Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 48 (2002)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: THE COSET WEIGHT DISTRIBUTIONS OF CERTAIN BCH CODES AND A FAMILY OF CURVES
Autor: van der Geer, G. / van der Vlugt, M.
Kapitel: §2. DISSECTING THE JACOBIAN
DOI: https://doi.org/10.5169/seals-66065

equals the number of singular points of C on C_i. Put $r = 12/\ell$. Then by the symmetry we have $HC_i = r$. On the other hand, the adjunction formula

$$C_i^2 + K_S C_i = C_i^2 - HC_i = C_i^2 - r = 2g(C_i) - 2,$$

where K_S is the canonical divisor of S, and the identity

$$4r = 4HC_i = CC_i = C_i^2 + \sum_{j \neq i} C_i C_j = C_i^2 + r$$

imply $C_i^2 = 3r$ and $g(C_i) = r + 1$. In particular, C_i cannot be contained in a hyperplane and spans $\mathbf{P}^3$. Clifford's theorem applied to the hyperplane section $H|C_i$ of C_i says that $h^0(H|C_i) \leq r/2 + 1$, hence $r \geq 6$. Then $\ell = 2$ and we have two components. Again, by Clifford, these curves must be hyperelliptic and the linear system $H|C_i$ is $3g_2^1$. But since $3g_2^1$ is contained in the canonical system $|K_{C_i}|$ this factors through the hyperelliptic involution, which contradicts the fact that C_i is embedded in $\mathbf{P}^3$ as a non-rational curve. This proves that C is irreducible.

(1.3) COROLLARY. *If $\lambda \neq 0$ the normalization $\widetilde{C}$ of C is an irreducible smooth curve of genus* 13.

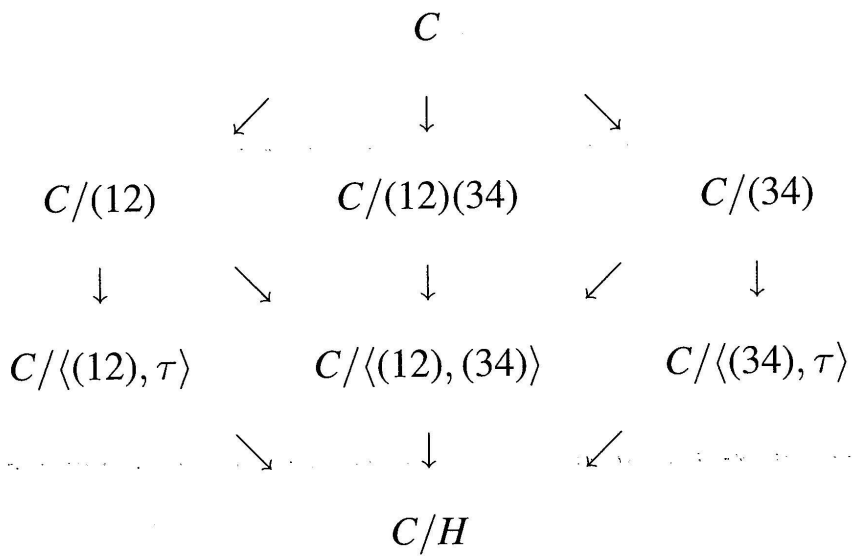
Proof. On the cubic surface S we have $(C + K_S)C = (4 - 1)HC = 36$. This implies that for $\widetilde{C}$ we have $2g(\widetilde{C}) - 2 = 36 - 12 = 24$. □

§2. DISSECTING THE JACOBIAN

For the sake of convenience when we refer to a curve in the sequel we shall always mean the normalization of (a completion of) that curve. In particular, by the genus we mean the geometric genus of the curve and if we speak of the number of rational points we mean the number of rational points of the normalization. Note that an absolutely irreducible curve D has a unique complete non-singular model D' obtained by normalizing any completion of the curve. Any automorphism of the curve D defines uniquely an automorphism of the normalization D'.

