More on the minimum distance of cyclic codes

de Rooij, P.J.N.; van Lint, J.H.

Published in:
IEEE Transactions on Information Theory

DOI:
10.1109/18.61137

Published: 01/01/1991

Citation for published version (APA):
More on the Minimum Distance of Cyclic Codes

P. J. N. de Rooij and J. H. van Lint

Abstract—It was recently shown that the so-called Jensen bound is generally weaker than the product method and the shifting method introduced by van Lint and Wilson. We show that the minimum distance of the two cyclic codes of length 65 for which it is known that the product method does not produce the desired result can be proved using Jensen's method with some adaptations.

Index Terms—Minimum distance, 2-D-cyclic code, concatenated code, shifting.

I. INTRODUCTION

In 1986 a new method for calculating the minimum distance of cyclic codes was developed by J. H. van Lint and R. M. Wilson [4]. Their paper contained two related methods: a matrix-product method and a method called “shifting.” Previous bounds, such as the BCH bound, the Hartmann–Zemor bound and the method developed by Roos are all special cases of this method. It turned out that the minimum distance of all cyclic codes of length < 63 (all codes in that paper are binary codes) with two exceptions can be determined using this method. The number of cyclic codes of length 63 is exceedingly large, and it is not clear how many of them can be handled by this method. For the codes of length 65, it was shown by M. H. M. Smid [7] that again all but two of these codes can be handled by the product method. The first purpose of this correspondence is to determine the minimum distance of these two exceptional codes (for which presently only computer searches have established the minimum distance).

In 1985 J. M. Jensen [3] developed another method for calculating the minimum distance of cyclic codes based on the idea of Berlekamp and Justesen of representing these codes as two-dimensional cyclic codes. Jensen's method was recently analyzed by the first author in his master's thesis [6] with the rather disappointing result that the method is usually weaker than shifting. (However, the amount of computation required for shifting is often quite large.) The second purpose of this correspondence is to show that, with some extra tricks, Jensen's method is strong enough to handle the two cyclic codes of length 65 that could not be done by the product method. Clearly, it is not of great importance to consider two isolated examples of length 65, but the method of this correspondence can be used in many other situations e.g., for Blokh-Zyablov codes [2]. Hence, explaining the method that we use in our examples in Section III is our main goal.

In the following, we shall use terminology, notation, and results from the paper by Jensen on the structure of cyclic codes. We assume that the reader is familiar with that paper and also with the product method. In Section II we only briefly review what we shall need in the sequel.

II. DEFINITIONS

Let G be an Abelian group of order nN that is the direct product of two cyclic subgroups G₁ and G₂ of order n resp. N, that is, G = G₁ x G₂ contains (w.l.o.g.) the elements \( \{x^i | 0 \leq i \leq n-1\} \) and \( \{y^j | 0 \leq j \leq N-1\} \) where \( x^n = y^N = 1 \). Furthermore let q be a prime power and gcd(nN,q) = 1.

Definition 2.1: The group algebra \( F_qG \) is the ring (with unity) consisting of all (formal) polynomials

\[
e(x,y) = \sum_{i=0}^{n-1} \sum_{j=0}^{N-1} c_{ij} x^i y^j, \quad \text{where } c_{ij} \in F_q.
\]

Definition 2.2: A 2-D cyclic code of size n by N over the alphabet \( F_q \) is an ideal in \( F_qG \).

We represent a codeword by the corresponding polynomial or by the \( n \times N \) matrix \( [c_{ij}] \). We shall not distinguish between these notations.

If gcd(n,N) = 1, then the Chinese remainder theorem shows that every element \( x^iy^j \) is a power of \( Z = xy \), so \( Z \) is a generator of \( G \). Thus \( G \) is cyclic.

Using this, the following can be derived (cf. [1]).

Theorem 2.3: If gcd(n,N) = 1 and G and q are as above, then a 2-D cyclic code \( C \) in \( F_qG \) is cyclic.

The converse is true as well.

Theorem 2.4: A cyclic code of length \( nN \), with gcd(n,N) = 1 is 2-D cyclic.

In the following, \( \theta \) will denote a minimal cyclic code and we shall use the symbol \( \theta \), for the idempotent of this code. It is well
known that the code is isomorphic to the field of the same cardinality. Berlekamp and Justesen have shown [1] that the concatenation of a minimal cyclic inner code $\langle \theta_i \rangle$ of dimension $k$ over $F_p$ and a cyclic outer code $\langle \theta \rangle$ over $F_q$ is a $(2-D)$ cyclic code. We denote this concatenation by $\langle \theta \rangle \circ \langle \theta_i \rangle$. For the mapping from a word in the inner code to the corresponding letter in the outer code, we choose the isomorphism $\phi_i : \langle \theta \rangle \rightarrow F_q$ given by $\phi_i(a(x)) = \beta_\theta(a)$, where $\beta_\theta$ is a nonzero of the code. Denote the inverse of $\phi_i$ by $\phi_i^{-1}$.

