

# A new bound for the minimum distance of cyclic codes

Emanuele Betti

Dipartimento di Matematica "U. Dini", Università di Firenze

e-mail: betti@math.unifi.it

## Abstract

**M**ANY lower bounds exist for the minimum Hamming distance of cyclic codes, among others the BCH [2], Hartmann-Tzeng [3], and Roos [4] bounds. They are usually based on patterns in the complete defining set of the code. We present a similar bound, which is based on a pattern which has never been noted before. Our lower bound is stronger than the BCH bound, but its relation with other classical bounds is not clear: for some codes it performs better than the Roos and the Hartmann-Tzeng bounds, while for others it performs worse. We present the conjecture that the new bound asymptotically performs as well as the Roos bound.

## 1. Notations

Let  $\mathbb{F}_q$  denote the finite field with  $q$  elements,  $C$  denote an arbitrary  $\mathbb{F}_q[n, k, d]$  cyclic code and  $g_C \in \mathbb{F}_q[x]$  denote the generator polynomial of  $C$ . We always assume that  $n$  is relatively prime to  $q$ . Let  $\mathbb{F}$  be the splitting field of  $x^n - 1$  over  $\mathbb{F}_q$  and let  $\alpha$  be a primitive  $n$ -th root of unity in  $\mathbb{F}$ . We denote by  $S_C$  the complete defining set of  $C$  with respect to  $\alpha$ , i.e.:

$$S_C = \{0 \leq i \leq n-1 \mid g_C(\alpha^i) = 0\}.$$

The degree of  $g_C$  is  $n - k$  and  $c \in C$  if and only if  $c(\alpha^i) = 0$  for any  $i \in S_C$ .

## 2. The main result

We denote by  $R(n, S_C)$  the vector  $(u_0, \dots, u_{n-1}) \in \{0, \Delta\}^n$  such that  $u_i = \begin{cases} 0, & \text{if } i \in S_C, \\ \Delta, & \text{otherwise.} \end{cases}$

**Theorem 1** Let  $C$  be an  $\mathbb{F}_q[n, k, d]$  cyclic code with complete defining set  $S_C$ . Suppose that there are  $m, \ell \in \mathbb{N}$ ,  $m, \ell \geq 1$  and  $i_0 \in \{0, \dots, n-1\}$  such that:

- $(i_0 + j)_n \in S_C$ ,  $\forall j = 0, \dots, m\ell - 1$ ,
- $(i_0 + j)_n \in S_C$ ,  $\forall j = (m+h)\ell + 1, \dots, (m+h)\ell + \ell - 1$ ,  $\forall 0 \leq h \leq m$ .

Then:

$$d \geq m\ell + \ell.$$

In other words, the assumptions in Theorem 1 are equivalent to saying that  $R(n, S_C)$  "contains" (allowing for wrapping) a block of the form:

$$\overbrace{0, \dots, 0}^{\ell}, \dots, \overbrace{0, \dots, 0}^{\ell}, \overbrace{\Delta, 0, \dots, 0}^{\ell}, \dots, \overbrace{\Delta, 0, \dots, 0}^{\ell}.$$

The proof is given in [1].

## 3. Some remarks and examples

**Remark 1** Theorem 1, with  $\ell = 1$ , gives the BCH bound.

**Example 1** Let  $C$  be the binary code of length 45 with defining set

$$S_C = C_0 \cup C_1 \cup C_3 \cup C_7 \cup C_9,$$

where:

$$\begin{aligned} C_0 &= \{0\}, \\ C_1 &= \{1, 2, 4, 8, 16, 32, 19, 38, 31, 17, 34, 23\}, \\ C_3 &= \{3, 6, 12, 24\}, \\ C_7 &= \{7, 14, 28, 11, 22, 44, 43, 41, 37, 29, 13, 26\}, \\ C_9 &= \{9, 18, 36, 27\}. \end{aligned}$$

Then  $R(n, S_C)$  has the form:

$$(0, 0, 0, 0, 0, \Delta, 0, 0, 0, 0, \Delta, 0, 0, 0, 0, \dots, \Delta, 0, 0)$$

and Theorem 1 applied with  $i_0 = 0$ ,  $\ell = 5$  and  $m = 1$  ensures that the distance of  $C$  is at least 10 ( $d_A = 10$ ). The

BCH bound gives 8, and so do the Hartmann-Tzeng and the Roos bounds. The actual distance is 10.

**Example 2** Let  $C$  be the cyclic code of length 24 over  $\mathbb{F}_5$  with complete defining set

$$S_C = \{0, 1, 2, 3, 5, 6, 7, 9, 10, 11, 15, 21\}.$$

Then  $R(n, S_C)$  has the form:

$$(0, 0, 0, 0, \Delta, 0, 0, 0, \Delta, 0, 0, 0, \Delta, \Delta, \dots).$$

Applying Theorem 1 with  $\ell = 4$ ,  $m = 1$ ,  $i_0 = 0$ , we obtain that the minimum distance of  $C$  is at least 8 ( $d_A = 8$ ). The BCH and Hartmann-Tzeng bounds give 5, Roos gives 6 and the actual distance is 8.

