Zeitschrift: 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

Kapitel: §3. BOUNDS FOR N(A,B)

Autor: van der Geer, G. / van der Vlugt, M.

DOI: https://doi.org/10.5169/seals-66065

(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*

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

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

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

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

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

If $\mathrm{Tr}(A+1)=0$ we have 12 rational points in the fibres above $0,1,\infty$, while there are none if $\mathrm{Tr}(A+1)=1$. Then (12) implies for $N(A,B)$ the inequalities

$$(q-11-13[2\sqrt{q}])/24 \leq N(A,B) \leq (q+1+13[2\sqrt{q}])/24\,.$$

By employing the decomposition of the Jacobian, especially Corollary (2.4), and taking into account that the possible values of the trace of Frobenius t of supersingular elliptic curves are $t=0,\ \pm\sqrt{2q}$ for $q=2^m$ with m odd we can refine these bounds and we obtain our main result on the numbers $N(A,B)$:

(3.1) THEOREM. *For $q=2^m$ with m odd the number $N(A,B)$ satisfies the following inequalities:*

$$(q-11-2\sqrt{2q}-8[2\sqrt{q}])/24 \leq N(A,B) \leq (q+1+2\sqrt{2q}+8[2\sqrt{q}])/24\,. \tag{13}$$

Proof. The curve C_{f_1} is a supersingular elliptic curve, which implies that $-2\sqrt{2q} \leq 2t(C_{f_1}) \leq 2\sqrt{2q}$. Since the curve C_{f_3} has genus 1, $C_{f_1+f_3}$ has genus 2 and C_{g_λ} has genus 2 we obtain from the Hasse-Weil-Serre bound

$$-8[2\sqrt{q}] \leq 2t(C_{f_3})+2t(C_{f_1+f_3})+t(C_{g_\lambda}) \leq 8[2\sqrt{q}]\,.$$

Then it follows from Corollary (2.4) that the trace of Frobenius of $C_{A,B}$ is in the interval

$$[-2\sqrt{2q}-8[2\sqrt{q}],2\sqrt{2q}+8[2\sqrt{q}]]$$

which yields (13).

In the following table we illustrate this by listing the intervals in which the numbers lie according to (13).

TABLE 1

q	32	128	512	2048	8192
interval	$[0,4]$	$[0,14]$	$[4,38]$	$[50,120]$	$[270,412]$

For some further reflections on $N(A,B)$ we restrict our attention to the case $q=2^m$ with m odd. The practice of searching for curves with many points tells us that is is highly improbable that in a fibre product of curves the traces of Frobenius of the individual components simultaneously reach their maximal (or minimal) value. Hence it is very unlikely that the bounds given in (13) will be reached.

We intend to design an interval which contains almost all values of $N(A,B)$ using the description of C as a fibre product of the curves C_{f_i} for $i = 1,2,3$ given in (11) and a probabilistic argument on the distribution of traces of Frobenius.

The curves C_{f_1} and C_{f_2} are supersingular elliptic curves with the same trace of Frobenius $t = t(C_{f_i}) = 0, \pm\sqrt{2q}$. The curve $C_{f_1+f_2}$ has genus 3 which implies

$$-3[2\sqrt{q}] \leq t(C_{f_1+f_2}) \leq 3[2\sqrt{q}]\,.$$

So the trace of Frobenius for the normalization of the fibre product $C_{f_1} \times_{\mathbf{P}^1} C_{f_2}$ satisfies

$$-3[2\sqrt{q}] - 2\sqrt{2q} \leq t \leq 3[2\sqrt{q}] + 2\sqrt{2q}\,.$$

We compute bounds for the number of $x \in \mathbf{P}^1 - \{0,1,\infty\}$ above which we have 4 points in the fibre of $C_{f_1} \times_{\mathbf{P}^1} C_{f_2}$ If $\mathrm{Tr}(A+1) = 0$ we find in total 8 points above $x = 0,1,\infty$, while we find none if $\mathrm{Tr}(A+1) = 1$. Subsequently we take into account that completely splitting $x \in \mathbf{P}^1 - \{0,1,\infty\}$ occur in pairs $(x, 1/x)$ and we obtain the following proposition.

