

A theory for the distance of cyclic codes

Massimiliano Sala (msala@bcric.ucc.ie)

Boole Centre for Research in Informatics, UCC Cork, Ireland

(Part of this work is jointly with E. Betti and F. Ponchio)

Workshop D1: Gröbner Bases in Cryptography, Coding Theory,
and Algebraic Combinatorics, RICAM/RISC, Linz, Austria, 2006

1/V/2006

BCRI/CGC

<http://www.bcri.ucc.ie>

We provide a unified approach to the study of lower bounds on the distance of cyclic codes.

We show that all known bounds fall within two classes and that many of them fall within a specific subclass.

We also provide new bounds, relations between bounds and counterexamples to claimed bounds.

Keywords: Cyclic codes, DFT, Hamming distance.

\mathcal{C} : class of cyclic codes (s.t. $(n, q) = 1$),

$\mathcal{C}_{q,n}$: the class of cyclic codes of length n over \mathbb{F}_q ,

so that $\mathcal{C} = \cup_{(n,q)=1} \mathcal{C}_{q,n}$.

We have seen in previous talks the bijective correspondence:

$$\mathcal{C}_{q,n} \longleftrightarrow \{g \in \mathbb{F}_q[z] \mid g \mid (z^n - 1)\}.$$

It is very important to be able to give bounds on the distance of cyclic codes, especially lower bounds.

An obvious way of computing the distance is to check the weight of any codeword, whose computation time is **exponential** in n .

In mathematics we are used to definitions and proofs given in a well-specified setting, however in this type of literature you can find ambiguous statements, where the exact setting is not clear. In the first ten slides we will play around this ambiguity.

Would you be surprised if an *exponential-time* bound performs better than a *polynomial-time* bound?

Would you be surprised if a bound using *more* information than another obtains better results?

Can the *same* bound perform differently on the *same* codes?

Definition 1. A map $\delta : \mathcal{C} \rightarrow \mathbb{N} \cup \{\infty\}$ is called a **(lower) bound** on \mathcal{C} , if

$$\delta(C) \leq d(C), \quad \forall C \in \mathcal{C}.$$

Let C be a code in \mathcal{C} and $\mathcal{F} \subset \mathcal{C}$. Let δ be a bound on \mathcal{C} . We say that:

- δ is **tight** on C , if $\delta(C) = d(C)$,
- δ is **tight** on \mathcal{F} , if $\delta(C) = d(C)$, $\forall C \in \mathcal{F}$.

An established standard way of measuring the performance of a bound is to compute

$$\mathbf{N}_\delta = |\{C \mid C \in \cup_{n \leq 61} \mathcal{C}_{2,n}, \delta(C) < d(C)\}|$$

that is, to count on how many codes (in a benchmark set) the bound is not tight.

We have analyzed all bounds known in literature (up to our knowledge), but we will mention in this talk only the following:

- the BCH bound (Bose, Ray-Chaudhuri, and Hocquenghem),
- the HT bound (Hartmann and Tzeng),
- the Roos bound,
- the Schaub bound,
- the VW bound (Van-Lint and Wilson, *shifting bound*),
- the Boston bounds,
- the A bound (Betti and Sala),
- the SP singleton-procedure bound (Sala).

We will use a [CL] to mark classical results or definitions and an [N] for our contribution.

On a paper you can find the following values for the tightness of a few bounds:

$$N_{BCH} = 433, N_{HT} = 373, N_{Roos} = 333.$$

However, on another paper you can find this value:

$$N_{BCH} = 147.$$

In another paper it is claimed

$$N_{VW} = 2,$$

but someone else says

$$N_{VW} = 18.$$

Confused? I was!

In the introduction of [vLW86] (where the VW bound is presented) we read:

In many cases the results are considerably stronger than previously known lower bounds.

This claim is true for the time and the paper is one of the most valuable contributions to this research area.

However the authors forgot to mention that the VW bounds is **exponential-time**, while the others compared in that paper are **polynomial-time**.

Moreover, the VW bound uses **more** information on the code than the one used by the others.

We can find a similar situation in [ALdV96], where the authors compare the Schaub bound and other bounds. They refer to the values given by the Schaub bound as to “numerical results”. We read:

*The numerical results are **surprisingly** higher than all previous known lower bounds.*

As in the VW case, here the “better” bound is exponential-time (rather than polynomial-time) and uses more information on the code. Would you be **surprised** as well?