The following theorem is a variation of our bound.

**Theorem 2** Let  $C$  be an  $\mathbb{F}_q[n, k, d]$  cyclic code with complete defining set  $S_C$ . Suppose that there are  $m, \ell \in \mathbb{N}$ ,  $m, \ell \geq 1$  and  $i_0 \in \{0, \dots, n-1\}$  such that:

- $(i_0 + j)_n \in S_C$ ,  $\forall j = h\ell, h\ell + 1, \dots, h\ell + \ell - 2$ ,  $\forall 0 \leq h \leq m$ .
- $(i_0 + j)_n \in S_C$ ,  $\forall j = (m+1)\ell, (m+1)\ell + 1, \dots, (m+1)\ell + m\ell - 1$ .

Then:

$$d \geq m\ell + \ell.$$

Theorem 2 states that we can apply our bound even if the pattern in the defining set is obtained by the reflection of the pattern given in Theorem 1, i.e., if  $R(n, S_C)$  contains (allowing for wrapping) a block of the form:

$$\overbrace{0, \dots, 0, \Delta}^{\ell}, \dots, \overbrace{0, \dots, 0, \Delta}^{\ell}, \overbrace{0, \dots, 0}^{\ell}, \dots, \overbrace{0, \dots, 0}^{\ell}.$$

## 4. Numerical results

In the following tables, we denote by "A" the new bound (the joint application of Theorem 1 and 2), by "R" the Roos bound, by  $n$  the length and by  $N_{\text{codes}}$  the number of codes of length  $n$ . B and H represent the BCH and the Hartmann-Tzeng bound respectively. The values in Tables 1, 3, 5, 7, 9 and 11 represent the number of codes for which each bound is *not* tight. The values in Tables 2, 4, 6, 8, 10 and 12 represent how many times the bound "A" performs better than the BCH, the Hartmann-Tzeng and the Roos bound, and vice versa.

$n$	$N_{\text{codes}}$	B	H	R	A
31	128	82	80	71	82
33	32	11	9	9	11
35	64	24	22	16	24
45	256	69	36	26	67
51	256	166	159	148	158
63	8192	5954	5615	4990	5791

Table 1: Tightness over  $\mathbb{F}_2$ , for some  $31 \leq n \leq 63$

$n$	$N_{\text{codes}}$	A > B	A > H	H > A	A > R	R > A
22	64	28	26	0	20	8
26	1024	163	122	148	50	291
32	512	4	0	56	0	62
40	8192	1134	780	1110	388	2408
41	64	9	2	30	1	33
44	512	100	92	8	50	92

Table 4: Comparison over  $\mathbb{F}_3$ ,  $22 \leq n \leq 44$

$n$	$N_{\text{codes}}$	B	H	R	A
12	512	54	30	12	30
16	512	294	264	226	262
18	1024	72	36	24	36
20	128	46	34	28	40
24	32768	17352	14758	13084	15006
30	4096	1482	1230	1104	1050

Table 7: Tightness over  $\mathbb{F}_7$ ,  $12 \leq n \leq 30$

$n$	$N_{\text{codes}}$	A > B	A > H	H > A	A > R	R > A
10	1024	40	40	30	40	90
15	1024	30	30	70	0	170
16	128	0	0	6	0	16
20	32768	1750	1120	1490	820	7010
24	8192	1074	888	528	304	2110
28	512	52	50	14	20	86

Table 10: Comparison over  $\mathbb{F}_{11}$ ,  $10 \leq n \leq 28$

$n$	$N_{\text{codes}}$	A > B	A > H	H > A	A > R	R > A
31	128	10	8	42	4	50
33	32	2	0	8	0	8
35	64	0	0	2	0	16
45	256	2	2	40	2	47
51	256	22	11	70	9	100
63	8192	652	286	2586	144	4322

Table 2: Comparison over  $\mathbb{F}_2$ ,  $31 \leq n \leq 63$

$n$	$N_{\text{codes}}$	B	H	R	A
22	64	40	40	40	32
24	16384	9120	8132	6792	8108
31	2048	1979	1969	1938	1975
36	4096	1788	1160	712	1012
39	2048	1804	1779	1741	1788
44	4096	2612	2532	2512	2508

Table 5: Tightness over  $\mathbb{F}_5$ ,  $22 \leq n \leq 44$

$n$	$N_{\text{codes}}$	A > B	A > H	H > A	A > R	R > A
12	512	24	12	12	12	30
16	512	72	46	42	28	148
18	1024	36	24	24	12	24
20	128	14	12	12	12	20
24	32768	3944	2604	3878	1872	8090
30	4096	480	432	420	372	582

