TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 351, Number 9, Pages 3609–3639
S 0002-9947(99)02179-0
Article electronically published on May 3, 1999

WEIGHT DISTRIBUTIONS OF GEOMETRIC GOPPA CODES

IWAN M. DUURSMA

ABSTRACT. The in general hard problem of computing weight distributions of linear codes is considered for the special class of algebraic-geometric codes, defined by Goppa in the early eighties. Known results restrict to codes from elliptic curves. We obtain results for curves of higher genus by expressing the weight distributions in terms of L-series. The results include general properties of weight distributions, a method to describe and compute weight distributions, and worked out examples for curves of genus two and three.

1. INTRODUCTION

The problem that motivated this work comes from coding theory. We sketch the problem in a geometric setting (a setting encouraged in [26]):

> For a given set of n rational points in projective space over a finite field of q elements, determine the number of hyperplanes that intersect the set in a given number of points.

The solution is described by an $n+1$-tuple of integers, called the *weight distribution*. For weight distributions of codes in general, we quote from [4]:

> Analytically describing the weight distribution of a code is a difficult problem ... For an arbitrary linear code, we will not be able to give such a formula.

For geometric Goppa codes [11] (also called algebraic-geometric codes, or AG-codes), the points are chosen on a smooth curve embedded in projective space. The classical Reed-Solomon codes correspond to an embedding of the projective line. The weight distribution problem was solved for Reed-Solomon codes around 1965 by different authors [2], [8], [14]. The approach in this work yields a generating function. We may assume that the line is embedded as a rational curve, say of degree $k-1$,

$$(1 : x : \ldots : x^{k-1}) : \mathbf{P}^1 \longrightarrow \mathbf{P}^{k-1}.$$

Fix n rational points, for $n \leq q+1$. The generating function

$$A(U,T) = \frac{(1+U-T)^n}{(1-T)(1-qT)} = \sum A_{i,j} U^i T^j$$

Received by the editors December 27, 1996 and, in revised form, July 15, 1997.
1991 *Mathematics Subject Classification.* Primary 11T71, 14G15, 94B27.
Key words and phrases. Algebraic curve over a finite field, algebraic-geometric code, weight distribution.
This work was initiated while the author was a post-doc at the CNRS Laboratoire de Mathématiques Discrètes, Luminy, France, with support by the Netherlands Organization for Scientific Research NWO.

gives the number $A_{i,k-1-i}$ of hyperplanes that contain precisely i of the n points (with arbitrary positive multiplicity). The parameter $j = k-1-i$ provides an upper bound on the degree of the non-rational intersection. The substitution $U = UT$ replaces j with $k-1$ as second parameter. And the weight distribution of the embedding $\mathbf{P}^1 \longrightarrow \mathbf{P}^{k-1}$ is described by the coefficient of T^{k-1} in $A(UT, T)$. The case of elliptic curves has been studied in [6], [15]. Properties of their weight distribution are derived from the group law on the set of rational points. For curves of arbitrary genus, weight distributions have been estimated with Clifford's theorem [15], with asymptotic results in [30]. Research Problem 10.4. [19] asks for:

> Find the weight enumerator of other classes of algebraic-geometric codes which have (genus) $\gamma > 1$; for example, find the weight enumerator for Hermitian codes.

In the function field setting, the problem asks for the number of effective divisors in a given divisor class whose support contains a fixed number of rational points. This formulation leads us, in Theorem 7.7, to an analytical formula $A(U, T)$ for the case of arbitrary genus. General results for weight distributions follow from the formula. It satisfies a functional equation and we are able to recognize and to interpret different terms in the formula. On the other hand, the formula yields a method for computing weight distributions. Implicitly, it involves the L-functions for the Hilbert class field extension of the function field. These play an essential role in Theorem 10.3, which aims at computing weight enumerators explicitly for genus greater than one. In the last section, we consider embeddings of the Hermitian curve of degree four and compute their weight distribution. We believe the Hermitian curve of degree five is well within reach, if one uses additional properties of the particular curve. In general, however, the complexity of the computations grows exponentially with the genus. Paraphrasing the earlier quotation: for an arbitrary curve, we will not be able to compute the coefficients of the generating function $A(U, T)$.

Although the analogy with distribution problems in number theory is sometimes useful, we aim to be self-contained in the setting of function fields, where we have our applications. Sections 2 to 6 deal with the distribution of all effective divisors over all divisor classes. First, we define the distribution as a formal expression. The definition is justified by simple group and set theoretic axioms satisfied by the divisor class group. Compared to the standard zeta function, which only enumerates effective divisors, the difference is in taking coefficients in a group algebra rather than in the rational integers. Sections 3 and 4 prepare for the transformation to explicit expressions. They deal with the automorphism group of the curve and the Tate-pairing respectively. Some eigenvalue techniques are introduced from algebraic combinatorics. Sections 5 and 6 summarize consequences of the Riemann-Roch theorem and of Hilbert's theorem on class field extensions. Section 7 defines geometric Goppa codes and gives a generating function for their weight distribution. Section 8 is concerned with duality of weight distributions. Section 9 applies some of the results to arbitrary linear codes. Section 10 deals with the computation of weight distributions. Section 11 defines a new family of codes with bounded parameters. Section 12 presents results for the Hermitian curve of degree four.

2. Divisor class groups

We define a class of Dirichlet L-series as our main tool in studying divisor class groups. We take the function field point of view and arrive at the definition in a straightforward and natural way.

Let K be an algebraic function field in one variable with finite constant field and let $\mathcal{P}_K$ be the set of all the places of K. The *group of divisors* $D(K)$ is the free abelian group generated by the set of places $\mathcal{P}_K$. The principal divisors (f), for a nonzero $f \in K$, form a subgroup $P(K)$ of $D(K)$. The quotient $D(K)/P(K)$ is the *divisor class group* $C(K)$. We note that $C(K)$ is finitely generated of the form $\Gamma \times \mathbf{Z}$. The finite torsion subgroup Γ of $C(K)$ can be described as the group of divisor classes of degree zero. The situation is summarized by the two exact sequences

$$0 \longrightarrow P(K) \longrightarrow D(K) \longrightarrow C(K) \longrightarrow 0,$$

$$0 \longrightarrow \Gamma \longrightarrow C(K) \xrightarrow{\deg} \mathbf{Z} \longrightarrow 0. \tag{1}$$

The set of places $\mathcal{P}_K$ of K generates the *semigroup of effective divisors* $E(K)$. The Riemann-Roch problem asks for the number of effective divisors $|C \cap E(K)|$ in a given divisor class C. We first define a function $L(T)$ that gives the answer at least formally. We will use it in Section 7 to answer the following modification of the problem:

> For a given set of rational places $\mathcal{P} \subset \mathcal{P}_K$, determine the number of effective divisors from a given divisor class C with a given number of places from $\mathcal{P}$ in the support.

This will answer the geometric problem described in the Introduction.

Let $\mathbf{C}C(K)$ be the complex group algebra of $C(K)$. Its elements are the functions

$$f : C(K) \longrightarrow \mathbf{C}, \quad f(C) = 0 \text{ almost everywhere.}$$

A basis for $\mathbf{C}C(K)$ as infinite dimensional complex vector space is given by the characteristic functions X^C, for $C \in C(K)$. Let $\mathbf{C}[[C(K)]]$ be the complex algebra of functions

$$f : C(K) \longrightarrow \mathbf{C}, \quad f(C) = 0 \text{ if } \deg(C) < 0,$$

such that the ring operations coincide with $\mathbf{C}C(K)$ on operands of finite support.

Lemma 2.1. *The* distribution L_K*, defined as the function that assigns to each divisor class its number of effective divisors, is an element of* $\mathbf{C}[[C(K)]]$.

As an element of $\mathbf{C}[[C(K)]]$, the distribution L_K is represented as an infinite sum $\sum_C L(C)X^C$. We agree to write $L(C)$, without index.

Lemma 2.2. *Let* $\overline{D}$ *be the image in* $C(K)$ *of a divisor* $D \in D(K)$*. The distribution* L_K *has an Euler expansion*

$$L_K = \prod_{P \in \mathcal{P}_K} (1 - X^{\bar{P}})^{-1} \in \mathbf{C}[[C(K)]].$$

Proof. Combine the definition of L_K and that of effective divisors. □

Another somewhat formal consequence arises from the sequence (1). Note that the sequence splits, but that there exists no canonical projection $C(K) \longrightarrow \Gamma$. For a divisor class E of degree one, not necessarily effective, we have a projection $[\,] = [\,]_E$,

$$0 \longrightarrow \langle E \rangle \longrightarrow C(K) \xrightarrow{[\,]} \Gamma \longrightarrow 0, \tag{2}$$

and $C(K) = \Gamma \times \langle E \rangle$. The characteristic function of E is denoted by $T = X^E$.

Lemma 2.3. *With E as free generator for $C(K)$, and $T = X^E$, we have a representation $L_K = L(T)$ with coefficients in $\mathbf{C}\Gamma$,*

$$L(T) = \prod_{P \in \mathcal{P}_K} (1 - X^{[\bar{P}]} T^{\deg(P)})^{-1} \in \mathbf{C}\Gamma[[T]].$$

Proof. From the previous lemma and $\bar{P} = [\bar{P}] + \deg(P)E$. □

In writing $L(T)$, we assume that the function field K has been fixed. While the distribution L_K is uniquely determined, the representation $L(T)$ depends on the choice of E as a free generator. Different representations differ by a transformation $T = X^{E-E'}T'$. The further properties of $L(T)$ use some well-known properties of the group algebra $\mathbf{C}\Gamma$. It is a finite commutative algebra with natural basis $\{X^g : g \in \Gamma\}$. The eigenvectors for multiplication by X^g in $\mathbf{C}\Gamma$ do not depend on $g \in \Gamma$. And the set of common eigenvectors provides another natural basis for $\mathbf{C}\Gamma$.

Lemma 2.4. *Let Γ be a finite abelian group. For a character χ of Γ, let*

$$e_\chi = \frac{1}{|\Gamma|} \sum_{g \in \Gamma} \chi(-g) X^g.$$

For $g \in \Gamma$, the element $\mathbf{e}_\chi$ is an eigenvector for the multiplication by X^g,

$$X^g \, e_\chi = \chi(g) \, e_\chi.$$

Proof. Straightforward. □

Let $\hat{\Gamma}$ be the group of characters of Γ.

Proposition 2.5. *The set $\{e_\chi : \chi \in \hat{\Gamma}\}$ gives the basis of primitive orthogonal idempotents for $\mathbf{C}\Gamma$. For $g \in \Gamma$,*

$$X^g = \sum_{\chi \in \hat{\Gamma}} \chi(g) e_\chi.$$

Proof. After the lemma, the two claims are equivalent. When written out they express the first and second orthogonality relations on characters. A direct proof of the first claim is in [10, Appendix]. □

Definition 2.6. We define $L(T, g) \in \mathbf{C}[[T]]$ and $L(T, \chi) \in \mathbf{C}[[T]]$ as the coordinates of $L(T)$ with respect to the bases $\{X^g\}$ and $\{e_\chi\}$ respectively,

$$L(T) = \sum_g L(T, g) X^g = \sum_\chi L(T, \chi) e_\chi.$$

For the coordinate function $L(T, g)$, we have the following interpretation.

Lemma 2.7. *The function $L(T, g) \in \mathbf{C}[[T]]$ is the generating function for the number of effective divisors $L(g + rE)$ in the divisor class $g + rE$, where $T = X^E$,*

$$L(T, g) = \sum_{r \geq 0} L(g + rE)T^r.$$

With respect to the basis of primitive idempotents $\{e_\chi\}$, both addition and multiplication in $\mathbf{C}\Gamma$ are defined componentwise. And the coordinate functions $L(T, \chi)$ take a convenient form.