“Serious” matters we are going to do:

- review defining sets and sub-codes,
- review the relation between the DFT and the distance,
- introduce a family of bounds called **root bounds**,
- list which bounds fall in this class,
- present a theorem on the **optimal** root bound,
- provide counterexamples to two bounds claimed in the literature,
- introduce the sub-class of **strong root bounds**,
- list which bounds fall in this class,
- introduce the class of **border bounds**,
- list which bounds fall in this class,
- present an **equivalence theorem**.

We denote by $S_{C,\alpha}$ the complete defining set of C with respect to α , i.e.:

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

Any linear subcode C' of C that is cyclic will be called a *cyclic subcode*, and in this case we will write $C' < C$ if C' is not null. The cyclic subcodes of C are generated by $\{\langle g \rangle \mid g_C \mid g, g \mid z^n - 1\}$ and there are

$$\sum_{i=1}^{r-s} \binom{r-s}{i} = 2^{r-s} - 1$$

non-null cyclic subcodes (including C itself), where r is the number of irreducible factors of $z^n - 1$ and s the number of those of g . They are

$$\sim 2^n$$

in the worst-case

Definition 2 (N). *Let $\mathcal{S} \subset \mathbb{N} \times \mathbb{N}$ be s.t.*

$$(q, n) \in \mathcal{S} \iff q = p^m, p \text{ is a prime, } m \geq 1, n \geq 1, (n, p) = 1.$$

We denote by \mathcal{Z} the class of all functions

$$\zeta : \mathcal{S} \mapsto \bigcup_{p \text{ prime}} \overline{\mathbb{F}_p}$$

s.t. $\zeta(q, n)$ is a primitive n -th root of unity over \mathbb{F}_p .

Note that primitive roots depend only on the characteristic p .

In other words, fixing $\zeta \in \mathcal{Z}$ we choose a “canonical” n -th root of unity for each q .

Definition 3 (CL). *Let $C_1, C_2 \in \mathcal{C}_{q,n}$. We say that C_1 and C_2 are naturally equivalent if there are two primitive n -th roots of unity over \mathbb{F}_q , α and β , s.t.*

$$S_{C_1, \alpha} = S_{C_2, \beta}.$$

A classical result on cyclic codes can be given in our context as follows.

Theorem 4 (CL). *Let C_1 and C_2 be naturally equivalent cyclic codes. Then*

$$d(C_1) = d(C_2).$$

Furthermore, let C_1 be in $\mathcal{C}_{q,n}$. Let α and β be primitive n -th roots of unity. Then there is a unique cyclic code C_2 in $\mathcal{C}_{q,n}$ s.t.

$$S_{C_1, \alpha} = S_{C_2, \beta}.$$

From the defining set one finds the defining sets of naturally equivalent codes, in a manner independent of the field size, but dependent only on n . Let $l \geq 1$, $(l, n) = 1$,

$$S = \{i_1, \dots, i_r\} \mapsto S' = \{j_1, \dots, j_r\}$$

where $j_h \equiv i_h l \pmod{n}$ and $0 \leq j_h \leq n - 1$.

The same operation will send subcodes in naturally equivalent subcodes.

Definition 5. Let $\bar{a} = (a_0, \dots, a_{n-1})$ be a vector over a field \mathbb{K} . We denote by $\mathbf{M}(\bar{a})$ the circulant matrix:

$$M(\bar{a}) = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-2} & a_{n-1} \\ a_1 & a_2 & \dots & a_{n-1} & a_0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n-1} & a_0 & \dots & a_{n-3} & a_{n-2} \end{pmatrix}.$$

Let $\bar{a} = (a_0, \dots, a_{n-1}) \in \mathbb{K}^n$. The **Discrete Fourier Transform** (or **DFT** for short) of \bar{a} is the vector:

$$\text{DFT}(\bar{a}) = (A_0, \dots, A_{n-1}), \quad A_i = \sum_{j=0}^{n-1} a_j \alpha^{ij}.$$

If we represent a word $c \in C$ as a polynomial in $\mathbb{F}_q[z]$, then the zero components of its DFT **correspond** to the zeros of c , since $A_i = c(\alpha^i)$ for any i .

We collect in one statement some known results.

Theorem 6 (CL). *Let $C \in \mathcal{C}$ and let $\text{DFT}(C)$ be the code formed by the DFT of the words of C . Then*

$$d = \min\{\text{rk}(M(\text{DFT}(c))) \mid c \in C, c \neq 0\}.$$

Thus, the problem of finding the distance of a code is equivalent to finding the minimum rank of the corresponding set of matrices. In particular any bound for one is also a bound for the other one.

This result does not look **impressive**, since computing the rank of $M(\text{DFT}(c))$ is much more expensive than computing the weight of c . Yet, it is the starting point of our theory.

