ELSEVIER

Discrete Mathematics 152 (1996) 185–190

DISCRETE MATHEMATICS

On the weight hierarchy of the semiprimitive codes☆

Tor Helleseth[a,*], P. Vijay Kumar[b]

[a] *Department of Informatics, University of Bergen Høyteknologisenteret, N-5020 Bergen, Norway*

[b] *Communication Sciences Institute, EE-Systems, EEB 534, University of Southern California, Los Angeles, CA 90089-2565, USA*

Received 27 July 1993; revised 11 March 1994

Abstract

An irreducible cyclic (n, k) code is said to be semiprimitive if $n = (2^k - 1)/N$ where $N > 2$ divides $2^j + 1$ for some $j \geqslant 1$. The complete weight hierarchy of the semiprimitive codes is determined when $k/2j$ is odd. In the other cases, when $k/2j$ is even, some partial results on the generalized Hamming weights of the semiprimitive codes are obtained. We apply the above results to find the generalized Hamming weight of some classes of dual codes of primitive BCH codes with designed distance $N + 2$ when $k/2j$ is odd.

1. Introduction

Let $F = GF(2^k)$ be a finite field with 2^k elements and let ψ be a generator of the multiplicative group $F^* = F \setminus \{0\}$.

Let $h(x) \in GF(2)[x]$ be an irreducible polynomial of degree k and period n. Then any irreducible (n, k) code C over $GF(2)$ can be described as

$$C = \{c(a) \mid c(a) = (Tr(a), Tr(a\beta), \ldots, Tr(a\beta^{n-1})), a \in F\}$$

where β is a zero of $h(x)$ and $Tr(x)$ denotes the trace function from $GF(2^k)$ to $GF(2)$. Note that k is the multiplicative order of $2 \pmod n$.

An irreducible cyclic code is said to be semiprimitive if $\beta = \psi^N$ where $N > 2$ and $N \mid 2^j + 1 \mid 2^k - 1$ for some integer $j \geqslant 1$. Observe that in this case k is even and $2j \mid k$. The length of the code C is $n = (2^k - 1)/N$.

For $N \mid 2^k - 1$ we define

$$P_i = \{f \in F \mid f = \psi^l, l \equiv i \pmod N\}$$

Then P_0 is the set of nonzero Nth powers in F and $P_i = \psi^i P_0$ for $0 \leqslant i \leqslant N - 1$.

☆ This work was supported in part by the Norwegian Research Council and the National Science Foundation under Grant Number NCR-9016077.

* Corresponding author.

SSDI 0012-365X(94)00234-7

Baumert and McEliece [1] computed the weight distribution of the semiprimitive codes as given in the following result.

Lemma 1. *Let C be a semiprimitive code where $N > 2$ and $N|2^j + 1|2^k - 1$ for some $j \geqslant 1$. Then C is a two-weight code and the Hamming weight, $w(\boldsymbol{c}(a))$, of a nonzero codeword $\boldsymbol{c}(a)$ is given by*

$$w(\boldsymbol{c}(a)) = \begin{cases} (2^{k-1} - (-1)^{(k/2j)+1}(N-1)2^{(k/2)-1})/N & \text{if } a \in P_0, \\ (2^{k-1} - (-1)^{(k/2j)}2^{(k/2)-1})/N & \text{if } a \in F^* \setminus P_0, \end{cases}$$

where P_0 is the set of nonzero Nth powers in F^*.

There is a vectorspace isomorphism from F to C given by $a \to \boldsymbol{c}(a)$. It is useful to observe that in the case when $k/2j$ is odd the vectors of C of minimum weight correspond exactly to $a \in P_0$ while the maximum weight vectors correspond to $a \in F^* \setminus P_0$. In the case when $k/2j$ is even the situation is the opposite.

2. The weight hierarchy

For any code D, let $\chi(D)$ be the support of D, i.e., the set of positions where not all of the codewords of D are zero. The rth generalized Hamming weight of a code C is defined by

$$d_r(C) = \min\{|\chi(D)| \,|\, D \text{ is an } r\text{-dimensional subcode of } C\}.$$

The weight hierarchy of a code C is the set of generalized Hamming weights $\{d_r(C)\}$, $1 \leqslant r \leqslant k$.

The weight hierarchy has been determined for the Golay code, Reed-Muller codes by Wei [13], for codes meeting the Griesmer bound by Helleseth et al. [6].