Lemma 2.8. *The function $L(T, \chi) \in \mathbf{C}[[T]]$ has a product expansion*

$$L(T, \chi) = \prod_P (1 - \chi([\bar{P}])T^{\deg P})^{-1} \in \mathbf{C}[[T]].$$

Proof. Lemma 2.3 and Lemma 2.4. □

The lemma shows that the coordinate functions $L(T, \chi)$ are nothing but Dirichlet L-series of the function field K after a change of variables $T = q^{-s}$. But they are of a particularly easy kind. They correspond to Dirichlet characters of trivial conductor. The Dirichlet L-series are important for various reasons. Their appearance in this section has a computational motivation. The distribution $L(T)$ in Lemma 2.3 is computed with multiplications over $\mathbf{C}\Gamma$, i.e. matrix multiplications over $\mathbf{C}$. The coordinate functions $L(T, \chi)$ in Lemma 2.8 can be computed with scalar multiplications over $\mathbf{C}$.

3. Automorphisms

Automorphisms of the function field K act naturally on all of $\mathcal{P}$, $D(K)$, $P(K)$, $C(K)$, Γ, and $\hat{\Gamma}$. With an automorphism group acting on the group Γ, we can afford to work in the invariant subalgebra S of the group algebra $\mathbf{C}\Gamma$. We define bases for S and we define coordinate functions with respect to these bases. Working with subalgebras like S has proven to be an extremely useful technique in algebraic combinatorics [3], [5]. The results we need have short proofs, which are included.

For E as in (2), let A be a subgroup of automorphisms of K that fixes E. In particular, the action of A on $C(K)$ is described by the action on Γ. Note that A acts in a canonical way on $\hat{\Gamma}$ via composition, $\alpha(\chi) = \chi \circ \alpha$.

Definition 3.1. Let $\boldsymbol{\Omega} = \{\Omega_0 = 0, \Omega_1, \ldots, \Omega_r\}$ be the orbits of Γ under A, and let

$$\omega_i = \sum_{g \in \Omega_i} X^g, \qquad i = 0, 1, \ldots, r.$$

Let $\boldsymbol{\mathcal{E}} = \{\mathcal{E}_0 = 0, \mathcal{E}_1, \ldots, \mathcal{E}_s\}$ be the orbits of $\hat{\Gamma}$ under A, and let

$$e_j = \sum_{\chi \in \mathcal{E}_j} e_\chi, \qquad j = 0, 1, \ldots, s.$$

The sizes of the classes in $\boldsymbol{\Omega}$ and $\boldsymbol{\mathcal{E}}$ are called *degrees* and *multiplicities* respectively and are not necessarily comparable. On the other hand, it is well-known that $r = s$. In fact, the action of $\alpha \in A$ on $\mathbf{C}\Gamma$ can be described by either $X^g \mapsto X^{\alpha g}$ or $e_\chi \mapsto e_{\alpha^{-1}\chi}$. And both $\{\omega_i\}$ and $\{e_j\}$ give a vector space basis for the invariant subalgebra S. The latter basis has the following important property.

Proposition 3.2. *The basis* $\{e_j : j = 0, 1, \ldots, s\}$ *gives the basis of primitive orthogonal idempotents for* S.

Proof. Since the e_χ, for $\chi \in \hat{\Gamma}$, are orthogonal idempotents, so are the e_j, for $j = 0, 1, \ldots, s$. All elements of S, in particular the primitive idempotents, can be expressed on the basis $\{e_j\}$. It follows that the e_j are primitive idempotents for S. □

Corollary 3.3. *The element* e_j *is an eigenvector for the multiplication by* ω_i.

$$\omega_i \, e_j = \sum_{g \in \Omega_i} \chi(g) \, e_j,$$

for any $\chi \in \mathcal{E}_j$.

Proof. The first claim uses the proposition. For the eigenvalue, multiply both sides of the equality by e_χ, for any $\chi \in \mathcal{E}_j$, and compare $\omega_i \, e_\chi = \sum_{g \in \Omega_i} \chi(g) \, e_\chi$ with Lemma 2.4. □

The corollary contains the following observation.

Lemma 3.4. *For all* $i = 0, 1, \ldots, r$ *and* $j = 0, 1, \ldots, s$,

$$\begin{aligned} \sum_{g \in \Omega_i} \chi(g) &= \sum_{g \in \Omega_i} \chi'(g), \qquad \text{for } \chi, \chi' \in \mathcal{E}_j, \\ \sum_{\chi \in \mathcal{E}_j} \chi(g) &= \sum_{\chi \in \mathcal{E}_j} \chi(g'), \qquad \text{for } g, g' \in \Omega_i. \end{aligned}$$

Proof. A direct proof uses

$$\frac{1}{|A|} \sum_{\alpha \in A} \chi(\alpha g) = \frac{1}{|\Omega_i|} \sum_{g \in \Omega_i} \chi(g) = \frac{1}{|\mathcal{E}_j|} \sum_{\chi \in \mathcal{E}_j} \chi(g). \quad \square$$

Definition 3.5. Let $\boldsymbol{\Omega}$ and $\boldsymbol{\mathcal{E}}$ be partitions as in Definition 3.1. The *first eigenmatrix* P and the *second eigenmatrix* Q are defined by

$$\begin{aligned} P_{j,i} &= \sum_{g \in \Omega_i} \chi(g), \quad \chi \in \mathcal{E}_j. \\ Q_{i,j} &= \sum_{\chi \in \mathcal{E}_j} \chi(g), \quad g \in \Omega_i. \end{aligned}$$

The first columns of P and Q consist of ones only. The degrees and the multiplicities can be found in the first rows of P and Q respectively.

Proposition 3.6. *With* P *and* Q *as defined above, the conversion of the bases* $\{\omega_i\}$ *and* $\{e_j\}$ *becomes*

$$(\omega_i) = (e_j)(P_{j,i}), \qquad (e_j) = (\omega_i)\frac{1}{|\Gamma|}(\overline{Q}_{i,j}). \tag{3}$$

Proof. The first part follows Corollary 3.3. For the second part, to see the coefficients, it suffices to have e_j expressed on the basis $\{X^g\}$ of $\mathbf{C}\Gamma$. Use Definition 3.1 and Lemma 2.4. □

In particular,

$$P\overline{Q} = |\Gamma| I. \tag{4}$$

For a known first eigenmatrix P and for known multiplicities, the second eigenmatrix Q follows immediately. With Lemma 3.4,

$$|\Omega_i| Q_{i,j} = |\mathcal{E}_j| P_{j,i}. \tag{5}$$

Theorem 3.7. *Let S be the invariant subalgebra of $\mathbf{C}\Gamma$ defined at the start of the section. The distribution $L(T)$ is contained in $S[[T]]$. We define coordinate functions $L(T, \omega_i) \in \mathbf{C}[[T]]$ and $L(T, e_j) \in \mathbf{C}[[T]]$,*

$$L(T) = \sum_i L(T, \omega_i)\omega_i = \sum_j L(T, e_j) e_j.$$

We have $L(T, \omega_i) = L(T, g)$, for any $g \in \Omega_i$, and $L(T, e_j) = L(T, \chi)$, for any $\chi \in \mathcal{E}_j$. The coordinate functions are transformed into one another as

$$L(T, \omega_i) = \frac{1}{|\Gamma|} L(T, e_j)(\overline{Q}_{i,j})^T, \qquad L(T, e_j) = L(T, \omega_i)(P_{j,i})^T.$$

Proof. The transformation follows with (3). □

Both in group theory and in algebraic combinatorics, generalizations of the algebra S exist. An algebra $S = \mathbf{C}[\omega_0, \omega_1, \ldots, \omega_r]$ that is generated by the characteristic functions of a partition $\Omega = \{\Omega_0 = 0, \Omega_1, \ldots, \Omega_r\}$ of a group Γ is called a *Schur ring (of dimension $r+1$) over* Γ if it has dimension $r+1$ as complex vector space. The converse of Lemma 3.4 can be useful. If the lemma holds for partitions $\mathbf{\Omega}$ and $\boldsymbol{\mathcal{E}}$, then the equalities in Corollary 3.3 hold, the partition $\mathbf{\Omega}$ defines a Schur ring and the partition $\boldsymbol{\mathcal{E}}$ defines its primitive idempotents.

A further generalization runs as follows. As a subalgebra of $\mathbf{C}\Gamma$, the algebra S has a natural regular representation on the basis $\{X^g : g \in \Gamma\}$. A characteristic function ω_i is represented by a $0,1$-matrix A_i of size $|\Gamma|$. The matrices $\{A_i\}$ represent a set of disjoint relations $\{R_i\}$ on $\Gamma \times \Gamma$, with $(g, g') \in R_i$ if and only if $g - g' \in \Omega_i$. A set of disjoint relations $\{R_i\}$ on a set $X \times X$ is called an *association scheme (of $r+1$ classes) over X* if the algebra $S = \mathbf{C}[A_0, A_1, \ldots, A_r]$ has dimension $r+1$ as complex vector space [3], [5]. Often, one starts with a given relation R_1 on $X \times X$, which is then studied through an association scheme containing it.

By their very definition, there is an apparent duality between the partitions $\mathbf{\Omega}$ and $\boldsymbol{\mathcal{E}}$. The partition $\boldsymbol{\mathcal{E}}$ defines a Schur ring $\hat{S}$ contained in $\mathbf{C}\hat{\Gamma}$, for which the partition $\mathbf{\Omega}$ defines the primitive idempotents. The matrix Q becomes first eigenmatrix and the matrix P the second eigenmatrix. We call a partition *self-dual* if the eigenmatrices P, Q are equal. An example is the partition of Γ and $\hat{\Gamma}$ into elements. We give a nontrivial example. Proposition 4.6 will give a family of nontrivial examples.

Example 3.8. Let K be the function field of the curve defined by $y^2 + y = x^5$ over F_{16}. The field K has 33 rational places; hence it is maximal with zeta-function $Z_K(T) = (1 + 4T)^4/(1 - T)(1 - 16T)$. All automorphisms fix the place at infinity ∞. We let $E = \overline{\infty}$ and take A the group of all geometric automorphisms. The

place corresponding to the point $(0,0)$ has stabilizer of order five,

$$\begin{aligned} x &\mapsto x' = \zeta x, \\ y &\mapsto y' = y, \end{aligned} \tag{6}$$

for $\zeta^5 = 1$. The set of automorphisms

$$\begin{aligned} x &\mapsto x' = x + a, & (x') &= (a,b) + (a,b+1) - 2\infty, \\ y &\mapsto y' = y + a^8x^2 + a^4x + b^4, & (y') &= 5(a,b) - 5\infty, \end{aligned}$$

for $a, b \in F_{16}$ such that $b^2 + b = a^5$, acts transitively on the finite places of degree one. Hence A has order 160. The group Γ is elementary abelian of order 625. An elementary way, though not the shortest way, to see that Γ is annihilated by five involves functions of the type y' above, for $a, b \in \overline{F}_{16}$. Table 1 gives the order of the automorphisms and the number of fixed points. By Burnside's lemma there are eight orbits. They are listed in Table 2. Under the Frobenius, the number of orbits reduces to six, with new orbits $\Omega_4 \cup \Omega_5$ and $\Omega_6 \cup \Omega_7$. To find the character partition $\boldsymbol{\mathcal{E}}$, we will first recall the Tate-pairing. It allows us to identify the character group $\hat{\Gamma}$ with Γ. It turns out that, under the geometric automorphisms, the orbits of the character group $\hat{\Gamma}$ coincide with those of Γ. On $\hat{\Gamma}$, the Frobenius also yields two new orbits. They correspond to $\Omega_1 \cup \Omega_2$ and $\Omega_6 \cup \Omega_7$ and differ from those on Γ.