Definition 7 (\mathbb{N}).

We denote by \mathcal{D} the following subset of $\mathbb{N} \times 2^{\mathbb{N}}$:

$$(n, S) \in \mathcal{D} \quad \Leftrightarrow \quad n \geq 1, S \subset \{0, \dots, n-1\}.$$

Let $(n, S) \in \mathcal{D}$. Let $S = \{i_1, \dots, i_m\}$. We denote by $(n, S)^{\#}$ the following set of subsets of $\{0, \dots, n-1\}$

$$(n, S)^{\#} = \{S_1, \dots, S_r\},$$

where $r = |\mathbb{Z}_n^*|$ and for any $l \in \mathbb{Z}_n^*$ there is an i such that $S_i = \{li_h \mid 1 \leq h \leq m\}$.

For any function $\zeta \in \mathcal{Z}$ we define a map from \mathcal{C} to \mathcal{D} :

$$\phi_{\zeta} : \mathcal{C} \rightarrow \mathcal{D}, \quad \phi_{\zeta}(C) = (n, S_{C, \alpha}),$$

where $\alpha = \zeta(p, n)$. We can prove that it is surjective.

Definition 8 (\mathbb{N}).

A **root function** is a map $f : \mathcal{D} \rightarrow \mathbb{N} \cup \{\infty\}$ such that:

$$\forall \zeta \in \mathcal{Z}, \forall C \in \mathcal{C}, \quad f \circ \phi_\zeta(C) \leq d(C).$$

We denote by \mathcal{R} the class of all root functions.

Given $f \in \mathcal{R}$, we say that f is **invariant** if $f(n, S) = f(n, T)$, for any $T \in (n, S)^\#$. We say that f is **monotone** if for any (n, S) and (n', S') in \mathcal{D} we have

$$n = n', S \subset S' \quad \Rightarrow \quad f(n, S) \leq f(n, S').$$

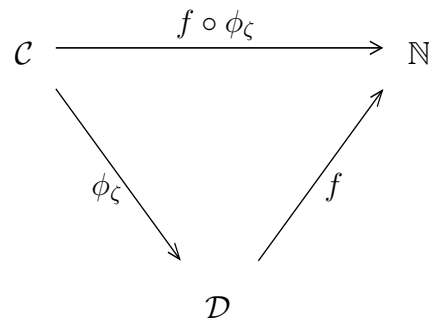
For any $\zeta \in \mathcal{Z}$ and any $f \in \mathcal{R}$, composite map

$$f_{\mathcal{D}, \zeta} = f \circ \phi_\zeta : \mathcal{C} \mapsto \mathbb{N} \cup \{\infty\}$$

is called the **root bound** associated to f and ζ . We denote by \mathcal{R}_D the class of all root bounds.

A lower bound is a map that gives an estimate on the distance of a cyclic code.

With a root bound this estimate is given while **ignoring all information about the code** except for the length and its defining sets. In particular, no information on the underlying field is used.



We define a map \mathbf{f} from \mathcal{D} to $\mathbb{N} \cup \{\infty\}$, as follows

$$\mathbf{f}(n, S) = \max\{f(n, S) \mid f \in \mathcal{R}\}.$$

Theorem 9 (N). *Map \mathbf{f} is a root function, which is **maximal** in \mathcal{R} , monotone and invariant.*

Its associated root bound $\mathbf{f}_{\mathcal{D}}$ is obviously the optimal root bound, i.e. the **best** you can do to lower bound the distance if you only use defining sets.

Definition 10 (N).

For any $\zeta \in \mathcal{Z}$ and any $(n, S) \in \mathcal{D}$, we define two sets, $V_{(n,S)}^\zeta \subset \mathcal{C}$ and $T_{(n,S)}^\zeta \subset \mathbb{N}$, as follows

$$V_{(n,S)}^\zeta = \{C \mid C \in \mathcal{C}, \phi_\zeta(C) = (n, S)\}$$

$$T_{(n,S)}^\zeta = \{d(C) \mid C \in \mathcal{C}, \phi_\zeta(C) = (n, S)\} = \{d(C)\}_{C \in V_{(n,S)}^\zeta}$$

Definition 11 (N).

We define $\mathbf{g} : \mathcal{D} \mapsto \mathbb{N} \cup \{\infty\}$, by choosing an arbitrary $\zeta \in \mathcal{Z}$ and setting

$$\mathbf{g}(n, S) = \min T_{(n,S)}^\zeta, \quad \text{for any } (n, S) \in \mathcal{D}.$$

Our main theorems on root bounds are the following

Theorem 12 (N). *Map g is a well-defined root function. Moreover*

$$\boxed{g = f}$$

Theorem 13 (N).

$$\boxed{f_{\mathcal{D}} \neq d}$$

What we call root bounds are sometimes called “BCH-like” bounds, since they include the BCH bound and its generalizations (HT bound, Roos bound, etc.).

