Ann. Sci. Math. Québec **32** (2008), no 1, 57–62

DIMENSION AND MINIMUM DISTANCE OF A CLASS OF BCH CODES

KENZA GUENDA

RÉSUMÉ. Dans cet article, on détermine la dimension des codes BCH de petite distance construite et de longueur $n = q^m + 1$, où $m > 1$. Nous calculons aussi la distance minimale et nous donnons des bornes supérieures pour celle-ci. Ceci a été fait en étudiant la forme des classes cyclotomiques modulo n et par une généralisation des résultats de Farr et Peterson.

ABSTRACT. In this paper, we determine the dimension of the BCH codes with small designed distance of length $n = q^m + 1$, such that $m > 1$. We also calculate the minimum distance and give upper bounds for it. This has been done by studying the structure of the cyclotomic classes modulo n and by generalizing some results of Farr and of Peterson.

1. Introduction

Let q be a prime power and α be a fixed primitive n-th root of unity in $\mathbb{F}_q$. We consider $B_q(n, \delta)$, the narrow sense BCH code of length n and designed distance δ over $\mathbb{F}_q$. Indeed, this is a cyclic code generated by a polynomial which is of the form

$$g(x) = \prod_{i \in T} (x - \alpha^i), \text{ with } T = \bigcup_{1 \leq j < \delta} Cl(j),$$

where $Cl(j) = \{jq^l \pmod n \,|\, l \in \mathbb{N}\}$ is the cyclotomic class of j modulo n over $\mathbb{F}_q$. The set T is called *the defining set of the code*. Since, often, we may have $Cl(j) = Cl(i)$ for $i \neq j$, the determination of the dimensions of such codes can be a hard task. Recently, in [1], Aly, Klappenecker and Sarvepalli gave the dimension of $B_q(n, \delta)$ codes that are not necessarily primitive, for a certain range of designed distances. However, for $n = q^m + 1$, we cannot apply the results "$\delta = 1$" in [1, Theorem 10].

In the present paper we give the dimension of the narrow sense BCH codes of length $n = q^m + 1$, $m > 1$, and designed distance δ smaller than q, and we give upper bounds on the minimum distance. In the second section, we study the properties of the cyclotomic classes $Cl(j)$ modulo the integer $n = q^m+1$, when j is such that $1 \leq j < q$ and $m > 1$. In the third section, we use these properties to give the dimension of $B_q(n, \delta)$, when $\delta \leq q$. Finally, in the last section, we give an improvement on the bound of d, the minimum distance of $B_q(n, \delta)$, as a generalization of Farr's Theorem [4] to

Reçu le 26 novembre 2006 et, sous forme définitive, le 14 janvier 2009.

the non binary and the non primitive cases. Another generalization of Theorem 9.2.3 of Peterson [4] to the non binary cases gives us the true minimum distance of the codes when the designed distance divides n. Furthermore, due to this generalization, we also get another upper bound when m is odd. Note that in general, the determination of the minimum distance is an NP-Hard problem. The bound on it allows to find physically d, when we cannot find it mathematically. We close by giving a numerical table for different parameters which illustrates the results on the minimum distances of these codes.

2. Properties of the cyclotomic classes

We start by proving a result which will be useful throughout the rest of the paper.

Lemma 2.1. *Let q be a prime power, m be a positive integer larger than 1, and $n = q^m + 1$. Then the cardinality of $Cl(1)$ modulo n is $2m$.*

Proof. It is well known that $|Cl(1)| = \text{ord}_n(q)$, where $\text{ord}_n(q)$ defines the smallest integer t such that $q^t \equiv 1 \pmod{n}$. Since $q^{2m} \equiv 1 \pmod{q^m+1}$, we have to prove that $2m$ is the smallest integer such that $q^{2m} \equiv 1 \pmod{q^m+1}$. Assume that there exists an integer $1 \leq r < 2m$ such that $q^r \equiv 1 \pmod{q^m+1}$. Then r divides $2m$. Since $q^r = k(q^m+1)+1$, we have $r > m$. This implies that r is such that $1 < m < r < 2m$ and r divides $2m$; merely there exists no integer which satisfies these conditions. □

Lemma 2.2. *Let q be a prime power, m be a positive integer larger than 1, and $n = q^m + 1$. Then all the cyclotomic classes*

$$Cl(s) = \{sq^l \pmod{n} \mid l \in \mathbb{N}\},$$

with $1 \leq s < q$, have cardinality $|Cl(s)| = 2m$.

Proof. Let s be an integer with $1 \leq s < q$. By Lemma 2.1, $|Cl(1)| = 2m$. If we assume that $|Cl(s)| = i < 2m$, then i divides $2m$ and furthermore, i is the smallest integer which verifies $sq^i \equiv s \pmod{n}$. Therefore,

$$s(q^i - 1) \equiv 0 \pmod{q^m+1}.$$

This yields $s \geq (q^m+1)/(q^i-1)$.