TABLE 1. Automorphisms acting on Γ, for $y^2 + y = x^5/\mathbf{F}_{16}$.

order	fixed points	frequency
1	625	1
2	1	1
2	25	10
4	1	20
5	5	64
10	1	64

TABLE 2. Orbits of Γ, for $y^2 + y = x^5/\mathbf{F}_{16}$.

i	$\lvert\Omega_i\rvert$	$\Omega_i + 2\infty$		
0	1	2∞		
1	32	$P + \infty$,	$\deg(P) = 1$	
2	32	$2P$,	$\deg(P) = 1$	
3	80	Q,	$\deg(Q) = 2$	
4	80	$(a,b) + (a',b')$,	$(a-a')^5 = 1$,	$(0,0) + (1,\alpha) \in \Omega_4$
5	80	$(a,b) + (a',b')$,	$(a-a')^5 = 1$,	$(0,0) + (1,\bar{\alpha}) \in \Omega_5$
6	160	$(a,b) + (a',b')$,	$(a-a')^5 = \alpha$	
7	160	$(a,b) + (a',b')$,	$(a-a')^5 = \bar{\alpha}$	

4. Tate-pairing

The distribution $L(T)$ is a formal series in T with coefficients in the subalgebra S of $\mathbf{C}\Gamma$. The main step in making the series explicit is the computation of the eigenmatrices P and Q. This is feasible if S is of small dimension. The matrices contain the eigenvalues for multiplication in S,

$$P_{j,i} = \sum_{g \in \Omega_i} \chi(g), \ \chi \in \mathcal{E}_j.$$

The L-series $L(T, \chi)$ can be computed using these eigenvalues and the transformation that yields the functions $L(T, g)$ is given by the eigenmatrices. This section focuses on the computation of the eigenmatrices.

For the evaluation of characters on Γ, we can in some cases rely on a natural pairing, defined on $\Gamma \times \Gamma$. We use a reduced form of the Tate-pairing for abelian varieties over local fields. Frey and Rück [9, Proposition 2.3] use a result of Lichtenbaum to obtain an explicit formulation of the pairing . Also, they show that the pairing is well-defined over a finite field after reduction [9, Proposition 2.5]. The explicit formulation is suitable for computing particular eigenmatrices.

Let K be a function field with constant field k of size q and divisor class group $C(K) = D(K)/P(K)$. Recall that Γ is the torsion subgroup of $C(K)$.

Definition 4.1. For $m > 0$ prime to q, let

$$\Gamma_m = \{\overline{D} \in \Gamma : mD \in P(K)\}.$$

For a function $f \in K$ and a divisor $E = \sum n_P P$ with $(f) \cap E = \emptyset$, let

$$f(E) = \prod f(P)^{n_P} \in k^*.$$

Lemma 4.2. *For a divisor D with $mD \in P(K)$, let $f \in K$ be a function with $(f) = mD$. Let E be a divisor of degree zero such that $D \cap E = \emptyset$. The following hold.*

(a) *The value $f(E)$ does not depend on the choice of f.*
(b) *For $D \in P(K)$, we have $f(E) \in {k^*}^m$.*
(c) *For $E \in P(K)$, we have $f(E) \in {k^*}^m$.*
(d) *For $E \in mD(K)$, we have $f(E) \in {k^*}^m$.*

Proof. Properties (b) and (d) are obvious. Property (a) follows with $deg(E) = 0$. Property (c) follows from the Weil reciprocity $f((g)) = g((f))$, for $f, g \in K$ such that $(f) \cap (g) = \emptyset$. □

Theorem 4.3. [9] *Let the constant field k of K contain the m-th roots of unity. The Tate-pairing $\{-,-\}_m$, defined as*

$$\begin{aligned} \{-,-\}_m : \quad & \Gamma_m \times \Gamma/m\Gamma \longrightarrow k^*/{k^*}^m, \\ & \{\overline{D}, \overline{E}\}_m = f(E), \end{aligned}$$

is non-degenerate.

Proof. The pairing is well-defined by the lemma. For the non-degeneracy, see [9]. □

The easy part of the proof is contained in Lemma 4.2, which gives that the pairing is well-defined. To obtain a self-contained proof for particular results obtained with the pairing, it suffices to verify ad hoc that the pairing is non-degenerate.

Lemma 4.4. *For an automorphism α of the function field K, we have*

$$\{\alpha\overline{D}, \alpha\overline{E}\}_m = \alpha\{\overline{D}, \overline{E}\}_m.$$

Proof. Immediate with $\alpha f(\alpha P) = \alpha(f(P))$, that is, $f - a \in P$ if and only if $\alpha f - \alpha a \in \alpha P$. □

Example 4.5. Example 3.8 continued. The curve defined by $y^2 + y = x^5$ over F_{16} has class group $\Gamma = \Gamma_5$ of exponent five and rank four. The Tate-pairing is well-defined for $m = 5$. We may identify the character group with $\Gamma/5\Gamma = \Gamma$. For finite points $(a, b), (a', b')$ with $a \neq a'$, we evaluate the pairing

$$\{(a, b) - (a, b + 1), (a', b') - (a', b' + 1)\}_5 \in k^*/k^{*5}.$$

Example 3.8 gives y' with $(y') = 5(a, b) - 5\infty$ and further evaluation is straightforward. Table 3 gives the result for $(a, b), (a', b')$ among

$$(0, 0), (\gamma^{3i}, \gamma^5), (\gamma^{5+3i}, \gamma^8), (\gamma^{10+3i}, \gamma^4), \quad i = 0, 1, 2, 3, 4.$$

In the five by five matrices lines and columns add up to zero modulo five. Observe also that the lemma applies with α as in (6). The four indicated lines with the appropriate sign correspond to $(a, b) = (\gamma^8, \gamma^8), (\gamma^2, \gamma^2), (\gamma, \gamma), (\gamma^4, \gamma^4)$ respectively. These are the only four lines in the matrix corresponding to a Frobenius orbit that are independent.

TABLE 3. Evaluation of the Tate-pairing.

0	0	0	0	0	0	2	2	2	2	2	1	1	1	1	1	
0	0	3	1	4	2	4	3	0	0	3	3	0	1	1	0	
0	2	0	3	1	4	3	4	3	0	0	0	3	0	1	1	
0	4	2	0	3	1	0	3	4	3	0	1	0	3	0	1	
0	1	4	2	0	3	0	0	3	4	3	1	1	0	3	0	
0	3	1	4	2	0	3	0	0	3	4	0	1	1	0	3	
3	1	2	0	0	2	0	4	0	0	1	0	1	3	2	4	
3	2	1	2	0	0	1	0	4	0	0	4	0	1	3	2	+
3	0	2	1	2	0	0	1	0	4	0	2	4	0	1	3	
3	0	0	2	1	2	0	0	1	0	4	3	2	4	0	1	
3	2	0	0	2	1	4	0	0	1	0	1	3	2	4	0	−
4	2	0	4	4	0	0	1	3	2	4	0	0	3	2	0	
4	0	2	0	4	4	4	0	1	3	2	0	0	0	3	2	
4	4	0	2	0	4	2	4	0	1	3	2	0	0	0	3	−
4	4	4	0	2	0	3	2	4	0	1	3	2	0	0	0	+
4	0	4	4	0	2	1	3	2	4	0	0	3	2	0	0	

Proposition 4.6. *The partition Ω of Γ_m into orbits under the geometric automorphisms is self-dual. The partition $\boldsymbol{\mathcal{E}}$ of the character group of Γ_m into orbits under the Frobenius automorphism is stable under $Frob/p$.*

Proof. Characters $\{-, \overline{E}\}$ and $\{-, \overline{E}'\}$ are in the same orbit if and only if there exists $\alpha \in A$ with

$$\{-, \overline{E}'\} = \{\alpha(-), \overline{E}\} = \{-, \alpha^{-1}\overline{E}\},$$

i.e. if and only if $\overline{E}$ and $\overline{E}'$ are in the same orbit. For the second claim, use

$$\{Frob(-), Frob(\frac{1}{p}\overline{E})\} = Frob\{-, \frac{1}{p}\overline{E}\} = \{-, \frac{1}{p}\overline{E}\}^p = \{-, \overline{E}\}.$$

□

Example 4.7. Example 4.5 continued. The partition $\boldsymbol{\mathcal{E}}$ of the characters into orbits under the geometric automorphisms is the same as the partition $\boldsymbol{\Omega}$ for group elements. Hence the eigenmatrices P and Q coincide. They are completely determined by Tables 2 and 3. For $x + y = -1, xy = -31$,

$$P = Q = \begin{bmatrix} 1 & 32 & 32 & 80 & 80 & 80 & 160 & 160 \\ 1 & 7 & 7 & -20 & 5 & 5 & 5\,x & 5\,y \\ 1 & 7 & 7 & -20 & 5 & 5 & 5\,y & 5\,x \\ 1 & -8 & -8 & -5 & 10 & 10 & 0 & 0 \\ 1 & 2 & 2 & 10 & 15 & -10 & -10 & -10 \\ 1 & 2 & 2 & 10 & -10 & 15 & -10 & -10 \\ 1 & x & y & 0 & -5 & -5 & 5 & 5 \\ 1 & y & x & 0 & -5 & -5 & 5 & 5 \end{bmatrix}$$

In particular, $P\overline{P} = 625I$ by (4). Under the group of all automorphisms, including the Frobenius, the number of orbits reduces to six. The partition Ω has new orbits $\Omega_4 \cup \Omega_5$ and $\Omega_6 \cup \Omega_7$. The partition $\mathcal{E}$ has new orbits $\mathcal{E}_1 \cup \mathcal{E}_2$ and $\mathcal{E}_4 \cup \mathcal{E}_5$. The eigenmatrices for the coarser partitions can be computed from the given eigenmatrices in a straightforward way with Definition 3.5.

5. Functional equation

We continue the description of the distribution $L(T)$ of effective divisors over divisor classes and of its coordinate functions $L(T, g)$ and $L(T, \chi)$. Similar to the zeta function, which describes the enumeration of effective divisors, we obtain that the distribution $L(T)$ is a rational function that satisfies a functional equation. The relevant information of $L(T) \in \mathbf{C}\Gamma[[T]]$ is contained in a finite term $L^*(T) \in \mathbf{C}\Gamma[T]$ that satisfies the same functional equation. All properties follow from the Riemann-Roch theorem.

For the function field K, let W denote the canonical divisor class and γ the genus. The Riemann-Roch theorem claims, for the dimension $l(C)$ of an arbitrary divisor class C,

$$l(C) - l(W - C) = \deg(C) + 1 - \gamma.$$

As in Section 2, our interest is in the number $L(C)$ of effective divisors in the divisor class C. For

$$L(C) = (q^{l(C)} - 1)/(q - 1),$$

we obtain

$$L(C) = (q^{\deg(C)+1-\gamma} - 1)/(q - 1) + L(W - C)\, q^{\deg(C)+1-\gamma}. \tag{7}$$

As in Lemma 2.7, let $L(T, g)$ be the generating function of $L(g + rE)$, for $r \geq 0$,

Lemma 5.1. *The function $L(T,g)$ can be written as*

$$L(T,g) = \frac{T^\gamma}{(1-T)(1-qT)} + L^*(T,g),$$

with $L^*(T,g)$ a polynomial with non-negative integer coefficients. The degree of $L^*(T,g)$ is at most $2\gamma-2$. For precisely one $g \in \Gamma$ the degree is $2\gamma-2$.