Notice that $\psi(1)$ is equal to the idempotent $\theta_i(x)$ of the inner code. Denote the mapping from a word in $\mathbb{F}_q$ to a matrix in $\langle \theta \rangle \circ \langle \theta_i \rangle$, as $\Psi_i$; denote the inverse mapping as $\Phi_i$. ($\Psi_i$ is an injective homomorphism $F_q \rightarrow G \rightarrow F_q$.)

Jensen has shown that a 2-D cyclic code in $F_qG$ can be decomposed in a unique way into the direct sum of such concatenated codes $\langle \theta \rangle \circ \langle \theta_i \rangle$. (For proofs see [3].) Before we give this theorem, we introduce some notation. We have several inner codes $\langle \theta_i \rangle$ now; so, we have several fields $F_q$ too. From now on we will denote the field $F_q$ corresponding to $\langle \theta_i \rangle$ by $F_q$. Let $\Theta = \Phi_i(1)$. Then $\langle \Theta \rangle = \Psi_i(F_qG)$). Jensen’s result is as follows.

**Theorem 2.5:** Let $\mathcal{E} \subseteq F_qG$ be a 2-D cyclic code. Then the following holds:

1) $\mathcal{E} = \bigoplus_{i \in I} \langle \theta_i \rangle \subseteq \langle \Theta \rangle$ and $I = \{ s \in \mathcal{E}, \theta_i \neq 0 \};$
2) $\mathcal{E} = \bigoplus_{i \in I} \langle \theta_i \rangle \circ \langle \theta_i \rangle$, where $\theta_i = \Phi_i(1).$

In this way we can construct a 2-D cyclic code too, as follows from the next theorem.

**Theorem 2.6:** Let there be given a number of minimal cyclic codes $\langle \theta_i \rangle$ of dimension $k_i$ in $F_{q_i}G_i$ and cyclic codes $\langle \theta \rangle$ in the inner field $\mathbb{F}_q$. Let $\mathcal{E} = \bigoplus_{i \in I} \langle \theta_i \rangle \subseteq \langle \Theta \rangle$, a 2-D cyclic code of dimension $\sum_{i \in I} k_i \dim(\mathbb{F}_i)$. We can easily derive a lower bound on the minimum distance of a (2-D) cyclic code from the decomposition into concatenated codes. Denote the minimum distances of the composing codes as $d_{\max} = \max_{i \in I} \langle \theta_i \rangle \circ \langle \theta_i \rangle$, $d_{\min} = \min_{i \in I} \langle \theta_i \rangle \circ \langle \theta_i \rangle$. Take a word $\mathcal{E} \subseteq \langle \theta \rangle \circ \langle \theta_i \rangle$, where $\mathcal{E} \subseteq \langle \theta \rangle \circ \langle \theta_i \rangle$. Now let $I = \max(s \in \mathcal{E}, \theta_i \neq 0)$. Now $\mathcal{E}$ has at least $d_{\min} = \min_{i \in I} \langle \theta_i \rangle \circ \langle \theta_i \rangle$. With this we find the following theorem.

**Theorem 2.7:** Let $\mathcal{E} = \bigoplus_{i \in I} \langle \theta_i \rangle \circ \langle \theta_i \rangle$, with $\mathcal{E} \subseteq F_qG_i$, for all $\theta_i \in I$. Then the minimum distance $d$ of $\mathcal{E}$ satisfies:

$$d \geq \min_{l \in \mathcal{E}} \{d_{l}, d_{\min} \mid l \in I \}.$$  

The value of $d$ found in this theorem still depends on the ordering of the idempotents $\theta_i$, i.e., the ordering of the indices $x$ as elements of $I$. We find the maximal value using the ordering of the $\theta_i$ that satisfies $d_{l_{\min}} \leq d_{l_{\min}} \leq \cdots \leq d_{l_{\max}}$, where $d_{\max}$ denotes $\max(s \in \mathcal{E}, \theta_i \neq 0)$. When applying Theorem 2.7 we will always assume that the composing codes are ordered in this way.

From now on we choose as index for a primitive idempotent $\theta$, the smallest value of $s$ satisfying $\theta(\beta^{s}) \neq 0$. So in this notation, if $\beta$ is an $n$th root of unity and $k$ is the smallest positive integer such that $\beta^k = s \text{mod} n$, then $\theta(x) = 1$ is the idempotent of the code with generator $g(x) = (x^{n-1})/(\beta^k - 1)$, where $\beta = \alpha$, $\gamma = \alpha^s$. We will not renumber explicitly if we use Theorem 2.7. Finally, we introduce the Jensen bound.

**Definition 2.8:** The Jensen bound is the estimate for the minimum distance of a cyclic code of length $nN$ found by using Theorem 2.6 and Theorem 2.7.