Theorem 13 can be rephrased:

If you get a bound which depends only on the information given by the defining sets, it does not matter how smart you are and how much computation power you have, your bound cannot be tight on all cyclic codes.

Let \mathcal{U} be a set formed by three elements, which we call $\{\Delta, \Delta^+, 0\}$. We endow \mathcal{U} with two operations, sum and product, according to the following logical tables:

\cdot	Δ	Δ^+	0
Δ	Δ	Δ	0
Δ^+	Δ	Δ^+	0
0	0	0	0

$+$	Δ	Δ^+	0
Δ	Δ	Δ	Δ
Δ^+	Δ	Δ	Δ^+
0	Δ	Δ^+	0

The set \mathcal{U} plays the role of a field where we have partial information on the element values. More precisely, let \mathbb{K} be a field and $k \in \mathbb{K}$, we say that:

- k is Δ^+ , if we know for sure that k is different from 0 ,
- k is 0 , if we know for sure that k is 0 ,
- k is Δ , otherwise.

One should regard an element of \mathcal{U} as *the information we have* on a field element, rather than a way to indicate its value. For example the sum rule $\Delta^+ + \Delta^+ = \Delta$ is equivalent to the sentence “if we sum two nonzero values, we will have no information on the outcome”.

It is possible to introduce in \mathcal{U} some notions of linear algebra, but the definitions are cumbersome, because \mathcal{U} is not a field and \mathcal{U} cannot be endowed with the structure of vector space. From now on, I assume that you have an intuitive idea of vectors, linear dependence/independence, rank for a matrix, etc.

Definition 14 (N). *Let $n \geq 1$ and $S \subset \{0, \dots, n-1\}$. We denote by $R(n, S)$ the vector (u_0, \dots, u_{n-1}) in \mathcal{U}^n such that $u_i = 0$, if $i \in S$, $u_i = \Delta$ otherwise.*

Example 15. *Let $n = 4$, $S = \{1, 2\}$. Then we have*

$$R(n, S) = R(4, \{1, 2\}) = (\Delta, 0, 0, \Delta).$$

Example 16. *Let $n = 6$, $S = \{0, 2, 5\}$. Then we have*

$$R(n, S) = R(6, \{0, 2, 5\}) = (0, \Delta, 0, \Delta, \Delta, 0).$$

Definition 17 (N). *Given a vector $\mathbf{v} \in \mathcal{U}^n$ we denote by $\mathcal{A}(\mathbf{v})$ the set of vectors $\mathbf{u} \in \mathcal{U}^n \setminus \mathbf{0}$ s.t.*

- $\mathbf{u}[i] = 0$, if $\mathbf{v}[i] = 0$,
- $\mathbf{u}[i] = \Delta^+$, if $\mathbf{v}[i] = \Delta^+$,
- $\mathbf{u}[i] = \Delta^+$ or $\mathbf{u}[i] = 0$, if $\mathbf{v}[i] = \Delta$.

Theorem 18 (CL). *Let C be a cyclic code of length n , defining set $S_{C,\alpha}$ and distance d . Then:*

$$\min\{\text{rk}(M(\mathbf{u})) \mid \mathbf{u} \in \mathcal{A}(R(n, S_{C,\alpha}))\} \leq d$$

Definition 19 (N).

Let A be a matrix over \mathcal{U} . We denote the j -th column of A by $A[j]$ and the (i, j) -th entry of A by $A[i, j]$. We say that $A[j]$ is a **singleton** if it has only one non-zero component $A[i, j]$, i.e. $A[i, j] = \Delta^+$ and $A[l, j] = 0$ for $l \neq i$. When this happens, we say that the i -th row is the row **corresponding** to the singleton.

Singleton-procedure.

$$A_3 = \begin{pmatrix} 0 & \Delta^+ & \Delta & 0 \\ 0 & 0 & \Delta^+ & \Delta^+ \\ \Delta^+ & 0 & 0 & \Delta \end{pmatrix} \rightarrow A_2 = \begin{pmatrix} 0 & \Delta^+ & \Delta^+ \\ \Delta^+ & 0 & \Delta \end{pmatrix}, \begin{matrix} j = 2 \\ i = 1 \end{matrix} \rightarrow A_1 = (\Delta^+, \Delta^+), \begin{matrix} j = 1 \\ i = 2 \end{matrix}.$$

Theorem 20 (N). *If the singleton procedure is successful for a set of rows, then they are linearly independent over \mathcal{U} .*

Proposition 21. *Let $A = M(\mathbf{v})$, $\mathbf{v} \in \mathcal{U}^n$. Let $r \geq 0$. If \mathbf{v} has the form*

$$\mathbf{v} = (\overbrace{0, \dots, 0}^r, \Delta^+, *, \dots, *),$$

where $*$ denotes any element. Then $\text{rk}(A) \geq r + 1$.