Proof. With (7),

$$L^*(T,g) = \sum_{r=0}^{\gamma-1} L(g+rE)T^r + \sum_{r\geq\gamma} L(W-g-rE)q^{r+1-\gamma}T^r.$$

The contribution is trivial for $r > 2\gamma-2$. The only nontrivial term for $r = 2\gamma-2$ occurs for $g = W-(2\gamma-2)E$. □

The zeta function $Z(T)$ is the generating function for the number of all effective divisors of degree r, for $r \geq 0$. Hence

Corollary 5.2. *The zeta function $Z(T)$ can be written as*

$$Z(T) = \frac{|\Gamma|T^\gamma}{(1-T)(1-qT)} + Z^*(T),$$

with $Z^*(T)$ a polynomial of degree $2\gamma-2$ with non-negative integer coefficients.

Proof. Use the previous lemma and $Z(T) = \sum_g L(T,g)$. □

We define a $\mathbf{C}$-linear involution on $\mathbf{C}\Gamma$ via $\overline{X^g} = X^{-g}$, or what amounts to the same $\overline{e_\chi} = e_{\chi^{-1}}$.

Theorem 5.3. *The distribution $L(T)$ is a rational function,*

$$L(T) = \sum_g \frac{T^\gamma}{(1-T)(1-qT)} X^g + L^*(T),$$

with functional equation

$$L(T) = \overline{L(1/qT)} X^{[W]} (qT^2)^{\gamma-1} \in \mathbf{C}\Gamma(T).$$

The polynomial $L^*(T)$ is of degree $2\gamma-2$.

Proof. $L(T) = \sum_g L(T,g)X^g$, and the lemma yields the rationality and the degree of $L^*(T)$. We include a direct proof of the functional equation, but see the remark below. It is well defined over $\mathbf{C}\Gamma(T)$, but not over the ring $\mathbf{C}\Gamma[[T]]$ because of the operation $T \mapsto 1/qT$. First, we observe that the leading term

$$\sum_g \frac{T^\gamma}{(1-T)(1-qT)} X^g$$

satisfies the functional equation. The remaining term

$$L^*(T) = \sum_g L^*(T,g)X^g$$

is polynomial of degree $2\gamma-2$ and can be considered over $\mathbf{C}\Gamma[[T]]$. Or over $\mathbf{C}[[C(K)]]$ after the substitution $T = X^E$. As in the proof of the lemma,

$$\sum_g L^*(T,g)X^g = \sum_{\deg C=0}^{\gamma-2} L(C)X^C + \sum_{\deg C=\gamma-1} L(C)X^C + \sum_{\deg C=\gamma}^{2\gamma-2} L(W-C)q^{\deg C+1-\gamma}X^C. \tag{8}$$

In the functional equation, a term $L(C)X^C$ on the left gives rise to a term $L(C)\ q^{\gamma-1-\deg(C)}\ X^{W-C}$ on the right. This transforms the remaining term $L^*(T)$ into itself. □

The functional equation of $L(T)$ is equivalent to the functional equation

$$L(T,\chi) = L(1/qT,\chi^{-1})\chi([W])(qT^2)^{\gamma-1} \tag{9}$$

of its coordinate functions $L(T,\chi)$. The more general version of (9), for arbitrary abelian L-functions of the function field K, was conjectured by Hasse and proved by Weissinger [32]. The polynomial term $L^*(T)$ describes the important contribution of the special divisors. We denote the right-hand side of (8) by L^*_K. Some proofs for the functional equation of the zeta function use a different polynomial term that enumerates all divisors of degree at most $2\gamma-2$ [31], [24].

Lemma 5.4. *For a non-trivial character χ,*

$$L(T,\chi) = L^*(T,\chi)$$

is a polynomial of degree $2\gamma-2$ with cyclotomic integer coefficients. For the trivial character χ_0,

$$L(T,\chi_0) = Z(T), \qquad L^*(T,\chi_0) = Z^*(T).$$

Proof. For an arbitrary character χ, $L(T,\chi) = \sum_g \chi(g)L(T,g)$ and $L^*(T,\chi) = \sum_g \chi(g)L^*(T,g)$. Now use Lemma 5.1. □

Example 5.5. Example 4.7 continued. For the curve $y^2+y=x^5/\mathbf{F}_{16}$,

$$Z(T) = \frac{625T^2}{(1-T)(1-16T)} + (1+33T+16T^2).$$

Let $\mathbf{\Omega}$ and $\boldsymbol{\mathcal{E}}$ be the partitions into six classes of Γ and $\hat{\Gamma}$ respectively. Tables 4 and 5 give the coordinate functions of $L^*(T)$.

TABLE 4. The series $L^*(T,\chi)$, for $\chi \in \mathcal{E}_j$ $(x+y=-1, xy=-31)$.

j	$\lvert\mathcal{E}_j\rvert$	$L^*(T,\chi)$
0	1	$1+33T+16T^2$
1	64	$1+8T+16T^2$
2	80	$1-7T+16T^2$
3	160	$1+3T+16T^2$
4	160	$1+(x+1)T+16T^2$
5	160	$1+(y+1)T+16T^2$

TABLE 5. The series $L^*(T,g)$, for $g \in \Omega_i$.

i	$\lvert\Omega_i\rvert$	$L^*(T,g)$
0	1	$1+T+16T^2$
1	32	T
2	32	0
3	80	0
4	160	0
5	320	0

6. Hilbert class fields

It is obvious from the definitions that the functions $L(T,g)$ have as their sum the zeta function of the function field K,

$$Z_K(T) = \sum_g L(T,g).$$

It is not obvious that the product of the functions $L(T,\chi)$ yields the zeta function of a function field K', that is finite over K,

$$Z_{K'}(T) = \prod_\chi L(T,\chi). \tag{10}$$

This can be established with the help of class field theory. Outside this section, we will only use the following result.

Theorem 6.1. *The reciprocal zeros of $L(T,\chi)$ have absolute value $q^{1/2}$.*

Proof. Apply the analogue of the Riemann hypothesis in Weil's theorem to the function field K'. □

The main theorems of class field theory go far beyond what is needed to prove (10). We recall briefly that only (part of) Hilbert's theorem on class fields is needed. We present the theorem by Hilbert in the original ideal formulation for number fields. It was first proved by Furtwangler. Being in the function field case, we need some care to apply the result.

Theorem 6.2. *For a given number field K, there exists uniquely an abelian extension K'/K satisfying the following conditions:*

(a) *The galois group of K'/K is isomorphic to the class group of the ring of integers O of K.*
(b) *The extension K'/K is unramified.*
(c) *For a prime ideal P in K, let f be minimal such that P^f is principal. Then P has relative degree f in K'/K.*
(d) *Every ideal in K is, when extended to K', principal.*

Proof. See e.g. [13], which also contains some of the older references. □

We will not need (d), the principal ideal theorem, which was proved only in 1930. And we add to (b) the fact that all archimedean primes split in K'/K. The theorem follows in a straightforward way from the later obtained much more general theorems by Takagi and Artin. Using the idèle notation introduced by Chevalley,

these theorems obtain a natural form suited to both the number field case and the function field case [1], [13].

We will see that the proper interpretation of Hilbert's theorem for K a function field will imply (10). A careful translation is carried out in [23]. We need a Dedekind domain in the role of ring of integers. Let ∞ be a fixed rational place of K, if necessary after a finite constant field extension, and let $E = \overline{\infty}$ denote its divisor class as in (2). Let O be the ring of functions with poles at ∞ only. The class group of O is given by $C(K)/\langle E\rangle \simeq \Gamma$. Decomposition of places in the extension K'/K of K is to be understood as decomposition of ideals in O in the integral closure O' of O in K'. The place ∞ splits completely in K'/K. An ideal P^f is principal in O if and only if $f(P - \deg(P)\infty)$ is principal in K.

Proposition 6.3. *For a function field K, fix a rational place ∞ with divisor class $E = \overline{\infty}$. Let K'/K be the maximal abelian unramified extension of K in which ∞ splits completely. Then*

$$Z_{K'}(T) = \prod_{\chi} L(T, \chi),$$

with the $L(T,\chi)$ defined as in Definition 2.6, for $T = X^E$.

Proof. As in [12, Theorem 6]:

$$\begin{aligned}
\prod_{\chi} L(T,\chi) &= \prod_{\chi}\prod_{P}(1-\chi([\bar{P}])T^{\deg P})^{-1},\\
&= \prod_{P}\prod_{\chi}(1-\chi([\bar{P}])T^{\deg P})^{-1},\\
&= \prod_{P}\Big(\prod_{\zeta^f=1}(1-\zeta T^{\deg P})^{-1}\Big)^{|\Gamma|/f},\\
&= \prod_{P}((1-T^{f\deg P})^{-1})^{|\Gamma|/f},\\
&= \prod_{P}\prod_{P'|P}(1-T^{\deg P'})^{-1},\\
&= \prod_{P'}(1-T^{\deg P'})^{-1},\\
&= Z_{K'}(T).
\end{aligned}$$

Note that all of (a),(b) and (c) in Theorem 6.2 are used. □

For a different choice of the place ∞, we find a twist of the extension K'/K. Now consider our original claim (10) for the case $T = X^E$, with E not the class of a rational place. Clearly, the claim still holds if we choose for K'/K the proper twist. Indeed, there are $[K' : K] = |\Gamma|$ twists of K'/K, some of which correspond to a splitting place, some of which do not. Let k' be the constant field of degree $|\Gamma|$ over k. The compositum $k'K'/K$ is of degree $|\Gamma|^2$. From [1]: "It is invariantly defined and is actually the correct generalization of the Hilbert Class Field." In our case, the class E is always assumed to be fixed (though it need not be the class of a rational place). And we can refer to the proper twist K'/K as the Hilbert Class Field.

7. Geometric Goppa codes

We first give the definitions and some basic results for general linear codes, and will then consider the class of geometric Goppa codes. For details and for the omitted proofs we refer to [18], [28], [4] for coding theory, and to [29], [26], [20], [24] for geometric Goppa codes.

A *linear code* C of *length* n is a subspace of the space of all n-letter words over a finite field. The elements of C are called *codewords*. For applications, such as in communication or in information storage, it is important that the codeword as a whole can be recovered if not all its letters are reliable. This leads to a packing problem with respect to the Hamming metric. The Hamming distance of two words is defined as the number of positions at which they differ. For a code with *minimum Hamming distance* d, a codeword with at most t unreliable letters at t unknown positions can be recovered if $2t < d$. A linear code of *dimension* $k \geq 1$ contains non-trivial codewords with at least $k-1$ zeros, i.e. within distance $n-k+1$ of the all zero codeword. Thus

$$k + d \leq n + 1.$$

The inequality is called the Singleton bound. Codes for which the bound is tight are called maximum-distance-separable (MDS). Important examples are the codes obtained with the rational embedding in the Introduction.

Definition 7.1. The *weight distribution* of a code C is the vector $(A_0, A_1, \ldots, A_n)$, where A_i is the number of codewords with precisely i coordinates different from zero. In particular $A_0 = 1, A_1 = \ldots = A_{d-1} = 0, A_d > 0$.

The most important theorem for weight distributions of linear codes is the following, whose proof is elementary. The dual of a linear code is defined as the set of vectors that is orthogonal to the code with respect to the standard inner product.

Theorem 7.2 (MacWilliams identities)**.** *Let* $W = W(U,V) = \sum A_i U^{n-i} V^i$ *be the homogeneous* weight enumerator *of a linear code* C *of length* n *and dimension* k*. The dual linear code* C' *has weight enumerator*

$$W'(U,V) = q^{-k} W(U + (q-1)V, U - V).$$

We turn to the definition of a geometric Goppa code [11]. For such codes, we will be able to describe the weight distribution. Let K be an algebraic function field in one variable with finite constant field, and let $\mathcal{P}_K$ be the set of all the places of K. For a divisor D, let $L(D)$ be the associated space of functions f with $(f) + D \geq 0$.

