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: §5. The covering radius

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

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

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 $\gamma = (\gamma_0, \ldots, \gamma_{50})$ 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:

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

has a solution $(x_1, \ldots, x_5) \in \mathbf{F}_q^5$. 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 homogenize (15) the system

$$(16) \qquad \sum_{i=1}^{5} x_i = 0, \qquad \sum_{i=1}^{5} x_i^3 = Bx_0^3, \qquad \sum_{i=1}^{5} x_i^5 = Cx_0^5$$

defines a projective variety V of dimension 2 in the five dimensional projective space $\mathbf{P}^5$.

We intersect V with the hyperplane $x_0 + x_5 = 0$ and obtain a system of equations of the form (2). By using the results of Section 1 (especially Corollary (1.3)) one can easily show that $\rho(BCH(3)) = 5$ for $m \geq 10$. We leave the details to the reader.

As a final remark we would like to point out that we think that many more problems on cyclic codes can be attacked succesfully using methods from algebraic geometry as is done in this paper. We refer to [C] for a list of such problems.

REFERENCES

[A-M] ASSMUS, E. F., JR. and H. F. MATTSON, JR. Some 3-error-correcting BCH codes have covering radius 5. *IEEE Trans. Info. Th. 22* 1976, 348–349.

[C] CHARPIN, P. Open problems on cyclic codes. In: *Handbook of Coding Theory I*, V.S. Pless, W.C. Huffman Eds., Elsevier Science BV, Amsterdam, 1998, 963–1063.

[C-Z] CHARPIN, P. and V. ZINOVIEV. On coset weight distributions of the 3-error-correcting BCH codes. *SIAM J. Discrete Math. 10* (1997), 128–145.

[H] HELLESETH, T. All binary 3-error-correcting BCH codes of length $2^m - 1$ have covering radius 5. *IEEE Trans. Info. Th. 24* (1978), 257–258.

[H-B] VAN DER HORST, J. A. and T. BERGER. Complete decoding of triple-error-correcting binary BCH codes. *IEEE Trans. Info. Th. 22* (1976), 138–147.

[vL] VAN LINT, J. H. *Introduction to Coding Theory (3rd ed.).* Graduate Texts in Mathematics 86, Springer, Berlin, 1999.

[Mi] MILNE, J. S. Jacobian varieties. In: *Arithmetic Geometry* (Storrs 1984), G. Cornell, J. H. Silverman Eds., Springer, New York, 1986, 167–212.

[Mu] MUMFORD, D. *Curves and Their Jacobians.* The University of Michigan Press, Ann Arbor, Mich., 1975.