)|\mathrm{PGL}_2(\mathbb{F}_q)|}{|\mathrm{Aut}_{\mathbb{F}_q}(E)|(q+1-t)} = \frac{(q-1)|\mathrm{PGL}_2(\mathbb{F}_q)|}{|\mathrm{Aut}_{\mathbb{F}_q}(E)|}$$

quartics $f_4(x,y)$ with $w^2 = f_4(x,y)$ isomorphic to E. □

Let $N(t)$ be the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves within the isogeny class $I(t)$ of curves having $\#E(\mathbb{F}_q) = q+1-t$, and let $N_A(t)$ be the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves in $I(t)$ where each isomorphism class is weighted by $1/|\mathrm{Aut}_{\mathbb{F}_q}(E)|$. Let $\mathrm{QR}^S_{C_{1,4}}(X,Y,Z)$ be the contribution to $\mathrm{QR}_{C_{1,4}}(X,Y,Z)$ from quartics with distinct roots over $\overline{\mathbb{F}}_q$ so that

$$\mathrm{QR}_{C_{1,4}}(X,Y,Z) = \mathrm{QR}^S_{C_{1,4}}(X,Y,Z) + \mathrm{QR}^{\mathrm{sing}}_{C_{1,4}}(X,Y,Z).$$

Corollary 1. *Suppose q is odd. We have*

$$\mathrm{QR}^S_{C_{1,4}}(X,X^2,1) = \sum_{t^2 \le 4q} N_A(t)(q-1)^2 q(q+1) X^{q+1-t}.$$

We now give expressions for $N_A(t)$ in terms of class numbers of orders in quadratic imaginary fields. For $d<0$ with $d \equiv 0,1 \pmod 4$, let $h(d)$ denote the class number of the unique quadratic order of discriminant d. Let

$$h_w(d) \stackrel{\mathrm{def}}{=} \begin{cases} h(d)/3, & \text{if } d=-3; \\ h(d)/2, & \text{if } d=-4; \\ h(d), & \text{else,} \end{cases}$$

and let

$$H_w(\Delta) \stackrel{\text{def}}{=} \sum_{\substack{d^2|\Delta \\ \Delta/d^2 \equiv 0,1 \pmod 4}} h_w(\Delta/d^2)$$

be the Hurwitz-Kronecker class number.

The following result is stated for prime fields $\mathbb{F}_p$ where $p \geq 5$, with slightly different notation, on page 654 of Lenstra's paper [15], in which he says that it is basically due to Deuring [5]. The details for the extension to all finite fields are contained in Chapter 4, particularly Theorem 4.5, of the paper of Waterhouse [26]. Schoof gives an unweighted version as Theorem 4.6 in [21].

Theorem 3 (Sizes of isogeny classes with weights)**.** *Let $t \in \mathbb{Z}$. Suppose $q = p^v$ where $p \neq 2$ is prime. Then*

$$\begin{aligned} 2N_A(t) &= H_w(t^2 - 4q) && \text{if } t^2 < 4q \text{ and } p \nmid t \\ &= H_w(-4p) && \text{if } t = 0 \\ &= 1/3 && \text{if } t^2 = 3q \text{ and } p = 3 \end{aligned}$$

if q is not a square, and

$$\begin{aligned} 2N_A(t) &= H_w(t^2 - 4q) && \text{if } t^2 < 4q \text{ and } p \nmid t \\ &= \left(1 - \left(\tfrac{-4}{p}\right)\right)/2 && \text{if } t = 0 \\ &= \left(1 - \left(\tfrac{-3}{p}\right)\right)/3 && \text{if } t^2 = q \\ &= (p-1)/12 && \text{if } t^2 = 4q \end{aligned}$$

if q is a square, and $N_A(t) = 0$ in all other cases.

As above, let $N_{A,2\times 2}(t)$ denote the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$ with $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and where each class is weighted by the size of the automorphism group of a curve in that class. The count of unweighted isomorphism classes of elliptic curves with full 2-torsion is given in Lemma 4.8 of Schoof [21]. Similar arguments give the weighted version, or paying particular attention to curves of j-invariant 0 and 1728 with $|\mathrm{Aut}_{\mathbb{F}_q} E| > 2$ we can easily deduce the weighted statement from the unweighted one.

Lemma 1. *Let $q = p^v$ where $p \neq 2$ is prime. Suppose that $t \in \mathbb{Z}$ satisfies $t^2 \leq 4q$.*

(1) *If $p \nmid t$ and $t \equiv q + 1 \pmod 4$, then*

$$2N_{A,2\times 2}(t) = H_w\left(\frac{t^2 - 4q}{4}\right).$$

(2) *If $t^2 = q, 2q$, or $3q$, then $N_{A,2\times 2}(t) = 0$.*
(3) *If $t^2 = 4q$, then $N_{A,2\times 2}(t) = N_A(t)$.*
(4) *Let $t = 0$. If $q \equiv 1 \pmod 4$, then $N_{A,2\times 2}(t) = 0$. If $q \equiv 3 \pmod 4$, then $2N_{A,2\times 2}(t) = h_w(-p)$.*

Otherwise we have $N_{A,2\times 2}(t) = 0$.

We now turn to the full computation of $\mathrm{QR}_{C_{1,4}}(X, Y, Z)$. The main problem we need to solve is the following. Suppose that there are M smooth quartics $f_4(x, y)$ such that $w^2 = f_4(x, y)$ has exactly $q + 1 - t$ $\mathbb{F}_q$-points. Let M_k be the number of these quartics with k $\mathbb{F}_q$-rational roots, so $M_0 + M_1 + M_2 + M_3 + M_4 = M$. We

need the individual values of the M_i. If a quartic $f_4(x,y)$ defined over $\mathbb{P}^1(\mathbb{F}_q)$ has 4 distinct roots and 3 of them are $\mathbb{F}_q$-rational, then the fourth root is also $\mathbb{F}_q$-rational. Therefore, $M_3 = 0$ and we can determine M_1 using a very elementary observation.

Lemma 2. *Suppose that $q+1-t$ is odd and that there are M smooth quartics $f_4(x,y)$ such that $w^2 = f_4(x,y)$ has exactly $q+1-t$ $\mathbb{F}_q$-points. Then $M_1 = M$ and $M_0 = M_2 = M_4 = 0$. Suppose that $q+1-t$ is even and that there are M smooth quartics $f_4(x,y)$ such that $w^2 = f_4(x,y)$ has exactly $q+1-t$ $\mathbb{F}_q$-points. Then $M_1 = 0$.*

Proof. The number of $\mathbb{F}_q$-rational points of $w^2 = f_4(x,y)$ is the number of $\mathbb{F}_q$-rational roots of $f_4(x,y)$ plus twice the number of points of $\mathbb{P}^1(\mathbb{F}_q)$ for which the quartic takes a non-zero square value. Therefore, if $q+1-t$ is odd, then the number of roots of $f_4(x,y)$ is odd. If $q+1-t$ is even, then the number of roots of $f_4(x,y)$ is even. □

We suppose that $q+1-t$ is even and determine how these M quartics break up into those that have $0, 2$, and 4 $\mathbb{F}_q$-rational roots. We first note that for an elliptic curve in affine Weierstrass form $y^2 = f(x) = x^3 + ax + b$, the roots of the homogeneous quartic $y(x^3 + axy^2 + by^3)$ give the 2-torsion points of E. When we consider curves given by $w^2 = f_4(x,y)$, a homogeneous quartic on $\mathbb{P}^1(\mathbb{F}_q)$, there is a similar correspondence between roots of $f_4(x,y)$ and 2-torsion points of E.

Lemma 3. *Let E be an elliptic curve defined over $\mathbb{F}_q$ and suppose that there are M quartics $f_4(x,y)$ with $w^2 = f_4(x,y)$ isomorphic to E. Let $M = M_0 + M_2 + M_4$, where M_k is the number of quartics with k $\mathbb{F}_q$-rational roots.*

(1) *If $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z}$, then $M_0 = M_2 = \frac{M}{2}$ and $M_4 = 0$.*
(2) *If $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then $M_0 = \frac{3M}{4}, M_2 = 0$, and $M_4 = \frac{M}{4}$.*

Proof. We describe how to find all quartics $f_4(x,y)$ with $w^2 = f_4(x,y)$ isomorphic to E. Riemann-Roch implies that a degree 2 divisor on E has a 2-dimensional space of sections. Given such a divisor, choosing a basis for this space of sections gives a degree 2 map to $\mathbb{P}^1$. We take this divisor to be $(O)+(P)$, where O is the identity element of the group law of E and P is another $\mathbb{F}_q$-rational point of E.