Definition 7.3. Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\} \subset \mathcal{P}_K$ be a subset of rational places, and let D be a divisor of K with support disjoint from $\mathcal{P}$. The linear code $C(\mathcal{P}, D)$ of length n is defined as the set of codewords

$$(f(P_1), f(P_2), \ldots, f(P_n)), \qquad \text{for } f \in L(D).$$

For a function field K of genus γ, the parameters of a geometric Goppa code satisfy the Goppa bound

$$k + d \geq n + 1 - \gamma.$$

This explains partly why the construction is interesting. The codes can be chosen large while maintaining a good separation of the codewords. Good codes are

obtained from curves with many rational points, for a given genus. A first step towards computing weight distributions of geometric Goppa codes is a translation into a problem on divisors.

Lemma 7.4. *Let $C(\mathcal{P}, D)$ be a geometric Goppa code with $\deg D < n$. For $i < n$, the number of codewords with precisely i zeros is equal to $q-1$ times the number of effective divisors $E \in |D|$ with precisely i places of $\mathcal{P}$ in the support.*

Proof. A codeword $\boldsymbol{c} \in C(\mathcal{P}, D)$ determines uniquely the function $f \in L(D)$ with $\boldsymbol{c} = (f(P_1), f(P_2), \dots, f(P_n))$ if we assume $\deg D < n$. Let $E = (f) + D$. A codeword $\boldsymbol{c}$ has i zeros if and only if E has i places of $\mathcal{P}$ in its support. For we assumed $D \cap \mathcal{P} = \emptyset$, whence

$$(f)_0 \cap \mathcal{P} = ((f)_0 + D - (f)_\infty) \cap \mathcal{P} = E \cap \mathcal{P}.$$

A divisor $E \in |D|$ determines up to a scalar multiple a function $f \in L(D)$ and a codeword $c \in C(\mathcal{P}, D)$. □

Codes with a non-trivial kernel $L(D - \mathcal{P})$ are called *abundant codes* and form a small but interesting class [21]. For such codes, the lemma needs to be modified by correcting for the size of the kernel.

The distribution $L(T)$ gives us the number of effective divisors in the linear system $|D|$. But it does not tell how they intersect with the set $\mathcal{P}$. To be able to distinguish between places in $\mathcal{P}$ and places not in $\mathcal{P}$ in the support of an effective divisor, we use a distribution $\Lambda(T)$. The notation is defined in Section 2.

Definition 7.5. For a set $\mathcal{P}$ of rational places of the function field K, let

$$\Lambda_{\mathcal{P}} = \prod_{P \in \mathcal{P}} (1 + X^{\bar{P}}) \in \mathbf{C}[[C(K)]].$$

In analogy with Lemma 2.3, we next consider a representation $\Lambda_{\mathcal{P}} = \Lambda(T)$ with coefficients in $\mathbf{C}\Gamma$.

Lemma 7.6. *For E a divisor class of degree one, and for $T = X^E$,*

$$\Lambda(T) = \prod_{P \in \mathcal{P}} (1 + X^{[\bar{P}]} T^{\deg(P)}) \in \mathbf{C}\Gamma[T].$$

Let $\Omega = ([\bar{P}] : P \in \mathcal{P})$. The elements of Ω are either all zero, for genus zero, or all different, for genus at least one. Since $P \in \mathcal{P}$ is of degree one, we may write

$$\Lambda(T) = \prod_{g \in \Omega} (1 + X^g T) \in \mathbf{C}\Gamma[T]. \tag{11}$$

We now have two different coordinate functions at our disposal. The coordinate function $L(T, g) \in \mathbf{C}[T]$ is the generating function for the number of all effective divisors in the divisor class $g + rE$. The coordinate function $\Lambda(T, g) \in \mathbf{C}[T]$ is the generating function for the number of sums of r different rational places in the divisor class $g + rE$. Together, $L(T)$ and $\Lambda(T)$ enable us to formulate a generating function for weight distributions.

Theorem 7.7. *The distribution of effective divisors that contain precisely a given number of elements from $\mathcal{P}$ is given by*

$$A(U, T) = L(T)\Lambda(U - T) \in \mathbf{C}\Gamma[U](T).$$

The coordinate function $A(U,T,g) \in \mathbf{C}[U][[T]]$ is the generating function for the number of effective divisors in the divisor class $g+(i+j)E$ with precisely i elements of $\mathcal{P}$ in the support.

Proof. The local factor in $A(U,T)$ at a place $P \in \mathcal{P}$ is, for $g = [\bar{P}]$,

$$\frac{1+X^g(U-T)}{1-X^gT} = 1 + X^gU + X^{2g}UT + X^{3g}UT^2 + \cdots .$$

Hence the variable U keeps track of the precise number of places $P \in \mathcal{P}$ that contribute to a term of $A(U,T)$. □

The variable U provides a notation other than T for X^E. By writing U for T at appropriate places in the distribution $L(T)$, we find the finer distribution $A(U,T)$ of effective divisors with a given number of places from $\mathcal{P}$ in the support. With $U = T$, the distribution $A(U,T)$ reduces to $A(T,T) = L(T)$.

The geometric interpretation of $A(U,T)$ is as follows. Let X be a smooth curve with function field K. Choose a basis $f_0, f_1, \ldots, f_{k-1}$ of $L(D)$ and consider the embedding

$$(f_0 : f_1 : \ldots : f_{k-1}) : X \longrightarrow \mathbf{P}^{k-1}.$$

The zeros of a codeword $(f(P) : P \in \mathcal{P})$, for $f \in L(D)$, form the intersection of the embedded set $\mathcal{P}$ with a hyperplane in $\mathbf{P}^{k-1}$. The intersection divisors of the hyperplanes are the elements of the linear system of the divisor D. And the theorem gives the generating function for the number of hyperplanes containing a fixed number of rational points $P \in \mathcal{P}$. From Theorem 5.3, we see that $A(U,T)$ consists of a constant term and of a contribution due to special divisors.

Lemma 7.8. *Let*

$$A^*(U,T) = L^*(T)\Lambda(U-T)$$

define the contribution due to special divisors. Then $A^*(U,T) \in \mathbf{C}\Gamma[U,T]$. And the coefficients of $A^*(U,T)$ and $A(U,T)$ at T^j coincide for $j = 0, 1, \ldots, \gamma-1$.

Proof. Both $L^*(T)$ and $\Lambda(T)$ are polynomial; hence so is $A^*(U,T)$. The second statement expresses that all effective divisors of degree up to $\gamma-1$ are special. Formally, the difference $A(U,T) - A^*(U,T) = (L(T) - L^*(T))\Lambda(U-T)$ has leading degree γ in the variable T. □

For $j \geq \gamma$, either the constant term or the term $A^*(U,T)$ may have negative coefficients. For large j, weight distributions of geometric Goppa codes are close to those of random codes, which is made precise in [30]. If the zeta function of the function field is known, estimates can be obtained by averaging over divisor classes [7].

Theorem 7.9. *For a function field K with zeta function $Z(T)$, the average weight distribution*

$$\overline{A}(U,T) = \frac{1}{|\Gamma|}\sum_g A(U,T,g) = \frac{1}{|\Gamma|}Z(T)(1+U-T)^n.$$

Proof.

$$\frac{1}{|\Gamma|}\sum_g A(U,T,g) = \frac{1}{|\Gamma|}A(U,T,\chi_0) = \frac{1}{|\Gamma|}L(T,\chi_0)\Lambda(U-T,\chi_0). \quad \square$$

In Section 9, we follow the opposite direction and define for an arbitrary linear code a zeta function as a function of its weight distribution.

8. Duality of weight distributions

We show that the generating function $A(U,T)$ has a functional equation that expresses the MacWilliams identity for geometric Goppa codes in an intrinsic form. We already saw in Theorem 5.3 that the factor $L(T)$ has a functional equation and consider now the factor $\Lambda(U-T)$.

Lemma 8.1. *For $\Lambda(T)$, defined with $\mathcal{P} = \{P_1, P_2, \ldots, P_n\} \subset \mathcal{P}_K$,*

$$\Lambda(T) = \overline{\Lambda(1/T)} X^{[\Sigma \bar{P}]} T^n.$$

Proof. Use (11), and

$$\prod_{g \in \Omega} (1 + X^g T) = \prod_{g \in \Omega} (1 + X^{-g} T^{-1}) X^g T. \quad \square$$

While $A(U,T)$ contains precisely the information we are interested in, it is often more convenient to work with the related distribution $B(U,T) = A(U+T,T) = L(T)\Lambda(U)$. Its interpretation is given by

Proposition 8.2. *The distribution of effective divisors (counted with multiplicities) that contain at least a given number of elements from $\mathcal{P}$ is given by*

$$B(U,T) = L(T)\Lambda(U) \in \mathbf{C}\Gamma[U](T).$$

The coordinate function $B(U,T,g) \in \mathbf{C}[U][[T]]$ is the generating function for the number of effective divisors (counted with multiplicities) in the divisor class $g + (i+j)E$ with at least i elements of $\mathcal{P}$ in the support.

Proof. Terms $X^g U^i T^j$ in $B(U,T)$ come from effective divisors in the class $g + (i+j)E$ that are the sum of i places from $\mathcal{P}$ and an arbitrary effective divisor of degree j. $\square$

Weight distributions with multiplicities appear in [4, p.437]. Their usefulness for geometric Goppa codes is pointed out in [15]. For an application of Clifford's theorem, see [26, Theorem 3.1.54]. The proposition gives the weight distribution with multiplicities through a generating function. As with the function $A(U,T)$, we define for $B(U,T)$ the contribution due to special divisors by

$$B^*(U,T) = L^*(T)\Lambda(U) \in \mathbf{C}\Gamma[U,T].$$

Proposition 8.3. *The distributions $A(U,T)$ and $B(U,T)$ have functional equations*

$$\begin{aligned} A(U,T) &= \overline{A(1/(U-T)+1/qT, 1/qT)} X^{[W+\Sigma\bar{P}]} (U-T)^n (qT^2)^{\gamma-1}, \\ B(U,T) &= \overline{B(1/U, 1/qT)} X^{[W+\Sigma\bar{P}]} U^n (qT^2)^{\gamma-1}. \end{aligned}$$

The same functional equations hold for $A^*(U,T)$ and $B^*(U,T)$ respectively.

Proof. Use Theorem 5.3 and Lemma 8.1. $\square$

Let $D = g + aE$ and $D' = g' + a'E$ be divisors with $D + D' = W + \Sigma P$. The weight distributions of $C(\mathcal{P}, D)$ and $C(\mathcal{P}, D')$ are given by the coefficients $A_{a-j,j,g}$ and $A_{a'-j,j,g'}$ in $A(U,T)$ respectively. The functional equation yields the following relations.

