Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 236-242*

Bounds for the minimum distance in constacyclic codes

Diana Radkova dradkova@fmi.uni-sofia.bg
Faculty of Mathematics and Informatics, Sofia University,
5 James Bouchier blvd, 1164 Sofia, BULGARIA

A. J. van Zanten A.J.vanZanten@twi.tudelft.nl
Delft University of Technology, Faculty of Information Technology and Systems
Department of Mathematics, P.O. Box 5031,
2600 GA Delft, THE NETHERLANDS

Abstract. In algebraic coding theory it is common practice to require that $(n, q) = 1$, where n is the word length and $F = \mathrm{GF}(q)$ is the alphabet. In this paper, which is about constacyclic codes, we shall stick to this practice too. Since linear codes have the structure of linear subspaces of F^n, an alternative description of constacyclic codes in terms of linear algebra appears to be another quite natural approach. Due to this description we derive lower bounds for the minimum distance of constacyclic codes that are generalizations of the well known BCH bound, the Hartmann-Tzeng bound and the Roos bound.

Definition 1. *Let a be a nonzero element of $F = \mathrm{GF}(q)$. A code C of length n over F is called constacyclic with respect to a, if whenever $\mathbf{x} = (c_1, c_2, \ldots, c_n)$ is in C, so is $\mathbf{y} = (ac_n, c_1, \ldots, c_{n-1})$.*

Let a be a nonzero element of F and let

$$\psi_a : \begin{cases} F^n \to F^n \\ (x_1, x_2, \ldots, x_n) \mapsto (ax_n, x_1, \ldots, x_{n-1}) \end{cases}.$$

Then $\psi_a \in \operatorname{Hom} F^n$ and it has the following matrix

$$B_n(a) = B_n = \begin{pmatrix} 0 & 0 & 0 & \ldots & a \\ 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

with respect to the standard basis $e = (\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n)$. The characteristic polynomial of B_n is $f_{B_n}(x) = (-1)^n(x^n - a)$. We shall denote it by $f(x)$. We assume that $(n, q) = 1$. The polynomial $f(x)$ has no multiple roots and splits into distinct irreducible monic factors $f(x) = (-1)^n f_1(x) \ldots f_t(x)$. Let $U_i = \operatorname{Ker} f_i(\psi_a),\ i = 1, \ldots, n$. For the proof of the following theorem we refer to [1].

Theorem 1. *Let C be a linear constacyclic code of length n over F. Then the following facts hold.*

1) C is a constacyclic code iff C is a ψ_a-invariant subspace of F^n;

2) $C = U_{i_1} \oplus \cdots \oplus U_{i_s}$ for some minimal ψ_a-invariant subspaces U_{i_r} of F^n and $k := \dim {}_F C = k_{i_1} + \cdots + k_{i_s}$, where k_{i_r} is the dimension of U_{i_r};

3) $f_{\psi_a|_C}(x) = (-1)^k f_{i_1}(x) \dots f_{i_s}(x) = g(x)$;

4) $\mathbf{c} \in C$ iff $g(B_n)\mathbf{c} = \mathbf{0}$;

5) the polynomial $g(x)$ has the smallest degree with respect to property 4);

6) $\mathrm{r}\,(g(B_n)) = n - k$, where $\mathrm{r}\,(g(B_n)) = n - k$ is the rank of the matrix $g(B_n)$.