A point $P \in E(\mathbb{F}_q)$ gives a map from E to $\mathbb{P}^1$ by taking sections of the divisor $(O)+(P)$. A root of this quartic corresponds to a point $Q \in E(\overline{\mathbb{F}}_q)$ with $2Q \sim O+P$ or $2Q = P$ in the group law on the curve.

We vary over all choices of P and consider how many Q occur as points with $2Q = P$. If $\#E(\mathbb{F}_q)$ is odd, then the map $P \to 2P$ is an isomorphism, so every P gives exactly one such Q. If $\#E(\mathbb{F}_q)$ is even, then there are two possibilities for the group structure of $E(\mathbb{F}_q)[2]$. If $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z}$, then $1/2$ of points of $E(\mathbb{F}_q)$ have 0 preimages under the map $P \to 2P$, and $1/2$ have exactly 2. If $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then $1/4$ of points of $E(\mathbb{F}_q)$ have 4 preimages under the map $P \to 2P$, and $3/4$ have none. □

We can now state the main result about $\mathrm{QR}^S_{C_{1,4}}(X,Y,Z)$.

Theorem 4. *Suppose $q = p^v$ where p is an odd prime. Then $\mathrm{QR}^S(X, Y, Z)$ is equal to $(q-1)^2 q(q+1)$ times*

$$\sum_{\substack{t^2 \le 4q \\ t \equiv 1 \pmod 2}} N_A(t) X Y^{\frac{q-t}{2}} Z^{\frac{q+t}{2}}$$
$$+ \sum_{\substack{t^2 \le 4q \\ t \equiv 0 \pmod 2}} \left((N_A(t) - N_{A,2\times 2}(t)) \left(\frac{1}{2} X^2 Y^{\frac{q-1-t}{2}} Z^{\frac{q-1+t}{2}} + \frac{1}{2} Y^{\frac{q+1-t}{2}} Z^{\frac{q+1+t}{2}} \right) \right.$$
$$\left. + N_{A,2\times 2}(t) \left(\frac{1}{4} X^4 Y^{\frac{q-3-t}{2}} Z^{\frac{q-3+t}{2}} + \frac{3}{4} Y^{\frac{q+1-t}{2}} Z^{\frac{q+1+t}{2}} \right) \right).$$

Combining Proposition 1, Theorem 3, Lemma 1, and Theorem 4 completely determines $\mathrm{QR}_{C_{1,4}}(X, Y, Z)$.

We also give the quadratic residue weight enumerator of $C'_{1,h}$, the classical Reed-Solomon code of order h, as it can be computed easily from the analogous weight enumerator of $C_{1,h}$. Recall that we get the classical Reed-Solomon code by puncturing the projective one at a single point; that is, we choose one of the $q+1$ coordinates of our code and consider the image of the map that takes a codeword to the element of $\mathbb{F}_q^q$ that comes from deleting this coordinate.

Proposition 3. *Suppose that $h \le q$ and that the quadratic residue weight enumerator of $C_{1,h}$ is given by*

$$\mathrm{QR}_{C_{1,h}}(X, Y, Z) = \sum_{\substack{j,k \ge 0 \\ j+k \le q+1}} A_{q+1-j-k,j,k} X^{q+1-j-k} Y^j Z^k.$$

Then the $X^{q-j-k} Y^j Z^k$ coefficient of the quadratic residue weight enumerator of the classical Reed-Solomon code of order h is

$$\frac{(q+1-j-k) A_{q+1-j-k,j,k} + (j+1) A_{q-j-k,j+1,k} + (k+1) A_{q-j-k,j,k+1}}{q+1},$$

where $A_{i,j,k} = 0$ if any of $i, j, k < 0$.

Proof. We consider all of the $A_{q+1-j-k,j,k}$ codewords of $C_{1,h}$ that have exactly $q+1-j-k$ coordinates equal to zero, j equal to non-zero quadratic residues, and k equal to non-zero quadratic non-residues. The action of $\mathrm{PGL}_2(\mathbb{F}_q)$ is transitive on $\mathbb{F}_q$-points, so the proportion of these codewords that have a zero in a chosen coordinate is $\frac{q+1-j-k}{q+1}$. Similar computations give the other two terms in the sum. □

2.2. **The MacWilliams theorem for the quadratic residue weight enumerator.** Now that we have an expression for $\mathrm{QR}_{C_{1,4}}(X, Y, Z)$ we use a variation of the MacWilliams theorem to derive formulas for the coefficients of $\mathrm{QR}_{C_{1,4}^\perp}(X, Y, Z) = \mathrm{QR}_{C_{1,q-5}}(X, Y, Z)$.

Theorem 5. *Let $C \subseteq \mathbb{F}_q^N$ be a linear code where q is an odd prime power. Then*

$$\mathrm{QR}_C(X, Y, Z) = \frac{1}{|C^\perp|} \mathrm{QR}_{C^\perp}(X', Y', Z'),$$

where

$$\begin{aligned} X' &= X + \frac{q-1}{2}(Y+Z), \\ Y' &= X + \frac{-(Y+Z) + \epsilon_q\sqrt{q}(Y-Z)}{2}, \\ Z' &= X + \frac{-(Y+Z) + \epsilon_q\sqrt{q}(Z-Y)}{2}, \end{aligned}$$

and

$$\epsilon_q = \begin{cases} 1 & \text{if } q \equiv 1 \pmod 4, \\ i & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

We first recall the definition of the complete weight enumerator and the MacWilliams theorem for it and then prove Theorem 5 by specializing certain variables. We follow the construction as described in Chapter 5 of [18]. Let $w_0, w_1, \dots, w_{q-1}$ be an enumeration of the elements of $\mathbb{F}_q$ with $w_0 = 0$. The composition of $c = (c_1, \dots, c_n) \in \mathbb{F}_q^n$ is defined by $\operatorname{comp}(c) = (s_0, s_1, \dots, s_{q-1})$, where $s_i = s_i(c)$ is the number of coordinates c_j equal to w_i. We consider the additive group algebra $\mathbb{C}[\mathbb{F}_q]$. In $\mathbb{C}[\mathbb{F}_q]$ we denote the elements of $\mathbb{F}_q$ by z_i, where z_i corresponds to w_i.

For $c = (c_1, \dots, c_N) \in \mathbb{F}_q^N$, let $F(c) = z_0^{s_0} z_1^{s_1} \cdots z_{q-1}^{s_{q-1}}$, where $\operatorname{comp}(c) = (s_0, \dots, s_{q-1})$. The complete weight enumerator of C is

$$\operatorname{CW}_C(z_0, z_1, \dots, z_{q-1}) \stackrel{\text{def}}{=} \sum_{c \in C} F(c) = \sum_{s=(s_0,\dots,s_{q-1})} A(s) z_0^{s_0} \cdots z_{q-1}^{s_{q-1}},$$

where $A(s)$ is the number of $c \in C$ with $\operatorname{comp}(c) = (s_0, \dots, s_{q-1})$.

We recall some basic facts about characters on $\mathbb{F}_q$. Suppose $q = p^v$ for p prime. There is an element $\beta \in \mathbb{F}_q$ such that $\{1, \beta, \beta^2, \dots, \beta^{v-1}\}$ is a basis for $\mathbb{F}_q$ as a vector space over $\mathbb{F}_p$. We uniquely identify the element

$$\gamma = \gamma_0 + \gamma_1\beta + \cdots + \gamma_{v-1}\beta^{v-1}$$

by $(\gamma_0, \dots, \gamma_{v-1})$. Let $\zeta = e^{2\pi i/p}$ and $\chi : \mathbb{F}_q \to \mathbb{C}$ be defined by

$$\chi(\gamma) = \zeta^{\gamma_0 + \gamma_1 + \cdots + \gamma_{v-1}}$$

for $\gamma = (\gamma_0, \dots, \gamma_{v-1}) \in \mathbb{F}_q$. This is an additive character of $\mathbb{F}_q$. The following version of the MacWilliams theorem for the complete weight enumerator is Theorem 10 in Chapter 5 of [18].

