On a method of Duursma to compute weight distributions via L-functions

Virgile Ducet

LIX

GT BAC, 18 décembre 2015

Motivation

Let X be a curve of genus g over a finite field $\mathbb{F}_q$, such that

$$\#X(\mathbb{F}_q) = n + 1.$$

Let P_0 be a fixed rational point of X, and let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be the set of rational points of X distinct from P_0. For $r > 0$, let

$$\mathcal{L}(rP_0) = \{f \in \mathbb{F}_q(X) : (f) + rP_0 \geqslant 0\},$$

and let $\mathcal{C}$ be the code image of the map

$$\mathcal{L}(rP_0) \to \mathbb{F}_q^n$$

defined by

$$f \mapsto (f(P_1), \ldots, f(P_n)).$$

Let w_i be the number of codewords of $\mathcal{C}$ with *exactly* i zero coordinates.

Equivalently, the bijection between $\mathcal{L}(rP_0)/\mathbb{F}_q^*$ and the linear system

$$|rP_0| = \{D \geqslant 0 : \overline{D} = r\overline{P_0} \in \mathrm{Pic}(X)\},$$

defined by

$$f \mapsto (f) + rP_0,$$

implies that w_i is $(q-1)$ times the number of elements of $|rP_0|$ with precisely i elements of $\mathcal{P}$ in the support.

Let w_i be the number of codewords of $\mathcal{C}$ with *exactly* i zero coordinates.

Equivalently, the bijection between $\mathcal{L}(rP_0)/\mathbb{F}_q^*$ and the linear system

$$|rP_0| = \{D \geqslant 0 : \overline{D} = r\overline{P_0} \in \mathrm{Pic}(X)\},$$

defined by

$$f \mapsto (f) + rP_0,$$

implies that w_i is $(q-1)$ times the number of elements of $|rP_0|$ with precisely i elements of $\mathcal{P}$ in the support.

DEFINITION:

We are interested in the *weight distribution*

$$\mathcal{W} = (w_0, w_1, \ldots, w_n)$$

of $\mathcal{C}$.

Duursma's L-function

We want to find a convenient counting function. Let $\mathbb{C}(\mathrm{Pic}(X))$ be the complex group algebra of functions

$$\Phi : \mathrm{Pic}(X) \to \mathbb{C}$$

such that $\Phi(c) = 0$ for almost all c. A canonical basis consists of the indicator functions $\mathbb{1}_c$.

Duursma's L-function

We want to find a convenient counting function. Let $\mathbb{C}(\mathrm{Pic}(X))$ be the complex group algebra of functions

$$\Phi : \mathrm{Pic}(X) \to \mathbb{C}$$

such that $\Phi(c) = 0$ for almost all c. A canonical basis consists of the indicator functions $\mathbb{1}_c$.

Set

$$L = \sum_{\substack{D \in \mathrm{Div}(X) \\ D \geqslant 0}} \mathbb{1}_{\overline{D}} = \prod_{P \in X(\overline{\mathbb{F}_q})} (1 - \mathbb{1}_{\overline{P}})^{-1}.$$

We want to compute $L(r\overline{P_0})$.

For any class $\overline{D} \in \mathrm{Pic}(X)$, write

$$\overline{D} = [\overline{D}] + \deg(D)\overline{P_0} \quad \in \mathrm{Pic}^0(X) \oplus \langle \overline{P_0} \rangle$$

with $[\overline{D}] = \overline{D} - \deg(D)\overline{P_0}$.

For any class $\overline{D} \in \mathrm{Pic}(X)$, write

$$\overline{D} = [\overline{D}] + \deg(D)\overline{P_0} \quad \in \mathrm{Pic}^0(X) \oplus \langle \overline{P_0} \rangle$$

with $[\overline{D}] = \overline{D} - \deg(D)\overline{P_0}$.

