A New Bound for Cyclic Codes Beating the Roos Bound

Matteo Piva and Massimiliano Sala

Department of Mathematics, University of Trento, Italy
piva@science.unitn.it, maxsalacodes@gmail.com

Abstract. We present a lower bound for the distance of a cyclic code, which is computed in polynomial time from the defining set of the code. Our bound beats other similar bounds, including the Roos bound, in the majority of computed cases.

Keywords: Cyclic code, BCH bound, Hartmann-Tzeng bound, Roos bound.

1 Introduction

Many lower bounds exist for the distance of a cyclic code, that elaborate in polynomial time some information from the defining set of the code, e. g. the BCH bound [1], the HT bound [2], the Roos bound [4] and BS bound [5]. We present a new bound which also has polynomial-time cost, beating all other similar bounds in the majority of computed cases. We call this bound " bound C "(Theorem 2). It comes from two preliminary results: bound A (Proposition 1) and bound B (Proposition 2).

2 Preliminaries

In this section we fix some notation and we recall the method we use to prove our result.
Let $(k)_n$ be the remainder of division k by n. Let $\mathbb{F}_q$ be a finite field with q elements, C indicates an arbitrary cyclic code $[n,k,d]$ over $\mathbb{F}_q$, and we denote with g the generator polynomial of C. From now on, we always assume that $\gcd(n,q)=1$. Let $\mathbb{F}$ be the splitting field of x^n-1 and let α be a primitive $n-$th root of unity in $\mathbb{F}$ then we indicate with S_C the defining set of C:

$$S_C = \left\{\, 1 \le i \le n-1 \mid g(\alpha^i) = 0 \,\right\}.$$

We collect together some definitions from [5] and [8]:

- Let $\mathcal{U}$ be a set of three symbols $\left\{\, 0, \Delta, \Delta^{+} \,\right\}$ then, with a little abuse of notation, $\mathcal{U} = (\mathcal{U}, +, \cdot)$ represents a field where we have partial information on the element value. More precisely: Δ^{+} represents an element for which we

T. Muntean, D. Poulakis, and R. Rolland (Eds.): CAI 2013, LNCS 8080, pp. 101–112, 2013.

are sure it is different from zero, 0 represents an element for which we are sure it is zero, $\varDelta$ represents an element for which we do not claim if it is zero or not. (The sum and the product on $\mathcal{U}$ are straightforward, but you can see [5], [8] or [6] for a complete description).

- $R(n, S_C)$ is the $n-$tuple $(u_0, \dots, u_{n-1}) \in \mathcal{U}^n$ such that

$$u_i = \begin{cases} 0, & \text{if } i \in S_C \\ \varDelta, & \text{otherwise.} \end{cases}$$

- $M(\mathbf{v}) \in \mathcal{U}^{n \times n}$ is the circulant matrix obtained from a $\mathbf{v} \in \mathcal{U}^n$.
- Given a $\mathbf{v} \in \mathcal{U}^n$ we denote by $\mathcal{A}(\mathbf{v})$ the set of all $\mathbf{u} \in \mathcal{U} \setminus \mathbf{0}$ s.t.

$$\begin{aligned} &\mathbf{u}[i] = 0, \text{ if } \mathbf{v}[i] = 0, \\ &\mathbf{u}[i] = \varDelta^{\!+}, \text{ if } \mathbf{v}[i] = \varDelta^{\!+}, \\ &\mathbf{u}[i] = \varDelta^{\!+} \text{ or } \mathbf{u}[i] = 0, \text{ if } \mathbf{v}[i] = \varDelta. \end{aligned}$$

We recall the singleton procedure (see [5], [8], [9]) to verify the linear independence of a set of rows on $\mathcal{U}$. For any matrix M, $M[i, j]$ is the (i, j) entry, $M[i]$ is the $i-$th row and $M(j)$ is the $j-$th column.

Definition 1. *Let M be a matrix over $\mathcal{U}$. We say that a column $M(j)$ is a* **singleton** *if it contains only one non-zero component $M[i, j]$, i.e. $M[i, j] = \varDelta^{\!+}$ and $M[t, j] = 0$ for $t \neq i$. When this happens we say that $M[i]$ is the row corresponding to the singleton.*

Any set of t rows of length n with $t \leq n$ forms a matrix $M_t \in \mathcal{U}^{t \times n}$. If a column $M(j)$ is a singleton, then the row corresponding to the singleton is clearly linear independent from the others. Then we delete the $j - th$ column and the corresponding row (we call this operation **s-deletion**), obtaining a new matrix, M_{t-1}, and we search for a new singleton in M_{t-1}. If this procedure can continue until we find a matrix M_1 with at least one $\varDelta^{\!+}$, we say that the singleton procedure is successful for the set of t rows considered.

Definition 2. *Let M be a matrix over $\mathcal{U}$, we denote by* $\mathrm{prk}(M)$ *the* pseudo rank *of M, i.e., the largest t such that there exists a set of t rows in M for which the singleton procedure is successful.*

Our interest for the rank of a matrix on $\mathcal{U}$ is due to the following result.

Theorem 1. *Let C be a cyclic code with defining set S_C and length n. If d is the distance of the code, then*

$$d \geq \min \{ \, \mathrm{prk}(M(\mathbf{u})) \mid \mathbf{u} \in \mathcal{A}(R(n, S_c)) \, \}$$

Proof. See [6] or [9].

