§1. A FAMILY OF CURVES

We show that for odd m the $N(A,B)$ lie in an explicit interval of length $\sim 1.57\sqrt{q}$, cf. [C-Z], where the interval is $\sim q/4$. Moreover, we argue that on statistical grounds one may expect that almost all $N(A,B)$ lie in an explicit interval of length $\sim 0.9\sqrt{q}$. We then give numerical results that confirm strongly these heuristics and extend the table of $BCH(3)$ codes with known coset weight distribution.

For an introduction to the theory of codes we refer to [vL] and for a general introduction to curves over finite fields to [S]. The reader can find basic facts about Jacobians in the survey paper [Mi] and a general introduction to curves and their Jacobians in [Mu].

§1. A FAMILY OF CURVES

We consider the algebraic curve $C' = C'_{A,B}$ in $\mathbf{P}^4$ given by the equations

$$s_1 = x_0\,, \quad s_3 = Ax_0^3\,, \quad s_5 = Bx_0^5\,, \tag{2}$$

where s_j is the j-th power sum $\sum_{i=1}^4 x_i^j$ in the variables $x_1,\ldots,x_4$. Let σ_j denote the j-th elementary symmetric function in $x_1,\ldots,x_4$. If we apply Newton's formulas for power sums we find

$$\begin{aligned} s_1 + x_0 &= \sigma_1 + x_0 = 0\,,\\ s_3 + Ax_0^3 &= (A+1)x_0^3 + \sigma_2 x_0 + \sigma_3 = 0\,,\\ s_5 + Bx_0^5 &= x_0\left((B+A)x_0^4 + (A+1)\sigma_2 x_0^2 + \sigma_4\right) = 0\,. \end{aligned}$$

This implies that the curve C' consists of the three lines in the hyperplane $x_0 = 0$ given by

$$x_i + x_j = x_k + x_l = 0\,, \quad \text{with} \quad \{i,j,k,l\} = \{1,2,3,4\}\,, \tag{3}$$

and a curve $C = C_{A,B}$ given by

$$\begin{aligned} \sigma_1 &= x_0\,,\\ \sigma_3 &= (A+1)x_0^3 + \sigma_2 x_0\,,\\ \sigma_4 &= (B+A)x_0^4 + (A+1)\sigma_2 x_0^2\,. \end{aligned} \tag{4}$$

The symmetric group S_4 operates on C' and on C by permuting the coordinates $x_1,\ldots,x_4$. Moreover, there is an involution τ acting on C via

$$(x_0 : x_1 : \ldots : x_4) \mapsto (x_0 : x_1 + x_0 : \ldots : x_4 + x_0)\,.$$

This involution commutes with the elements of S_4 and this gives rise to a group of 48 automorphisms of C.

We introduce the invariant

$$\lambda := B + A^2 + A + 1 \quad (\in \mathbf{F}_q).$$

In the following lemma and the rest of this section we shall work over an algebraic closure of $\mathbf{F}_q$.

(1.1) LEMMA.

i) *If* $\lambda \neq 0$ *then* C *has six ordinary double points, namely the points of the* S_4*-orbit of* $(0:1:1:0:0)$ *and no other singularities.*

ii) *If* $\lambda = 0$ *the curve* C *consists of* 12 *lines.*

Proof. The Jacobian matrix of (2) is

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ Ax_0^2 & x_1^2 & x_2^2 & x_3^2 & x_4^2 \\ Bx_0^4 & x_1^4 & x_2^4 & x_3^4 & x_4^4 \end{pmatrix}.$$

If the rank of this matrix is ≤ 2 for a point with coordinates $(x_0 : \ldots : x_4)$ then there exist α, β, γ with α, β, γ not all zero such that $\alpha + \beta x_i^2 + \gamma x_i^4 = 0$ for $i = 1, \ldots, 4$. Hence the coordinates x_i with $i = 1, \ldots, 4$ of a singular point of C can assume at most 2 different values and taking into account the equation $s_1 = x_0$ it follows that a singular point of C is in the S_4-orbit of a point of the form $(a:1:1:1:a+1)$ or of the form $(0:1:1:a:a)$ for some value of a. In the latter case we get from (4) that $a = 0$ and we find 6 singular points in the orbit of $(0:1:1:0:0)$. In the former case it follows from (4) that a satisfies

$$(5) \quad (A+1)a^3 + a^2 + a = 0, \quad \text{and} \quad (B+A)a^4 + (A+1)a^3 + a + 1 = 0.$$