Theorem 8.4. *Let* $(g+g')+(a+a')E = W+\Sigma P$. *For* $b \in \mathbf{Z}$,

$$\left(\sum_{j=0}^{\gamma-1+b} \binom{a-j}{a+1-\gamma-b} A_{a-j,j,g} + \frac{1}{q-1}\binom{n}{a+1-\gamma-b}\right) q^{-b/2}$$
$$= \left(\sum_{j=0}^{\gamma-1-b} \binom{a'-j}{a'+1-\gamma+b} A_{a'-j,j,g'} + \frac{1}{q-1}\binom{n}{a'+1-\gamma+b}\right) q^{b/2}.$$

Proof. We may apply the functional equation to $B^*(U,T)$ to obtain

$$B^*_{i,l,g} = B^*_{n-i,2\gamma-2-l,g'}\, q^{l+1-\gamma}.$$

Furthermore,

$$B_{i,l,g} - B^*_{i,l,g} = \frac{q^{l+1-\gamma}-1}{q-1}\binom{n}{i}, \quad \text{for } l \geq \gamma-1,$$

and zero otherwise. Hence, for $l \geq \gamma-1$,

$$B_{i,l,g} - \frac{q^{l+1-\gamma}-1}{q-1}\binom{n}{i} = B_{n-i,2\gamma-2-l,g'}\, q^{l+1-\gamma}.$$

Or

$$B_{i,l,g} + \frac{1}{q-1}\binom{n}{i} = \left(B_{n-i,2\gamma-2-l,g'} + \frac{1}{q-1}\binom{n}{n-i}\right) q^{l+1-\gamma}.$$

Because of symmetry the equality still holds for $l \leq \gamma-1$. For then $2\gamma-2-l \geq \gamma-1$. From $B(U,T) = A(U+T,T)$,

$$B_{i,l,g} = \sum_{j=0}^{l} \binom{i+l-j}{i} A_{i+l-j,j,g}.$$

Substitution in the previous expression with $a = i+l$, $a' = n+2\gamma-2-i-l$, and $b = l+1-\gamma$ gives the required result. □

The relations are the MacWilliams identities, Theorem 7.2. Up to notation, the relations on the A-coefficients occur in [4] and those on the B-coefficients in [15]. Indeed, the dual code of $C(\mathcal{P},D)$ is of the form $C(\mathcal{P},D')$ for a suitable divisor $D' \sim W + \sum P - D$. The proof involves the residue theorem and can be found in the cited books. The residue theorem enters implicitly in the proof of the theorem through the Riemann-Roch theorem.

Corollary 8.5. *The weight distributions of the codes* $C(\mathcal{P},D)$ *and* $C(\mathcal{P},D')$ *are determined by the combined set of coefficients* $A_{a-j,j,g}$ *and* $A_{a'-j,j,g'}$ *for* $j = 0,1,\ldots,\gamma-1$. *The remaining coefficients can be computed with the relations in the theorem.*

Proof. For $j \geq \gamma$, use the relations with $b > 0$ to compute $A_{a-j,j,g}$ and with $b < 0$ to compute $A_{a'-j,j,g'}$. □

This is a special case of a corollary to the general MacWilliams identities.

Theorem 8.6 ([15])**.** *Weight distributions of a linear code and its dual are determined by the combined partial distributions* $(A_i : i = d,\ldots,n-k)$ *and* $(A'_i : i = d',\ldots,n-k')$.

To interpret the corollary, observe that the relevant information is contained in $B^*(U,T) = L^*(T)\Lambda(U)$. It has degree $2\gamma - 2$ in T and in general it has $2\gamma - 1$ monomials of given total degree. The $2\gamma - 1$ coefficients for the code $C(\mathcal{P}, D)$ and those for the code $C(\mathcal{P}, D')$ are related through the functional equation. In the next section, we give a similar formulation for arbitrary linear codes. The first case where $B^*(U,T)$ is non-trivial arises for $\gamma = 1$.

Theorem 8.7 ([6], [15])**.** *For the code $C(\mathcal{P}, D)$ constructed with an elliptic curve and a divisor $D = g + aE$ of degree $a < n$, the number of words of weight $n - a$ is $q - 1$ times the number of different ways that $g \in \Gamma$ can be written as sum of a distinct elements $[\bar{P}]$, for $P \in \mathcal{P}$.*

Proof. For an elliptic curve, the only special divisor is the zero divisor and $L^*(T) = X^0 = 1 \in \mathbf{C}\Gamma$. Hence $B^*(U,T) = \Lambda(U)$ and $A^*(U,T) = \Lambda(U - T)$. With Lemma 7.4 and Lemma 7.8, the coefficient $A_{n-a} = (q-1)A_{a,0,g} = (q-1)A^*_{a,0,g}$. The interpretation of A_{n-a} follows with (11). □

9. Rational curves and linear codes

A generating function $A(U,T)$ for an arbitrary linear code will be defined by comparing the code with codes from the rational function field. For the rational function field K, let $\mathcal{P} \subset \mathcal{P}_K$ be a set of n rational places. The classgroup Γ is trivial and $L(T) = Z(T)$, $\Lambda(T) = (1+T)^n$. Hence,

$$A(U,T) = \frac{(1+U-T)^n}{(1-T)(1-qT)} = \sum A_{i,j} U^i T^j. \tag{12}$$

Lemma 9.1. *For a divisor D of degree $a = -1, 0, 1, 2, \ldots, n-1$, the code $C(\mathcal{P}, D)$ is of dimension $k = a + 1$ with weight distribution*

$$W_a = U^n + (q-1)\sum_{i=0}^{a} A_{i,a-i} U^i. \tag{13}$$

Proof. Combine Theorem 7.7 and Lemma 7.4. For the lemma, observe that none of the codes is of abundant type. □

We will consider (12) and (13) also for $n > q + 1$. In that case W_a no longer has the interpretation as weight distribution for the rational function field and may have negative coefficients. Note that

$$A(UT, T) = \sum_{a \geq 0} (W_a(U) - U^n)/(q-1)T^a.$$

Now let C be an arbitrary linear code of length n and minimum distance d. Let $a = n - d$ denote the maximum number of zeros in a non-trivial word of C. The weight enumerator W of C is a linear combination of $W_a, W_{a-1}, \ldots, W_0, W_{-1}$. In other words, if we write

$$W(U,T) = \sum_{a=-1}^{n-1} W_a(U) T^a,$$

then there exists a unique polynomial $P(T)$ of degree at most $a + 1$, such that W is the coefficient of T^a in $P(T)W(U,T)$.

Proposition 9.2. *The polynomials $P(T)$ and $P'(T)$, for dual codes C and C' respectively, are of the same degree* $\deg P = \deg P' = \gamma + \gamma'$, *for* $\gamma = n + 1 - k - d$ *and* $\gamma' = n + 1 - k' - d'$. *Furthermore,*

$$P'(T) = P(1/qT)q^{\gamma}T^{\gamma+\gamma'}, \tag{14}$$

and $P(1) = P'(1) = 1$.

Proof. Let $a = n - d$ and let

$$W = p_0 W_a + \cdots + p_\gamma W_{a-\gamma} + \cdots + p_{a+1} W_{-1}.$$

The code C has dimension $k = n + 1 - d - \gamma = a + 1 - \gamma$. The code with weight distribution W_a is of dimension $a + 1$ with dual weight distribution W_{n-a-2}. An application of the MacWilliams transform for a k-dimensional code yields

$$W' = p_0 q^{-\gamma} W_{n-a-2} + \cdots + p_\gamma W_{n-a+\gamma-2} + \cdots + p_{a+1} q^{a+1-\gamma} W_{n-1}.$$

Now W' is a linear combination of $W_{a'}, W_{a'-1}, \ldots, W_0, W_{-1}$, for $a' = n - d'$. In particular $p_j > 0$, for $j = a' - (n - a - 2)$. And $p_j = 0$ for $j > a' - (n - a - 2)$ or for $j > a + a' + 2 - n = (n - d) + (n - d') + 2 - (k + n - k) = \gamma + \gamma' \geq 0$. This proves the claim on the degree. The transformation from W to W' reverses the order of the coefficients p_j. And the scaling by powers of q in the transformation agrees with (14). Finally, since both W and each of the W_a contain a unique term U^n, we have that $1 = P(1)$. □

The parameter $\gamma = n + 1 - k - d$ is sometimes called the genus of a linear code. In [26, p.16], the genus is defined as the maximum of $n+1-k-d$ and $n+1-k'-d'$. In this paper, we use both γ and γ', but never their maximum.

Definition 9.3. For the code C with polynomial $P(T)$ as in the proposition, we define the zeta function

$$Z(T) = \frac{P(T)}{(1 - T)(1 - qT)}.$$

Corollary 9.4.

$$Z(T) = \frac{T^{\gamma}}{(1 - T)(1 - qT)} + Z^*(T),$$

for a polynomial $Z^*(T)$ of degree $\gamma + \gamma' - 2$.

It is now only natural to introduce for an arbitrary linear code functions $A(U, T)$, $B(U, T)$, $A^*(U, T)$, $B^*(U, T)$ similar to those defined for geometric Goppa codes. We indicate some of the properties without pursuing the details here.

Theorem 9.5. *For a code C with zeta function $Z(T)$, let*

$$A(U, T) = Z(T)(1 + U - T)^n = \sum A_{i,j} U^i T^j.$$

The code C has weight distribution

$$W = U^n + (q - 1) \sum_{i=0}^{a} A_{i,a-i} U^i.$$

The projective weight distribution $(W - U^n)/(q - 1)$ is obtained as the coefficient of T^a in $A(UT, T)$.

With $B^*(U,T) = Z^*(T)(1+U)^n$, we obtain, similar to the remark after Theorem 8.6, that $\gamma+\gamma'-1$ coefficients suffice to compute the weight distributions of a code and its dual. The transform in Theorem 7.2 becomes

Theorem 9.6. *The dual code C' of C has zeta function*

$$Z'(T) = Z(1/qT)q^{\gamma-1}T^{\gamma+\gamma'-2}.$$

Necessary and sufficient conditions for a code to be formally self-dual are $2k = n$ and $Z'(T) = Z(T)$.

Example 9.7. The average weight distribution for a function field K has $Z(T) = Z'(T) = Z_K(T)/|\Gamma|$. For two famous codes, the binary extended Hamming code of type $[8,4,4]$ and the ternary extended Golay code of type $[12,6,6]$, we compute zeta functions

$$Z(T) = \frac{(1+2T+2T^2)/5}{(1-T)(1-2T)}, \qquad Z(T) = \frac{(1+3T+3T^2)/7}{(1-T)(1-3T)}$$

respectively. They correspond with the average distribution of maximal elliptic curves over the field of two and three elements. This is not a coincidence. It is easy to show that the zeta function of a code with a transitive automorphism group is invariant under puncturing or shortening. The codes have a 3-transitive and a 5-transitive automorphism group respectively. After shortening we can compute the zeta function from codes generated by $(1,1,1,1,0)$ and $(1,1,1,1,1,1,0)$ respectively. And the latter codes have the unique weight distribution of a one-dimensional code defined on all the points of an elliptic curve.

One of the interesting topics that we leave undiscussed is that of constant field extensions. The zeta function $Z_L(T)$, for a constant field extension L/K, is determined by the zeta function $Z_K(T)$. For a given code C, the weight distribution does in general not determine the weight distribution after a constant field extension [16]. It does suffice however to consider finitely many constant field extensions. The relations between weight distributions for different constant field extensions appear to be important for the study of generalized Hamming weights [33], [27].

10. Computation of weight distributions

Weight distributions of geometric Goppa codes are closely related to the distribution of effective divisors over divisor classes, Lemma 7.4. Hence we were able to formulate in Theorem 7.7 a generating function $A(U,T)$ for weight distributions by a modification of the distribution $L(T)$ of effective divisors. We show that some of the properties of $L(T)$ that were established in Sections 3 and 4 carry over to $A(U,T)$ and we apply them to the computation of $A(U,T)$.

As in Section 3, for a function field K and a fixed divisor class E of degree one, let A be a group of automorphisms of K that fixes E. The group A acts on the torsion Γ of the divisor class group $C(K)$ of K. Let $S \subset \mathbf{C}\Gamma$ be the fixed subalgebra of $\mathbf{C}\Gamma$ under the action of A.

Lemma 10.1. *For a set of places $\mathcal{P}$ that is stable under A,*

$$\Lambda(T) \in S[T].$$

Proof. The coefficients are invariant under A, hence are in S. □

The function $A(U,T)$ is a priori an element of $\mathbf{C}\Gamma[U](T)$. Under the assumption of the lemma the coefficients are in S. Bases for S are given in Definition 3.1.

