§4. Numerical results

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **48 (2002)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.09.2024**

TABLE 2

q	32	128	512	2048	8192
interval	$[0,6]$	$[0,12]$	$[10,34]$	$[64,108]$	$[300,384]$

§4. NUMERICAL RESULTS

In order to obtain numerical results on $N(A,B)$ to test our heuristics the first remark is that $N(A_1,B) = N(A_2,B)$ if $\mathrm{Tr}(A_1) = \mathrm{Tr}(A_2)$. So we have to distinguish only between $\mathrm{Tr}(A) = 0$ and $\mathrm{Tr}(A) = 1$. We shall compute the trace of Frobenius for the seven factors of our Jacobian. We shall write $f_4 = f_1 + f_2$, $f_5 = f_1 + f_3$, $f_6 = f_2 + f_3$ and $f_7 = f_1 + f_2 + f_3$. The Jacobians of the curves C_{f_i} given by $y^2 + y = f_i$ for $i = 1, \dots, 7$ constitute the seven factors of $\mathrm{Jac}(C_{A,B})$. We write

$$n_{f_i} = \#\{x \in \mathbf{F}_q^* : \mathrm{Tr}(f_i(x)) = 0\}.$$

(4.1) PROPOSITION. *The number of solutions $N(A,B)$ over $\mathbf{F}_{q=2^m}$ with m odd of the system (1) with $\lambda = A^2 + A + 1 + B \neq 0$ is given by*

$$N(A,B) = \frac{2q - 2 - 2(n_{f_1} + n_{f_2} + n_{f_3} - n_{f_4} - n_{f_5} - n_{f_6} + n_{f_7})}{24} \quad \text{if } \mathrm{Tr}(A) = 0,$$

and

$$N(A,B) = \frac{-6q - 2 + 2\sum_{i=1}^{7} n_{f_i}}{24} \quad \text{if } \mathrm{Tr}(A) = 1.$$

Proof. As just explained we may take $A = 0$ or $A = 1$. Then $\lambda = B + 1 \neq 0$ and we set $f_1 = (B+1)(x^3 + x)$, $f_2 = (B+1)(1/x^3 + 1/x)$ and $f_3 = (B+1)(x + 1/x)$. Then $C_{1,B} = C_{f_1} \times_{\mathbf{P}^1} C_{f_2} \times_{\mathbf{P}^1} C_{f_3}$ and $C_{0,B} = C_{f_1+1} \times_{\mathbf{P}^1} C_{f_2+1} \times_{\mathbf{P}^1} C_{f_3+1}$. As in Theorem (2.3) the curves C_{f_i} for $i = 4, \dots, 7$ give the remaining traces of Frobenius.

The trace of Frobenius $t(C_{f_i})$ is of the form

$$t(C_{f_i}) = q + 1 - 2n_{f_i} - a_i,$$

where a_i is the contribution of $x = 0, \infty$, while the trace of Frobenius of C_{f_i+1} is

$$t(C_{f_i}) = -q + 3 + 2n_{f_i} - b_i,$$

where b_i is the contribution of $x = 0, \infty$. By analyzing these contributions from 0 and ∞ one gets the proposition.

We now give tables with the distribution of the numbers $N(A,B)$ for $q = 2^m$ with m odd and $5 \leq m \leq 13$. These tables are obtained by computing the numbers n_{f_i} and they solve the coset weight distribution problem for the corresponding $BCH(3)$ codes. The first unknown case up to now was $q = 2^9$, see [C-Z]. Moreover, the tables confirm our heuristics. We list the frequencies divided by $q/2$.

TABLE 3

$q = 2^5$:

$N(A,B)$	0	2
frequency	27	35

$q = 2^7$:

$N(A,B)$	0	2	4	6	8	10
frequency	2	28	98	84	35	7

$q = 2^9$:

$N(A,B)$	12	14	16	18	20	22	24	26	28	30	32
frequency	18	21	117	180	148	195	199	81	36	18	9

$q = 2^{11}$:

$N(A,B)$	66	68	70	72	74	76	78	80	82	84	86
frequency	22	66	88	55	176	264	187	374	374	374	451
$N(A,B)$	88	90	92	94	96	98	100	102	104	106	108
frequency	365	341	275	341	154	44	55	33	11	22	22

$q = 2^{13}$:

In this case we encounter a new phenomenon. The function $N(A,B)$ assumes even values in the interval $[290, 390]$, but not all even values are taken. This contradicts the expectation of [C-Z] that the values form a sequence of even integers without gaps. The frequency divided by $q/2$ of the value $290+2\ell$ with $0 \le \ell \le 50$ is given by

$$13\,\gamma_\ell + \begin{cases} 1 & \text{if } \ell = 11, \\ 1 & \text{if } \ell = 37, \\ 0 & \text{else,} \end{cases}$$

where $\gamma = (\gamma_0, \dots, \gamma_{50})$ is the vector

$$\gamma = (1,0,1,0,1,0,6,3,5,5,12,7,19,15,22,25,37,40,43,37,35,60,54,72,72,\\ 58,65,61,57,57,63,48,35,44,34,34,25,29,25,15,9,7,2,3,7,3,3,1,0,1,2).$$

In accordance with our heuristics less than 1% of the $N(A,B)$ lie outside the interval $[300,384]$.

§5. The covering radius

A problem in coding theory that precedes the coset weight distribution problem is the determination of the covering radius. It is defined for a binary linear code C of length n as the smallest integer ρ such that the spheres of radius ρ around the codewords cover $\mathbf{F}_2^n$. Equivalently, it is the maximum weight of a coset leader (by which we mean a vector of minimum weight in a coset of C in $\mathbf{F}_2^n$). It is an interesting parameter of a code since it provides information on the performance of the code when used in data compression.

In a series of papers [H-B], [A-M] and [H], of which [H-B] and [H] treat the case m even and [A-M] the case m odd, it was proved that the $BCH(3)$ code of length $n = 2^m - 1$ has covering radius

$$\rho(BCH(3)) = 5 \qquad \text{for} \quad m \ge 4\,.$$

The proofs for the various cases are very different. Using algebraic geometry we can give a unified proof.

In order to prove that $\rho(BCH(3)) = 5$ we have to show that for every $(A,B,C) \in \mathbf{F}_q^3$ the system of equations:

$$\begin{aligned} x_1 + \dots + x_5 &= A\,, \\ x_1^3 + \dots + x_5^3 &= B\,, \\ x_1^5 + \dots + x_5^5 &= C\,, \end{aligned} \tag{15}$$

has a solution $(x_1, \dots, x_5) \in \mathbf{F}_q^5$. On replacing x_i by $x_i + A$ we may assume without loss of generality that $A = 0$ and $(B,C) \neq (0,0)$. If we then