Let $K = \mathrm{GF}(q^m)$ be the splitting field of the polynomial $f(x) = (-1)^n(x^n - a)$ over F, where $0 \neq a \in F$. Let the eigenvalues of ψ_a be $\alpha_1, \dots, \alpha_n$, with $\alpha_i = \sqrt[n]{a}\alpha^i$, $i = 1, \dots, n$, where α is a primitive $n-$th root of unity and $\sqrt[n]{a}$ is a fixed, but otherwise arbitrary, zero of the polynomial $x^n - a$. Let $\mathbf{v}_i$ be the respective eigenvectors, $i = 1, \dots, n$. More in particular we have

$$B_n \mathbf{v}_i^t = \alpha_i \mathbf{v}_i^t, \quad \mathbf{v}_i = ({\alpha_i}^{n-1}, {\alpha_i}^{n-2}, \dots, \alpha_i, 1), \quad i = 1, \dots, n.$$

Let us consider the basis $v = (\mathbf{v_1}, \dots, \mathbf{v_n})$ of eigenvectors of ψ_a. We carry out the basis transformation $e \to v$, and obtain that

$$D = \begin{pmatrix} \alpha_1 & 0 & \dots & 0 \\ 0 & \alpha_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \alpha_n \end{pmatrix} = T^{-1} B_n T,$$

with

$$T = \begin{pmatrix} {\alpha_1}^{n-1} & {\alpha_2}^{n-1} & \dots & {\alpha_n}^{n-1} \\ {\alpha_1}^{n-2} & {\alpha_2}^{n-2} & \dots & {\alpha_n}^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ 1 & 1 & \dots & 1 \end{pmatrix}.$$

Let $\mathbf{u}_i = (\alpha_i, {\alpha_i}^2, \dots, {\alpha_i}^{n-1}, {\alpha_i}^n)$, $i = 1, \dots, n$. Then

$$\langle \mathbf{v}_i, \mathbf{u}_j \rangle = \sum_{k=1}^{n} \left(\frac{\alpha_i}{\alpha_j}\right)^k = \sum_{k=1}^{n} (\alpha^{i-j})^k = \begin{cases} n, \ for\ i = j \\ 0, \ otherwise \end{cases}.$$

From this it follows immediately that

$$T^{-1} = \frac{1}{n}\begin{pmatrix}\mathbf{u}_1\\ \mathbf{u}_2\\ \vdots\\ \mathbf{u}_n\end{pmatrix} = \frac{1}{n}\begin{pmatrix}\alpha_1 & {\alpha_1}^2 & \dots & {\alpha_1}^{n-1} & {\alpha_1}^n\\ \alpha_2 & {\alpha_2}^2 & \dots & {\alpha_2}^{n-1} & {\alpha_2}^n\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1} & {\alpha_n}^n\end{pmatrix}.$$

Let $h(x) = \frac{f(x)}{g(x)}$. Let $\deg h(x) = n-k = r$, and let its r zeros be $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_r}$ and its k nonzeros $\alpha_{j_1}, \alpha_{j_2}, \dots, \alpha_{j_k}$. It is obvious that the zeros of $g(x)$ are the nonzeros of $h(x)$ and vice versa. Assume that $\mathbf{c} = (c_1, c_2, \dots, c_n) \in F^n$ and let $\mathbf{c}' = T^{-1}\mathbf{c}$. We know $\mathbf{c} \in C$ iff $g(B_n)\mathbf{c} = \mathbf{0}$. The latter condition is equivalent to $g(D)\mathbf{c}' = T^{-1}g(B_n)TT^{-1}\mathbf{c} = T^{-1}g(B_n)\mathbf{c} = \mathbf{0}$, which, in its turn, is equivalent to $c'_{i_1} = c'_{i_2} = \dots = c'_{i_r} = 0$. Hence, we get the following necessary and sufficient condition for $\mathbf{c}$ to be a codeword in C

$$\mathbf{u}_{i_l}\mathbf{c} = 0,\ l = 1, \dots, r.$$

Theorem 2. *Let C be a linear constacyclic code of length n over F, $g(x) = f_{\psi_a|_C}(x)$ and $h(x) = \frac{f(x)}{g(x)}$. Let for some integers $b \geq 1$, $\delta \geq 1$ the following equalities*

$$h(\alpha_b) = h(\alpha_{b+1}) = \dots = h(\alpha_{b+\delta-2}) = 0$$

hold, i.e., the polynomial $h(x)$ has a string of $\delta - 1$ consecutive zeros. Then the minimum distance of the code C is at least δ.