Table 8: Comparison over  $\mathbb{F}_7$ ,  $12 \leq n \leq 30$

$n$	$N_{\text{codes}}$	B	H	R	A
15	512	132	114	72	102
21	512	156	150	114	132
33	512	244	238	238	244
35	512	278	264	232	278
39	512	308	290	276	248
43	128	118	118	115	118

Table 11: Tightness over  $\mathbb{F}_4$ ,  $15 \leq n \leq 43$

$n$	$N_{\text{codes}}$	B	H	R	A
22	64	40	40	40	32
26	1024	703	703	624	647
32	512	102	48	42	98
40	8192	5022	4556	4182	4622
41	64	55	55	53	55
44	512	304	296	294	276

Table 3: Tightness over  $\mathbb{F}_3$ ,  $22 \leq n \leq 44$

$n$	$N_{\text{codes}}$	A > B	A > H	H > A	A > R	R > A
22	64	28	26	0	20	8
24	16384	2004	1396	1684	856	4204
31	2048	256	99	649	26	1122
36	4096	776	344	256	328	700
39	2048	162	66	639	34	1031
44	4096	342	292	396	158	1212

Table 6: Comparison over  $\mathbb{F}_5$ ,  $22 \leq n \leq 44$

$n$	$N_{\text{codes}}$	B	H	R	A
10	1024	130	100	20	100
15	1024	320	250	140	290
16	128	52	46	42	52
20	32768	10440	8710	4500	9010
24	8192	4546	4120	3232	4046
28	512	316	302	302	316

Table 9: Tightness over  $\mathbb{F}_{11}$ ,  $10 \leq n \leq 28$

$n$	$N_{\text{codes}}$	A > B	A > H	H > A	A > R	R > A
15	512	30	30	18	24	66
21	512	48	30	6	24	48
33	512	18	12	42	12	74
35	512	24	8	18	0	196
39	512	72	72	84	72	170
43	128	6	6	12	6	18

Table 12: Comparison over  $\mathbb{F}_4$ ,  $15 \leq n \leq 43$

Let  $\mathcal{T}^R(\mathbb{F}_q)$  and  $\mathcal{T}^A(\mathbb{F}_q)$  be the total number of codes for which the Roos bound performs better than our bound, and vice versa, respectively, for  $q = 2, 3, 5, 7, 11$  and 4 and for the code lengths considered in the tables. Then:

$$\frac{\mathcal{T}^R(\mathbb{F}_2)}{\mathcal{T}^A(\mathbb{F}_2)} = \frac{4595}{159} \approx 28.9, \quad \frac{\mathcal{T}^R(\mathbb{F}_3)}{\mathcal{T}^A(\mathbb{F}_3)} = \frac{2971}{523} \approx 5.68, \quad \frac{\mathcal{T}^R(\mathbb{F}_5)}{\mathcal{T}^A(\mathbb{F}_5)} = \frac{8920}{1464} \approx 6.09, \quad \frac{\mathcal{T}^R(\mathbb{F}_7)}{\mathcal{T}^A(\mathbb{F}_7)} = \frac{9016}{2319} \approx 3.89, \quad \frac{\mathcal{T}^R(\mathbb{F}_{11})}{\mathcal{T}^A(\mathbb{F}_{11})} = \frac{9512}{1204} \approx 7.9, \quad \frac{\mathcal{T}^R(\mathbb{F}_4)}{\mathcal{T}^A(\mathbb{F}_4)} = \frac{630}{138} \approx 4.56.$$

It is clear from the previous values that our bound performs experimentally better with bigger fields. If the entries numbered  $m\ell + 1, m\ell + l + 1, \dots, 2m\ell + 1$  in  $R(n, S_C)$  are nonzeros, then other bounds do not perform as good as in the cases in which all or most of the entries are zeros. As the field size increases, the sizes of the cyclotomic sets tend to decrease leading to patterns with shorter sequences of consecutive zeros in  $S_C$ . Our bound, compared to other bounds, is likely to yield better results when applied to such patterns.

## References

- [1] E. Betti and M. Sala, "A new bound for the distance of a cyclic code from its defining set", *IEEE Trans. on Inf. Th.*, Accepted for publication.
- [2] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Inform. Control*, vol. 3, pp. 68-79, 1960.
- [3] C. R. P. Hartmann and K. K. Tzeng, "Generalization of the BCH bound," *Inform. Control*, vol. 20, no. 5, pp. 489-498, Jun. 1972.
- [4] C. Roos, "A new lower bound for the minimum distance of a cyclic code," *IEEE Trans. on Inf. Th.*, vol. 29, no. 3, p. 330-332, May 1983.