For the BCH codes very little is known. It has been shown by Feng et al. [5] that $d_2 = 8$ for all binary primitive double-error-correcting codes. Van der Geer and van der Vlugt [11] proved that $d_3 = 10$ for all binary primitive double-error-correcting BCH codes and $d_2 = 11$ in the triple-error-correcting case. Kabatianski [8] proved that $d_2 = 3t + 2$ for all sufficiently long t-error-correcting primitive BCH codes.

The generalized Hamming weights of the dual of the BCH codes are studied by Chung [3], Duursma et al. [4], and van der Geer and van der Vlugt [10, 12].

A simple, but very useful observation by Helleseth and Kumar [7] and van der Geer and van der Vlugt [12] is that for any r-dimensional subcode D of C it holds that

$$|\chi(D)| = \frac{1}{2^{r-1}} \sum_{\boldsymbol{d} \in D} w(\boldsymbol{d}). \tag{1}$$

Hence, to find the rth generalized Hamming weight of a code, it is enough to find the smallest sum of the weights for any r-dimensional subcode. In particular, if we can

find an r-dimensional subcode where all nonzero codewords have minimum weight d this subcode will have support size equal to $d_r = (2^r - 1)d/2^{r-1}$.

Lemma 2. *Let C be a semiprimitive code where $N > 2$ and $N|2^j + 1|2^k - 1$ for some $j \geqslant 1$. Let $m = m(N, k)$ be the largest divisor of k such that $\gcd(N, 2^m - 1) = 1$. Let k_0 be the greatest odd divisor of $k/2j$. Then $m \geqslant k_0 j$ and for $1 \leqslant r \leqslant m$ the generalized Hamming weight d_r of C equals*

$$d_r = (2^r - 1)d/2^{r-1}$$

where d is the minimum distance of C.

Proof. Since $\gcd(N, 2^m - 1) = 1$ and $m|k$, it follows that all the elements in the subfield $GF(2^m)$ of F are Nth powers. Therefore the nonzero vectors of the m-dimensional subspace $V_0 = GF(2^m)$ are contained in P_0. Further, the nonzero vectors of the m-dimensional subspace $V_1 = \psi\, GF(2^m)$ are contained in P_1 which is a subset of $F^* \backslash P_0$. Hence, from Lemma 1 it follows that there exist a subspace $V = V_0$ or $V = V_1$ such that

$$D = \{c(a) \mid a \in V\}$$

is an m-dimensional subcode of C which contains $2^m - 1$ nonzero vectors of minimum weight d. Therefore for $1 \leqslant r \leqslant m$, it follows from (1) that

$$d_r = (2^r - 1)d/2^{r-1}.$$

Since k_0 is odd and $N|2^j + 1$, it follows that $N|2^{k_0 j} + 1$ and therefore since $N > 1$ that $\gcd(N, 2^{k_0 j} - 1) = 1$, which implies $m \geqslant k_0 j$. □

In general it seems hard to determine the complete weight hierarchy for all the semiprimitive codes. However, in the case $N|2^j + 1|2^k - 1$ and $k/2j$ odd we can find the complete weight hierarchy.

Theorem 3. *Let C be a semiprimitive code where $N > 2$, $N|2^j + 1|2^k - 1$ and $k/2j$ is odd for some $j \geqslant 1$. Then $m = m(N, k) = k/2$ and the complete weight hierarchy of C is given by*

$$d_r = \begin{cases} (2r - 1)d/2^{r-1} & \text{if } 1 \leqslant r \leqslant m, \\ (2^r - 1)d/2^{r-1} + (N - 1)(2^m + 1)(1 - 2^{m-r})/N & \text{if } m < r \leqslant 2m, \end{cases}$$

where $d = (2^{2m-1} - (N - 1)2^{m-1})/N$ is the minimum distance of C.

Proof. Since $k_0 = k/2j$ is odd, it follows from Lemma 2 that $m = m(N, k) = k_0 j = k/2$ and $d_r = (2^r - 1)d/2^{r-1}$ for $1 \leqslant r \leqslant m = k/2$.

Let $r > m$ and define $V_i = \psi^i GF(2^m)$ and $V_i^* = V_i \backslash \{0\}$ for $i = 0, 1, \ldots, 2^m$. Observe that V_i^*, $i = 0, 1, \ldots, 2^m$ is a partition of $GF(2^{2m})^*$ and that $P_l = \bigcup_{i \equiv l (\mathrm{mod}\, N)} V_i^*$ for $l = 0, 1, \ldots, N - 1$.