We now analyze the absolutely irreducible curve $C = C_{A,B}$ for $\lambda \neq 0$ in more detail in order to decompose its Jacobian.

Let $H \subset \mathrm{Aut}(C)$ be the subgroup generated by the two permutations (12) and (34) and the involution τ. Then H is abelian of order 8 and isomorphic to $(\mathbf{Z}/2\mathbf{Z})^3$. Consider the following diagram of degree 2 coverings of curves



Let $u = (x_3 + x_4)/(x_1 + x_2)$. This is a H-invariant rational function on C, hence defines a rational function on C/H.

(2.1) PROPOSITION.

i) *The function* u *gives an isomorphism* $C/H \cong \mathbf{P}^1$.

ii) *The curve* $C/\langle(12),(34)\rangle$ *is a curve of genus* 1 *given by*

$$y^2 + y = \lambda u + \lambda/u + (A+1)\,.$$

iii) *The curve* $C/\langle(12),\tau)\rangle$ *is a curve of genus* 2 *given by*

$$y^2 + y = \lambda/u^3 + \lambda u\,.$$

iv) *The curve* $C/\langle(34),\tau\rangle$ *is a curve of genus* 2 *given by*

$$y^2 + y = \lambda u^3 + \lambda/u\,.$$

Proof. The divisor of u on C is of the form $H_{34}C - H_{12}C$, where H_{ij} is the hyperplane given by $x_i + x_j = 0$. Since both these hyperplanes contain the line $x_1 + x_2 = x_3 + x_4 = 0$ which intersects C in a divisor of degree 4 it follows that the divisor of u can be written as a difference of two divisors of degree $12 - 4 = 8$. Moreover, these divisors are invariant under the action of H. This implies that on C/H the function u defines a non-constant function with a single zero and a single pole. Therefore u defines an isomorphism $C/H \cong \mathbf{P}^1$. This proves i).

We now prove ii). Working with the affine equations (set $x_0 = 1$)

$$\sigma_1 = 1\,, \quad \sigma_3 = A + 1 + \sigma_2\,, \quad \sigma_4 = B + A + (A+1)\sigma_2\,,$$

we can write $u = (x_3 + x_4)/(x_1 + x_2) = 1 + 1/(x_1 + x_2)$, i.e.

$$x_1 + x_2 = 1/(u+1) \quad \text{and} \quad x_3 + x_4 = u/(u+1)\,.$$

We put $v := x_1x_2$ and $w := x_3x_4$. These functions are invariant under (12) and (34), but not under τ. Using

$$\sigma_2 = x_1x_2 + x_3x_4 + (x_1 + x_2)(x_3 + x_4) = v + w + u/(u+1)^2\,,$$
$$\sigma_3 = x_1x_2(x_3 + x_4) + (x_1 + x_2)x_3x_4 = (uv + w)/(u+1)\,,$$

the equation $\sigma_3 = A + 1 + \sigma_2$ implies

$$A(u+1)^2 + (u+1)(v + uw) + u^2 + u + 1 = 0\,, \tag{8}$$

while the equation $\sigma_4 = B + A + (A+1)\sigma_2$ yields

$$B + A + (A+1)(v + w + u/(u+1)^2) + vw = 0\,. \tag{9}$$

Elimination of w from (8) and (9) yields the equation

$$(u+1)^2v^2 + u(u+1)v = \lambda u^3 + \lambda u + (A+1)u + (A+1)^2u^2 + (A+1)^2\,.$$

Dividing by u^2 and and replacing $(u+1)v/u$ by η (i.e. $\eta = x_1x_2/(x_3 + x_4)$) gives

$$\eta^2 + \eta = \lambda u + \lambda/u + (A+1)/u + (A+1)^2/u^2 + (A+1)^2 \tag{10}$$

and this is, via $y = \eta + (A+1)/u + (A+1)$, clearly $\mathbf{F}_q$-isomorphic to

$$y^2 + y = \lambda u + \lambda/u + A + 1\,.$$

Since η is invariant under (12) and (34), but not under τ, the equation (10) describes the degree 2 cover $C/\langle(12),(34)\rangle$ of C/H.