Proof. Let $A_{r+1} \in \mathcal{U}^{(r+1) \times n}$ be the matrix obtained by the first $r + 1$ rows of $M(\mathbf{v})$. By induction on r we show that the singleton procedure is successful for A_{r+1} .

If $r = 0$, it is clear since Δ^+ is in \mathbf{v} .

$$A_{r+1} = \begin{pmatrix} 0 & \dots & 0 & 0 & \Delta^+ & * & \dots & \dots & \dots & \dots \\ * & 0 & \dots & 0 & 0 & \Delta^+ & * & \dots & \dots & \dots \\ \vdots & \ddots & \ddots & & \vdots & & \ddots & & & \\ * & \dots & & * & 0 & 0 & & \Delta^+ & * & \dots \end{pmatrix}$$

$A_{r+1}[r+1]$ is clearly a singleton and we erase the first row and the $(r+1)$ -th column, obtaining a matrix A_r , which corresponds to the first r rows of $M(\mathbf{v}')$

$$\mathbf{v}' = (\overbrace{0, \dots, 0}^{r-1}, \Delta^+, *, \dots, *).$$

□

Definition 22 (\mathbb{N}).

A **strong root function** is a map $f : \mathcal{D} \rightarrow \mathbb{N}$ such that:

$$\forall (n, S) \in \mathcal{D}, \quad f(n, S) \leq \min\{\text{rk}(M(\mathbf{u})) \mid \mathbf{u} \in \mathcal{A}(R(n, S))\}$$

We denote by \mathcal{R}^S the class of all strong root functions.

It is easy to see that a strong root function is actually a root function and so we can talk about **strong root bounds** as well.

What is important about strong root bounds is that:

- many known lower bounds are actually strong root bounds,
- all known strong root bounds are easy to reprove (and even sometimes to generalize) using a proof similar to that of Proposition 21.

Let $\mathbf{v} \in \mathcal{U}^n$. For us $(*)^i \subset \mathbf{v}$ means that \mathbf{v} “contains with overlapping” block $(*)^i$, where $*$ is any element of \mathcal{U} , that is,

$$\mathbf{v} = (v[0], \dots, v[j], \overbrace{*, \dots, *}^i, v[j+i+1], \dots, v[n-1]),$$

for some $0 \leq j \leq n-i-1$, or that

$$\mathbf{v} = (\overbrace{*, \dots, *}^{i_1}, v[i_1+1], \dots, v[n-i_2-1], \overbrace{*, \dots, *}^{i_2}),$$

where $1 \leq i_1, i_2$ and $i_1 + i_2 = i$.

For example, we have both $(0)^2, (\Delta^+)^2 \subset (\Delta^+, 0, 0, \Delta, \Delta^+)$. However, it is not true that $(\Delta^+)^4 \subset (\Delta^+, 0, \Delta^+, \Delta^+, \Delta, \Delta^+)$.

We extend our notation to multiple blocks, in an obvious way. For example, $(0)^2(\Delta^+)^3 \subset (\Delta, 0, 0, \Delta^+, \Delta^+, \Delta^+, 0, \Delta)$.

We need even blocks of blocks, with the obvious meaning, as for example

$$((0)^2(\Delta^+)^3)^2(\Delta)^3 \subset (\Delta, 0, 0, \Delta^+, \Delta^+, \Delta^+, 0, 0, \Delta^+, \Delta^+, \Delta^+, \Delta, \Delta, \Delta, 0).$$

Some strong root bounds:

- the BCH bound,
- the Hartmann-Tzeng bound,
- Boston's bound I,
- Boston's bound II,
- Boston's bound III,
- Boston's bound IV,
- bound A .

Any of them searches for some block structure contained in $R(n, S_{C,\alpha})$.

$$C \mapsto S_{C,\alpha} \mapsto R(n, S_{C,\alpha})$$

$$\text{BCH}(q = 2, \delta = 3, n = 7) \mapsto \{1, 2, 4\} \mapsto \{\Delta, 0, 0, \Delta, 0, \Delta, \Delta\}.$$

The following theorem was first presented in [BRC60] (the BCH bound).