Proof. If $\mathbf{c} = (c_1, c_2, \dots, c_n)$ is in C, then

$$\mathbf{u}_i\mathbf{c} = 0,\ i = b, b+1, \dots, b+\delta-2,$$

so that

$$\begin{pmatrix}\alpha_b & \alpha_b^2 & \dots & \alpha_b^{n-1} & \alpha_b^n\\ \alpha_{b+1} & \alpha_{b+1}^2 & \dots & \alpha_{b+1}^{n-1} & \alpha_{b+1}^n\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ \alpha_{b+\delta-2} & \alpha_{b+\delta-2}^2 & \dots & \alpha_{b+\delta-2}^{n-1} & \alpha_{b+\delta-2}^n\end{pmatrix}\begin{pmatrix}c_1\\ c_2\\ \vdots\\ c_n\end{pmatrix} = \begin{pmatrix}0\\ 0\\ \vdots\\ 0\end{pmatrix}.$$

Now let us suppose that $\mathbf{c}$ has weight $w \leq \delta - 1$, i.e., $c_i \neq 0$ iff $i \in \{a_1, a_2, \dots, a_w\}$. Then the last equality implies

$$\begin{pmatrix}\alpha_b^{a_1} & \dots & \alpha_b^{a_w}\\ \alpha_{b+1}^{a_1} & \dots & \alpha_{b+1}^{a_w}\\ \vdots & \ddots & \vdots\\ \alpha_{b+w-1}^{a_1} & \dots & \alpha_{b+w-1}^{a_w}\end{pmatrix}\begin{pmatrix}c_{a_1}\\ c_{a_2}\\ \vdots\\ c_{a_w}\end{pmatrix} = \begin{pmatrix}0\\ 0\\ \vdots\\ 0\end{pmatrix}.$$

Hence, the determinant of the matrix on the left is zero. But this determinant is equal to

$$\begin{vmatrix} \alpha_b^{a_1} & \dots & \alpha_b^{a_w} \\ \alpha_{b+1}^{a_1} & \dots & \alpha_{b+1}^{a_w} \\ \vdots & \ddots & \vdots \\ \alpha_{b+w-1}^{a_1} & \dots & \alpha_{b+w-1}^{a_w} \end{vmatrix} = \begin{vmatrix} \mu^{a_1}\alpha^{a_1 b} & \dots & \mu^{a_w}\alpha^{a_w b} \\ \mu^{a_1}\alpha^{a_1(b+1)} & \dots & \mu^{a_w}\alpha^{a_w(b+1)} \\ \vdots & \ddots & \vdots \\ \mu^{a_1}\alpha^{a_1(b+w-1)} & \dots & \mu^{a_w}\alpha^{a_w(b+w-1)} \end{vmatrix} =$$

$$= \mu^{a_1+\dots+a_w}\alpha^{(a_1+\dots+a_w)b} \begin{vmatrix} 1 & \dots & 1 \\ \alpha^{a_1} & \dots & \alpha^{a_w} \\ \vdots & \ddots & \vdots \\ \alpha^{a_1(w-1)} & \dots & \alpha^{a_w(w-1)} \end{vmatrix} \neq 0,$$

where $\mu = \sqrt[n]{a}$. The contradiction proves the statement. □

The next result follows easily from Theorem 2.

Corollary 1. *Let C be a linear constacyclic code of length n over F and let*

$$\alpha_b, \alpha_{b+s}, \dots, \alpha_{b+(\delta-2)s}$$

are zeros of $h(x)$, where $(s, n) = 1$. Then the minimum distance of C is at least δ.

The following theorem generalizes the Hartmann-Tzeng bound for linear constacyclic codes. Its proof is close to Roos' proof for cyclic codes in [2].