Theorem 6. *Let $C \subset \mathbb{F}_q^N$ be a linear code and χ the additive character on $\mathbb{F}_q$ defined above. Then $\operatorname{CW}_{C^\perp}(z_0, \dots, z_{q-1})$ is given by*

$$\frac{1}{|C|}\operatorname{CW}_C\left(\sum_{j=0}^{q-1}\chi(w_0w_j)z_j, \sum_{j=0}^{q-1}\chi(w_1w_j)z_j, \dots, \sum_{j=0}^{q-1}\chi(w_{q-1}w_j)z_j\right).$$

Recall that for the quadratic character η on $\mathbb{F}_q^*$ we have

$$\sum_{x \in \mathbb{F}_q^*}(1 + \eta(x))\chi(x) = 2\sum_{x \in \left(\mathbb{F}_q^*\right)^2}\chi(x).$$

The following is Theorem 5.15 in [16].

Lemma 4. *Suppose that $q = p^v$ is odd where p is an odd prime and $v \geq 1$. Let χ and η be defined as above. Then*

$$\sum_{x \in \mathbb{F}_q^*} \eta(x)\chi(x) = \epsilon_q \sqrt{q}, \quad \text{where } \epsilon_q = \begin{cases} (-1)^{v-1} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{v-1} i^v & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

We now prove Theorem 5.

Proof. Suppose we are in the setting of Theorem 6. Let $z_0 = X$, $z_i = Y$ if w_i is a non-zero quadratic residue, and $z_i = Z$ otherwise. We first note that

$$\sum_{i=0}^{q-1} \chi(w_0 w_i) z_i = X + \frac{q-1}{2}(Y + Z)$$

and that for $w_j \in \left(\mathbb{F}_q^*\right)^2$ we have

$$\sum_{i=0}^{q-1} \chi(w_j w_i) z_i = X + Y \sum_{x \in \left(\mathbb{F}_q^*\right)^2} \chi(x) + Z \sum_{x \in \mathbb{F}_q^* \setminus \left(\mathbb{F}_q^*\right)^2} \chi(x).$$

Since $\sum_{x \in \mathbb{F}_q^*} \chi(x) = -1$, applying Lemma 4 gives

$$\sum_{x \in \left(\mathbb{F}_q^*\right)^2} \chi(x) = \frac{-1 + \epsilon_q \sqrt{q}}{2}$$

and

$$\sum_{x \in \mathbb{F}_q^* \setminus \left(\mathbb{F}_q^*\right)^2} \chi(x) = \frac{-1 - \epsilon_q \sqrt{q}}{2},$$

where ϵ_q is defined as above. When $w_j \in \mathbb{F}_q^* \setminus \left(\mathbb{F}_q^*\right)^2$ the coefficients of Y and Z are switched. As $\mathrm{QR}_C(X, Y, Z)$ is symmetric in Y, Z, we may drop the negative signs in the definition of ε_q. Combining these observations completes the proof. □

3. Point count distributions for elliptic curves over $\mathbb{F}_q$

Let $t_E = q + 1 - \#E(\mathbb{F}_q)$ be the trace of Frobenius associated to E, and recall the definition of $N_A(t)$ from Section 2. Let

$$S_R^*(q) \stackrel{\text{def}}{=} \sum_{E/\mathbb{F}_q} \frac{t_E^{2R}}{|\mathrm{Aut}_{\mathbb{F}_q}(E)|} = \sum_{t^2 \leq 4q} t^{2R} N_A(t)$$

be the (weighted) $2R^{\text{th}}$ moment of $\#E(\mathbb{F}_q)$ over $\mathbb{F}_q$-isomorphism classes of elliptic curves $E/\mathbb{F}_q$.

Let $\mathrm{tr}_{\mathrm{SL}_2(\mathbb{Z}),k} T_q$ be the trace of the T_q Hecke operator acting on the space of weight k cusp forms for the full modular group and $C_R = (2R)!/(R!(R+1)!)$ be the R^{th} Catalan number. We also define the following combinatorial coefficients that show up repeatedly in our formulas:

$$a_{R,j} \stackrel{\text{def}}{=} \frac{2R - 2j + 1}{2R + 1} \binom{2R+1}{j} = \binom{2R}{j} - \binom{2R}{j-1}.$$

In particular, we have $a_{R,R} = C_R$ and $a_{R,0} = 1$.

If $q = p^v$ is a prime power we define

$$\rho(q,k) \stackrel{\text{def}}{=} -\text{tr}_{\text{SL}_2(\mathbb{Z}),k} T_q + \frac{k-1}{12} q^{k/2-1} \mathbb{1}_{v \equiv 0 \pmod 2} - \frac{1}{2} \sum_{0 \le i \le v} \min(p^i, p^{v-i})^{k-1} + \sigma_1(q) \mathbb{1}_{k=2},$$

where $\mathbb{1}_A$ is the indicator function of A being true and σ_1 is the sum-of-divisors function, that is, $\sigma_1(n) = \sum_{d|n} d$. Furthermore we set

$$\rho(1,k) \stackrel{\text{def}}{=} \frac{i^{k-2}}{4} + \frac{1}{3} \frac{\omega^{k-1} - \overline{\omega}^{k-1}}{\omega - \overline{\omega}} \quad \text{and} \quad \rho(p^{-1}, k) \stackrel{\text{def}}{=} 0,$$

where ω is a primitive 3^{rd} root of unity.

Theorem 7. *We have for prime $p \ge 3$ that*

$$\begin{aligned} S_0^*(p) &= p, \\ S_1^*(p) &= p^2 - 1, \\ S_2^*(p) &= 2p^3 - 3p - 1, \\ S_3^*(p) &= 5p^4 - 9p^2 - 5p - 1, \\ S_4^*(p) &= 14p^5 - 28p^3 - 20p^2 - 7p - 1, \\ S_5^*(p) &= 42p^6 - 90p^4 - 75p^3 - 35p^2 - 9p - 1 - \tau(p), \end{aligned}$$

where $\tau(p)$ is Ramanujan's τ-function. In general if $q = p^v$ with $p \neq 2$ we have

$$S_R^*(q) = \sum_{j=0}^{R} a_{R,j} q^j \left(\rho(q, 2R-2j+2) - p^{2R-2j+1} \rho(q/p^2, 2R-2j+2) \right) + \frac{p-1}{12} (4q)^R \mathbb{1}_{v \equiv 0 \pmod 2}.$$

Proof. Theorem 7 is due to Birch [2] in the prime field case. The generalization to all finite fields is well known, being implicit in the work of Ihara [11]. See also Section 3 of the paper of Brock and Granville [3]. □

For our application to computing the coefficients of the quadratic residue weight enumerator of the codes $C_{1,q-5}$ we prove the following variation of Birch's theorem for elliptic curves with rational 2-torsion.

Let

$$S_{2,R}^*(q) \stackrel{\text{def}}{=} \sum_{\substack{E/\mathbb{F}_q \\ E(\mathbb{F}_q)[2] \neq \{O\}}} \frac{t_E^{2R}}{|\text{Aut}_{\mathbb{F}_q}(E)|} = \sum_{\substack{t^2 \le 4q \\ t \equiv 0 \pmod 2}} t^{2R} N_A(t)$$

be the (weighted) $2R^{\text{th}}$ moment of the number of rational points of isomorphism classes of elliptic curves over $\mathbb{F}_q$ with at least one non-zero rational 2-torsion point.

Let $\text{tr}_{\Gamma_0(4),k} T_q$ be the trace of the Hecke operator T_q acting on the space of classical cusp forms $S_k(\Gamma_0(4))$ of weight k for the congruence subgroup $\Gamma_0(4)$, similarly for the congruence subgroup $\Gamma_0(2)$.