Theorem 23 (CL). *Let $C \in \mathcal{C}_{q,n}$ with generator polynomial g . Suppose that there exist $i, \ell \in \{0, \dots, n-1\}$ such that:*

$$g(\alpha^{i+j}) = 0, \quad 0 \leq j \leq \ell - 1.$$

Then:

$$d \geq \ell + 1.$$

Definition 24 (N).

Let f_{BCH} be the following map $f_{\text{BCH}} : \mathcal{D} \rightarrow \mathbb{N}$,

$$f_{\text{BCH}}(n, S) = \max\{\ell \in \mathbb{N} \mid (0)^\ell \subset R(n, S)\} + 1.$$

Theorem 25 (N).

Map f_{BCH} is a strong root function and the BCH bound is the associated bound.

The following theorem was first presented in [HT72] (the HT bound).

Theorem 26 (CL). *Let $C \in \mathcal{C}_{q,n}$ with generator polynomial g . Suppose that there exist $i_0, \ell, s, r \in \mathbb{N}$ s.t. $(r, n) < \ell$ and*

$$g(\alpha^{i_0+i+jr}) = 0, \quad 0 \leq i \leq \ell - 1, \quad 0 \leq j \leq s - 1.$$

Then

$$d \geq \ell + s.$$

Definition 27 (N). *For any r, s, n we denote by $\rho = \rho(r, s, n)$ the quotient of rs divided by n .*

Let f_{HT} be the following map $f_{\text{HT}} : \mathcal{D} \rightarrow \mathbb{N}$,

$$f_{\text{HT}}(n, S) = \max\{i \in \mathbb{N} \mid i = \ell + s\},$$

where ℓ, s are such that there exist $r \in \mathbb{N}$, $(r, n) < \ell$, for which

$$((0^\ell)(\Delta^{r-\ell}))^s \subset R(n, S)^\rho.$$

Theorem 28 (N). *Map f_{HT} is a strong root function.*

The following four theorems were first presented in [Bos01].

Theorem 29 (CL). *Let $C \in \mathcal{C}_{q,n}$. If $3 \nmid n$ and $\{0, 1, 3, 4\} \subset S_{C,\alpha}$, then*

$$d \geq 4.$$

Theorem 30 (CL). *Let $C \in \mathcal{C}_{q,n}$. If $\{0, 1, 3, 5\} \subset S_{C,\alpha}$, then*

$$d \geq 4.$$

Theorem 31 (CL). *Let $C \in \mathcal{C}_{q,n}$. If $3 \nmid n$ and $\{0, 1, 3, 4, 6\} \subset S_{C,\alpha}$, then*

$$d \geq 5.$$

Theorem 32 (CL). *Let $C \in \mathcal{C}_{q,n}$. If $4 \nmid n$ and $\{0, 1, 2, 4, 5, 6, 8\} \subset S_{C,\alpha}$, then*

$$d \geq 6.$$

Definition 33 (N). *Let f_{B1} , f_{B2} , f_{B3} and f_{B4} be the following maps from \mathcal{D} to \mathbb{N} ,*

$$f_{B1}(n, S) = \begin{cases} 4, & \text{if } (0, 0, \Delta, 0, 0) \subset R(n, S) \text{ and } 3 \nmid n, \\ 1, & \text{otherwise.} \end{cases}$$

$$f_{B2}(n, S) = \begin{cases} 4, & \text{if } (0, 0, \Delta, 0, \Delta, 0) \subset R(n, S), \\ 1, & \text{otherwise.} \end{cases}$$

$$f_{B3}(n, S) = \begin{cases} 5, & \text{if } (0, 0, \Delta, 0, 0, \Delta, 0) \subset R(n, S) \text{ and } 3 \nmid n, \\ 1, & \text{otherwise.} \end{cases}$$

$$f_{B4}(n, S) = \begin{cases} 6, & \text{if } (0, 0, 0, \Delta, 0, 0, 0, \Delta, 0) \subset R(n, S) \text{ and } 4 \nmid n, \\ 1, & \text{otherwise.} \end{cases}$$

Theorem 34 (N). *Maps f_{B1} , f_{B2} , f_{B3} and f_{B4} are strong root functions and their associated bounds are generalizations of the Boston bounds I, II, III and IV.*

Bound A.