For iii) we remark that the function field extension of $C/\langle(12),\tau\rangle$ over C/H is generated by the function $z = x_3 + x_1x_2/(x_3 + x_4)$. Then $z + z^{(34)} = x_3 + x_4 = u/(u+1)$. Moreover,

$$\begin{aligned} z \cdot z^{(34)} &= x_3x_4 + x_1x_2 + (x_1x_2)^2/(x_3 + x_4)^2 \\ &= w + v + \eta^2 \\ &= A(u+1)/u + 1 + 1/u(u+1) + \eta + \eta^2\,, \end{aligned}$$

where we used $w = A(u+1)/u + 1 + 1/u(u+1) + v/u$ obtained from (8) and $v + v/u = \eta$. By (10) this implies that z satisfies the equation

$$z^2 + \frac{u}{u+1}z = \frac{\lambda(u^4 + u^3) + (A^2 + A)u^3 + \lambda(u^2 + u) + Au^2 + A^2 + 1}{u^2(u+1)}\,.$$

Dividing by $(u/(u+1))^2$ and replacing $(u+1)z/u$ by ζ gives the equation

$$\zeta^2 + \zeta = \lambda u + \lambda/u^3 + (A^2 + A) + 1/u + 1/u^4 + A/u^2 + A^2/u^4\,.$$

Via $\zeta \mapsto \zeta + A + 1/u + (A+1)/u^2$ we get the $\mathbf{F}_q$-isomorphic curve

$$\zeta^2 + \zeta = \lambda u + \lambda/u^3\,.$$

Part iv) is now obtained by applying the permutation (13)(24). This changes u into u^{-1} and proves the result.

(2.2) THEOREM. *The normalization of the curve C is the normalization of the fibre product over $\mathbf{P}^1$ with affine coordinate x of the three hyperelliptic curves given by*

$$y^2 + y = \lambda x^3 + \lambda/x,$$
$$y^2 + y = \lambda/x^3 + \lambda x,$$
$$y^2 + y = \lambda x + \lambda/x + A + 1.$$

Proof. This follows directly from the diagram and the preceding proposition.

Note that equivalently, C is the fibre product of the three curves C_{f_i} of genus 1 with affine equation $y^2 + y = f_i$, where f_i for $i = 1, 2, 3$ is given by

$$\begin{aligned} f_1 &= \lambda x^3 + \lambda x + A + 1, \\ f_2 &= \lambda/x^3 + \lambda/x + A + 1, \\ f_3 &= \lambda x + \lambda/x + A + 1, \end{aligned} \tag{11}$$

since f_1, f_2 and f_3 generate the same space of functions as the right hand sides in the theorem. This description allows us to dissect the Jacobian of C.

(2.3) THEOREM. *The Jacobian of $C_{A,B}$ decomposes up to isogeny over $\mathbf{F}_q$ as a product of five supersingular elliptic curves, two ordinary elliptic curves and three 2-dimensional factors of 2-rank 1.*

Proof. From the description of $C = C_{A,B}$ as a fibre product we see that $\mathrm{Jac}(C)$ decomposes as a product of seven factors: three elliptic curves $\mathrm{Jac}(C_{f_i})$, two 2-dimensional factors $\mathrm{Jac}(C_{f_1+f_3})$, $\mathrm{Jac}(C_{f_2+f_3})$, and two 3-dimensional factors $\mathrm{Jac}(C_{f_1+f_2})$ and $\mathrm{Jac}(C_{f_1+f_2+f_3})$. The 2-rank of $\mathrm{Jac}(C_{f_i})$ is 0 for $i = 1, 2$ and 1 for $i = 3$. The 2-ranks of $\mathrm{Jac}(C_{f_1+f_3})$ and $\mathrm{Jac}(C_{f_2+f_3})$ are 1 since these hyperelliptic curves have two Weierstrass points.