If $q = p^v$ is a prime power we define

$$\tau(q,k) \stackrel{\text{def}}{=} \frac{k-1}{12} q^{\frac{k}{2}-1} \mathbb{1}_{v \equiv 0 \pmod 2} + \frac{1}{3} \text{tr}_{\Gamma_0(4),k} T_q - \text{tr}_{\Gamma_0(2),k} T_q - \frac{1}{2} \sum_{0 \le i \le v} \min(p^i, p^{v-i})^{k-1} + \frac{2}{3} \sigma_1(q) \mathbb{1}_{k=2}.$$

Furthermore we set

$$\tau(1,k) \stackrel{\text{def}}{=} \frac{i^{k-2}}{4} \quad \text{and} \quad \tau(p^{-1},k) \stackrel{\text{def}}{=} 0.$$

Theorem 8. *If $q=p$ is an odd prime we have*

$$\begin{aligned} S^*_{2,0}(p) &= \frac{1}{3}(2p-1), \\ S^*_{2,1}(p) &= \frac{1}{3}p(2p-1)-1, \\ S^*_{2,2}(p) &= \frac{4}{3}p^3-\frac{2}{3}p^2-3p-1+\frac{1}{3}a(p), \end{aligned}$$

where $a(p)$ is the p^{th} Fourier coefficient of $\eta^{12}(2z)$, the unique normalized Hecke eigenform of weight 6 for $\Gamma_0(4)$. In general if $q=p^v$ with p an odd prime we have

$$S^*_{2,R}(q) = \sum_{j=0}^{R} a_{R,j}q^j\left(\tau(q,2R-2j+2)-p^{2R-2j+1}\tau(q/p^2,2R-2j+2)\right) + \frac{p-1}{12}(4q)^R \mathbb{1}_{v\equiv 0 \pmod 2}.$$

We prove this theorem in Section 4.

Finally, let

$$S^*_{2\times 2,R}(q) \stackrel{\text{def}}{=} \sum_{\substack{E/\mathbb{F}_q \\ E(\mathbb{F}_q)[2]\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}}} \frac{t_E^{2R}}{|\mathrm{Aut}_{\mathbb{F}_q}(E)|} = \sum_{\substack{t\equiv q+1 \pmod 4 \\ t^2\le 4q}} t^{2R}N_{A,2\times 2}(t)$$

be the weighted $2R^{\text{th}}$ moment of elliptic curves over $\mathbb{F}_q$ with full rational 2-torsion. Let

$$\phi(q,k) \stackrel{\text{def}}{=} -\frac{1}{6}\mathrm{tr}_{\Gamma_0(4),k}T_q + \frac{k-1}{12}q^{k/2-1}\mathbb{1}_{v\equiv 0 \pmod 2} - \frac{1}{4}\sum_{0\le i\le v}\min(p^i,p^{v-i})^{k-1} + \frac{1}{6}\sigma_1(q)\mathbb{1}_{k=2}.$$

Furthermore we set

$$\phi(1,k) = \phi(p^{-1},k) \stackrel{\text{def}}{=} 0.$$

Theorem 9. *If $q=p$ is an odd prime we have*

$$\begin{aligned} S^*_{2\times 2,0}(p) &= \frac{1}{6}p-\frac{1}{3}, \\ S^*_{2\times 2,1}(p) &= \frac{1}{6}p^2-\frac{1}{3}p-\frac{1}{2}, \\ S^*_{2\times 2,2}(p) &= \frac{1}{3}p^3-\frac{2}{3}p^2-\frac{3}{2}p-\frac{1}{2}-\frac{1}{6}a(p), \end{aligned}$$

where $a(p)$ is the p^{th} Fourier coefficient of $\eta^{12}(2z)$, the unique normalized Hecke eigenform of weight 6 for $\Gamma_0(4)$. In general if $q=p^v$ with p an odd prime we have

$$S^*_{2\times 2,R}(q) = \sum_{j=0}^{R} a_{R,j}q^j\left(\phi(q,2R-2j+2)-p^{2R-2j+1}\phi(q/p^2,2R-2j+2)\right) + \frac{p-1}{12}(4q)^R \mathbb{1}_{v\equiv 0 \pmod 2}.$$

Proof. Theorem 9 is essentially due to Ahlgren [1] in the prime field case. The generalization to all finite fields follows the same lines as Theorem 8 so we omit it. □

Remarks.

(1) Our results re-prove the "vertical" Sato-Tate law for elliptic curves with specified rational 2-torsion, which is of course already known in much greater generality; see, e.g., [12]. On the other hand, we believe the full formula for the moments in terms of traces of Hecke operators to be new and interesting in its own right.
(2) The case $R = 0$ of Theorem 8 is a special case of work of Eichler from the 1950s [7] and is elementary. A nice exposition is given by Moreno [19]; see Theorem 5.10.
(3) Theorem 7 can be understood in terms of counting rational points on fibered products of the universal elliptic curve. Work of Deligne and others relate this problem to cohomology groups of Kuga-Sato varieties. For an introduction to these ideas see the book [6], particularly Proposition 1.5.12 and Section 2.4. It is likely that our results can be interpreted in this setting by taking fibered products of modular curves of level 2; however, we have opted instead for arguments similar in spirit to Birch's original proof.
(4) Note that the coefficient of $\mathrm{tr}_{\Gamma_0(4),k} T_q$ in $\tau(q,k)$ and $\phi(q,k)$ differs by exactly a factor of $-1/2$. We will use this fact crucially in the following proof.

Proof of Theorem 2. Recall the definitions of M_v and $M_{v,R}(N)$ for $N = 1, 2, 4$ from just above the statement of Theorem 2 in Section 1. For notational convenience, let

$$a = \frac{-1 + \epsilon_q \sqrt{q}}{2},$$
$$\overline{a} = \frac{-1 - \epsilon_q \sqrt{q}}{2},$$

and note that $a + \overline{a} = -1$. The MacWilliams substitution (cf. Theorem 5) is

$$X \mapsto X + \frac{q-1}{2}(Y + Z),$$
$$Y \mapsto X + aY + \overline{a}Z,$$
$$Z \mapsto X + \overline{a}Y + aZ.$$

We use $\mapsto$ to denote this substitution below. As a preliminary step we prove the following weaker version of Theorem 2.

Lemma 5. *For each fixed v, j, k and $\epsilon \in \{\pm 1\}$, there exists*

$$h \in M_v + M_{v,\lfloor \frac{j+k}{2} \rfloor}(1) + M_{v,\lfloor \frac{j+k}{2} \rfloor}(2) + M_{v,\lfloor \frac{j+k}{2} \rfloor}(4)$$

such that $A_{q+1-j-k,j,k} = h(q)$ for all v^{th} powers of odd primes $q = p^v$ satisfying $q \equiv \epsilon \pmod 4$.

Proof. By Proposition 1, the substitution $\mapsto$ applied to $\mathrm{QR}^{\mathrm{sing}}_{C_{1,4}}(X, Y, Z)$ produces only polynomials as coefficients. Thus we need only consider the smooth part,

$\mathrm{QR}^S_{C_{1,4}}(X,Y,Z)$. We only consider the first term in Theorem 4,

$$(q-1)^2q(q+1)X \sum_{\substack{t^2\le 4q\\ t\equiv 1 \pmod 2}} N_A(t)Y^{\frac{q-t}{2}}Z^{\frac{q+t}{2}}, \tag{1}$$

the other terms being treated similarly.

We apply the MacWilliams substitution and the trinomial expansion to (1). We write the trinomial coefficients as

$$\binom{n}{a,b} \stackrel{\text{def}}{=} \frac{\Gamma(n+1)}{\Gamma(n+1-a-b)\Gamma(a+1)\Gamma(b+1)}.$$

This definition makes sense even when a,b or $n-(a+b)$ is negative. Then

$$Y^{\frac{q-t}{2}}Z^{\frac{q+t}{2}} \mapsto \tag{2}$$
$$\sum_{j_Y,j_Z,k_Y,k_Z} \binom{\frac{q-t}{2}}{j_Y,j_Z}\binom{\frac{q+t}{2}}{k_Y,k_Z} X^{q-j_Y-j_Z-k_Y-k_Z}(aY)^{j_Y}(\overline{a}Y)^{k_Y}(aZ)^{k_Z}(\overline{a}Z)^{j_Z},$$

and we multiply this expression by

$$X \mapsto X + \frac{q-1}{2}(Y+Z).$$

Expanding the result we have that the coefficient of $X^{q+1-j-k}Y^jZ^k$ is

$$\begin{aligned} &\sum_{\substack{j_Y+k_Y=j\\ j_Z+k_Z=k}} \binom{\frac{q-t}{2}}{j_Y,j_Z}\binom{\frac{q+t}{2}}{k_Y,k_Z} a^{j_Y+k_Z}\overline{a}^{k_Y+j_Z} \\ &+\frac{q-1}{2}\sum_{\substack{j_Y+k_Y+1=j\\ j_Z+k_Z=k}} \binom{\frac{q-t}{2}}{j_Y,j_Z}\binom{\frac{q+t}{2}}{k_Y,k_Z} a^{j_Y+k_Z}\overline{a}^{k_Y+j_Z} \\ &+\frac{q-1}{2}\sum_{\substack{j_Y+k_Y=j\\ j_Z+k_Z+1=k}} \binom{\frac{q-t}{2}}{j_Y,j_Z}\binom{\frac{q+t}{2}}{k_Y,k_Z} a^{j_Y+k_Z}\overline{a}^{k_Y+j_Z}. \end{aligned} \tag{3}$$