Definition 35 (N). *Let f_A be the following map $f_A : \mathcal{D} \rightarrow \mathbb{N}$,*

$$f_A(n, S) = \max\{i \in \mathbb{N} \mid i = m\ell + \ell\},$$

where m and ℓ are s.t. either

$$((0)^\ell)^m ((\Delta)^1 (0)^{\ell-1})^{m+1} \subset R(n, S),$$

or

$$((0)^{\ell-1} (\Delta)^1)^{m+1} ((0)^\ell)^m \subset R(n, S).$$

Theorem 36 (N). *Map f_A is a strong root function.*

The following two theorems were first presented in [Bos01] (Boston bound A and B).

Theorem 37 (CL). *Let $C \in \mathcal{C}_{q,n}$. If $4 \nmid n$ and $\{0, 1, 4, 5, 8\} \subset S_{C,\alpha}$, then*

$$d \geq 5.$$

Theorem 38 (CL). *Let $C \in \mathcal{C}_{q,n}$. If $3 \nmid n$ and $\{0, 1, 3, 4, 6, 7, 9\} \subset S_{C,\alpha}$, then*

$$d \geq 7.$$

Theorem 39 (N).

Boston bound A and B are false.

Proof. Let $C \in \mathcal{C}_{2,15}$ be s.t.

$$S_{C,\alpha} = \{0, 1, 2, 4, 5, 8, 10\}.$$

According to Boston bound A, $d \geq 5$. However, $d = 4$.

Let $C \in \mathcal{C}_{11,20}$ be s.t.

$$S_{C,\alpha} = \{0, 1, 3, 4, 5, 6, 7, 9, 11, 13, 15, 17, 19\}.$$

According to Boston bound B, $d \geq 7$. However, $d = 6$. □

There are two other bounds, the Roos bound and Boston bound V, which are root bounds but probably not strong root bounds. Their root functions are as follows:

Roos bound

$$f_{\text{Roos}}(n, S) = \max\{i \in \mathbb{N} \mid i = \ell + s\},$$

where ℓ, s are s. t. there exists $r \in \mathbb{N}$, $(r, n) < \ell$, and there exists s integers $0 \leq k_1 < k_2 < \dots < k_s < \ell + s$, so that:

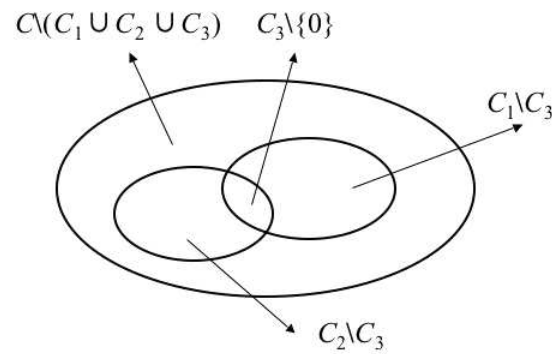
$$((\Delta)^l)^{k_1-1}(0)^l((\Delta)^l)^{k_2-k_1}(0)^l \dots ((\Delta)^l)^{k_s-k_{s-1}}(0)^l \subset R(n, S)^\rho.$$

Boston bound V

$$f_{\text{B5}}(n, S) = \begin{cases} 6, & \text{if } R(n, s) = (0, 0, \Delta, 0, 0, \Delta, 0, 0, \Delta, \dots) \text{ and } 3 \nmid n, \\ 1, & \text{otherwise.} \end{cases}$$

Border bounds

Since even the optimal root bound cannot be tight on \mathcal{C} , we need to consider bounds that use more information on a code. In literature we find at least three such bounds and all of them use the same kind of extra information: they need to know the cyclic subcodes of \mathcal{C} .



The key is the following rewriting

Proposition 40 (CL).

$$d(C) = \min_{D < C} \{ \min_{c \in \hat{D}} \text{rk}(M(\text{DFT}(c))) \} ,$$

where \hat{D} is the set of all words (**border words**) of D which are not contained in any of its cyclic subcodes.

Since my time is nearly finished, I will not give formal definitions for these bounds. The idea is to compute a sort of $M(R'(S_{D,\alpha}))$ for any D cyclic subcode of C and then take the minimum.

The advantage of this approach is that now R' contains only 0 and Δ^\dagger and so computations are more precise, the disadvantage is that we have to consider all cyclic subcodes, which are $\sim 2^n$ in the worst case, and hence **all** border bounds are exponential-time.

What differentiates one border bound from another is the algorithm which is used to check linear independence in matrix over \mathcal{U} . We call such algorithms **independence-check procedures**.

If we consider the singleton procedure used in our previous proofs, then it identifies a (relatively) fast border bound. We call this bound the **singleton-procedure** bound, which first appeared in [Sal01].

In [Sch88] there is another independence-check procedure, which defines a bound which we call the **Schaub** bound. We do not detail it here, but it is much more time-consuming than the singleton-procedure.