Since V_i is a vectorspace of dimension m, any r-dimensional subspace D_r of $GF(2^{2m})$ contains at least $2^{r-m}-1$ vectors from V_i^* for all i, $0 \leqslant i \leqslant 2^m$. Hence, any r-dimensional subspace of $GF(2^{2m})$ contains at least $(N-1)((2m+1)/N)(2^{r-m}-1)$ elements from $GF(2^{2m})^* \backslash P_0$, i.e., the elements from V_i^* where $0 \leqslant i \leqslant 2^m$ and $i \not\equiv 0 \pmod N$. Since the mapping $a \to \boldsymbol{c}(a)$ gives an isomorphism from $GF(2^{2m})$ to C, it follows from Lemma 1 that any r-dimensional subcode of C has at least $(N-1)((2m+1)/N)(2^{r-m}-1)$ codewords of the maximum weight in the two-weight code C.

To find d_r for $r > m$, it is therefore sufficient to find an r-dimensional subcode of C with exactly $(N-1)((2m+1)/N)(2^{r-m}-1)$ codewords of the maximum weight and the remaining nonzero codewords of minimum weight in the subcode.

Let U be an r-dimensional subspace of $GF(2^{2m})$ containing $GF(2^m)$. Then $U = \langle u_1, u_2, \ldots, u_{r-m}, f_1, \ldots, f_m \rangle$ where $u_i \in GF(2^{2m}) \backslash GF(2^m)$, $f_j \in GF(2^m)$ for $1 \leqslant i \leqslant r-m$, $1 \leqslant j \leqslant m$. Then U is a disjoint union of $GF(2^m)$ and $2^{r-m}-1$ cosets of the form $u + GF(2^m)$ where $u \in U \backslash GF(2^m)$.

We will show that each such coset $u + GF(2^m)$ where $u \in U \backslash GF(2^m)$ contains $(N-1)\frac{2^m+1}{N}$ elements from $GF(2^m)^* \backslash P_0$ and $(2^m - N + 1)/N$ elements from P_0. This follows since for fixed $u \in U \backslash GF(2^m)$ then $u + f \in V_i$ has exactly one solution $f \in GF(2^m)$ for any $i = 1, 2, \ldots, 2^m$. Suppose, $u + f_1 \in V_i$ and $u + f_2 \in V_i$, then $f_1 + f_2 \in V_i$ which implies $f_1 = f_2$ since $1 \leqslant i \leqslant 2^m$. Further, since $GF(2^m)$ contains $2^m - 1$ nonzero elements from P_0, it follows that the r-dimensional subcode D of C given by

$$D = \{\boldsymbol{c}(u) \mid u \in U\}$$

has the following weight distribution:

$\frac{2^m-N+1}{N}(2^{r-m}-1) + 2^m - 1$	words of weight	$d = (2^{2m-1} - (N-1)2^{m-1})/N$,
$(N-1)\frac{2^m+1}{N}(2^{r-m}-1)$	words of weight	$d + 2^{m-1} = (2^{2m-1} + 2^{m-1})/N$,
1	word of weight	0.

In particular, this subcode D contains as few maximum weight codewords as possible. Hence, from (1) we can find d_r by summing over all the weights in D, which leads to

$$d_r = \frac{1}{2^{r-1}} \sum_{\boldsymbol{d} \in D} w(\boldsymbol{d}) = (2^r - 1)d/2^{r-1} + (N-1)(2^m+1)(1-2^{m-r})/N$$

which implies the result in the theorem. □

This result was obtained in a different way by van der Vlugt [9].

It is also straightforward to obtain bounds on d_r in the case when $k/2j$ is even, using this method and construct subcodes with as many words as possible of the minimum

weight d. We leave further details to the reader. We have, however, so far been unable to find the complete weight hierarchy in the case where $k/2j$ is even.

It is interesting to note that the results on the weight hierarchy for the semiprimitive codes when $k/2j$ are odd, can be applied to find some of the generalized Hamming weights of some dual of BCH codes with designed distance $N+2$. No similar connections hold in the case when $k/2j$ is even. In fact, the following theorem extends some results in Duursma et al. [4], and van der Geer and van der Vlugt [10] on the weight hierarchy of some duals of the BCH codes.

Theorem 4. *Let $N > 2$, $N|2^j + 1|2^k - 1$ and $k/2j$ odd for some $j \geqslant 1$. The dual code of a primitive BCH code of length $2^k - 1$ and designed distance $N+2$ has generalized Hamming weights*

$$d_r = (2^r - 1)d/2^{r-1}$$

for $1 \leqslant r \leqslant k/2$, where $d = 2^{k-1} - (N-1)2^{(k/2)-1}$.