For each fixed j_Y,j_Z,k_Y,k_Z the product of two trinomial coefficients above is a polynomial in q and t of degree at most $j_Y+j_Z+k_Y+k_Z$ in t. For all but finitely many of the tuples (j_Y,j_Z,k_Y,k_Z), the polynomial we get is 0. We need consider only the terms of the sum (3) which are of even degree in t since the odd degree terms are all killed by the sum over t later. Note then that for each fixed j,k the even degree part of the sum (3) is a polynomial in q and t. We call this polynomial $p_{j,k}(t,q)$. The coefficient of $X^{q+1-j-k}Y^jZ^k$ in the MacWilliams substitution applied to (1) is therefore

$$(q-1)^2q(q+1) \sum_{\substack{t^2\le 4q\\ t\equiv 1 \pmod 2}} N_A(t)p_{j,k}(t,q),$$

and we may form expressions for these coefficients in terms of the sums $S^*_R(q) - S^*_{2,R}(q)$ for $0\le R\le \lfloor\frac{j+k}{2}\rfloor$.

Applying Theorems 7 and 8 we get a formula for the coefficient of $X^{q+1-j-k}Y^jZ^k$ in the expression which results from applying $\mapsto$ to (1) involving polynomials in p, $\rho(q,k)$, $\rho(q/p^2,k)$, $\tau(q,k)$, and $\tau(q/p^2,k)$. The other terms in Theorem 4 are treated similarly, using Theorems 8 and 9. □

Now we proceed to prove the stronger statement of Theorem 2. Take the expression in Theorem 4 and consider it now not as a polynomial but as a real-analytic function on the open octant $\mathbb{R}^3_{>0}$. We can now rearrange the expression found in Theorem 4 to find that $\mathrm{QR}^S_{C_{1,4}}(X,Y,Z)$ is equal to $(q-1)^2q(q+1)$ times

(4)
$$X\sum_{t^2\le 4q} N_A(t)Y^{\frac{q-t}{2}}Z^{\frac{q+t}{2}} + \frac{1}{2}\left(X-Y^{1/2}Z^{1/2}\right)^2 \sum_{\substack{t\equiv 0 \pmod 2\\ t^2\le 4q}} N_A(t)Y^{\frac{q-t-1}{2}}Z^{\frac{q+t-1}{2}} + \frac{1}{4}\left(X^2-YZ\right)^2 \sum_{\substack{t\equiv 0 \pmod 2\\ t^2\le 4q}} N_{A,2\times 2}(t)Y^{\frac{q-t-3}{2}}Z^{\frac{q+t-3}{2}}.$$

Let us denote the three terms in (4) by $f_1(X,Y,Z)$, $f_2(X,Y,Z)$ and $f_{2\times 2}(X,Y,Z)$, respectively. The term $f_{2\times 2}$ is a polynomial in X,Y,Z, but neither f_1 nor f_2 is a polynomial. Next we apply the MacWilliams substitution to (4), giving three new real-analytic functions:

$$g_1(X,Y,Z) \stackrel{\text{def}}{=} f_1\left(X+\frac{q-1}{2}(Y+Z), X+aY+\overline{a}Z, X+\overline{a}Y+aZ\right),$$
$$g_2(X,Y,Z) \stackrel{\text{def}}{=} f_2\left(X+\frac{q-1}{2}(Y+Z), X+aY+\overline{a}Z, X+\overline{a}Y+aZ\right),$$
$$g_{2\times 2}(X,Y,Z) \stackrel{\text{def}}{=} f_{2\times 2}\left(X+\frac{q-1}{2}(Y+Z), X+aY+\overline{a}Z, X+\overline{a}Y+aZ\right).$$

Lemma 6. *Each of g_1, g_2, and $g_{2\times 2}$ admits a convergent Laurent series in a neighborhood of $(X,Y,Z)=(\infty,0,0)$.*

Proof. We take X^{-1},Y,Z for our variables around $(\infty,0,0)$. The lemma is clear for $g_{2\times 2}$. To prove the lemma for g_2 it suffices to show that the MacWilliams substitution applied to $\left(X-Y^{1/2}Z^{1/2}\right)^2$ is a Laurent series in X^{-1},Y,Z. Indeed, using the power series expansion for $(1+u)^{1/2}$ about $u=0$, which is absolutely and uniformly convergent on compacts in $|u|<1$, we have

$$\begin{aligned}(YZ)^{1/2} \mapsto & X\left(1-\frac{Y+Z}{X}+\frac{(aY+\overline{a}Z)(\overline{a}Y+aZ)}{X^2}\right)^{1/2}\\ &= X\left(1-\frac{Y+Z}{2X}+O_{Y,Z}(X^{-2})\right).\end{aligned}$$

Here $O_{Y,Z}(X^{-2})$ represents the higher order terms in this Laurent series expansion which have at least order 2 in the variable X^{-1} and unspecified orders in Y and Z. We thus have

$$\left(X-Y^{1/2}Z^{1/2}\right)^2 \mapsto \left(\frac{q}{2}\right)^2(Y+Z)^2+O_{Y,Z}(X^{-1}).$$

The term g_1 is treated similarly. For any $t\in\mathbb{Z}$ with $t^2\le 4q$ we have

$$Y^{\frac{q-t}{2}}Z^{\frac{q+t}{2}} \mapsto X^q\left(1+\frac{aY+\overline{a}Z}{X}\right)^{\frac{q-t}{2}}\left(1+\frac{\overline{a}Y+aZ}{X}\right)^{\frac{q+t}{2}}.$$

We again apply the power series expansion for $(1+u)^{1/2}$ around $u=0$ to get a convergent Laurent series expansion. □

By the lemma it suffices to study the coefficient of $(1/X)^{j+k-(q+1)}Y^jZ^k$ in the Laurent series expansion of each of g_1, g_2 and $g_{2\times 2}$ separately and to show that the sum of the three coefficients is in the module prescribed by the statement of Theorem 2. Following the same technique as Lemma 5 we pick out the coefficient of $(1/X)^{j+k-(q+1)}Y^jZ^k$ from g_1 and apply Theorem 7 to evaluate $S_R^*(q)$. Theorem 7 only yields polynomials in p and traces of Hecke operators on spaces of cusp forms for $\mathrm{SL}_2(\mathbb{Z})$, so there is nothing more to show concerning g_1.

We extract the coefficient of $(1/X)^{j+k-(q+1)}Y^jZ^k$ in the Laurent series expansion of g_2. It is given by a sum over t, and we study the highest power of t in the summand. By Theorems 7, 8 and 9 this will give the highest weight trace of a Hecke operator possible in the final expression for $\mathrm{QR}_{C_{1,q^{-5}}}(X,Y,Z)$.