Set $T = \mathbb{1}_{\overline{P_0}}$, we obtain a function

$$L = L(T) = \prod_{P \in X(\overline{\mathbb{F}_q})} \left(1 - \mathbb{1}_{[\overline{P}]} T^{\deg(P)}\right)^{-1} \quad \in \mathbb{C}(\mathrm{Pic}^0(X))[[T]].$$

In the basis $\{\mathbb{1}_c\}_{c\in\mathrm{Pic}^0(X)}$, we write

$$L(T) = \sum_{c\in\mathrm{Pic}^0(X)} L(T,c)\mathbb{1}_c.$$

In the basis $\{\mathbb{1}_c\}_{c\in\mathrm{Pic}^0(X)}$, we write

$$L(T) = \sum_{c\in\mathrm{Pic}^0(X)} L(T,c)\mathbb{1}_c.$$

Note that

$$L(T,c) = \sum_{i\geqslant 0} \#|c+iP_0|T^i \quad \in \mathbb{Z}[[T]],$$

and that $\#|rP_0|$ is the coefficient of T^r in $L(T,0)$.

Dual Basis

For every $\chi \in \widehat{\mathrm{Pic}^0(X)}$, set

$$e_\chi = \frac{1}{\#\mathrm{Pic}^0(X)} \sum_{c \in \mathrm{Pic}^0(X)} \chi(-c)\mathbb{1}_c \quad \in \mathbb{C}(\mathrm{Pic}^0(X)).$$

Dual Basis

For every $\chi \in \widehat{\mathrm{Pic}^0(X)}$, set

$$e_\chi = \frac{1}{\#\mathrm{Pic}^0(X)} \sum_{c \in \mathrm{Pic}^0(X)} \chi(-c) \mathbb{1}_c \quad \in \mathbb{C}(\mathrm{Pic}^0(X)).$$

The e_χ form a basis of orthogonal idempotents of $\mathbb{C}(\mathrm{Pic}^0(X))$ and satisfy the relation

$$\mathbb{1}_c e_\chi = \chi(c) e_\chi.$$

Dual Basis

For every $\chi \in \widehat{\mathrm{Pic}^0}(X)$, set

$$e_\chi = \frac{1}{\#\mathrm{Pic}^0(X)} \sum_{c \in \mathrm{Pic}^0(X)} \chi(-c)\mathbb{1}_c \quad \in \mathbb{C}(\mathrm{Pic}^0(X)).$$

The e_χ form a basis of orthogonal idempotents of $\mathbb{C}(\mathrm{Pic}^0(X))$ and satisfy the relation

$$\mathbb{1}_c e_\chi = \chi(c) e_\chi.$$

In this basis, we write

$$L(T) = \sum_{\chi \in \widehat{\mathrm{Pic}^0}(X)} L(T, \chi) e_\chi,$$

and we see that

$$L(T, \chi) = \prod_{P \in X(\overline{\mathbb{F}_q})} \left(1 - \chi([\overline{P}])\, T^{\deg(P)}\right)^{-1} \quad \in \mathbb{C}[[T]].$$

Class Field Theoretical interlude

Set $K = \mathbb{F}_q(X)$ and let H_{P_0} be the P_0-Hilbert class field of K, which is the maximal (finite) abelian extension of K which is unramified and totally split at P_0. Thus we have an isomorphism

$$\mathrm{Gal}(H_{P_0}/K) \cong \mathrm{Pic}^0(X),$$

and it turns out that the L-functions $L(T, \chi)$ just defined coincide with the Hecke L-functions $L_{H_{P_0}}(T, \chi)$ of the abelian extension H_{P_0}/K.

Automorphisms Group

Problem: The size of the Jacobian becomes quickly huge. For instance, the Hermitian curve over $\mathbb{F}_{16}$ has a Jacobian of cardinality $5^{12} = 244140625$.

Automorphisms Group

Problem: The size of the Jacobian becomes quickly huge. For instance, the Hermitian curve over $\mathbb{F}_{16}$ has a Jacobian of cardinality $5^{12} = 244140625$.