Proof. From the Carlitz–Uchiyama [2] bound it follows that for the weight of any codeword in the dual of the primitive BCH code of designed distance $2t+1$ it holds that

$$2^{k-1} - (t-1)2^{(k/2)} \leqslant d \leqslant 2^{k-1} + (t-1)2^{(k/2)}.$$

It is important to note that repeating every codeword N times in a semiprimitive code of length $n = (2^k - 1)/N$ is a subcode of the dual of a BCH code of designed distance $N + 2 = 2t + 1$, since a typical codeword in the repeated semiprimitive code is $c(a) = (Tr(a), Tr(a\psi^N), \ldots, Tr(a\psi^{(2^k-2)N}))$, where ψ is a primitive element in $GF(2^k)$.

In particular in the semiprimitive case when $k/2j$ is odd the minimum distance of the repeated semiprimitive code is

$$2^{k-1} - (t-1)2^{k/2} = 2^{k-1} - (N-1)2^{(k/2-1)}$$

which therefore equals the minimum distance of the dual of the BCH code of designed distance $N+2$. Hence, if the semiprimitive code contains a subspace of dimension $m = m(N,k) = k/2$ of vectors of minimum weight, the same is true for the BCH code. This completes the proof. □

Remark. One should observe that combining the arguments in Theorem 4 with Theorem 3 give an upper bound for d_r for the duals of the BCH codes above also in the case $k/2 < r \leqslant k$.

3. Conclusions

We have completely determined the weight hierarchy of the semiprimitive codes in the case $N > 2$, $N|2^j + 1|2^k - 1$ and $k/2j$ odd for some $j \geqslant 1$. Clearly, one may apply

this method to obtain bounds for d_r also in the case $k/2j$ is even by constructing subcodes with many vectors of minimum weight d. To completely determine the weight hierarchy in the other case when $k/2j$ is even is still an open problem.

A code C is said to satisfy the chain condition if there is a chain of subcodes $D_1 \subset D_2 \subset \cdots \subset D_k = C$ such that $\dim D_i = i$ and $|\chi(D_i)| = d_i$ for $1 \leqslant i \leqslant k$. It follows directly from the proof of Theorem 3 that the chain condition holds for these codes.

Finally, we would like to remark that it is straightforward to generalize the results above to nonbinary semiprimitive codes and to the corresponding duals of the nonbinary BCH codes.

Acknowledgements

The authors would like to thank H. Stichtenoth for communicating his results in [4] to us which partly inspired the present paper.

References

[1] L.D. Baumert and R.J. McEliece, Weights of irreducible cyclic codes, Inform. and Control 20 (1972) 159–175.
[2] L. Carlitz and S. Uchiyama, Bounds for exponential sums, Duke Math. J. 24 (1957) 37–41.
[3] H. Chung, The second generalized Hamming weights of double-error correcting binary BCH codes and their dual codes, Lecture Notes in Computer Science, Vol. 539 (Springer, Berlin, 1991) 118–129.
[4] I. Duursma, H. Stichtenoth and C. Voss, Generalized Hamming weights for duals of BCH codes and maximal algebraic function fields, preprint, 1993.
[5] G.L. Feng, K.K. Tzeng and V.K. Wei, On the generalized Hamming weights of several classes of cyclic codes, IEEE Trans. Inform. Theory 38 (1992) 1125–1130.
[6] T. Helleseth, T. Kløve and Ø. Ytrehus, On the generalized Hamming weights of linear codes, IEEE Trans. Inform. Theory 38 (1992) 1133–1140.
[7] T. Helleseth and V. Kumar, On the weight hierarchy of the Kasami codes, Discrete Math. 145 (1995) 133–143.
[8] G. Kabatianski, On the second generalized Hamming weight, in: Proc. Internat. Workshop on Algebraic and Combinatorial Coding Theory, Voneshta Voda, Bulgaria, June 1992.
[9] M. van der Vlugt, The weight hierarchy of irreducible cyclic codes, submitted for publication.
[10] G. van der Geer and M. van der Vlugt, Fibre products of Artin–Schreier curves and generalized Hamming weights of codes, Report 93-05, University of Amsterdam, 1993.
[11] G. van der Geer and M. van der Vlugt, On generalized Hamming weights of BCH-codes, IEEE Trans. Inform. Theory 40 (1994) 543–546.
[12] G. van der Geer and M. van der Vlugt, The second generalized Hamming weights of the dual codes of double-error correcting binary BCH codes, Bull. London Math. Soc. 27 (1995) 82–86.
[13] V.K. Wei, Generalized Hamming weights for linear codes, IEEE Trans. Inform. Theory 37 (1991) 1412–1418.