3 Statement of Bound A and Bound B

Proposition 1 (bound A). *Let C be an $\mathbb{F}_q[n,k,d]$ cyclic code with defining set S_C and* $\gcd(q,n)=1$*. Suppose that there are $\ell,\ m,\ r,\ s \in \mathbb{N}$, $1 \le m \le \ell$ and $i_0 \in \{ 0,\dots,n-1 \}$ such that* $\gcd(n,m+r)<m$ *or* $\gcd(n,m+r)=1$*. If:*

a) $(i_0+j)_n \in S_C$, $\forall j = 0,\dots,\ell-1$,
b) $(i_0+j)_n \in S_C$,

$$\begin{aligned}&\forall j = i_0+\ell+r+h(m+r)+1,\dots,\ i_0+\ell+r+m+h(m+r)\\ &\forall 0 \le h \le s-1\end{aligned}$$

then

$$d \ge \ell+1+s-r\left\lfloor \frac{\ell}{m+r} \right\rfloor - \max\{ (\ell)_{m+r}-m, 0 \}. \tag{1}$$

In other words, the assumptions of Proposition 1 are equivalent to saying that $R(n,S_C)$ contains a block of the form $(0^\ell \Delta^r)(0^m \Delta^r)^s$, i.e. :

$$\underbrace{0\dots0}_{\ell}\underbrace{\Delta\dots\Delta}_{r}(\underbrace{0\dots0}_{m}\underbrace{\Delta\dots\Delta}_{r})^s \subset R(n,S_C).$$

Remark 1. We can see Proposition 1 as generalization of the HT bound. In fact with $\ell=m$ our statement becomes the same of the general Hartmann-Tzeng bound (see [8] and [3]).

We are able to prove another bound, similar to the previous:

Proposition 2 (bound B). *Let C be an $[n,k,d]$ cyclic code over $\mathbb{F}_q$ with defining set S_C. Suppose that there are $m,\ell,s \in \mathbb{N}$, $m,\ell \ge 1$, $s \ge m+1$,* $\gcd(n,\ell)<\ell-1$ *or* $\gcd(n,\ell)=1$*. If there is $i_0 \in \{0,\dots,n-1\}$ such that:*

a) $(i_0+j)_n \in S_C$, $j=0,\dots,m\ell-1$,
b) $(i_0+j)_n \in S_C$, $j=(m+h)\ell+1,\dots,(m+h)\ell+\ell-1$, $0 \le h \le s-1$,

Then:

$$d \ge m\ell+\ell+s-m-1.$$

In other words, the assumptions of Proposition 2 are equivalent to saying that $R(n,S_C)$ contains a block of the form $(0^{\ell m}\Delta)(0^{\ell-1}\Delta^r)^s$, i.e. :

$$\underbrace{0\dots0}_{\ell m}\Delta(\underbrace{0\dots0}_{\ell-1}\Delta)^s \subset R(n,S_C).$$

Remark 2. Proposition 2 is a generalization of the BS bound ([5]), except for the uncommon cases in which $\ell|n$, since $\gcd(n,\ell)\le\ell$ and $\gcd(n,\ell)=\ell \iff \ell|n$.

4 Proofs of Bound A and Bound B

In this section we provide the proof of Proposition 1, and we sketch the proof of Proposition 2.

Remark 3. The main tool we use to prove Proposition 1 and Proposition 2 is Theorem 1 which, in principle, allows us to work only with matrices that have as entries just 0 or Δ^+. Nevertheless during the proof we use matrices that have also Δ as entry. This fact must not worry the reader, since when a Δ appears we mean it can be indifferently 0 or Δ^+, and the correctness of the proof is not affected by such decision.

Proof (of Proposition 1). The general plan of the proof is as follow. Thanks to Theorem 1 we aim at proving that

$$\min\{\ \mathrm{prk}(M(\mathbf{v}))|\mathbf{v}\in\mathcal{A}(R(n,S_c))\ \}\geq\ell+1+s-r\left\lfloor\frac{\ell}{m+r}\right\rfloor-\max\{\ (\ell)_{m+r}-m,0\ \}.$$

In order to do that, for any $\mathbf{v}\in\mathcal{A}(n,S_C)$, we need to choose $\ell+s+1$ rows in $M(\mathbf{v})$ and we must prove that, discarding at most $r\left\lfloor\frac{\ell}{m+r}\right\rfloor+\max\{\ (\ell)_{m+r}-m,0\ \}$ rows, we actually obtain a set of rows for which the singleton procedure is successful.

We can suppose w.l.o.g. that $i_0=n-\ell$ (see Lemma 3.1 in [5]), so that:

$$\mathbf{v}=\underbrace{\Delta\ldots\Delta}_{r}(\underbrace{0\ldots0}_{m}\underbrace{\Delta\ldots\Delta}_{r})^s\ldots\underbrace{0\ldots0\ldots0}_{\ell}.$$

We introduce two notions releated to $\mathbf{v}$ (see [8]). From now on, the meaning of $\mathbf{v}$ is fixed.