The Schaub bound is believed to share with the VW bound the position of “best” bounds, since its performance are excellent compared with “classical” bounds (which are root bounds and polynomial-time), but it is exponential-time and uses more information, so I am not surprised at all.

Theorem 41 (N).

The Schaub bound and the singleton-procedure bound are equivalent,

i.e. on the same code they give the same value.

In [vLW86] the VW bound is presented. We do not have time to detail it, but it was noted that it outperforms all “classical” bounds and even the Schaub bound, since apparently

$$N_{\text{VW}} = 2 > N_{\text{Schaub}} = 18.$$

In [vLW86] there are other bounds but we do not treat them.

However, we are able to show the following.

Theorem 42 (N). *The VW bound is a **border bound**.
Moreover,*

The VW bound is equivalent to the Schaub bound

(and hence to the singleton-procedure bound).

Since it is exponential-time, we are not surprised by its excellent performance w.r.t. “classical” (polynomial-time) bounds. However, the difference in the value of N_δ (2 and 18) looks odd.

A careful examination of both papers, [vLW86] and [Sch88], shows that actually the authors are not happy with using their good bounds, but they strengthen their results using theorems specific to the underlying field. Since they use different “tricks”, their numerical results are slightly different. *However the advantage of using extra tricks is small and for longer lengths negligible.*

Final comments

The “best” known bounds are still the VW bound and the Schaub bound, and they can be computed relatively fast using the singleton-procedure, but their cost is exponential-time.

The best polynomial-time bound is still the Roos bound, even if a new bound (bound A) is not far from it with longer lengths.

We suggest that people should be extremely **careful** when comparing bounds.

([EB06], [Sal01], [FP03])

Remark. *We do not have time to give details in this talk, but **Gröbner bases** can be easily used to prove root bounds ([MS03])*

Open problems

Problem 1. *Find an effective algorithm for computing \mathbf{f} (or $\mathbf{f}_{\mathcal{D}}$).*

Problem 2. *Is there a finite field \mathbb{F}_q s.t. $\mathbf{f}_{\mathcal{D}}$ is tight on $\bigcup_{n \geq 1, (n,q)=1} \mathcal{C}_{q,n}$?*

Problem 3. *Show that Boston bound V is not a strong root bound.*

Problem 4. *Show that the Roos bound is not a strong root bound.*

Problem 5. *Find new strong root bounds by inspecting ranks with the singleton procedures.*

References

- [ALdV96] Daniel Augot and Françoise Levy-dit Vehel, *Bounds on the minimum distance of the duals of BCH codes*, IEEE Trans. Inform. Theory **42** (1996), no. 4, 1257–1260. MR MR1445645 (97m:94035)
- [Bos01] Nigel Boston, *Bounding minimum distances of cyclic codes using algebraic geometry*, International Workshop on Coding and Cryptography (Paris, 2001), Electron. Notes Discrete Math., vol. 6, Elsevier, Amsterdam, 2001, p. 10 pp. (electronic). MR MR1985260 (2004e:94039)
- [BRC60] R. C. Bose and D. K. Ray-Chaudhuri, *On a class of error correcting binary group codes*, Information and Control **3** (1960), 68–79. MR MR0112768 (22 #3619)
- [EB06] Massimiliano Sala Emanuele Betti, *A theory for distance bounding cyclic codes*, Work in progress, University College Cork, 2006.
- [FP03] Massimiliano Sala Federico Ponchio, *A lower bound on the distance of cyclic codes*, BCRI preprint, www.bcricucc.ie 7, University College Cork, Boole Centre BCRI, UCC Cork, Ireland, 2003.

- [HT72] C. R. P. Hartmann and K. K. Tzeng, *Generalizations of the BCH bound*, Information and Control **20** (1972), 489–498. MR MR0345706 (49 #10437)
- [MS03] Teo Mora and Massimiliano Sala, *On the Gröbner bases of some symmetric systems and their application to coding theory*, J. Symbolic Comput. **35** (2003), no. 2, 177–194. MR MR1958953 (2004c:94118)
- [Sal01] Massimiliano Sala, *On some algebraic methods for coding theory*, Ph.D. thesis, University of Milan, Milan, Italy, 2001.
- [Sch88] T. Schaub, *A linear complexity approach to cyclic codes*, Ph.D. thesis, Swiss Federal Inst. of Tech., Zurich, 1988.
- [vLW86] Jacobus H. van Lint and Richard M. Wilson, *On the minimum distance of cyclic codes*, IEEE Trans. on Inf. Th. **32** (1986), no. 1, 23–40. MR MR831557 (87j:94017)