Hence $a \neq 0$ and (5) is equivalent to

$$(6) \qquad \begin{aligned} (A+1)a^2 + a + 1 &= 0, \\ (B+A)a^2 + (A+1)a + (A+1) &= 0. \end{aligned}$$

The resultant of (6) equals $(B + A^2 + A + 1)^2$, hence (6) has a solution if and only if $\lambda = B + A^2 + A + 1$ vanishes. In that case the Jacobian matrix has rank 2 for the solutions of (6).

So if $\lambda \neq 0$ the curve C has six singular points, namely the S_4-orbit of $(0:1:1:0:0)$. For the local structure near $(0:1:1:0:0)$ we eliminate x_0 from (2) and find that the curve C' in $\mathbf{P}^3$ is given by

$$s_3 = As_1^3, \quad s_5 = Bs_1^5.$$

Upon taking affine coordinates $\xi_1 = (x_1 + x_2)/x_1$, $\xi_2 = x_3/x_1$, $\xi_3 = x_4/x_1$ we find the equations

$$\xi_1 + \xi_1^2 + \xi_1^3 + \xi_2^3 + \xi_3^3 = A(\xi_1 + \xi_2 + \xi_3)^3,$$
$$\xi_1 + \xi_1^4 + \xi_1^5 + \xi_2^5 + \xi_3^5 = B(\xi_1 + \xi_2 + \xi_3)^5.$$

This shows that ξ_1 lies in m^3, with m the maximal ideal of $(0,0,0)$ in $\mathbf{A}^3$ and defines the tangent plane at $(0,0,0)$ to the cubic surface S given by the cubic equation. Moreover, this is also the lowest order term of the quintic equation. Therefore, locally near the origin C' is given by

$$\xi_1 = 0, \quad (\xi_2 + \xi_3)(\xi_2\xi_3 + (A+1)(\xi_2 + \xi_3)^2) = 0. \tag{7}$$

which shows that C' has a triple point and C has a node at this point.

If $\lambda = 0$ and a satisfies $(A+1)a^2 + a + 1 = 0$ then a is a solution of (6) and the S_4-orbit of points of the form $(a : x : x : 1 : a+1)$ with arbitrary x is on C. So the equations

$$x_i + x_j = 0, \quad (a+1)x_k + x_l = 0 \quad \text{with} \quad \{i,j,k,l\} = \{1,2,3,4\}$$

define a line on C and this gives 12 lines on C. Since C has degree 12 the curve C decomposes as the union of 12 lines. This proves ii).

REMARK. It follows from the preceding proof that for $\lambda \neq 0$ points on C for which $x_1, \ldots, x_4$ are not all distinct lie on one of the lines (3).

(1.2) PROPOSITION. *If $\lambda \neq 0$ then C is irreducible.*

Proof. Suppose that $C = \sum_{i=1}^{\ell} C_i$ is a sum of irreducible components C_i with $\ell \geq 2$. Since C is connected at least one of the singular points is an intersection point of two distinct components C_i. By the S_4-symmetry then each of the six singular points is an intersection point of two different components. This implies that the components C_i are non-singular. Since the permutation (34) interchanges the two branches of C in $(0:1:1:0:0)$ (cf. (7)) the group S_4 acts transitively on the branches through a singular point, so S_4 acts transitively on the set of components.

Let S be the smooth cubic surface in $\mathbf{P}^4$ given by the equations $s_1 = x_0$, $s_3 = Ax_0^3$. On S the curve C is linearly equivalent to $4H$ with H the hyperplane section of S. Now the intersection number HC_i equals the intersection number with the hyperplane $x_0 = 0$, i.e. the intersection number of C_i with the three lines (3), and since the intersection is transversal HC_i

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