Definition 3. *Let $1\leq i'\leq n$. We say that i' is the* **primary pivot** *of $\mathbf{v}$ if $\mathbf{v}[i']$ is the first Δ^+ that occurs in $\mathbf{v}$, i.e.*

$$i'=\min\{h\mid\mathbf{v}[h]=\Delta^+\}\,.$$

We can suppose that $1\leq i'\leq r$, otherwise $\mathbf{v}=0^r(0^m\Delta^r)^s\ldots0^\ell$ and so $(0^{\ell+r+m}\Delta^r)(0^m\Delta^r)^{s-1}\subset\mathbf{v}$ and the bound would be trivially satisfied, since it would give:

$$\begin{aligned}d&\geq\ell+r+m+1+s-1-\left\lfloor\frac{\ell+r+m}{m+r}\right\rfloor r-\max\{\ (\ell+m+r)_{m+r}-m,0\ \}\\&=\ell+r+m+s-\left\lfloor\frac{\ell}{m+r}\right\rfloor r-\max\{\ (\ell)_{m+r}-m,0\ \}\\&\geq\ell+r+1+s-\left\lfloor\frac{\ell}{m+r}\right\rfloor r-\max\{\ (\ell)_{m+r}-m,0\ \}\,.\end{aligned}$$

Definition 4. *Let $n,m,r,s\in\mathbb{N}$ s. t. $m,\ s\geq1$, $n\geq m+r$ and $(n,m+r)\leq m$. $((0)^m(\Delta)^r)^s\subset\mathbf{v}$. Then there are i'' in $\{1,\ldots,n\}$, $k\in\mathbb{N}$ and $t\in\{1,\ldots,m\}$, with the following properties:*

1. $\mathbf{v}[i''] = \Delta^{+}$,
2. $i'' \equiv (s+k)(m+r)+t \mod (n)$,
3. $\mathbf{v}[i] = 0$, *for any* i *s.t.*

$$i \equiv (s+k')(m+r)+j \mod (n)\,,$$

where $k' \in \{0,\dots,k-1\}$ *and* $j \in \{1,\dots,m\}$.

We call such i'' *the* **secondary pivot** *of* $\mathbf{v}$ *with respect to block* $((0)^m(\Delta)^r)^s$.

It is possible to show that if $\gcd(m+r,n) \le m$ (which includes the classical case $\gcd(m+r,n)=1$), then the secondary pivot exists.

We can suppose $s(m+r)+r+1 \le i'' \le s(m+r)+r+m$, otherwise we have $(0^\ell \Delta^r)(0^m\Delta^r)^{s+1} \subset \mathbf{v}$ and the bound is trivially satisfied:

$$\begin{aligned} d &\ge \ell+1+s+1-\left\lfloor \frac{\ell}{m+r} \right\rfloor r - \max\{\,(\ell+m+r)_{m+r}-m,0\,\} \\ &\ge \ell+1+s-\left\lfloor \frac{\ell}{m+r} \right\rfloor r - \max\{\,(\ell)_{m+r}-m,0\,\}\,. \end{aligned}$$

We note that $\mathbf{v}[i''-z\cdot(m+r)]=0$ for any $z=1,\dots,s$. Moreover, i' and i'' may coincide, but this is not a problem.

Now, we are going to choose $(\ell+1+s)$ rows of $M(\mathbf{v})$. We start from the $((n-i'+k)_n+1)-$ th rows with $k=1,\dots,m$, that is, we take the rows with the primary pivot in the first position and its shifts up to the $(m-1)-$th shift included. We collect these rows in submatrix T_1.

$$T_1 = \left(\begin{array}{cccccccccccccccccccccc}
\Delta^{+} & \dots & 0 & \dots & 0 & \Delta & \dots & \Delta & \dots & 0 & \dots & 0 & \Delta & \dots & \Delta^{+} & \dots & \dots & \dots & 0 & \dots & \dots & 0 \\
0 & \Delta^{+} & \dots & 0 & \dots & 0 & \Delta & \dots & \Delta & \dots & 0 & \dots & 0 & \Delta & \dots & \Delta^{+} & \dots & \dots & \dots & 0 & \dots & 0 \\
0 & 0 & \Delta^{+} & \dots & 0 & \dots & 0 & \Delta & \dots & \Delta & \dots & 0 & \dots & 0 & \Delta & \dots & \Delta^{+} & \dots & \dots & \dots & 0 & \dots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & \dots & 0 & \Delta^{+} & \dots & 0 & \dots & 0 & \Delta & \dots & \Delta & \dots & 0 & \dots & 0 & \Delta & \dots & \Delta^{+} & \dots & \dots & 0 & \dots \\
 & & & \downarrow & & & & & & & & & & & & & & & & & & \\
 & & & m & & & & & & & & & & & & & & & & & &
\end{array}\right)$$

We now consider the $(k+1)$-th rows for $k=m,\dots,\ell$, collected in submatrix T_2.

$$T_2 = \left(\begin{array}{cccccccccccccccccccccc}
0 & \dots & 0 & \Delta & \dots & \Delta & \dots & 0 & \dots & 0 & \Delta & \dots & \Delta & \dots & \Delta^{+} & \dots & \dots & \dots & \dots & 0 & \dots & \dots \\
0 & \dots & \dots & 0 & \Delta & \dots & \Delta & \dots & 0 & \dots & 0 & \Delta & \dots & \Delta & \dots & \Delta^{+} & \dots & \dots & \dots & \dots & 0 & \dots \\
0 & \dots & 0 & \dots & 0 & \Delta & \dots & \Delta & \dots & 0 & \dots & 0 & \Delta & \dots & \Delta & \dots & \Delta^{+} & \dots & \dots & \dots & \dots & \dots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & \dots & \dots & 0 & \dots & 0 & \dots & 0 & \Delta & \dots & \Delta & \dots & 0 & \dots & 0 & \Delta & \dots & \Delta & \dots & \Delta^{+} & \dots & \dots \\
0 & \dots & 0 & \dots & 0 & \dots & 0 & \dots & 0 & \Delta & \dots & \Delta & \dots & 0 & \dots & 0 & \Delta & \dots & \Delta & \dots & \Delta^{+} & \dots \\
 & & \downarrow & & & & & & \downarrow & & & & & & & & & & & & & \\
 & & m & & & & & & \ell & & & & & & & & & & & & &
\end{array}\right)$$