So let G be a subgroup of $\mathrm{Aut}_{\mathbb{F}_q}(X)$ fixing P_0. We consider the action of G on $\mathrm{Pic}^0(X)$ and $\widehat{\mathrm{Pic}^0(X)}$ and the quotient spaces

$$\Omega = G\backslash\mathrm{Pic}^0(X) = \{\Omega_1, \dots, \Omega_s\}$$

and

$$\mathcal{E} = G\backslash\widehat{\mathrm{Pic}^0(X)} = \{\mathcal{E}_1, \dots, \mathcal{E}_s\}.$$

Definition:

For the quotient algebra $G\backslash\mathbb{C}(\mathrm{Pic}^0(X))$, we define the two basis

$$\omega_i = \sum_{c\in\Omega_i} \mathbb{1}_c, \quad i = 1, \dots, s$$

and

$$e_j = \sum_{\chi\in\mathcal{E}_j} e_\chi, \quad j = 1, \dots, s$$

and the matrices of passage $\mathcal{Q}$ and $\mathcal{R}$ defined by

$$\mathcal{Q}_{j,i} = \sum_{c\in\Omega_i} \chi(c), \quad \chi \in \mathcal{E}_j$$

and

$$\mathcal{R}_{i,j} = \sum_{\chi\in\mathcal{E}_j} \chi(c), \quad c \in \Omega_i.$$

In the quotient bases, we can write

$$L(T) = \sum_{i=1}^{s} L(T, \omega_i)\omega_i = \sum_{j=1}^{s} L(T, e_j)e_j.$$

In the quotient bases, we can write

$$L(T) = \sum_{i=1}^{s} L(T,\omega_i)\omega_i = \sum_{j=1}^{s} L(T,e_j)e_j.$$

The matrices of passage allow to switch between both representations:

$$L(T,\omega_i) = \frac{1}{\#\mathrm{Pic}^0(X)} \sum_j L(T,e_j)\overline{\mathcal{R}}^t_{i,j}$$

and

$$L(T,e_j) = \sum_i L(T,\omega_i)\mathcal{Q}^t_{j,i}.$$

Now, these newly defined coordinate series $L(T, \omega_i)$ and $L(T, e_j)$ are constant within an orbit, meaning that for every $1 \leqslant i, j \leqslant s$ and for any representative $c_i \in \Omega_i$ and $\chi_j \in \mathcal{E}_j$, we have

$$L(T, \omega_i) = L(T, c_i)$$

and

$$L(T, e_j) = L(T, \chi_j).$$

Now, these newly defined coordinate series $L(T,\omega_i)$ and $L(T,e_j)$ are constant within an orbit, meaning that for every $1 \leqslant i,j \leqslant s$ and for any representative $c_i \in \Omega_i$ and $\chi_j \in \mathcal{E}_j$, we have

$$L(T,\omega_i) = L(T,c_i)$$

and

$$L(T,e_j) = L(T,\chi_j).$$

Gathering everything, we get:

$$L(T,0_{\mathrm{Pic}^0(X)}) = \frac{1}{\#\mathrm{Pic}^0(X)} \sum_{j=1}^{s} L(T,\chi_j)\#\Omega_j.$$

Summary

- To compute weight distributions we used a geometric point of view: count the number of elements in the linear system $|rP_0|$ which have exactly i rational points in their support.

Summary

- To compute weight distributions we used a geometric point of view: count the number of elements in the linear system $|rP_0|$ which have exactly i rational points in their support.
- We expressed the cardinality of $|rP_0|$ as the coefficient of T^r in an L-series $L(T, 0)$, defined as a coordinate of a general counting function L in a vector space indexed by $\mathrm{Pic}^0(X)$.

Summary

- To compute weight distributions we used a geometric point of view: count the number of elements in the linear system $|rP_0|$ which have exactly i rational points in their support.
- We expressed the cardinality of $|rP_0|$ as the coefficient of T^r in an L-series $L(T, 0)$, defined as a coordinate of a general counting function L in a vector space indexed by $\mathrm{Pic}^0(X)$.
- We considered the quotient space of $\mathrm{Pic}^0(X)$ under the action of a subgroup G of the automorphism group of the curve X, to obtain a smaller basis.