Following the same reasoning as in the proof of Lemma 5 we have

(5)

$$Y^{\frac{q-t-1}{2}}Z^{\frac{q+t-1}{2}} \mapsto$$

$$\sum_{j_Y,j_Z,k_Y,k_Z} \binom{\frac{q-1-t}{2}}{j_Y,j_Z}\binom{\frac{q-1+t}{2}}{k_Y,k_Z} X^{q-1-j_Y-j_Z-k_Y-k_Z}(aY)^{j_Y}(\overline{a}Y)^{k_Y}(aZ)^{k_Z}(\overline{a}Z)^{j_Z},$$

which we multiply by

$$\frac{1}{2}\left(\left(\frac{q}{2}\right)^2(Y+Z)^2 + O_{Y,Z}(X^{-1})\right). \tag{6}$$

The coefficient of $(1/X)^{j+k-(q+1)}Y^jZ^k$ is given by the terms of (5) satisfying

$$\begin{aligned} j_Y + k_Y + 2 &= j,\\ j_Z + k_Z &= k, \end{aligned}$$

or

$$\begin{aligned} j_Y + k_Y + 1 &= j,\\ j_Z + k_Z + 1 &= k, \end{aligned}$$

or

$$\begin{aligned} j_Y + k_Y &= j,\\ j_Z + k_Z + 2 &= k. \end{aligned}$$

The highest power of t appearing in each of the 3 cases is $j+k-2$. Thus the coefficient of $(1/X)^{j+k-(q+1)}Y^jZ^k$ in the Laurent series for g_2 is given by polynomials in q and $S_{2,R}^*(q)$ for $0 \le R \le \lfloor \frac{j+k-2}{2} \rfloor$.

We may apply the same reasoning to $g_{2\times 2}$. We have

$$\frac{1}{4}\left(X^2 - YZ\right)^2 \mapsto \frac{1}{4}q^2(Y+Z)^2X^2 + O_{Y,Z}(X), \tag{7}$$

where the $O_{Y,Z}(X)$ notation has the same meaning as before. Note that the leading terms in (7) and (6) differ only by a factor of $2X^2$. Applying the substitution $\mapsto$ to $Y^{\frac{q-t-3}{2}}Z^{\frac{q+t-3}{2}}$ and expanding with the trinomial expansion one gets an expression identical to (2) but with each instance of $q-1$ replaced by $q-3$. As in the case of g_2, the highest power of t in the coefficient of $(1/X)^{j+k-(q+1)}Y^jZ^k$ in $g_{2\times 2}$ is $j+k-2$. Comparing (6) and (7) we see that the coefficient of t^{j+k-2} within the coefficient of $(1/X)^{j+k-(q+1)}Y^jZ^k$ of $g_{2\times 2}$ differs from that of g_2 by exactly a factor of 2 .

The term $\mathrm{tr}_{\Gamma_0(4),k}T_q$ appears in $\tau(q,k)$ and $\phi(q,k)$ with coefficients differing by a factor of $-1/2$. Thus if $j+k-2$ is even, then $\mathrm{tr}_{\Gamma_0(4),j+k}T_q$ always cancels out

of the $(1/X)^{j+k-(q+1)}Y^jZ^k$ coefficient of $g_2 + g_{2\times 2}$. We have therefore that the Laurent series coefficients of $g_1 + g_2 + g_{2\times 2}$ lie in the prescribed module, and thus that the weight enumerator coefficients do as well. □

4. The Eichler-Selberg trace formula and the proof of Theorem 8

Our main tool is the Eichler-Selberg trace formula. Our reference is Knightly and Li [13], "Statement of the final result".

Recall the Kronecker symbol $\left(\frac{\Delta}{n}\right)$, which we only use when Δ is a discriminant. For n an odd prime the Kronecker symbol is defined to be the quadratic residue symbol, and for $n = 2$ we define

$$\left(\frac{\Delta}{2}\right) \stackrel{\text{def}}{=} \begin{cases} 0 & \text{if } 2 \mid \Delta, \\ 1 & \text{if } \Delta \equiv 1 \pmod 8, \\ -1 & \text{if } \Delta \equiv 5 \pmod 8. \end{cases}$$

Lemma 7. *For $d < 0$, $d \equiv 0, 1 \pmod 4$ and $f \in \mathbb{N}$ we have*

$$h_w(f^2 d) = h_w(d) f \prod_{p \mid f} \left(1 - \left(\frac{d}{p}\right)\frac{1}{p}\right).$$

Proof. This is a standard result. See, e.g., Corollary 7.28 of [4]. □

Proposition 4 (ESTF for odd prime powers q and $\Gamma_0(2)$)**.** *Let $q = p^v$ be an odd prime power. Let $t \in \mathbb{Z}$ run over integers such that $t^2 < 4q$. Let α and $\overline{\alpha}$ be the two roots of $X^2 - tX + q = 0$ in $\mathbb{C}$.*

We have

$$\begin{aligned} \operatorname{tr}_{\Gamma_0(2),k} T_q =& \frac{k-1}{4} q^{\frac{k}{2}-1} \mathbb{1}_{v \equiv 0 \pmod 2} \\ &- \frac{1}{2} \sum_{t \equiv 0 \pmod 2} \frac{\alpha^{k-1} - \overline{\alpha}^{k-1}}{\alpha - \overline{\alpha}} \sum_{\substack{m^2 \mid t^2 - 4q \\ \frac{t^2-4q}{m^2} \equiv 0,1 \pmod 4 \\ \operatorname{ord}_2 m = 0}} h_w\left(\frac{t^2-4q}{m^2}\right) \\ &- \frac{3}{2} \sum_{t \equiv q+1 \pmod 4} \frac{\alpha^{k-1} - \overline{\alpha}^{k-1}}{\alpha - \overline{\alpha}} H_w\left(\frac{t^2-4q}{4}\right) \\ &- \sum_{0 \le i \le v} \min(p^i, p^{v-i})^{k-1} + \sigma_1(q) \mathbb{1}_{k=2}. \end{aligned}$$

Proof. Proposition 4 is a simplification of the standard Eichler-Selberg trace formula, where we have performed a careful but tedious case check of the behavior of the Hecke polynomial $X^2 - tX + q$ modulo 2 and 4 and of the discriminant $t^2 - 4q$ modulo 16. The details are similar to but less complicated than those of the proof of Proposition 5 so we omit them. □

Proposition 5 (ESTF for odd prime powers q and $\Gamma_0(4)$)**.** *Let $q = p^v$ be an odd prime power. Let $t \in \mathbb{Z}$ run over integers such that $t^2 < 4q$. Let α and $\overline{\alpha}$ be the two roots of $X^2 - tX + q = 0$ in $\mathbb{C}$.*

We have

$$\operatorname{tr}_{\Gamma_0(4),k} T_q = \frac{k-1}{2} q^{\frac{k}{2}-1} \mathbb{1}_{v\equiv 0 \pmod 2} - 3 \sum_{t\equiv q+1 \pmod 4} \frac{\alpha^{k-1}-\overline{\alpha}^{k-1}}{\alpha-\overline{\alpha}} H_w\left(\frac{t^2-4q}{4}\right) - \frac{3}{2} \sum_{0\le i\le v} \min(p^i, p^{v-i})^{k-1} + \sigma_1(q)\mathbb{1}_{k=2}.$$

Proof. Apart from trivial simplifications the formula above differs from that appearing in Knightly and Li [13] only by the weights appearing in the sum over t. Specifically, to derive Proposition 5 from the standard formula in [13] it suffices to show that

$$3\cdot \mathbb{1}_{t\equiv q+1 \pmod 4} H_w\left(\frac{t^2-4q}{4}\right) = \frac{1}{2} \sum_{\substack{m^2 \mid t^2-4q \\ \frac{t^2-4q}{m^2}\equiv 0,1 \pmod 4}} h_w\left(\frac{t^2-4q}{m^2}\right) \mu(t,m,q),$$

where

$$\mu(t,m,q) \stackrel{\text{def}}{=} \frac{\psi(4)}{\psi(4/(4,m))} \sum_{c\in(\mathbb{Z}/4\mathbb{Z})^\times} 1,$$

c runs through all elements of $(\mathbb{Z}/4\mathbb{Z})^\times$ that lift to solutions of $c^2 - tc + q \equiv 0 \pmod{4(4,m)}$, and

$$\psi(N) \stackrel{\text{def}}{=} [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{\ell \mid N} \left(1+\frac{1}{\ell}\right).$$