Note that T_1 and T_2 have no common rows. Note also that in T_2 for any row $h=1,\dots,\ell+1-m$ and any column $1 \le j \le (s-1)(m+r)+m$ we have:

$$T_2[h,j]=\Delta \implies T_2[h,j+(m+r)]=\Delta \tag{2}$$

Our third and last submatrix, T_3, is formed by the $((n-r-k\cdot(m+r))_n+1)$−th rows, for $k=0,\dots,(s-1)$:

$$T_3=\left(\begin{array}{cccccccccccccccccccccc}
0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots \\
0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
 & & \downarrow & & & \downarrow & & \downarrow & & & & & & & & & & & & & \downarrow & \\
 & & m & & & m+r & & \begin{array}{c} i''-r- \\ (s-1)(m+r) \end{array} & & & & & & & & & & & & & i''-r &
\end{array}\right)$$

Lemma 1. *The singleton procedure is successful for T_3 and thus $\mathrm{prk}(T_3)=s$.*

Proof. We note that the rows of T_3, by construction, have the property that $T_3[a+1,h]=T_3[a,h+(m+r)]$ because each row is a $(m+r)$ left shift of the previous one. This is sufficient to prove that $T_3(i''-r-(s-1)(m+r))$ is a singleton. We claim that the $s-$th row of T_3 corresponds to a singleton. Indeed

$$T_3[s,i''-r-(s-1)(m+r)]=T_3[1,i''-r-(s-1)(m+r)+(s-1)(m+r)]=$$

$$T_3[1,i''-r]=\varDelta^{+}$$

and for $k=1,\dots,s-1$:

$$T_3[k,i''-r-(s-1)(m+r)]=T_3[1,i''-r-(s-1)(m+r)+(k-1)(m+r)]=$$

$$T_3[i''-r-(s-k)(m+r)]=0$$

so we can s-delete it. Once this is done, we might also s-delete the $(s-1)-th$ row, since

$$T_3[s-1,i''-r-(s-2)(m+r)]=T_3[1,i''-r-(s-2)(m+r)+(s-2)(m+r)]=$$

$$T_3[1,i''-r]=\varDelta^{+}$$

and for $k=1,\dots,s-2$:

$$T_3[k,i''-r-(s-2)(m+r)]=T_3[i''-r-(s-2)(m+r)+(k-1)(m+r)]=$$

$$T_3[1,i''-r-(s-1-k)(m+r)]=0.$$

In this way for any row of T_3 we obtain a singleton in $T_3\,(i''-r-k(m+r))$ for $k=0,\dots,s-1$, by recursively s-deleting from the last row to the first.

Collecting all these submatrices T_1, T_2, T_3, we obtain an $(\ell+1+s)\times n$ matrix T, as follows:

$$T=\left(\begin{array}{cccccccccccccccccccccccccl}
\varDelta^{+} & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta^{+} & \dots & \dots & \dots & 0 & \dots & \dots & 0 & \rightarrow & 1 & \\
0 & \varDelta^{+} & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta^{+} & \dots & \dots & \dots & 0 & \dots & 0 & & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & & \mathbf{T_1} \\
0 & 0 & \varDelta^{+} & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta^{+} & \dots & \dots & \dots & 0 & \dots & & & \\
\hline
0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & \dots & \dots & \dots & 0 & \dots & \dots & \rightarrow & m+1 & \\
0 & \dots & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & \dots & \dots & \dots & 0 & \dots & & & \\
0 & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & \dots & \dots & \dots & \dots & & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \dots & & & \mathbf{T_2} \\
0 & \dots & 0 & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & \dots & \dots & & & \\
0 & \dots & 0 & \dots & 0 & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & \rightarrow & \ell+1 & \\
\hline
0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & & & \\
0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \dots & & & \mathbf{T_3} \\
0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \rightarrow & \begin{array}{c}\ell+1\\+s\end{array} & \\
 & & \downarrow & & & \downarrow & & & & & & & & & & & & & & & & & & & \\
 & & m & & & m+r & & & & & & & & & & & & & & & & & & &
\end{array}\right)$$

Observe that the rows from $(m+1)$ to $(\ell+s+1)$ have a block of zero in the first m positions and then we can obviously s-delete the first m rows (i.e the rows of T_1). After these first m s-deletions we obtain a matrix T' composed of the last $(\ell+1+s-m)$ rows of T, as the following:

$$T'=\left(\begin{array}{cccccccccccccccccccccccccc}
0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & \dots & \dots & \dots & 0 & \dots & \dots & \rightarrow & m+1 \\
0 & \dots & . & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & \dots & \dots & \dots & 0 & \dots & & \\
0 & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & \dots & \dots & \dots & \dots & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \dots & & \\
0 & \dots & 0 & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & \dots & \dots & & \\
0 & \dots & 0 & \dots & 0 & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & \rightarrow & \ell+1 \\
0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & & \\
0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \dots & & \\
0 & \dots & 0 & \varDelta & \dots & \varDelta & \dots & \varDelta^{+} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \rightarrow & \ell+1+s \\
 & & \downarrow & & & \downarrow & & & & & & & & & & & & & \downarrow & & \downarrow & & & \\
 & & m & & & m+r & & & & & & & & & & & & & s(m+r) & & i''-r & & &
\end{array}\right)$$

where $1+s(m+r)\le i''-r\le m+s(m+r)$ by hypothesis. We note that T' is composed by the rows of T_2 and T_3.