Summary

- To compute weight distributions we used a geometric point of view: count the number of elements in the linear system $|rP_0|$ which have exactly i rational points in their support.
- We expressed the cardinality of $|rP_0|$ as the coefficient of T^r in an L-series $L(T, 0)$, defined as a coordinate of a general counting function L in a vector space indexed by $\mathrm{Pic}^0(X)$.
- We considered the quotient space of $\mathrm{Pic}^0(X)$ under the action of a subgroup G of the automorphism group of the curve X, to obtain a smaller basis.
- We defined a dual basis for this space and matrices of passage between the canonical basis and this dual basis, allowing to switch between both depending on what is most convenient.

Summary

- To compute weight distributions we used a geometric point of view: count the number of elements in the linear system $|rP_0|$ which have exactly i rational points in their support.
- We expressed the cardinality of $|rP_0|$ as the coefficient of T^r in an L-series $L(T, 0)$, defined as a coordinate of a general counting function L in a vector space indexed by $\mathrm{Pic}^0(X)$.
- We considered the quotient space of $\mathrm{Pic}^0(X)$ under the action of a subgroup G of the automorphism group of the curve X, to obtain a smaller basis.
- We defined a dual basis for this space and matrices of passage between the canonical basis and this dual basis, allowing to switch between both depending on what is most convenient.

We will now use the explicit frame provided by characters to compute the series $L(T, \chi_j)$, before coming back to $L(T, 0_{\mathrm{Pic}^0(X)})$.

The Tate-Lichtenbaum pairing

For $m > 0$ prime to q let

$$\mathrm{Pic}^0(X)_m = \{\overline{D} \in \mathrm{Pic}^0(X) : mD \text{ is principal}\}$$

be the m-torsion points of $\mathrm{Pic}^0(X)$.

The Tate-Lichtenbaum pairing

For $m > 0$ prime to q let

$$\mathrm{Pic}^0(X)_m = \{\overline{D} \in \mathrm{Pic}^0(X) : mD \text{ is principal}\}$$

be the m-torsion points of $\mathrm{Pic}^0(X)$.

Hypothesis: Assume that $m|(q-1)$.

The map

$$\{\cdot,\cdot\}_m : \mathrm{Pic}^0(X)_m \times \mathrm{Pic}^0(X)/m\mathrm{Pic}^0(X) \to \mathbb{F}_q^*/{\mathbb{F}_q^*}^m$$

defined by

$$(\overline{D}, \overline{E}) \mapsto f(E) = \prod_P f(P)^{v_P(E)},$$

where $m\overline{D} = (f)$, is a well-defined non-degenerate pairing called the *Tate-Lichtenbaum pairing*.

Thus, if m is such that $m\mathrm{Pic}^0(X) = 0$, we obtain a pairing

$$\mathrm{Pic}^0(X) \times \mathrm{Pic}^0(X) \to \mathbb{F}_q^*/{\mathbb{F}_q^*}^m \cong \langle \zeta_m \rangle,$$

for a primitive mth-root of unity ζ_m.

Therefore, by fixing for instance a class $\overline{D}$, we get a character

$$\chi_{\overline{D}} = \{\overline{D}, \cdot\} : \mathrm{Pic}^0(X) \to \langle \zeta_m \rangle.$$

Thus, if m is such that $m\mathrm{Pic}^0(X) = 0$, we obtain a pairing

$$\mathrm{Pic}^0(X) \times \mathrm{Pic}^0(X) \to \mathbb{F}_q^*/\mathbb{F}_q^{*\,m} \cong \langle \zeta_m \rangle,$$

for a primitive mth-root of unity ζ_m.

Therefore, by fixing for instance a class $\overline{D}$, we get a character

$$\chi_{\overline{D}} = \{\overline{D}, \cdot\} : \mathrm{Pic}^0(X) \to \langle \zeta_m \rangle.$$

EXAMPLE:

If X is an optimal curve over $\mathbb{F}_{q^2}$, that is if $\#X(\mathbb{F}_{q^2}) = q^2 + 1 + 2gq$, then

$$\mathrm{Pic}^0(X) \cong (\mathbb{Z}/(q+1)\mathbb{Z})^g,$$

thus $m = q + 1$ will do (and note that $m | (q^2 - 1)$).

By non-degeneracy, the characters of $\mathrm{Pic}^0(X)$ are exactly the $\chi_{\overline{D}}$, for $\overline{D} \in \mathrm{Pic}^0(X)$.