(3.2) PROPOSITION. *If we let*

$$M(f_1,f_2) = \frac{1}{2}\#\{x \in \mathbf{P}^1(\mathbf{F}_q) - \{0,1,\infty\} : x \text{ splits completely in } C_{f_1} \times_{\mathbf{P}^1} C_{f_2}\}$$

then we have for $\mathrm{Tr}(A+1) = 0$

$$\frac{q - 7 - 3[2\sqrt{q}] - 2\sqrt{2q}}{8} \leq M(f_1,f_2) \leq \frac{q - 7 + 3[2\sqrt{q}] + 2\sqrt{2q}}{8}$$

and for $\mathrm{Tr}(A+1) = 1$

$$\frac{q + 1 - 3[2\sqrt{q}] - 2\sqrt{2q}}{8} \leq M(f_1,f_2) \leq \frac{q + 1 + 3[2\sqrt{q}] + 2\sqrt{2q}}{8}\,.$$

We now consider the effect of the elliptic curve C_{f_3} in the fibre product. The j-invariant of C_{f_3} is $\lambda^{-4} \in \mathbf{F}_q^*$. This implies that $t(C_{f_3})$ is odd. For $\mathrm{Tr}(A+1) = 0$ we have $t(C_{f_3}) \equiv 1 \pmod 4$ and there are 4 rational points together above $x = 0,1,\infty$, while if $\mathrm{Tr}(A+1) = 1$ we have $t(C_{f_3}) \equiv 3 \pmod 4$ and 2 rational points above $0,1,\infty$. Furthermore, each element of $\mathbf{F}_q^*$ occurs exactly once as j-invariant in the family of curves C_{f_3}. That implies that $t(C_{f_3})$ assumes each odd integer value in the interval $[-[2\sqrt{q}], [2\sqrt{q}]]$. So the number of completely splitting pairs assumes each integral value in the intervals mentioned in the following proposition.

(3.3) PROPOSITION. *If we let*

$$M(f_3) = \frac{1}{2}\#\{x \in \mathbf{P}^1(\mathbf{F}_q) - \{0,1,\infty\} : \ x \textit{ splits completely in } C_{f_3}\}$$

then $M(f_3)$ assumes all integer values in the intervals

$$\left[\frac{q-3-[2\sqrt{q}]}{4}, \frac{q-3+[2\sqrt{q}]}{4}\right] \qquad \textit{if } \operatorname{Tr}(A+1) = 0\,,$$
$$\left[\frac{q-1-[2\sqrt{q}]}{4}, \frac{q-1+[2\sqrt{q}]}{4}\right] \qquad \textit{if } \operatorname{Tr}(A+1) = 1\,.$$

Finally, we combine the two preceding propositions via a heuristic argument. Let

$$M(f_1,f_2,f_3)$$
$$= \frac{1}{2}\#\{x \in \mathbf{P}^1(\mathbf{F}_q) - \{0,1,\infty\} : x \text{ splits completely on } C_{f_1} \times_{\mathbf{P}^1} C_{f_2} \times_{\mathbf{P}^1} C_{f_3}\}$$

Since there are $(q-2)/2$ pairs $(x, 1/x)$ $(x \neq 0,1,\infty)$ we expect

$$2\left(\frac{q-3-[2\sqrt{q}]}{4}\right)\left(\frac{q-7-3[2\sqrt{q}]-2\sqrt{2q}}{8}\right)/(q-2) \leq M(f_1,f_2,f_3)$$
$$\leq 2\left(\frac{q-1+[2\sqrt{q}]}{4}\right)\left(\frac{q+1+3[2\sqrt{q}]+2\sqrt{2q}}{8}\right)/(q-2)\,.$$

If we work this out and neglect terms of order $1/\sqrt{q}$ and lower we find

$$(14) \quad \frac{q-4[2\sqrt{q}]-2\sqrt{2q}+4+4\sqrt{2}}{16} \leq M(f_1,f_2,f_3)$$
$$\leq \frac{q+4[2\sqrt{q}]+2\sqrt{2q}+14+4\sqrt{2}}{16}\,.$$

Each completely splitting pair yields 16 solutions of (1) so to estimate the number of S_4-orbits of solutions $N(A,B)$ we multiply the interval by $16/24$ to get an interval I. Since $N(A,B)$ is even we adapt the endpoints of the interval I just obtained slightly. Namely we consider the smallest interval with endpoints the positive even integers which contains I and we denote this interval by I^{even}.

(3.4) HEURISTICS. *The odds are that the values of $N(A,B)$ are in the interval*

$$I^{\text{even}} = \left[\frac{q-4[2\sqrt{q}]-2\sqrt{2q}+4\sqrt{2}+4}{24}, \frac{q+4[2\sqrt{q}]+2\sqrt{2q}+4\sqrt{2}+14}{24}\right]^{\text{even}}.$$

We illustrate this by a little table.