We use the singletons of T_3 to proceed with the singleton procedure, but in order to do that we have to discard some rows in T_2. More precisely, let us define:

$$B_k=\{\,h \mid T_2[h,i''-r-k(m+r)]=\varDelta\,\}\qquad\text{for } k=0,\dots,s-1$$

then the rows to discard in T_2 in order that $T(i''-r-k(m+r))$ becomes a singleton for $k=0,\dots,s-1$ are:

$$\mathbf{B}=\cup_{k=0}^{s-1}B_k. \tag{3}$$

Lemma 2. *Let $0\le k<k'\le s-1$, then $B_{k'}\subseteq B_k$.*

Proof. Obvious from (2).

Corollary 1. $\mathbf{B} = B_0 = \{\, h \mid T_2[h, i'' - r] = \Delta \,\}$.

Thanks to Corollary 1, since $s(m+r)+1 \leq i'' - r \leq s(m+r)+m$, if we define $\eta_j = |\,\{\, h \mid T_2[h, s(m+r)+j] = \Delta \,\}\,|$, we have:

$$|\mathbf{B}| \leq \max\{\, \eta_j \mid 1 \leq j \leq m \,\}\,.$$

and we can further improve this result with the following lemma, which is not difficult to prove.

Lemma 3. *For* $1 \leq j \leq m$*:*

$$\eta_1 \geq \eta_2 \geq \cdots \geq \eta_m.$$

Thanks to lemma 3 we are able to estimate the maximal number of rows of T_2 that we have to discard.

Lemma 4.

$$|\mathbf{B}| \leq \eta_1 \leq \left\lfloor \frac{\ell}{m+r} \right\rfloor r + \max\{\, (\ell)_{m+r} - m, 0 \,\}$$

Proof. For Corollary 1 and Lemma 3 we have $|\mathbf{B}| \leq \eta_1$*. Now:*

$$\eta_1 = |\,\{\, h \mid T_2[h, s(m+r)+1] = \Delta \,\}\,|, \ \textit{but recall}\ 1 \leq h \leq \ell + 1 - m.$$

We rewrite $\mathbf{v}$ *in the worst case where* $i'' = s(m+r)+r+1$*:*

$$\begin{array}{cccccccccccccc}
\mathbf{v} = & \Delta & \ldots & \Delta & 0 \ldots & 0 & (\Delta^r 0^m)^{s-2} \; \Delta \ldots & \Delta & 0 & \ldots & 0 & \Delta \ldots \Delta & \Delta^{+} \ldots\ldots \\
 & \downarrow & & \downarrow & & \downarrow & & & \downarrow & & \downarrow & & \downarrow \\
 & 1 & & r & & m+r & & & s(m+r)-m+1 & & s(m+r) & & s(m+r)+r+1
\end{array}$$

Since $T_2[1, s(m+r)+1] = \mathbf{v}[s(m+r)+1-m] = 0$*, we have*

$$\begin{aligned}
\eta_1 &= |\,\{\, h \mid T_2[h, s(m+r)+1] = \Delta, 1 \leq h \leq \ell + 1 - m \,\}\,| \\
&= |\,\{\, h \mid T_2[h, s(m+r)+1] = \Delta, 2 \leq h \leq \ell + 1 - m \,\}\,|.
\end{aligned}$$

Now $T_2[h+1, j] = T_2[h, j-1]$ *(for* $h \geq 1$*) and* $T_2[1, j] = \mathbf{v}[j-m]$*, by construction of* T_2*. So:*

$$\begin{aligned}
\eta_1 &= |\,\{\, h \mid T_2[h, s(m+r)+1] = \Delta, 2 \leq h \leq \ell + 1 - m \,\}\,| \\
&= |\,\{\, h \mid T_2[1, s(m+r)+1-(h-1)] = \Delta, 2 \leq h \leq \ell + 1 - m \,\}\,| \\
&= |\,\{\, h \mid \mathbf{v}[s(m+r) - m + 2 - h] = \Delta, 2 \leq h \leq \ell + 1 - m \,\}\,| \\
&= |\,\{\, h \mid \mathbf{v}[s(m+r) + 2 - h] = \Delta, 2 \leq h \leq \ell + 1 \,\}\,|
\end{aligned}$$

Thus, to compute η_1 *we have to count the number of* Δ*'s we meet,* $\mathbf{v}[s(m+r)]$ *to* $\mathbf{v}[s(m+r) - \ell + 1]$ *(i.e. from* $\mathbf{v}[s(m+r)]$ *and going back of* ℓ *positions). Let us consider the worst case, which is when* $\ell \leq s(m+r)$*. Passing through* *the block $(0^m \Delta^r)$ from right to left of ℓ positions, every $m+r$ steps we meet a block formed by r Δ's and m 0's, thus the contibute to η_1 per block is by r. Since we move only by ℓ positions, we can meet no more than $\left\lfloor \frac{\ell}{m+r} \right\rfloor$ blocks and so we have $\eta_1 \leq \left\lfloor \frac{\ell}{m+r} \right\rfloor r + \eta_1'$, where η_1' are the Δ's coming from the last $(\ell)_{m+r}$ steps left. The first m-positions we meet doing the last $(\ell)_{m+r}$ steps are zero, since they correspond to the last block $(\Delta^r 0^m)$, thus η_1' can be at most $(\ell)_{m+r} - m$ and it is non-negative only if $(\ell)_{m+r} \geq m$. In conclusion: $\eta_1 \leq \left\lfloor \frac{\ell}{m+r} \right\rfloor r + \max\{\,(\ell)_{m+r} - m, 0\,\}$.*