By non-degeneracy, the characters of $\mathrm{Pic}^0(X)$ are exactly the $\chi_{\overline{D}}$, for $\overline{D} \in \mathrm{Pic}^0(X)$.

Furthermore, for every $\phi \in \mathrm{Aut}(X)$ we have

$$\chi_{\phi(\overline{D})} = \chi_{\overline{D}} \circ \phi^{-1} = \phi^{-1} \cdot \chi_{\overline{D}},$$

so that taking characters via the Tate-Lichtenbaum pairing "preserves equivalence classes under $\mathrm{Aut}(X)$". In other words, the characters χ_j representing the classes

$$\{\mathcal{E}_j\}_{j=1,\dots,s} = G \backslash \widehat{\mathrm{Pic}^0(X)}$$

are the $\{\chi_{\overline{D_i}}\}_{i=1,\dots,s}$, where $\overline{D_i}$ is any representative of the class $\Omega_i \in G\backslash \mathrm{Pic}^0(X)$.

Back to L-functions

For $c \in \mathrm{Pic}(X)$, let $\ell(c)$ be the dimension of the Riemann-Roch space of any divisor in c. The Riemann-Roch theorem states that

$$\ell(c) - \ell(W - c) = \deg(c) + 1 - g,$$

where W is the canonical divisor of X.

Because of the bijection between $|c|$ and $\mathrm{Proj}(\mathcal{L}(c))$, we have

$$L(c) = \frac{q^{\ell(c)} - 1}{q - 1},$$

whence

$$L(c) = \frac{q^{\deg(c)+1-g} - 1}{q - 1} + L(W - c)q^{\deg(c)+1-g}.$$

Coming back to our coordinate function $L(T,c)$, we get that

$$L(T,c) = \sum_{i=0}^{\infty} L(c+iP_0)T^i = \frac{T^g}{(1-T)(1-qT)} + L^*(T,c),$$

where

$$L^*(T,c) = \sum_{i=0}^{g-1} L(c+iP_0)T^i + \sum_{i=g}^{2g-2} L(W-c-iP_0)q^{i+1-g}T^i$$

is a polynomial of degree less than $2g-2$ with non-negative integer coefficients.

Since the basis $\{e_\chi\}_\chi$ is formed of orthogonal idempotents and $\mathbb{1}_c e_\chi = \chi(c) e_\chi$, we have

$$L(T,\chi) = L(T)e_\chi = \sum_c L(T,c)\mathbb{1}_c e_\chi = \sum_c \chi(c) L(T,c)$$

is a polynomial of degree less than $2g-2$ with non-negative integer coefficients (except in the case where χ is the trivial character, in which case $L(T,\chi)$ is the zeta function of X).

Since the basis $\{e_\chi\}_\chi$ is formed of orthogonal idempotents and $\mathbb{1}_c e_\chi = \chi(c) e_\chi$, we have

$$L(T,\chi) = L(T)e_\chi = \sum_c L(T,c)\mathbb{1}_c e_\chi = \sum_c \chi(c) L(T,c)$$

is a polynomial of degree less than $2g-2$ with non-negative integer coefficients (except in the case where χ is the trivial character, in which case $L(T,\chi)$ is the zeta function of X).

To summarize: If $\chi_j = 0$ then $L(T,\chi_j) = Z(X;T)$. Otherwise we have

$$L(T,\chi_j) = 1 + \sum_{i=1}^{s} \sum_{k=1}^{2g-2} \sum_{\substack{D \geqslant 0 \in \mathrm{Div}(X) \\ \deg(D)=k \text{ and } [\overline{D}] \in \Omega_i}} \chi_j([\overline{D}]) T^k$$

Why bother?

REMARK:

At this point we can wonder why did we introduce the series $L(T, \chi)$, since

1. actually we are interested in what happens inside $|rP_0|$, whose cardinality can be read directly from the $L(T, 0)$;
2. we use the $L(T, c)$ to compute the $L(T, \chi)$!

Why bother?