We check the cases $(4,m) = 1, 2, 4$ one-by-one and after a lengthy but trivial computation derive

$$\mu(t,m,q) = \begin{cases} 2\cdot \mathbb{1}_{t\equiv 0 \pmod 4} & \text{if } q\equiv 3 \pmod 4 \text{ and } (4,m)=1, \\ 2\cdot \mathbb{1}_{t\equiv 2 \pmod 4} & \text{if } q\equiv 1 \pmod 4 \text{ and } (4,m)=1, \\ 2\cdot \mathbb{1}_{t\equiv 2 \pmod 4} & \text{if } q\equiv 1 \pmod 4 \text{ and } (4,m)=2, \\ 4\cdot \mathbb{1}_{t\equiv 4 \pmod 8} & \text{if } q\equiv 3 \pmod 8 \text{ and } (4,m)=2, \\ 4\cdot \mathbb{1}_{t\equiv 0 \pmod 8} & \text{if } q\equiv 7 \pmod 8 \text{ and } (4,m)=2, \\ 6\cdot \mathbb{1}_{t\equiv \pm 2 \pmod{16}} & \text{if } q\equiv 1, 13 \pmod{16} \text{ and } (4,m)=4, \\ 6\cdot \mathbb{1}_{t\equiv \pm 6 \pmod{16}} & \text{if } q\equiv 5, 9 \pmod{16} \text{ and } (4,m)=4, \\ \text{does not occur} & \text{if } q\equiv 3 \pmod 4 \text{ and } (4,m)=4. \end{cases}$$

If $q \equiv 3 \pmod 4$, then $t^2 - 4q$ can only take the values $4, 5, 8, 13 \pmod{16}$, hence the last entry above.

In all cases above we have $4 \mid t^2-4q$, so we use Lemma 7 to rewrite the $\operatorname{ord}_2 m = 0$ cases in the above in terms of m with $\operatorname{ord}_2 m = 1$. First assume $q \equiv 3 \pmod 4$ and that $\operatorname{ord}_2 m = 0$. We know $\operatorname{ord}_2(t^2-4q) = 2$ and $t \equiv 0 \pmod 4$ so that

$$\frac{t^2-4q}{4m^2} \equiv \begin{cases} 1 \pmod 8 & \text{if } t+q \equiv 7 \pmod 8, \\ 5 \pmod 8 & \text{if } t+q \equiv 3 \pmod 8. \end{cases}$$

By Lemma 7 if $\operatorname{ord}_2 m = 0$ and $q \equiv 3 \pmod 4$, then

$$h_w\left(\frac{t^2-4q}{m^2}\right) = h_w\left(\frac{t^2-4q}{4m^2}\right) \begin{cases} 1 & \text{if } t+q \equiv 7 \pmod 8, \\ 3 & \text{if } t+q \equiv 3 \pmod 8. \end{cases}$$

Now we turn to the $q \equiv 1 \pmod 4$ and $\operatorname{ord}_2 m = 0$ case. One easily checks that $t \equiv 2 \pmod 4$ and $q \equiv 1 \pmod 4$ imply $\operatorname{ord}_2(t^2 - 4q) \geq 3$; thus

$$h_w\left(\frac{t^2-4q}{m^2}\right) = 2h_w\left(\frac{t^2-4q}{4m^2}\right).$$

Collecting all the above terms, one arrives at the claimed formula. □

Recall the definition of $\tau(q,k)$ from just above Theorem 8.

Lemma 8. *Suppose q is an odd prime power. Let $\alpha, \overline{\alpha} \in \mathbb{C}$ be solutions to $X^2 - tX + q = 0$ and $H_w(\Delta)$ as in Section 2. We have*

$$\frac{1}{2} \sum_{\substack{t \equiv 0 \pmod 2 \\ t^2 < 4q}} \frac{\alpha^{k-1} - \overline{\alpha}^{k-1}}{\alpha - \overline{\alpha}} H_w(t^2 - 4q) = \tau(q,k).$$

Proof. Take 2/3 times the formula of Proposition 5 minus 2 times the result of Proposition 4. One finds that

$$\begin{aligned} \tau(q,k) &= \frac{1}{2} \sum_{t \equiv 0 \pmod 2} \frac{\alpha^{k-1} - \overline{\alpha}^{k-1}}{\alpha - \overline{\alpha}} \sum_{\operatorname{ord}_2 m = 0} h_w\left(\frac{t^2-4q}{m^2}\right) \\ &\quad + \frac{1}{2} \sum_{t \equiv q+1 \pmod 4} \frac{\alpha^{k-1} - \overline{\alpha}^{k-1}}{\alpha - \overline{\alpha}} \sum_{\operatorname{ord}_2 m \geq 1} h_w\left(\frac{t^2-4q}{m^2}\right). \end{aligned}$$

In each case $q \equiv 1, 3 \pmod 4$ one checks that these m give the complete list defining $H_w(t^2 - 4q)$; hence Lemma 8 follows. □

For general prime powers q we need some additional definitions. Let

$$\omega(q,k) \stackrel{\text{def}}{=} \frac{1}{2} \sum_{\substack{t \equiv 0 \pmod 2 \\ p \nmid t \\ t^2 < 4q}} \frac{\alpha^{k-1} - \overline{\alpha}^{k-1}}{\alpha - \overline{\alpha}} H_w(t^2 - 4q) = \sum_{\substack{t \equiv 0 \pmod 2 \\ p \nmid t \\ t^2 < 4q}} \frac{\alpha^{k-1} - \overline{\alpha}^{k-1}}{\alpha - \overline{\alpha}} N_A(t)$$

be the contribution from ordinary elliptic curves. We set

$$A_q \stackrel{\text{def}}{=} \frac{\alpha_0^{k-1} - \overline{\alpha_0}^{k-1}}{\alpha_0 - \overline{\alpha_0}},$$

where α_0 and $\overline{\alpha_0}$ are the two roots in $\mathbb{C}$ of $X^2 + q = 0$. We also let

$$\omega'(q,k) \stackrel{\text{def}}{=} \frac{1}{2} \sum_{\substack{t \equiv 0 \pmod 2 \\ p \nmid t \\ t^2 < 4q}} \frac{\alpha^{k-1} - \overline{\alpha}^{k-1}}{\alpha - \overline{\alpha}} H_w(t^2 - 4q) + A_q N_A(0)$$

be the contribution from elliptic curves whose ring of endomorphisms over $\mathbb{F}_q$ is an order in a quadratic field. Lastly, recall that we set

$$\tau(1,k) = \frac{i^{k-2}}{4} \quad \text{and} \quad \tau(p^{-1},k) = 0.$$

Lemma 9. *Suppose $q = p^v$ is an odd prime power with $0 \leq 2i < v$. We have*

$$(p^i)^{k-1} \omega(q/p^{2i}, k) = \frac{1}{2} \sum_{\substack{t^2 < 4q \\ \operatorname{ord}_p t = i \\ t \equiv 0 \pmod 2}} \frac{\alpha^{k-1} - \overline{\alpha}^{k-1}}{\alpha - \overline{\alpha}} H_w(t^2 - 4q).$$

Proof. Observe that if $0 < i$, then

$$p^i = p^i\left(1-\frac{1}{p}\right) + p^{i-1}\left(1-\frac{1}{p}\right) + \cdots + p\left(1-\frac{1}{p}\right) + 1,$$

and if $0 \le 2i < v$, then

$$(p^i)^{k-1}\omega(q/p^{2i},k) = \frac{1}{2}\sum_{\substack{(p^it)^2<4q\\ p\nmid t\\ t\equiv 0 \pmod 2}} \frac{\alpha^{k-1}-\overline{\alpha}^{k-1}}{\alpha-\overline{\alpha}} p^i H_w(t^2-4q/p^{2i})$$

with $\alpha, \overline{\alpha}$ being solutions in $\mathbb{C}$ to $X^2-(p^it)X+q$.