Thanks to Lemma 4, discarding at most $\left\lfloor \frac{\ell}{m+r} \right\rfloor r + \max\{\,(\ell)_{m+r} - m, 0\,\}$ rows of T_2, we can remove by s-deletions T_3 from T'. The matrix that remains, $\widetilde{T}$, is a submatrix of T_2 not having row indeces in $\mathbf{B}$ which has full rank, since T_2 has full rank, adopting the singleton procedure as can be seen by Lemma 3.2 in [5].

Example 1. Let us suppose C be a cyclic code of length n, with defining set S_C satisfying the assumptions of Proposition 1 with parameters $\ell = 7$, $m = 2$, $r = 1$, $s = 5$. We want to prove that for Proposition 1 the distance of the code C is at least $d \geq 7 + 1 + 5 - \left\lfloor \frac{7}{2+1} \right\rfloor 1 - \max\left\{\,(7)_{3+2} - 2, 0\,\right\} = 11$. Let $\mathbf{v} \in \mathcal{A}(R(n, S_C))$ with $\mathbf{v}[1] = \Delta^+$. The matrix T is:

$$
\begin{array}{ccccccccccccccccccccccccccc}
\Delta^+ & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \dots \\
0 & \Delta^+ & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \dots \\
\hline
0 & 0 & \Delta^+ & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \dots \\
0 & 0 & 0 & \Delta^+ & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \dots \\
0 & 0 & 0 & 0 & \Delta^+ & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \dots & \dots \\
0 & 0 & 0 & 0 & 0 & \Delta^+ & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \dots & \dots \\
0 & 0 & 0 & 0 & 0 & 0 & \Delta^+ & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \dots & \dots \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \Delta^+ & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \dots & \dots \\
\hline
0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \dots \\
0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \dots \\
0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \dots \\
0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \dots \\
0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \dots
\end{array}
$$

For the secondary pivot we have two possibilities: $i'' = 11$ or $i'' = 12$. We show that in both cases it is possible to obtain 11 s-deletions, removing at most $\left\lfloor \frac{7}{2+1} \right\rfloor 1 + \max\left\{\,(7)_{3+2} - 2, 0\,\right\} = 2$ rows from the matrix T.

Case 1: $i'' = 11$.

$$
\begin{array}{cccccccccccccccccccccccccccl}
\Delta^+ & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \to & \text{1st s-deletion} \\
0 & \Delta^+ & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \to & \text{2nd s-deletion} \\
0 & 0 & \Delta^+ & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \to & \text{8th s-deletion} \\
0 & 0 & 0 & \Delta^+ & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \to & \textbf{REMOVED} \\
0 & 0 & 0 & 0 & \Delta^+ & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \dots & \to & \text{9th s-deletion} \\
0 & 0 & 0 & 0 & 0 & \Delta^+ & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \dots & \to & \text{10th s-deletion} \\
0 & 0 & 0 & 0 & 0 & 0 & \Delta^+ & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \dots & \to & \textbf{REMOVED} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \Delta^+ & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \dots & \to & \text{11th s-deletion} \\
0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \to & \text{7th s-deletion} \\
0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \to & \text{6th s-deletion} \\
0 & 0 & \Delta & 0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \to & \text{5th s-deletion} \\
0 & 0 & \Delta & 0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \to & \text{4th s-deletion} \\
0 & 0 & \Delta & \Delta^+ & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \Delta & \dots & \to & \text{3rd s-deletion}
\end{array}
$$

Case 2: $i'' = 12$.