Theorem 3. *Let C be a constacyclic code of length n over F, $g(x) = f_{\varphi|_C}(x)$, $h(x) = \frac{f(x)}{g(x)}$ and let α be a primitive n-th root of unity in $K = \mathrm{GF}(q^m)$. Assume that there exist integers s, b, c_1 and c_2 where $s \geq 0$, $b \geq 0$, $(n, c_1) = 1$ and $(n, c_2) < \delta$, such that*

$$h(\alpha_{b+i_1c_1+i_2c_2}) = 0, \quad 0 \leq i_1 \leq \delta - 2,\ 0 \leq i_2 \leq s.$$

Then the minimum distance d of C satisfies $d \geq \delta + s$.

Proof. We use induction on s. For $s = 0$ the assertion follows from Corollary 1, since $(n, c_1) = 1$. Take some $s > 0$ and assume that the theorem holds, i.e.,

$$h(\alpha_{b+i_1c_1+i_2c_2}) = 0, \quad 0 \leq i_1 \leq \delta - 2,\ 0 \leq i_2 \leq s$$

defines a constacyclic code C of minimum distance $d \geq \delta + s$. We have that $\mathbf{c} \in C$ iff $\mathbf{u}_k\mathbf{c} = 0$, $k = b + i_1c_1 + i_2c_2$, $0 \leq i_1 \leq \delta - 2$, $0 \leq i_2 \leq s$. So, we obtain

that $U\mathbf{c} = \mathbf{0}$, where U is the following matrix

$$U = \begin{pmatrix} \alpha_b & \alpha_b^2 & \dots & \alpha_b^{n-1} & \alpha_b^n \\ \alpha_{b+c_1} & \alpha_{b+c_1}^2 & \dots & \alpha_{b+c_1}^{n-1} & \alpha_{b+c_1}^n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_{b+(\delta-2)c_1} & \alpha_{b+(\delta-2)c_1}^2 & \dots & \alpha_{b+(\delta-2)c_1}^{n-1} & \alpha_{b+(\delta-2)c_1}^n \\ \alpha_{b+c_2} & \alpha_{b+c_2}^2 & \dots & \alpha_{b+c_2}^{n-1} & \alpha_{b+c_2}^n \\ \alpha_{b+c_1+c_2} & \alpha_{b+c_1+c_2}^2 & \dots & \alpha_{b+c_1+c_2}^{n-1} & \alpha_{b+c_1+c_2}^n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_{b+(\delta-2)c_1+c_2} & \alpha_{b+(\delta-2)c_1+c_2}^2 & \dots & \alpha_{b+(\delta-2)c_1+c_2}^{n-1} & \alpha_{b+(\delta-2)c_1+c_2}^n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_{b+sc_2} & \alpha_{b+sc_2}^2 & \dots & \alpha_{b+sc_2}^{n-1} & \alpha_{b+sc_2}^n \\ \alpha_{b+c_1+sc_2} & \alpha_{b+c_1+sc_2}^2 & \dots & \alpha_{b+c_1+sc_2}^{n-1} & \alpha_{b+c_1+sc_2}^n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_{b+(\delta-2)c_1+sc_2} & \alpha_{b+(\delta-2)c_1+sc_2}^2 & \dots & \alpha_{b+(\delta-2)c_1+sc_2}^{n-1} & \alpha_{b+(\delta-2)c_1+sc_2}^n \end{pmatrix}.$$