If $i \leq m-1$, we have

$$s \geq \frac{q^m+1}{q^i-1} \geq \frac{q^m+1}{q^{m-1}-1} > q,$$

which is impossible since $s < q$.

If $i = m$, we have $sq^m = s + k(q^m+1)$ and $sq^m = -s + s(q^m+1)$. By adding the two equalities, we get

$$2sq^m = (k+s)(q^m+1).$$

Now, since $(q^m, q^m+1) = 1$, one has $2s \equiv 0 \pmod{q^m+1}$ and hence, $2s \geq q^m+1$. This is impossible since $s < q$ and $m > 1$.

Since $i < 2m$ and i divides $2m$, there is no other possibility for i. □

Lemma 2.3. *Let q be a prime power, m be a positive integer larger than 1, and $n = q^m + 1$. Suppose that s and s' are distinct integers with $1 \leq s, s' < q$. Then the cyclotomic classes $Cl(s)$ and $Cl(s')$ are disjoint.*

Proof. Assume the existence of two distinct integers s and s' with $1 \leq s, s' < q$ and $Cl(s) = Cl(s')$. Then there exist integers $1 \leq i < 2m$ and $1 \leq j < 2m$ such that $s \equiv q^i s' \pmod{n}$ and $s' \equiv q^j s \pmod{n}$. We have that i and j must be different from $2m$, otherwise, we will have $s \equiv q^{2m} s' \pmod{n}$, which implies $s \equiv s' \pmod{n}$. This is impossible since $s < q$ and $s' < q$.

Now, $q^i s' \equiv s \pmod{n}$ if and only if $q^i s' - s = k(q^m + 1)$, with $k \in \mathbb{Z}$. If $k < 0$, we will get $q > s = q^i s' - k(q^m + 1) \geq q^i + q^m + 1$. For any value of i, this is impossible. Consequently

$$q^i s' - s = k(q^m + 1), \text{with } k \in \mathbb{N}^*.$$

Hence, $q^i s' \geq kq^m$ and then $s' > q^{m-i}$, which is impossible for $i \leq m - 1$. By the same arguments it is impossible to have $j \leq m - 1$.

For $m \leq i \leq 2m - 2$, we have $q^i s' = s + k(q^m + 1)$ and $q^m s = -s + s(q^m + 1)$. By adding the two equalities, we get

$$q^m(s + q^{i-m} s') = (s + k)(q^m + 1)$$

and consequently, q^m divides $s + k$ and

$$s + q^{i-m} s' \equiv 0 \pmod{q^m + 1}.$$

Therefore, $s + q^{i-m} s' \geq q^m + 1$. Since $s' < q$, we obtain

$$q > s > q^m - q^{i-m+1} + 1 \geq q^m - q^{m-1} + 1,$$

which is absurd. By the same arguments, it is impossible to have $m \leq j \leq 2m - 2$. If $i = 2m - 1$ and $j = 2m - 1$, then we have

$$q^{2m-1} s' = s + k(q^m + 1).$$

By multiplying by q, we get

$$q^{2m} s' = sq + knq.$$

But $q^{2m} \equiv 1 \pmod{n}$. Hence, one has $s' \equiv sq \pmod{n}$ and $s \equiv s'q \pmod{n}$. Therefore, $s' \equiv s'q^2 \pmod{n}$ and $s \equiv sq^2 \pmod{n}$, that is, $|Cl(s')| = 2$ and $|Cl(s)| = 2$, which is absurd. □

3. The dimension of the BCH codes

Using the results of the previous section, we get the following theorem.

Theorem 3.1. *Let q be a prime power and m be an integer larger than 1. A BCH code $B_q(n, \delta)$ of length $n = q^m + 1$ and designed distance δ with $2 \leq \delta \leq q$ has dimension k given by*

$$k = q^m + 1 - 2m(\delta - 1).$$

Proof. From Lemma 2.3, the cyclotomic classes for $j < q$ are disjoints. Then, we can deduce that the defining set of $B_q(n, \delta)$ is the union of $\delta - 1$ disjoint cyclotomic classes. By Lemma 2.2, these classes have cardinality $2m$. Hence, the polynomial generator of $B_q(n, \delta)$ is of degree $2m(\delta - 1)$. Therefore, we have

$$\dim B_q(n, \delta) = q^m + 1 - 2m(\delta - 1),$$

which proves the claim. □

4. The minimum distance

The following corollary gives an important upper bound on the minimum distance.

Corollary 4.1. *Let $B_q(n, \delta)$ be a BCH code of length $n = q^m + 1$ and designed distance $\delta \leq q$ such that*

$$\sum_{i=0}^{2(\delta-1)} \binom{q^m+1}{i} (q-1)^i > q^{2m(\delta-1)}. \tag{1}$$

Then, we have

$$d \leq 4(\delta - 1). \tag{2}$$

Proof. Assume that $d \geq 4(\delta - 1) + 1$. From Theorem 3.1, the dimension is $q^m + 1 - 2m(\delta - 1)$. Thus, by the sphere-packing bound, we have

$$\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{q^m+1}{i} (q-1)^i \leq q^{2m(\delta-1)},$$

which implies

$$\sum_{i=0}^{2(\delta-1)} \binom{q^m+1}{i} (q-1)^i \leq q^{2m(\delta-1)}.$$

This is in contradiction with condition (1) . □

It is sometimes possible to give exactly the minimum distance of a BCH code, as it is given by the following generalization of Peterson's Theorem to the non binary cases.