Proposition 10.2. *For a set of places $\mathcal{P}$ that is stable under A, the distributions $A(U,T)$ and $B(U,T)$ have coefficients in the subalgebra $S \subset \mathbf{C}\Gamma$. The subalgebra has two natural bases, that define decompositions*

$$\begin{aligned} A(U,T) &= \sum_i A(U,T,\omega_i)\omega_i = \sum_j A(U,T,e_j)e_j \in S[U](T), \\ B(U,T) &= \sum_i B(U,T,\omega_i)\omega_i = \sum_j B(U,T,e_j)e_j \in S[U](T). \end{aligned}$$

Proof. Use Theorem 3.7 and the previous lemma. Or use directly the interpretation of $A(U,T)$ given in Theorem 7.7. □

For the weight distribution of a geometric Goppa code, we need to know the coordinates on the basis (ω_i). But the coordinates on the basis (e_j) are easier to compute. Hence,

Theorem 10.3. *The coordinate function $A(U,T,\omega_i)$ can be computed with*

$$\begin{aligned} A(U,T,e_j) &= L(T,e_j)\Lambda(U-T,e_j), \\ A(U,T,\omega_i) &= \frac{1}{\Gamma}(\overline{Q}_{i,j})A(U,T,e_j). \end{aligned}$$

Proof. The second step is the coordinate transformation (3). The first step uses that the e_j are idempotents in a commutative algebra, in particular

$$A(U,T)e_j = L(T)\Lambda(U-T)e_j = L(T)e_j\Lambda(U-T)e_j. \quad \square$$

Because of the first step, the computation of weight distributions with the theorem is feasible only if we can compute the L-series $L(T,e_j)$. That is, if we can compute the L-series for the Hilbert class field extension K'/K of K. Fortunately, many interesting curves have a large automorphism group that leads to relations among the L-series.

Lemma 10.4. *Let $T = X^E$. For an arbitrary automorphism $\alpha \in Aut(K)$,*

$$L(T,\chi\circ\alpha) = L(\chi(E-\alpha E)T,\chi).$$

Moreover, if $\mathcal{P}$ is stable under α,

$$\Lambda(T,\chi\circ\alpha) = \Lambda(\chi(E-\alpha E)T,\chi).$$

Proof. Write $L(T,\chi\circ\alpha)$ as in Lemma 2.8.

$$\begin{aligned} &\prod_{P\in\mathcal{P}_K} (1-\chi\circ\alpha(\bar{P}-(\deg P)E)T^{\deg P})^{-1} \\ &= \prod_{P\in\mathcal{P}_K} (1-\chi(\alpha\bar{P}-(\deg P)E+(\deg P)E-\alpha(\deg P)E)T^{\deg P})^{-1} \\ &= \prod_{P\in\mathcal{P}_K} (1-\chi(\bar{P}-(\deg P)E)(\chi(E-\alpha E)T)^{\deg P})^{-1}. \end{aligned}$$

For $\Lambda(T,\chi\circ\alpha)$ use Lemma 7.6. This time the product runs over $P\in\mathcal{P}$. □

We reformulate Theorem 10.3 with a weaker assumption on the group of automorphisms A.

Proposition 10.5. *Assume that the set $\mathcal{P}$ and the divisor class mE are both stable under $A \subset Aut(K)$. The terms in $A(U,T)$ of total degree a multiple of m have coefficients in the fixed subalgebra S of A in $\mathbf{C}\Gamma$.*

Proof. With the lemma, the substitution $T = \chi(E - \alpha E)T, U = \chi(E - \alpha E)U$ in $A(U,T)$ does not affect terms of total degree a multiple of m. □

The proposition implies that it may be convenient to perform the coordinate transformation in Theorem 10.3 termwise. Terms of degree a multiple of m can be expressed on a smaller basis and are therefore easier to compute. An application of the proposition with $m = 4$ will be given later for the Hermitian curve of degree four.

Example 10.6. Example 5.5 continued. We consider codes defined with the curve $y^2 + y = x^5/\mathbf{F}_{16}$, with for $\mathcal{P}$ the set of 32 finite rational points. To compute $A(U,T)$ with Theorem 10.3, it suffices after Example 4.7 and Example 5.5 to give $\Lambda(T)$. The coordinates $\Lambda(T,\chi)$ are determined by the second column of P in Example 4.7. They can also be computed directly from Tables 2 and 3. Let $a + b = -1, ab = -1$, and let $x = 5a + 2, y = 5b + 2$, i.e. $x + y = -1, xy = -31$. (See Table 6.)

TABLE 6. The series $\Lambda(T,\chi)$ $(a + b = -1, ab = -1)$.

j	$\lvert\mathcal{E}_j\rvert$	$\Lambda(T,\chi)$
0	1	$(1+T)^{32}$
1	64	$(1+T)^{12}\,(1-T+T^2-T^3+T^4)^5$
2	80	$(1-T+T^2-T^3+T^4)^8$
3	160	$(1+T)^8\,(1-T+T^2-T^3+T^4)^6$
4	160	$(1+T)^6\,(1-T+T^2-T^3+T^4)^4\,(1+aT+T^2)^5$
5	160	$(1+T)^6\,(1-T+T^2-T^3+T^4)^4\,(1+bT+T^2)^5$

11. Codes from class groups

We have introduced the partition $\mathbf{\Omega}$ of a class group Γ in order to describe weight distributions of geometric Goppa codes $C(\mathcal{P}, D)$. In this section, we briefly point out that the partition itself defines a class of codes. For $r > 0$, let $E_r \subset E(K)$ denote the set of effective divisors of degree r, and let

$$\Omega^r = ([\bar{D}] \in \Gamma : D \in E_r)$$

be the projection with multiplicities of E_r on the class group Γ. Thus $|\Omega^r| = |E_r|$.

Definition 11.1. The code $C(\Omega^r, \Gamma)$ of length $n = |\Omega^r|$ has as codewords

$$(\chi(g) : g \in \Omega^r), \qquad \text{for } \chi \in \hat{\Gamma}.$$

The code has the structure of the subgroup of Γ that is generated by Ω^r. The alphabet is given by the complex roots of unity whose order divides the exponent of the subgroup. In additive notation, the alphabet is their homomorphic image in the modular integers. It remains to describe the distance between codewords.

Lemma 11.2. *For $\chi \in \hat{\Gamma}$ of order m, the codeword $(\chi(g) : g \in \Omega^r)$ has precisely w non-trivial coordinates if and only if*

$$\sum_{\chi \in \langle \chi \rangle \setminus \chi_0} \sum_{g \in \Omega^r} \chi(g) = (m-1)n - mw.$$

Proof. Add χ_0 to the outer sum and change the order of summation. □

We assume that Ω^r generates Γ.

Proposition 11.3. *For $r > 0$, let the charactersum over Ω^r be bounded by M, for a non-principal character $\chi \in \hat{\Gamma}$,*

$$|\sum_{g \in \Omega^r} \chi(g)| \leq M.$$

For $\chi \in \hat{\Gamma}$ of order m, the weight w of the codeword $(\chi(g) : g \in \Omega^r)$ lies in the interval

$$\frac{m-1}{m}(n-M) \leq w \leq \frac{m-1}{m}(n+M).$$

Proof. Apply the bound to the lemma to obtain $|(m-1)n - mw| \leq (m-1)M$. □

Note that $M = n$ gives the trivial bound in case Ω^r does not generate Γ. The graph equivalent of the code in Definition 11.1 is the Cayley graph, coset graph or difference graph [17]. Such a graph has as vertices the elements of a group and two group elements are connected if and only if their difference is in a given subset. The proposition says that graphs with small eigenvalues correspond to codes with bounded weight distribution. For the function field K, let γ be the genus and q the size of the constant field.

Proposition 11.4. *For $r > 0$, and for a non-principal character $\chi \in \hat{\Gamma}$,*

$$|\sum_{\Omega^r} \chi(g)| \leq \binom{2\gamma - 2}{r} q^{r/2}.$$

Proof. The sum is the r-th coefficient in an L-series of degree $2\gamma - 2$. Now use Theorem 6.1. □

Example 11.5. Example 10.6 continued. We consider the code $C(\Omega^1, \Gamma)$ for the curve $y^2 + y = x^5/\mathbf{F}_{16}$. We may apply the proposition with $n = 33$, $m = 5$ and $M = 8$ to find $20 \leq w \leq 32$. The precise weights and their frequencies can be read off from Table 6. The rows in Table 3 generate a four dimensional code of length 16 over $\mathbf{F}_5$. It is obtained from $C(\Omega^1, \Gamma)$ by deleting one position ($g = 0$ at $P = \infty$) and taking half of the remaining positions (one of $\pm g$ at $P = (a, b), (a, b+1)$). The weight of a codeword is a priori in the range $10 \leq w \leq 16$, and the precise weight distribution is $(1, 0, \ldots, 0, 64, 0, 160, 320, 0, 0, 80)$.

The code $C(\Omega^r, \Gamma)$ is well-defined if we replace Ω^r with a proper subset $\Omega \subset \Omega^r$. On the other hand Proposition 11.4 no longer applies. A better approach is to fix Ω^r and to enlarge Γ to a ray class group of non-trivial conductor. The bound in Proposition 11.4 will be weaker.

12. Hermitian curve

The Hermitian curve $Y^qZ + YZ^q = X^{q+1}$ of degree $q+1$ over the field $\mathbf{F}_{q^2}$ attains the Hasse-Weil upper bound for the number of points on an algebraic curve. The numerator of the zeta function is completely determined and has $2\gamma = q(q-1)$ equal factors $(1+qT)$. We can therefore estimate weight distributions of Hermitian codes by their average weight distribution $\bar{A}(U,T)$ (Theorem 7.9). For curves of small degree, we may compute the actual weight distributions with Theorem 10.3.

The curve $Y^3Z + YZ^3 = X^4/\mathbf{F}_9$ is of genus 3 with 28 rational points and has class group $\Gamma = 4^6$. The automorphism group is of order $6048 = 28 \cdot 27 \cdot 8$ and acts 2-transitively on the rational points. We consider codes $C(\mathcal{P}, D)$ of length $n = 28$, i.e. $\mathcal{P}$ contains all the rational points. The class group has six orbits under the automorphism group. The partition into orbits is self-dual. The matrix $P = Q$ (Definition 3.5) was computed with the Tate-pairing (Theorem 4.3). Representatives for $L^*(T,\chi)$ and $\Lambda(T,\chi)$ are given in Table 7 and Table 8 respectively.

$$P = Q = \begin{bmatrix} 1 & 63 & 756 & 756 & 504 & 2016 \\ 1 & 63 & -12 & -12 & -8 & -32 \\ 1 & -1 & 36 & -28 & 24 & -32 \\ 1 & -1 & -28 & 36 & 24 & -32 \\ 1 & -1 & 36 & 36 & -40 & -32 \\ 1 & -1 & -12 & -12 & -8 & 32 \end{bmatrix}.$$

Table 7. Representatives for $L^*(T,\chi)$.

j	$\lvert\mathcal{E}_j\rvert$	$L^*(T,\chi)$
0	1	$1 + 28\,T + 406\,T^2 + 252\,T^3 + 81\,T^4$
1	63	$1 + 4\,T + 22\,T^2 + 36\,T^3 + 81\,T^4$
2	756	$1 + 8\,T + 30\,T^2 + 72\,T^3 + 81\,T^4$
3	756	$1 - 2\,T^2 + 81\,T^4$
4	504	$1 + 8\,T + 34\,T^2 + 72\,T^3 + 81\,T^4$
5	2016	$1 + 4\,T + 10\,T^2 + 36\,T^3 + 81\,T^4$

Table 8. Representatives for $\Lambda(T,\chi)$.