From the definition of α_i it follows that $\alpha_{b+lc_2}\alpha^{c_2} = \alpha_{b+(l+1)c_2}$, $0 \le l \le s$ and $\alpha_{b+i_1c_1+lc_2}\alpha^{c_2} = \alpha_{b+i_1c_1+(l+1)c_2}$, $0 \le i_1 \le \delta - 2$. Hence, every set of $\delta - 1$ consecutive zeros of $h(x)$ is obtained from the previous one by multiplying by $\beta = \alpha^{c_2}$. It follows that if we multiply the first column $\mathbf{b}_1$ of U by β, the second column $\mathbf{b}_2$ by β^2,..., the $n-$th column $\mathbf{b}_n$ by β^n, the resulting matrix U_0 contains all rows of U except the first $\delta - 1$ rows, whereas its last $\delta - 1$ rows are new and correspond to the zeros $\alpha_{b+(s+1)c_2}, \dots, \alpha_{b+(\delta-2)c_1+(s+1)c_2}$. Note that U need not be the full parity check matrix of C. However, we can interpret U as parity check matrix for a code C^* over K. If C^* has minimum distance d^*, then clearly $d \ge d^*$. We shall show that $d^* \ge \delta + s$. Since $d \ge d^*$ this implies the theorem. Since $(n, c_2) < \delta$, β has order $e = \frac{n}{(n,c_2)} > \frac{n}{\delta} \ge \frac{n}{d^*}$ and hence in the sequence $\beta, \beta^2, \dots, \beta^n$ each element occurs $\frac{n}{e} < d^*$ times. We now define the matrix

$$U' = \begin{bmatrix} U \\ U_o \end{bmatrix} = \begin{bmatrix} \mathbf{b}_1 & \mathbf{b}_2 & \dots & \mathbf{b}_n \\ \beta\mathbf{b}_1 & \beta^2\mathbf{b}_2 & \dots & \beta^n\mathbf{b}_n \end{bmatrix}.$$

We know that every $d^* - 1$ columns of U are linearly independent. We shall prove now that every d^* columns of U' are independent. In order to show this, let us suppose that U' contains d^* columns which are linearly dependent. Without loss of generality we may assume that these are the first d^* columns.

Then there will exist elements $\lambda_1, \lambda_2, \ldots \lambda_{d^*} \in K$ (not all zero) such that

$$\sum_{i=1}^{d^*} \lambda_i \mathbf{b}_i = \sum_{i=1}^{d^*} \lambda_i \beta^i \mathbf{b}_i = \mathbf{0}, \textit{ and so } \sum_{i=1}^{d^*-1} \lambda_i (\beta^i - \beta^{d^*}) \mathbf{b}_i = \mathbf{0}.$$

Since any $d^* - 1$ columns of U are linearly independent, it follows that $\lambda_i(\beta^i - \beta^{d^*}) = 0$ for $1 \leq i \leq d^* - 1$. However, $\lambda_i \neq 0$ for $1 \leq i \leq d^*$, again because no $d^* - 1$ columns of U are linearly dependent. Hence, we obtain $\beta = \beta^2 = \cdots = \beta^{d^*}$, which contradicts the fact that in the sequence $\beta, \beta^2, \ldots, \beta^n$ each element occurs less than d^* times. It immediately follows that the constacyclic code C' with zeros $\alpha_{b+i_1c_1+i_2c_2}$, $0 \leq i_1 \leq \delta - 2$, $0 \leq i_2 \leq s + 1$ of $h'(x)$, where $h'(x) = \frac{f(x)}{f_{\varphi|_{C'}}(x)}$, has minimum distance at least $d^* + 1$. □

Next, we shall derive an even more general bound for the minimum distance of constacyclic codes, which is similar to the so-called Roos bound for cyclic codes in [3]. Our proof and notation are also very close to the proof in [3], and therefore we shall partly omit it.

Let K be any finite field and $A = [\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n]$ any matrix over K with n columns $\mathbf{a}_i$, $1 \leq i \leq n$. Let C_A denote the linear code over K with A as parity check matrix. The minimum distance of C_A will be denoted as d_A.