Let $\Delta = t^2-4q/p^{2i} = ((p^it)^2-4q)/p^{2i}$. For such Δ we have that

$$p^iH_w(\Delta) = H_w(\Delta) + \sum_{j=1}^{i} p^j\left(1-\frac{1}{p}\right)H_w(\Delta).$$

Note that, since $p \nmid t$, Δ is a non-zero square modulo p. Moreover, if $d^2 \mid \Delta$, then we also have that $p \nmid d$ and that Δ/d^2 is a non-zero square modulo p. The definition of H_w and Lemma 7 imply that

$$\begin{aligned} p^iH_w(\Delta) &= \sum_{\substack{d'^2\mid p^{2i}\Delta\\ \frac{p^{2i}\Delta}{d'^2}\equiv 0,1(4)\\ \operatorname{ord}_p d' = i}} h_w\left(\frac{p^{2i}\Delta}{d'^2}\right) + \sum_{j=1}^{i}\sum_{\substack{d'^2\mid p^{2i}\Delta\\ \frac{p^{2i}\Delta}{d'^2}\equiv 0,1(4)\\ \operatorname{ord}_p d' = i-j}} h_w\left(\frac{p^{2i}\Delta}{d'^2}\right)\\ &= H_w(p^{2i}\Delta) = H_w\left((p^it)^2-4q\right). \end{aligned}$$

Thus we have the lemma. □

Lemma 10. *Suppose $q = p^v$ is an odd prime power. We have that*

$$\omega'(q,k) = \tau(q,k) - p^{k-1}\tau(q/p^2,k).$$

Proof. Lemmas 8 and 9 allow us to write

$$\tau(q,k) = \sum_{0\le 2i<v}(p^i)^{k-1}\omega(q/p^{2i},k) + \frac{1}{2}A_qH_w(-4q).$$

Now we need to do some calculation with these class numbers. The definition of H_w and Lemma 7 imply

$$\frac{1}{2}H_w(-4q) = \begin{cases} \frac{\sqrt{q}}{4} + \sigma_1(p^{v/2-1})N_A(0) & \text{if } v \equiv 0 \pmod 2,\\ \sigma_1(p^{\frac{v-1}{2}})N_A(0) & \text{if } v \equiv 1 \pmod 2, \end{cases}$$

and we also have

$$p^iA_q = p^i(i\sqrt{q})^{k-2} = (p^i)^{k-1}A_{q/p^{2i}}$$

from the definition. It follows that

$$\tau(q,k) = \sum_{0\le 2i<v}(p^i)^{k-1}\omega'(q/p^{2i},k) + \frac{\sqrt{q}}{4}A_q\mathbb{1}_{v\equiv 0 \pmod 2},$$

and changing variables we compute

$$p^{k-1}\tau(q/p^2,k) = \sum_{0<2i<v} (p^i)^{k-1}\omega'(q/p^{2i},k) + \frac{\sqrt{q}}{4}A_q \mathbb{1}_{v\equiv 0 \pmod 2}.$$

By subtracting we prove the lemma. □

Recall that we have set

$$a_{R,j} = \binom{2R}{j} - \binom{2R}{j-1}.$$

Lemma 11. *We have*

$$t^{2R} = \sum_{j=0}^{R} a_{R,j} q^j \frac{\alpha^{2R-2j+1} - \overline{\alpha}^{2R-2j+1}}{\alpha - \overline{\alpha}}.$$

Proof. This is an easy proof-by-induction exercise. □

Putting together Lemmas 9 and 11 we get

$$\sum_{\substack{t\equiv 0 \pmod 2 \\ t^2<4q}} t^{2R} N_A(t)$$
$$= \sum_{j=0}^{R} a_{R,j} q^j \left(\tau(q,2R-2j+2) - p^{2R-2j+1}\tau(q/p^2,2R-2j+2)\right).$$

If v is even we add the contribution from the terms corresponding to $t^2 = 4q$, i.e., those supersingular curves having ring of endomorphisms equal to a maximal order in a quaternion algebra over the base field. This concludes the proof of Theorem 8.

Acknowledgments

Part of this project grew out of the PhD thesis of the first author. He thanks Noam Elkies for his extensive guidance and for many helpful conversations. The authors also thank him for carefully reading a draft of this paper and the anonymous referee for helpful comments.

References

[1] Scott Ahlgren, *The points of a certain fivefold over finite fields and the twelfth power of the eta function*, Finite Fields Appl. **8** (2002), no. 1, 18–33, DOI 10.1006/ffta.2001.0315. MR1872789

[2] B. J. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc. **43** (1968), 57–60, DOI 10.1112/jlms/s1-43.1.57. MR0230682

[3] Bradley W. Brock and Andrew Granville, *More points than expected on curves over finite field extensions*, Finite Fields Appl. **7** (2001), no. 1, 70–91, DOI 10.1006/ffta.2000.0308. MR1803936

[4] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, 2nd ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013. MR3236783

[5] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper* (German), Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272. MR0005125

[6] Bas Edixhoven and Jean-Marc Couveignes (eds.), *Computational aspects of modular forms and Galois representations*: *How one can compute in polynomial time the value of Ramanujan's tau at a prime*, Annals of Mathematics Studies, vol. 176, Princeton University Press, Princeton, NJ, 2011. MR2849700

[7] Martin Eichler, *Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion* (German), Arch. Math. **5** (1954), 355–366, DOI 10.1007/BF01898377. MR0063406
[8] N. D. Elkies, *Linear codes and algebraic geometry in higher dimensions*. Preprint, 2006.
[9] Gerard van der Geer, René Schoof, and Marcel van der Vlugt, *Weight formulas for ternary Melas codes*, Math. Comp. **58** (1992), no. 198, 781–792, DOI 10.2307/2153217. MR1122080
[10] Norman E. Hurt, *Exponential sums and coding theory: a review*, Acta Appl. Math. **46** (1997), no. 1, 49–91, DOI 10.1023/A:1005794417363. MR1432471
[11] Yasutaka Ihara, *Hecke polynomials as congruence ζ functions in elliptic modular case*, Ann. of Math. (2) **85** (1967), 267–295, DOI 10.2307/1970442. MR0207655
[12] Nicholas M. Katz and Peter Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999. MR1659828
[13] Andrew Knightly and Charles Li, *Traces of Hecke operators*, Mathematical Surveys and Monographs, vol. 133, American Mathematical Society, Providence, RI, 2006. MR2273356
[14] Gilles Lachaud, *The parameters of projective Reed-Muller codes* (English, with French summary), Discrete Math. **81** (1990), no. 2, 217–221, DOI 10.1016/0012-365X(90)90155-B. MR1054981
[15] H. W. Lenstra Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), no. 3, 649–673, DOI 10.2307/1971363. MR916721
[16] Rudolf Lidl and Harald Niederreiter, *Introduction to finite fields and their applications*, 1st ed., Cambridge University Press, Cambridge, 1994. MR1294139
[17] John B. Little, *Algebraic geometry codes from higher dimensional varieties*, Advances in algebraic geometry codes, Ser. Coding Theory Cryptol., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 257–293, DOI 10.1142/9789812794017_0007. MR2509126
[18] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes. I*, North-Holland Mathematical Library, Vol. 16, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. MR0465509
[19] Carlos Moreno, *Algebraic curves over finite fields*, Cambridge Tracts in Mathematics, vol. 97, Cambridge University Press, Cambridge, 1991. MR1101140
[20] Gabriele Nebe, Eric M. Rains, and Neil J. A. Sloane, *Self-dual codes and invariant theory*, Algorithms and Computation in Mathematics, vol. 17, Springer-Verlag, Berlin, 2006. MR2209183
[21] René Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A **46** (1987), no. 2, 183–211, DOI 10.1016/0097-3165(87)90003-3. MR914657
[22] René Schoof, *Families of curves and weight distributions of codes*, Bull. Amer. Math. Soc. (N.S.) **32** (1995), no. 2, 171–183, DOI 10.1090/S0273-0979-1995-00586-0. MR1302786
[23] René Schoof and Marcel van der Vlugt, *Hecke operators and the weight distributions of certain codes*, J. Combin. Theory Ser. A **57** (1991), no. 2, 163–186, DOI 10.1016/0097-3165(91)90016-A. MR1111555
[24] Anders Bjært Sørensen, *Projective Reed-Muller codes*, IEEE Trans. Inform. Theory **37** (1991), no. 6, 1567–1576, DOI 10.1109/18.104317. MR1134296
[25] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-geometric codes*, Mathematics and its Applications (Soviet Series), vol. 58, Kluwer Academic Publishers Group, Dordrecht, 1991. MR1186841
[26] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560. MR0265369

Department of Mathematics, University of California, Irvine, California 92697-3875
E-mail address: nckaplan@math.uci.edu

École Polytechnique Fédérale de Lausanne, Section des Mathématiques, 1015 Lausanne, Switzerland
Current address: Departement Mathematik, ETH Zürich, HG G 66.4 Rämistrasse 101, 8092 Zürich, Switzerland
E-mail address: ian.petrow@math.ethz.ch