j	$\lvert\mathcal{E}_j\rvert$	$\Lambda(T,\chi)$
0	1	$(1+T)^{28}$
1	63	$(1+T)^{16}\,(1-T)^{12}$
2	756	$(1+T)^{10}\,(1-T)^{2}\,\left(1+T^2\right)^{8}$
3	756	$(1+T)^{6}\,(1-T)^{6}\,\left(1+T^2\right)^{8}$
4	504	$(1+T)^{12}\,(1-T)^{4}\,\left(1+T^2\right)^{6}$
5	2016	$(1+T)^{10}\,(1-T)^{6}\,\left(1+T^2\right)^{6}$

The stabilizer of a rational point gives a self-dual partition of Γ into 27 orbits. Under the Frobenius, this reduces to a non-self-dual partition of 21 orbits. From the coarser partition of six classes, we cannot deduce all different L-series and all different weight distributions. The coarser partition identifies characters whose L-series differ by a substitution $T = iT$, for $i^4 = 1$ (Lemma 10.4). But this suffices to describe the distribution of effective divisors of degree a multiple of four (Proposition 10.5). We apply Theorem 10.3 with these data to find the coefficients in $A(U, T, \omega)$ for i, j with $i + j \equiv 0 \pmod 4$. The relevant coefficients are presented in three tables, that correspond to $j = 0, 1, 2$ respectively (Corollary 8.5, Lemma 7.8). Each table has rows $a = i + j = 0, 4, \ldots, 28$ (the degree of the divisor D), columns $\omega_0, \omega_1, \ldots, \omega_5$ (the orbit of the divisor class of D), and entries $A_{a-j,j,\omega}$ (whose interpretation is given by Theorem 7.7). The orbit ω_0 contains unique divisor classes for a given degree. The classes are the multiples of a line, i.e of the canonical class. The column gives the intersection numbers for all homogeneous forms of a fixed degree. For example, the forms of degree four ($i + j = 16$) define a space of functions of dimension 14 on the curve. The tables show that $7119 \cdot 8$ of these forms intersect $\mathcal{P}$ in 16 points ($i = 16, j = 0$), that $139104 \cdot 8$ of them intersect $\mathcal{P}$ in 15 points ($i = 15, j = 1$), and that $1025136 \cdot 8$ of them intersect $\mathcal{P}$ in 14 points ($i = 14, j = 2$). All codes obtained with $i + j = 16$ are formally self-dual of type $[28, 14, 12]$ over $\mathbf{F}_9$.

TABLE 9. Coefficients of $A(U, T, \omega)$, for $j = 0$.

$i+j$	ω_0	ω_1	ω_2	ω_3	ω_4	ω_5
0	1	0	0	0	0	0
4	63	4	8	4	6	4
8	945	744	768	748	774	756
12	7119	7380	7416	7440	7412	7432
16	7119	7380	7416	7440	7412	7432
20	945	744	768	748	774	756
24	63	4	8	4	6	4
28	1	0	0	0	0	0

TABLE 10. Coefficients of $A(U, T, \omega)$, for $j = 1$.

$i+j$	ω_0	ω_1	ω_2	ω_3	ω_4	ω_5
0	0	0	0	0	0	0
4	0	0	1	4	0	3
8	2016	2080	2026	2044	1992	2021
12	60480	58176	57759	57528	57840	57630
16	139104	137952	137164	137080	137136	137082
20	29568	32384	31903	32164	31856	32079
24	0	576	522	556	552	561
28	0	0	1	0	0	0

TABLE 11. Coefficients of $A(U,T,\omega)$, for $j=2$.

$i+j$	ω_0	ω_1	ω_2	ω_3	ω_4	ω_5
0	0	0	0	0	0	0
4	0	6	1	0	0	0
8	1512	1932	1890	1940	1920	1947
12	167160	174410	175975	176692	175652	176325
16	1025136	1023048	1028476	1028136	1028880	1028478
20	560952	544770	548703	547304	548760	547626
24	24696	22972	23362	23300	23184	23255
28	0	30	25	36	36	33

TABLE 12. Weight distribution of a code over $\mathbf{Z}_4$ of length 28 and rank 7.

j	$\lvert\mathcal{E}_j\rvert$	weight
0	1	$W^{28}+X^{28}+Y^{28}+Z^{28}$
1	63	$W^{16}Y^{12}+W^{12}Y^{16}+X^{16}Z^{12}+X^{12}Z^{16}$
2	756	$W^{10}X^8Y^2Z^8+W^8X^{10}Y^8Z^2+W^2X^8Y^{10}Z^8+W^8X^2Y^8Z^{10}$
3	756	$2\,W^6X^8Y^6Z^8+2\,W^8X^6Y^8Z^6$
4	504	$W^{12}X^6Y^4Z^6+W^6X^{12}Y^6Z^4+W^4X^6Y^{12}Z^6+W^6X^4Y^6Z^{12}$
5	2016	$W^{10}X^6Y^6Z^6+W^6X^{10}Y^6Z^6+W^6X^6Y^{10}Z^6+W^6X^6Y^6Z^{10}$

The functions $\Lambda(T,\chi)$ give the weights of the code $C(\Omega^1,\Gamma)$ (Definition 11.1). Table 8 does not have all the functions. But it does contain the necessary information to describe a slightly larger code. If we write the codewords additively, i.e. over the alphabet $\mathbf{Z}/4\mathbf{Z}$, the enlarged code is obtained by adding the all one vector as generator to $C(\Omega^1,\Gamma)$. Table 12 is a mere translation of Table 8 into the standard notation for codes over $\mathbf{Z}/4\mathbf{Z}$.

CONCLUSION

In the setting of a function field in one variable over a finite constant field, a generating function for the weight distribution of algebraic-geometric codes can be formulated as $A(U,T) = L(T)\Lambda(U-T)$. The function $L(T)$ describes the distribution of effective divisors over divisor classes. The function $\Lambda(T)$ defines a restricted distribution that involves only the rational places. All functions have their coefficients in a group algebra. The function $L(T)$ relates to the L-series of the Hilbert class field. The function $\Lambda(T)$ can be interpreted as the weight distribution of a newly defined family of codes.

References

1. E. Artin and J.T. Tate. *Class field theory*. Math. Lecture Notes. Benjamin, New York, 1967.
2. E.F. Assmus Jr., H.F. Mattson Jr. and R.J. Turyn. Cyclic Codes. AFCRL-65-332, Air Force Cambridge Research Labs, Bedford, Mass., 1968. MR **36:**6383
3. E. Bannai and T. Ito. *Algebraic Combinatorics I: association schemes*. Benjamin / Cummings Publ. Co., Menlo Park, Calif., 1984. MR **87m:**05001
4. R. Blahut. *Theory and practice of error control codes*. Addison-Wesley, Reading, Mass., 1983. MR **85f:**94001
5. A.E. Brouwer, A.M. Cohen, and A. Neumaier. *Distance Regular Graphs*. Springer, 1989. MR **90e:**05001
6. Y. Driencourt and J.-F. Michon. Elliptic codes over a field of characteristic 2. *J. of Pure and Applied Algebra*, 45:15–39, 1987. MR **88m:**94029
7. I.M. Duursma. Average weight enumerators for geometric goppa codes. in: *ACCT-Proceedings*, p.82. Novgorod, Russia, 1994.
8. G.D. Forney. *Concatenated Codes*. The M.I.T. Press, Cambridge, Mass., 1966. MR **49:**12154
9. G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math.-Comp.*, 62(206):865–874, 1994. MR **94h:**11056
10. A. Fröhlich and M.J. Taylor. *Algebraic number theory*. Cambridge University Press, Cambridge, 1993. MR **94d:**11078
11. V.D. Goppa. Codes on algebraic curves. *Soviet Math. Dokl.*, 24:170–172, 1981. MR **82k:**94017
12. H. Heilbronn. Zeta-functions and L-functions. in: *Algebraic number theory*, eds. J.W.S. Cassels and A. Fröhlich. Academic Press, London, 1967. MR **36:**1414
13. S. Iyanaga. *The theory of numbers*, volume 8 of *Math. Lib.* North Holland, Amsterdam, 1975. MR **56:**2953
14. T. Kasami, S. Lin and W.W. Peterson. Some Results on Weight Distributions of BCH Codes. *IEEE Trans. Inf. Theor.*, 12:274, 1966.
15. G.L. Katsman and M.A. Tsfasman. Spectra of algebro-geometric codes. *Probl. Info. Trans.*, 23:262–275, 1987. MR **90a:**11149
16. T. Klove. The weight distribution of linear codes over $GF(q^l)$ having generator matrix over $GF(q)$. *Discrete Mathematics*,23:159–168, 1978. MR **81d:**94024
17. W.-C. W. Li. Character sums and abelian Ramanujan graphs. *J. of Numb. Th.*, 41:199–217, 1992. MR **93h:**11092
18. F.J. MacWilliams and N.J.A. Sloane. *The theory of error-correcting codes*. North Holland, Amsterdam, 1977. MR **57:**5408a; MR **57:**5408b
19. A.J. Menezes, I.F. Blake, R.C. Mullin, X. Gao, S.A. Vanstone, and T. Yaghoobian. *Applications of finite fields*, volume 0199 of *SECS*. Kluwer Acad. Publ., Dordrecht, The Netherlands, 1993.
20. C.J. Moreno. *Algebraic curves over finite fields*. Tracts in Mathematics. Cambridge Univ. Press, Cambridge, England, 1991. MR **92d:**11066
21. R. Pellikaan On the gonality of curves, abundant codes and decoding. in: *Proceedings AGCT-3*, Springer LNM 1518, Berlin 1992, 132–144. MR **93j:**14023
22. R. Pellikaan. On special divisors and the two variable zeta function of algebraic curves over finite fields. in: *Arithmetic, Geometry and Coding Theory*, eds. Pellikaan, Perret, Vlăduţ. deGruyter, Berlin, 1996. MR **97g:**11063
23. M. Rosen. The Hilbert class field in function fields. *Expo. Math.*, 5:365–378, 1987. MR **89b:**11094
24. H. Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer-Verlag, New York, 1993. MR **94k:**14016
25. M.A. Tsfasman. Global fields, codes and sphere packings. *Astérisque*, 198-200:373-396, 1991. MR **92j:**11063
26. M.A. Tsfasman and S.G. Vlăduţ. *Algebraic-geometric codes*. Kluwer Acad. Publ., Dordrecht, The Netherlands, 1991. MR **93i:**94023
27. M.A. Tsfasman and S.G. Vlăduţ. Geometric Approach to Higher Weights. *IEEE Trans. Infor. Th.*, 41:1564–1588, 1995. MR **97m:**94042
28. J.H. van Lint. *Introduction to coding theory*, volume 86 of *GTM*. Springer, Berlin, 1982. MR **84e:**94001
29. J.H. van Lint and G. van der Geer. *Introduction to coding theory and algebraic geometry*, volume 12 of *DMV Seminar*. Birkhaeuser, Basel, 1988. MR **91e:**94023

30. S.G. Vlăduţ. Two remarks on the spectra of algebraic geometry codes. in: *Arithmetic, Geometry and Coding Theory*, eds. Pellikaan, Perret, Vlăduţ. deGruyter, Berlin, 1996. MR **97g:**11064
31. A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Hermann, Paris, 1948. MR **10:**262c
32. J. Weissinger. Theorie der Divisorenkongruenzen. *Abh. Math. Sem. Hanischen Univ.*, 12:115-126, 1937.
33. V.K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Infor. Th.*, 37:1412–1418, 1991. MR **92i:**94019

AT&T Labs Research, 180 Park Avenue, Florham Park, New Jersey 07932

Current address: Department of Mathematics, University of Limoges, 123 avenue Albert Thomas, 87060 Limoges, France

E-mail address: duursma@unilin.fr