$$\begin{array}{ccccccccccccccccccccccccclll}
\varDelta^+ & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & \varDelta & \varDelta^+ & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \dots & \rightarrow & \text{1st s-deletion} \\
0 & \varDelta^+ & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & \varDelta & \varDelta^+ & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \dots & \rightarrow & \text{2nd s-deletion} \\
0 & 0 & \varDelta^+ & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & \varDelta & \varDelta^+ & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \dots & \rightarrow & \text{8th s-deletion} \\
0 & 0 & 0 & \varDelta^+ & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & \varDelta & \varDelta^+ & \varDelta & \varDelta & \varDelta & \varDelta & \dots & \rightarrow & \text{9th s-deletion} \\
\cancel{0} & \cancel{0} & \cancel{0} & \cancel{0} & \cancel{\varDelta^+} & \cancel{0} & \cancel{0} & \cancel{\varDelta} & \cancel{0} & \cancel{0} & \cancel{\varDelta} & \cancel{0} & \cancel{0} & \cancel{\varDelta} & \cancel{0} & \cancel{0} & \cancel{\varDelta} & \cancel{0} & \cancel{0} & \cancel{\varDelta} & \cancel{\varDelta} & \cancel{\varDelta^+} & \cancel{\varDelta} & \cancel{\varDelta} & \cancel{\varDelta} & \dots & \rightarrow & \textbf{REMOVED} \\
0 & 0 & 0 & 0 & 0 & \varDelta^+ & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & \varDelta & \varDelta^+ & \varDelta & \varDelta & \dots & \rightarrow & \text{10th s-deletion} \\
0 & 0 & 0 & 0 & 0 & 0 & \varDelta^+ & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & \varDelta & \varDelta^+ & \varDelta & \dots & \rightarrow & \text{11th s-deletion} \\
\cancel{0} & \cancel{0} & \cancel{0} & \cancel{0} & \cancel{0} & \cancel{0} & \cancel{0} & \cancel{\varDelta^+} & \cancel{0} & \cancel{0} & \cancel{\varDelta} & \cancel{0} & \cancel{0} & \cancel{\varDelta} & \cancel{0} & \cancel{0} & \cancel{\varDelta} & \cancel{0} & \cancel{0} & \cancel{\varDelta} & \cancel{0} & \cancel{0} & \cancel{\varDelta} & \cancel{\varDelta} & \cancel{\varDelta^+} & \dots & \rightarrow & \textbf{REMOVED} \\
0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & \varDelta & \varDelta^+ & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \dots & \rightarrow & \text{7th s-deletion} \\
0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & \varDelta & \varDelta^+ & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \dots & \rightarrow & \text{6th s-deletion} \\
0 & 0 & \varDelta & 0 & 0 & \varDelta & 0 & 0 & \varDelta & \varDelta & \varDelta^+ & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \dots & \rightarrow & \text{5th s-deletion} \\
0 & 0 & \varDelta & 0 & 0 & \varDelta & \varDelta & \varDelta^+ & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \dots & \rightarrow & \text{4th s-deletion} \\
0 & 0 & \varDelta & \varDelta & \varDelta^+ & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \varDelta & \dots & \rightarrow & \text{3rd s-deletion}
\end{array}$$

For Proposition 2 the proof proceeds similarly.

Proof (of Proposition 2). We can suppose:

(i) $\mathbf{v} = \underbrace{0\dots0\varDelta}_{\ell m+1}\overbrace{\underbrace{0\dots0\varDelta}_{\ell}\dots\dots\underbrace{0\dots0\varDelta}_{\ell}}^{s-\text{times}}\dots\,;$

(ii) $i' = \ell m + 1$;

(iii) $m\ell + s(\ell) + 2 \leq i'' \leq m\ell + s(\ell) + 1 + m$.

We take the rows $((n-(\ell m+1)+k)_n + 1)-$ th rows, with $k = 1, \dots, m\ell + \ell$: we take the rows with the primary pivot in first position and its shifts until the $(m\ell + \ell - 1)-$th shift:

$$T_1 = \left(\begin{array}{cccccccccccccccccccccccc}
\varDelta^+ & 0 & \dots & 0 & \varDelta & 0 & \dots & 0 & \varDelta & 0 & \dots & 0 & \varDelta & \dots & \varDelta^+ & \dots & \dots & 0 & \dots & \dots & \dots & 0 & \rightarrow & 1 \\
0 & \varDelta^+ & 0 & \dots & 0 & \varDelta & 0 & \dots & 0 & \varDelta & 0 & \dots & 0 & \varDelta & \dots & \varDelta^+ & \dots & \dots & 0 & \dots & \dots & \dots & & \\
0 & 0 & \varDelta^+ & 0 & \dots & 0 & \varDelta & 0 & \dots & 0 & \varDelta & 0 & \dots & 0 & \varDelta & \dots & \varDelta^+ & \dots & \dots & 0 & \dots & \dots & & \\
0 & \dots & 0 & \varDelta^+ & 0 & \dots & 0 & \varDelta & 0 & \dots & 0 & \varDelta & 0 & \dots & 0 & \varDelta & \dots & \varDelta^+ & \dots & \dots & \dots & \dots & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \\
\varDelta & \varDelta & 0 & \dots & 0 & \varDelta^+ & 0 & \dots & 0 & \varDelta & 0 & \dots & 0 & \varDelta & 0 & \dots & 0 & \varDelta & \dots & \varDelta^+ & \dots & \dots & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \\
\varDelta & \dots & \varDelta & 0 & \dots & 0 & \varDelta^+ & 0 & \dots & 0 & \varDelta & 0 & \dots & 0 & \varDelta & 0 & \dots & 0 & \varDelta & \dots & \varDelta^+ & \dots & \rightarrow & m\ell + \ell \\
 & & & \downarrow & & & \downarrow & & & & & & & & & & & & & & & & & \\
 & & & \ell & & & m\ell + \ell & & & & & & & & & & & & & & & & &
\end{array}\right)$$

and then we add $s-1$ rows: the $((n - i'' - (s\ell + 1))_n + (k+1)\ell)$ $-$th rows with $k = 1, \dots, s-1$, which are the rows with the secondary pivot in position $(k+1)\ell$ with $k = 1, \dots, s-1$.

$$T_2 = \left(\begin{array}{cccccccccccccccccccccccc}
\varDelta & \dots & \varDelta & 0 & \dots & 0 & \varDelta & 0 & \dots & 0 & \varDelta & \dots & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta^+ & \dots & \dots & \dots & \rightarrow & 1 \\
\varDelta & \dots & \varDelta & 0 & \dots & 0 & \varDelta & \dots & \dots & 0 & \dots & 0 & \varDelta & \dots & \varDelta^+ & \dots & \dots & \dots & \dots & \dots & \dots & \dots & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \\
\varDelta & \dots & \varDelta & 0 & \dots & 0 & \varDelta & 0 & \dots & 0 & \varDelta & \dots & \varDelta^+ & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \rightarrow & s-2 \\
\varDelta & \dots & \varDelta & 0 & \dots & 0 & \varDelta & \dots & \varDelta^+ & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \rightarrow & s-1 \\
 & & & & & & & & \downarrow & & & & \downarrow & & \downarrow & & & & \downarrow & & & & & \\
 & & & & & & & & 2\ell & & & & 3\ell & & (s-1)\ell & & & & s\ell & & & & &
\end{array}\right)$$

And collecting together the rows of T_1 and T_2, the proof concludes as in case of Proposition 1.