The curve $C_{f_1+f_2+f_3}$ is a curve of genus 3 defined by $y^2 + y = \lambda(x^3 + 1/x^3) + A + 1$ with automorphisms

$$\rho\colon (x, y) \mapsto (1/x, y), \quad \sigma\colon (x, y) \mapsto (x, y + 1).$$

The quotient of $C_{f_1+f_2+f_3}$ under ρ is the supersingular elliptic curve given by $y^2+y = \lambda(z^3+z)+A+1$ with $z = x+1/x$. Moreover, the curve $C_{f_1+f_2+f_3}$ admits a non-constant map to the ordinary elliptic curve $y^2 + y = \lambda(w + 1/w) + A + 1$ via $w = x^3$. So by Poincaré's complete reducibility theorem the Jacobian

$\mathrm{Jac}(C_{f_1+f_2+f_3})$ splits up to isogeny into a product of three elliptic curves and has 2-rank 1 since it has 2 ramification points.

Similarly, the quotient of $C_{f_1+f_2}$ by the automorphism ρ is the supersingular elliptic curve $y^2+y=\lambda z^3$, while the quotient under $\rho\sigma$ is a curve of genus 2 of 2-rank 1 defined by the equation $y^2+y=\lambda z^3+1/z$. Collecting these results we obtain the theorem.

For a smooth absolutely irreducible complete curve X defined over a field $\mathbf{F}_q$ we shall denote the trace of Frobenius by $t(X)$, i.e. $t(X)=q+1-\#X(\mathbf{F}_q)$, where $\#X(\mathbf{F}_q)$ is the number of $\mathbf{F}_q$-rational points of X.

(2.4) COROLLARY. *For $q=2^m$ with m odd the trace of Frobenius of $C_{A,B}$ equals $2t(C_{f_1})+2t(C_{f_3})+2t(C_{f_1+f_3})+t(C_{g_\lambda})$, where C_{g_λ} is the curve given by $y^2+y=g_\lambda$ with $g_\lambda=\lambda x^3+1/x$.*

Proof. The curves C_{f_1} and C_{f_2} are isomorphic via $x\mapsto 1/x$, so have the same trace of Frobenius. Since for $q=2^m$ with m odd the map $x\mapsto x^3$ is a bijection on $\mathbf{F}_q$, the curve $C_{f_1+f_2+f_3}$ given by $y^2+y=\lambda(x^3+1/x^3)+A+1$ and the ordinary factor of its Jacobian given by $y^2+y=\lambda(w+1/w)+A+1$ have the same trace of Frobenius, and this is $t(C_{f_3})$. Moreover, since $C_{f_1+f_3}$ and $C_{f_2+f_3}$ are isomorphic, we have $t(C_{f_1+f_3})=t(C_{f_2+f_3})$. Similarly, the supersingular component of $\mathrm{Jac}(C_{f_1+f_2})$ given by $y^2+y=\lambda z^3$ has the same trace of Frobenius as the rational curve $y^2+y=\lambda z$, i.e. 0. Therefore, the trace $t(C_{f_1+f_2})$ equals the trace of the genus 2 quotient $C_{f_1+f_2}/\rho\sigma$, and this is the curve $y^2+y=g_\lambda$.

We can interpret and augment the results obtained using the involution τ. The involution τ acts without fixed points on the normalization of C, hence by the Hurwitz-Zeuthen formula the genus of the quotient curve C/τ is 7. The Jacobian $\mathrm{Jac}(C)$ decomposes up to an isogeny

$$\mathrm{Jac}(C)\sim \mathrm{Jac}(C/\tau)\times P,$$

where P is the Prym variety of $C\to C/\tau$, i.e. the identity component of the norm map $\mathrm{Nm}\colon \mathrm{Jac}(C)\to \mathrm{Jac}(C/\tau)$. Since the curves $C/\langle(12),\tau\rangle=C_{f_2+f_3}$, $C/\langle(34),\tau\rangle=C_{f_1+f_3}$ and $C/\langle(12)(34),\tau\rangle=C_{f_1+f_2}$ are quotients of C/τ and the fibre product $C_{f_1+f_3}\times_{\mathbf{P}^1}C_{f_2+f_3}$ has genus 7 it follows readily that

$$C/\tau\cong C_{f_1+f_3}\times_{\mathbf{P}^1}C_{f_2+f_3}.$$

Note that the substitution $x\mapsto x/\lambda$ yields an isomorphism $C_{g_{\lambda^4}}\cong C_{f_1+f_3}$.