Theorem 4.2. *Suppose $n = ab$. Then the BCH code of designed distance a has minimum distance exactly a.*

Proof. See [4, Theorem 9.2.3]. □

For m odd, we have $q + 1 \mid q^m + 1$. Then, in this case, the BCH code $B_q(n, \delta)$ contains a codeword of weight $q + 1$. Hence, one has the following corollary.

Corollary 4.3. *The minimum distance of a BCH code of length $n = q^m + 1$, with m odd and designed distance $\delta \leq q$, is at most*

$$q + 1. \tag{3}$$

In the following numerical table, we compare the bounds given by Corollaries 4.1 and 4.3 with the Griesmer bound and with the true minimum distance d deduced from Theorem 4.2 or calculated by using MAGMA (when it is possible). We also used the fact that the BCH codes are indeed nested codes. Hence, we have the inequality $d_{BCH(n,\delta)} \leq d_{BCH(n,\delta+1)}$. In some cases, this fact allows us to give tight bounds or exactly d. The notation " $\times$ " means that the bound (3) is not verified and the notation " ? " means that we cannot give exactly d or a tight bound for it. However, we have the bounds (2) and (3) or the bound of Griesmner and the BCH bounds.

q	δ	m	Bound (2)	Griesmer bound	Bound (3)	d
5	2	2	4	4	$\times$	2
		3	4	5	6	2
		4	4	7	$\times$	2
		5	4	10	6	2
		7	4	12	6	2
5	4	2	12	10	$\times$	7
		3	12	15	6	6
		4	12	20	$\times$	$5 \leq d$
		5	12	24	6	$5 \leq d \leq 6$
		6	12	29	$\times$	?
		7	12	34	6	$4 \leq d \leq 6$
5	5	3	16	20	6	6
		4	16	26	$\times$	?
		5	16	33	6	6
		6	16	39	$\times$	?
7	3	2	8	7	$\times$	5
		3	8	11	8	4
		4	8	14	$\times$	$4 \leq d \leq 8$
		5	8	18	8	4
		6	8	21	$\times$	$3 \leq d \leq 5$
		7	8	25	8	$3 \leq d \leq 4$
7	4	2	12	11	$\times$	5
		3	12	11	8	4
		4	12	16	$\times$	?
		5	12	21	8	4
		6	12	27	$\times$	$4 \leq d \leq 5$
		7	12	31	8	4
7	5	2	16	14	$\times$	5
		3	16	14	8	$5 \leq d \leq 8$
		4	16	21	$\times$	?
		5	16	28	8	$5 \leq d \leq 8$
		6	16	35	$\times$	5
7	6	2	20	18	$\times$	9
		3	20	27	8	$6 \leq d \leq 8$
		4	20	35	$\times$	?
		5	20	44	8	$6 \leq d \leq 8$
		6	20	52	$\times$	?

q	δ	m	Bound 2	Griesmer bound	Bound 3	d
11	3	2	8	8	$\times$	5
		3	8	11	12	3
		4	8	15	$\times$	?
		5	8	19	12	3
11	4	2	12	12	$\times$	6
		3	12	17	12	4
		4	12	21	$\times$	?
		5	12	28	12	4
11	5	2	16	15	$\times$	$6 \leq d$
		3	16	22	12	?
		4	16	30	$\times$	?
		5	16	37	12	$5 \leq d \leq 6$
11	6	2	20	19	$\times$	?
		3	20	28	12	6
		4	20	37	$\times$	?
		5	20	46	12	6
13	5	2	16	15	$\times$	5
		3	16	23	14	?
		4	16	30	$\times$	?
		5	16	38	14	?
		6	16	43	$\times$	5

Acknowledgements. This paper was considerably improved by the valuable comments and suggestions of an anonymous referee; for this K. Guenda is greatly indebted to him.

REFERENCES

[1] S.A. Aly, A. Klappenecker and P.K. Sarvepalli, *On quantum and classical BCH codes*, IEEE Trans. Inform. Theory **53** (2007), no. 3, 1183–1188.

[2] W.C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003, xviii+646 pp.

[3] W.J. LeVeque, *Elementary theory of numbers*, Dover Books on Advanced Mathematics, Dover Publications, Inc., New York, 1990, viii+132 pp.

[4] F.J. Macwilliams and N.J.A. Sloane, *The theory of error correcting-codes*, Benjamin, Inc. Amsterdam, North-Holland, 1977.

K. GUENDA, U.S.T.H.B., FACULTÉ DE MATHÉMATIQUES, B.P. 32, EL ALIA 16111 BAB EZZOUAR, ALGER, ALGERIA.
guendakenza@gmail.com