Remark:
At this point we can wonder why did we introduce the series $L(T, \chi)$, since

1. actually we are interested in what happens inside $|rP_0|$, whose cardinality can be read directly from the $L(T, 0)$;
2. we use the $L(T, c)$ to compute the $L(T, \chi)$!

Remember: We want finer data than just the cardinality of $|rP_0|$, we want to know inside $|rP_0|$ how many divisors have a precise number of rational places in their support.

This requires the introduction of another series, whose computation will be much easier in the dual basis.

The Λ function

Let

$$\Lambda = \prod_{\mathcal{P}} (1 + \mathbb{1}_{\overline{P}}) \quad \in \mathbb{C}(\mathrm{Pic}(X)).$$

As before, we derive from this function a series

$$\Lambda(T) = \prod_{\mathcal{P}} (1 + \mathbb{1}_{[\overline{P}]} T) \quad \in \mathbb{C}(\mathrm{Pic}^0(X))[T].$$

Writing this function in the basis $\{\mathbb{1}_c\}_{c \in \mathrm{Pic}^0(X)}$ as follows

$$\Lambda(T) = \sum_{c \in \mathrm{Pic}^0(X)} \Lambda(T, c) \mathbb{1}_c,$$

we obtain coordinate functions $\Lambda(T, c)$ counting the number of divisors in $|c + iP_0|$ with i different rational places in the support.

As in the case of the L-functions, we can derive "dual" Λ-series

$$\Lambda(T, \chi) = \prod_{\mathcal{P}} (1 + \chi([\overline{P}])T) \quad \in \mathbb{C}[T],$$

for every character $\chi \in \widehat{\mathrm{Pic}^0(X)}$.

We can also take into account the action of the group G; we obtain a decomposition

$$\Lambda(T) = \sum_{i=1}^{s} \Lambda(T, \omega_i) \mathbb{1}_{\omega_i}$$

and

$$\Lambda(T) = \sum_{j=1}^{s} \Lambda(T, \chi_j) e_{\chi_j}$$

in the quotient basis and dual quotient basis respectively.

Final step: the A-function

Gathering the information from the L and Λ function solves our problem:

THEOREM (DUURSMA) Let

$$A(U,T) = L(T)\Lambda(U-T) \quad \mathbb{C}(\mathrm{Pic}^0(X))[U](T).$$

Then the coordinate series $A(U,T,c)$, for $c \in \mathrm{Pic}^0(X)$, is the generating series for the number of effective divisors in the class of $c + (i+j)P_0$ with precisely i places of $\mathcal{P}$ in their support.

Concretely, what this means is that if we write the coordinate

$$A(U, T, 0) = \sum_{i,j} A_{i,j} U^i T^j,$$

or, in the more convenient following form

$$A(UT, T, 0) = \sum_{r \geqslant 0} \sum_{i=0}^{r} A_{i,r-i} U^i T^r,$$

then the weight distribution of the code $\mathcal{C}(X, rP_0)$, for every $r \geqslant 0$, is described by the polynomial

$$\sum_{i=0}^{r} A_{i,r-i} U^i.$$

More precisely, we have

$$w_i = A_{i,r-i}$$

Strategy to compute $A(UT, T, 0)$

To compute $A(UT, T, 0)$, we compute the series

$$A(UT, T, \chi_j) = L(T, \chi_j)\Lambda(UT - T, \chi_j),$$

where as above the $\{\chi_j\}_{j=1,\ldots,s}$ are representatives of $G\backslash\widehat{\mathrm{Pic}^0(X)}$.

Then after applying the matrix of passage to come back to the basis $\{\mathbb{1}_{\omega_i}\}_{i=1,\ldots,s}$, we obtain

$$A(UT, T, 0) = \frac{1}{\#\mathrm{Pic}^0(X)} \sum_{j=1}^{s} A(UT, T, \chi_j)\#\Omega_j.$$