For any $m \times n$ matrix $X = [\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n]$ with nonzero columns $\mathbf{x}_i \in K^m$ for $1 \leq i \leq n$, we define the matrix $A(X)$ as

$$A(X) := \begin{pmatrix} x_{11}\mathbf{a}_1 & x_{12}\mathbf{a}_2 & \ldots & x_{1n}\mathbf{a}_n \\ x_{21}\mathbf{a}_1 & x_{22}\mathbf{a}_2 & \ldots & x_{2n}\mathbf{a}_n \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1}\mathbf{a}_1 & x_{m2}\mathbf{a}_2 & \ldots & x_{mn}\mathbf{a}_n \end{pmatrix}.$$

The following lemma describes how the parity check matrix A for a linear code can be extended with new rows in such a way that the minimum distance increases. A proof of this result is given by Roos (cf. [3]).

Lemma. If $d_A \geq 2$ and every $m \times (m + d_A - 2)$ submatrix of X has full rank, then $d_{A(X)} \geq d_A + m - 1$.

Definition 2. *A set $M = \{\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_l}\}$ of zeros of the polynomial $x^n - a$ in $K = \mathrm{GF}(q^m)$ will be called a consecutive set of length l if a primitive $n-$th root of unity β and an exponent i exist such that $M = \{\beta_i, \beta_{i+1}, \ldots, \beta_{i+l-1}\}$, with $\beta_s = \sqrt[n]{a}\beta^s$. More generally, one says that M is a consecutive set of $n-$th roots of unity if there is some primitive $n-$th root of unity β in K such that M consists of consecutive powers of β.*

Let $N = \{\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_t}\}$ be a set of zeros of the polynomial $x^n - a$. The $t \times n$ matrix over K the j_s-th row of which equals $(\alpha_{j_s}, \alpha_{j_s}^2, \ldots, \alpha_{j_s}^n)$ will be

denoted by U_N. (If N is a set of $n-$th roots of unity, the analogous matrix over K will be denoted as H_N.) So, it is clear that U_N is a parity check matrix for the constacyclic code C having N as a set of zeros for $h(x)$. Let C_N be the constacyclic code over K with U_N as parity check matrix, and let this code have minimum distance d_N. So, the minimum distance of C is at least d_N, since C is a subfield code of C_N (cf. [3]).

Theorem 4. *If N is a nonempty consecutive set of zeros of the polynomial $x^n - a$ and if M is a set of $n-$th roots of unity such that $|\overline{M}| < |M| + |N|$ for some consecutive set $\overline{M}$ containing M, then $d_{MN} \geq |M| + |N|$.*

Proof. Let us define $A := U_N$ and $X := H_M$. Then one may easily verify that $A(X) = U_{MN}$, where MN is the set of all products mn, $m \in M$, $n \in N$. Since N is a nonempty consecutive set, $d_N = |N| + 1 \geq 2$. Hence, the assertion of the theorem follows from the lemma above if in the matrix H_M every $|M| \times (|M| + |N| - 1)$ submatrix has full rank. It is sufficient to show that this is the case if $|\overline{M}| < |M| + |N|$ for some consecutive set $\overline{M} \supseteq M$. Observe that H_M is a submatrix of $H_{\overline{M}}$, and that in $H_{\overline{M}}$ every $|\overline{M}| \times |\overline{M}|$ submatrix is nonsingular, since the determinant of such a matrix is of Vandermonde type. So, it immediately follows that every $|M| \times |\overline{M}|$ submatrix of H_M has full rank. Since $|\overline{M}| < |M| + |N|$, this implies that every $|M| \times (|M| + |N| - 1)$ submatrix of H_M has full rank, which proves the theorem. □

References

[1] D. Radkova, A. Bojilov, A. J. van Zanten, Cyclic codes and quasi-twisted codes: an algebraic approach, Rep. MICC 07-08 Univ. Maastricht, 2007

[2] C. Roos, A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound, *J. Combin. Theory* Ser. A, 33, 1982, 229-232.

[3] C. Roos, A new lower bound for the minimum distance of a cyclic code, *IEEE Trans. Inform. Theory* 29, 1983, 330-332.