We summarize the results of Proposition 1 and Proposition 2 in a unique form that constitutes the statement of bound C.

Theorem 2 (bound C). *Let C be an $\mathbb{F}_q[n,k,d]$ cyclic code with defining set S_C and* $\gcd(q,n)=1$. *Suppose that there are ℓ, m, r, $s \in \mathbb{N}$, $1 \le m \le \ell$ and $i_0 \in \{0,\dots,n-1\}$ such that* $\gcd(n,m+r) < m$ *or* $\gcd(n,m+r)=1$. *If*

a) $(i_0+j)_n \in S_C$, $\forall j = 0,\dots,\ell-1$,
b) $(i_0+j)_n \in S_C$,

$$\forall j = i_0+\ell+r+h(m+r),\dots,\ i_0+\ell+r+m-1+h(m+r)$$
$$\forall 0 \le h \le s-1.$$

Then

$$d \ge \ell+1+s-r\left\lfloor\frac{\ell}{m+r}\right\rfloor - \max\{(\ell)_{m+r}-m,0\}. \tag{4}$$

In the particular case that for some ℓ' and m', $\ell=m'\ell'$, $m=\ell'-1$, $s \ge m'+1$ and $r=1$ we also have:

$$d \ge \ell'm'+\ell'+s-m'-1. \tag{5}$$

5 Computational Results and Costs

As explained in Remark 1 and in Remark 2 bound C is both a generalization of HT bound and BS bound (except when $\ell|n$) and so it is sharper and tighter. The relation between our bound and the Roos bound is not clear: sometimes our bound is sharper and tighter than Roos or but for other codes it is the opposite. However, from the computed codes it appears that bound C works better than the Roos bound in general. Although the BS bound sometimes beats the Roos bound, in the majority of computed cases the Roos bound is better, as reported in [5] and checked by us. Bound C is the first polynomial-time bound outperforming the Roos bound on a significant sample of codes.
As regards computational costs, bound C requires:

- n operations for i_0
- n operations for ℓ
- n operations for m
- n operations for r
- n operations for s

and so it costs $O(n^5)$ which is slightly more than the Roos bound which needs $O(n^4)$, in fact the latter requires at most:

- n operations for i_0,
- n operations for m,
- n operations for r,
- n operations for s

while the other bounds cost less: BCH-$O(n^2)$, HT-$O(n^3)$, bound BS-$O(n^{2.5})$. We tested all cyclic codes in the following range: on $\mathbb{F}_2$ with $15 \le n \le 125$, on $\mathbb{F}_3$ with $8 \le n \le 79$ and $82 \le n \le 89$, on $\mathbb{F}_5$ with $8 \le n \le 61$, on $\mathbb{F}_7$ with $8 \le n \le 47$. We have chosen the largest ranges that we could compute in a reasonable time.

In the following table we report the number of codes on which each bound considered is not tight.

Table 1. Bound tightness

	$\mathbb{F}_2$	$\mathbb{F}_3$	$\mathbb{F}_5$	$\mathbb{F}_7$	total
number of codes	70488	93960	1163176	106804	1434428
BCH	11192	16376	151219	13696	182483
HT	10531	15334	139161	11093	176119
BS	10959	15545	139783	11283	177570
ROOS	10014	14583	133546	10709	168852
bound C	10306	14565	131072	9541	165484

Acknowledgments. These bounds appear in the 2010 Master's thesis of the first author [10], who thanks his supervisor (the second author).

References

1. Bose, R.C., Ray Chaudhuri, D.K.: On a class of error correcting binary group codes. Information and Control 3, 68–79 (1960)
2. Hartmann, C.R.P., Tzeng, K.K.: Generalizations of the BCH bound. Information and Control 20, 489–498 (1972)
3. Roos, C.: A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound. Journal of Combinatorial Theory Ser. A 33, 229–232 (1982)
4. Roos, C.: A new lower bound for the minimum distance of a cyclic code. IEEE Trans. on Inf. Th. 29(3), 330–332 (1983)
5. Betti, E., Sala, M.: A New Bound for the Minimum Distance of a Cyclic Code From Its Defining Set. IEEE Trans. on Inf. Th. 52(8), 3700–3706 (2006)
6. Schaub, T.: A Linear Complexity Approach to Cyclic Codes. PhD thesis, Swiss Federal Inst. of Tech. Zurich (1988)
7. van Lint, J.H., Wilson, R.M.: On the minimum distance of cyclic codes. IEEE Trans. on Inf. Th. 32(1), 23–40 (1986)
8. Betti, E., Sala, M.: A theory for distance bounding cyclic codes. BCRI preprint 63 (2007), www.bcri.ucc.ie
9. Ponchio, F., Sala, M.: A lower bound on the distance of cyclic codes. BCRI preprint 7 (2003), http://www.bcri.ucc.ie
10. Piva, M.: Probabilità d'errore in decodifica con un nuovo bound. Master's thesis (Laurea), University of Trento, Department of Mathematics (2010)