Example 1

Let X_1 be the Hermitian curve over $\mathbb{F}_9$, defined by

$$y^3 + y = x^4.$$

It has genus 3 and $3^3 + 1 = 28$ rational points, so we get a code of length $n = 27$. For $r = 15$, we get a code of dimension $k = \ell(15P_0) = 13$ and minimal distance $d = 12$, with weight enumerator

$$32544U^{15} + 596160U^{14} + 4100544U^{13} + 25163424U^{12} + 161780328U^{11} + 834004512U^{10} + 3683371560U^{9} + 13983703272U^{8} + 44774204112U^{7} + 119315878704U^{6} + 260406224784U^{5} + 452841652080U^{4} + 603795387384U^{3} + 579645648072U^{2} + 356703891912U + 105690188936.$$

For every $d \leqslant i \leqslant n$, we let a_i be the number of codewords with i non-zero coordinates, so that

$$a_{n-i} = w_i.$$

i	$w_i = a_{n-i}$
0	105690188936
1	356703891912
2	579645648072
3	603795387384
4	452841652080
5	260406224784
6	119315878704
7	44774204112
8	13983703272
9	3683371560
10	834004512
11	161780328
12	25163424
13	4100544
14	596160
15	32544
27	1

Example 2

Let X_2 be the curve over $\mathbb{F}_{16}$ defined by the equation

$$y^2 + y = x^5.$$

It has genus 2, with 33 rational points, so it is optimal. So we get a code of length $n = 32$. For $r = 17$, we get an auto-dual code of dimension $k = \ell(17P_0) = 16$ and minimal distance $d = 15$, with weight enumerator

$$13509600U^{17} + 245901450U^{16} + 2930265600U^{15} + 37567392000U^{14} + 419015856000U^{13} + 4067086077600U^{12} + 34887938841600U^{11} + 261665716915200U^{10} + 1706425881576000U^{9} + 9598809072333000U^{8} + 46074126144284160U^{7} + 186068665636250880U^{6} + 620228883714518400U^{5} + 1661327339426172000U^{4} + 3437228998926336000U^{3} + 5155843490523840000U^{2} + 4989525960177765600U + 2338840293691716525.$$

0	2338840293691716525
1	4989525960177765600
2	5155843490523840000
3	3437228998926336000
4	1661327339426172000
5	620228883714518400
6	186068665636250880
7	46074126144284160
8	9598809072333000
9	1706425881576000
10	261665716915200
11	34887938841600
12	4067086077600
13	419015856000
14	37567392000
15	2930265600
16	245901450
17	13509600
32	1

Epilogue: zeta functions

The *weight enumerator* of the code $\mathcal{C}$ is the polynomial

$$W(x,y) = x^n + \sum_{i=d}^{n} w_{n-i} x^{n-i} y^i.$$

If the code is auto-dual, it can be written

$$W(x,y) = a_0 M_{n,d} + a_1 M_{n,d+1} + \cdots + a_{2g} M_{n,d+g},$$

where for every $i = 0, \ldots, g$, the term $M_{n,d+i}$ is the weight enumerator of an MDS code of length n and minimum distance $d+i$ (explicitly computable).

The *zeta function* of $\mathcal{C}$ is the polynomial

$$Z(\mathcal{C}, T) = a_0 + a_1 T + \cdots a_{2g} T^{2g}.$$

Thus the data of the weight distribution of a code is equivalent to the data of its zeta function. This zeta function (of a self-dual code) has the same functional equation than the one described by the Weil conjectures:

$$Z(\mathcal{C}; 1/qT) = Z(\mathcal{C}; T)q^{g-1}T^{2g-2}.$$

Furthermore, Duursma conjectures (in some cases) a Riemann hypothesis on the reciprocal zeroes of $Z(\mathcal{C}; T)$.

Thus the data of the weight distribution of a code is equivalent to the data of its zeta function. This zeta function (of a self-dual code) has the same functional equation than the one described by the Weil conjectures:

$$Z(\mathcal{C}; 1/qT) = Z(\mathcal{C}; T)q^{g-1}T^{2g-2}.$$

Furthermore, Duursma conjectures (in some cases) a Riemann hypothesis on the reciprocal zeroes of $Z(\mathcal{C}; T)$.

Questions

- Is there a cohomology theory behind this?
- Can we use it to compute zeta functions (and thus weight distributions) fast?

Ceci n'est pas une slide de fin !

Par contre ça oui !