(2.5) PROPOSITION. *Up to isogeny over* $\mathbf{F}_{q=2^m}$ *we have the splitting*

$$\mathrm{Jac}(C/\tau) \sim \mathrm{Jac}(C_{g_{\lambda^4}})^2 \times \mathrm{Jac}(C_{g_\lambda}) \times E\,,$$

where C_{g_λ} *is as in (2.4) and* E *is the elliptic curve* $y^2 + y = \lambda z^3$. *The Prym variety* P *is isogenous to a product of six elliptic curves:*

$$P \sim \mathrm{Jac}(C_{f_1})^2 \times \mathrm{Jac}(C_{f_3})^2 \times P'\,,$$

where P' *is a supersingular abelian surface whose trace of Frobenius* $t(P')$ *over* $\mathbf{F}_q$ *satisfies*

$$t(P') = \begin{cases} 0 & \text{if } m \text{ is odd,} \\ -2(q-1) + 2t(C_{f_3}) & \text{if } m \text{ is even.} \end{cases}$$

Proof. The splitting of $\mathrm{Jac}(C/\tau)$ follows directly from the description of C/τ as a fibre product and the splitting $\mathrm{Jac}(C_{f_1+f_2}) \sim \mathrm{Jac}(C_{g_\lambda}) \times E$ as obtained in (2.4). Furthermore, using Theorem (2.3) we see that

$$P \sim \mathrm{Jac}(C_{f_1}) \times \mathrm{Jac}(C_{f_2}) \times \mathrm{Jac}(C_{f_3}) \times \mathrm{Jac}(C_{f_1+f_2+f_3})\,.$$

We know $\mathrm{Jac}(C_{f_1}) \cong \mathrm{Jac}(C_{f_2})$ and that $\mathrm{Jac}(C_{f_1+f_2+f_3})$ splits up to isogeny as $\mathrm{Jac}(C_{f_3})$ and a 2-dimensional factor P' which is supersingular and up to isogeny a product of two elliptic curves. Using the map $x \mapsto w = x^3$ we see that $\#C_{f_1+f_2+f_3}(\mathbf{F}_q) = \#C_{f_3}(\mathbf{F}_q)$ if m is odd which implies $t(P') = 0$, while for m even

$$\#C_{f_1+f_2+f_3}(\mathbf{F}_q) - 2 = 3(\#C_{f_3}(\mathbf{F}_q) - 2)\,.$$

This implies

$$t(C_{f_1+f_2+f_3}) - t(C_{f_3}) = -2(q-1) + 2t(C_{f_3})$$

and hence $t(P') = -2(q-1) + 2t(C_{f_3})$. This proves the assertion.

§3. BOUNDS FOR $N(A,B)$

Since the curve $C = C_{A,B}$ has genus 13 if $\lambda = A^2 + A + 1 + B \neq 0$ the Hasse-Weil-Serre bound for the number of $\mathbf{F}_q$-rational points $\#C_{A,B}(\mathbf{F}_q)$ says

$$q + 1 - 13[2\sqrt{q}] \leq \#C_{A,B}(\mathbf{F}_q) \leq q + 1 + 13[2\sqrt{q}]\,. \tag{12}$$

The number $N(A,B)$ of S_4-orbits of solutions of (1) with distinct $x_i \in \mathbf{F}_q$ satisfies

$$N(A,B) = (\#C_{A,B}(\mathbf{F}_q) - \text{contribution of } x = 0, 1, \infty)/24\,.$$