The value of the Jensen bound depends on the choice of $n$ and $N$ (given $nN$), not on the choice of $Z$, the primitive $n$th root of unity $a$, or the $\beta_i$. Finally, the following theorem gives a correspondence between the nonzeros of a 2-D cyclic code consisting of one concatenated code only, and the nonzeros of its inner and outer code. For a proof see [5], Chapter 18.

**Theorem 2.9:** A pair $(\beta, \gamma)$ of an $n$th and an $N$th root of unity is a nonzero of the 2-D cyclic code $\langle \theta \rangle \circ \langle \theta \rangle$ if and only if $\beta \neq \beta_i$ and $\gamma \neq \gamma_i$, where $\beta_i$ is the nonzero of $\theta_i$ that is used in the definition of $\theta_i$, and $\gamma_i$ is a nonzero of $\theta_i$.

The nonzeros of a 2-D cyclic code can be found by taking the union of the nonzeros of its components.

**III. Application of the Jensen Bound**

The Jensen bound is based on the fact that any nonzero column in a matrix, representing a codeword of a 2-D cyclic code, has weight at least equal to the minimum distance of the inner code. Let us call such a column with minimal positive weight a “light” column and a column with larger weight “heavy.” Clearly, a stronger assertion than Theorem 2.7 can be made if one can show that in the representation of codewords of minimal weight, heavy columns must occur. As an introduction to our method we give the following example.

**Example 3.1:** Let $\beta$ be a primitive fifth root of unity in $F_{10}$. In our notation of Section II, $\beta_i \neq \beta$. Let $\theta_i$ be the primitive idempotent of the binary even weight code of length 5 (i.e., the code consisting of all the words of even weight) and let $\mathcal{E}_i$ be a cyclic code over $F_{10}$. Then the minimum distance of the code $\mathcal{E} = \langle \theta \rangle \circ \langle \theta_i \rangle$ is equal to $2\langle \theta \rangle \circ \langle \theta_i \rangle$ if and only if there is a word $b$ of minimum weight in $\mathcal{E}_i$, such that none of its symbols is in $\{1, \beta, \beta^2, \alpha, \alpha^2\}$. In order to prove this, we first observe that there are only five words of weight 4 in $\langle \theta \rangle$, and all other nonzero words have weight 2. The five heavy words are $x'\theta_1$, $x'\theta_2$, $x'\theta_3$. From this it immediately follows that a word $\beta' = 0, \cdots, 4$, results in a column of weight 4, and all other nonzero letters (field elements of $F_{10}$ that are not fifth roots of unity) give rise to a column of weight 2.

Remark: We have in fact shown that the weight of a word $\psi \in \langle \theta \rangle \circ \langle \theta_i \rangle$ is $4(|\{b : |b| = 1\} = 2 \{b : |b| \neq 0, 1\}$).

We now treat cyclic codes of length 65. In the notation of Section II, we take $n = 5$, $N = 13$. The two minimal cyclic codes of length 5 are the repetition code $\langle \theta \rangle$, isomorphic to $F_5$, and the even weight code $\langle \theta \rangle$, isomorphic to $F_5$. Let $\gamma$ be a primitive 13th root of unity in an extension field of $F_5$. The minimal cyclic codes of length 13 over $F_5$ are the codes $M_5$, with $\gamma$ a nonzero (i = 0, 1, 2, 4, 7), the only binary cyclic codes of length 13 are the repetition code and the even weight code. We denote a primitive element of $F_{10}$ by $\xi$ and we define the trace function $tr : F_{10} \rightarrow F_5$ by

$$tr(\eta) = \eta + \eta^4, \quad (\eta \in F_{10}).$$

Furthermore, if $\epsilon = \epsilon_{0, \cdots, \epsilon_{12}}$, then we shall write $tr(\epsilon)$ for the word with coordinates $tr(\epsilon_i)$. Let $a$ be a primitive 6th root of unity (in $F_{10}$). The minimal polynomial of $a^4$ is denoted by $m_i$. We have $x^{60} - 1 = m_i \cdot m_i \cdot m_i \cdot m_i \cdot m_i \cdot m_i$. We take $\beta = a^{4} = \gamma^4$.

The two cyclic codes of length 65 for which the method of van Lint and Wilson does not work have generators $m_i \cdot m_i \cdot m_i \cdot m_i \cdot m_i$, and $m_i \cdot m_i \cdot m_i$. By computer search the minimum distances of these codes were found to be 16, respectively 10. We shall now prove, using Jensen’s method, that the minimum distances are at least this large (equality is easily established since in the proofs we find codewords of the specified weights).

**Example 3.2:** Let $\mathcal{E}_i = \langle m_i \cdot m_i \cdot m_i \cdot m_i \cdot m_i \rangle$. The nonzeros of $\mathcal{E}_i$ are the zeros of $m_i \cdot m_i \cdot m_i$. We claim that $\mathcal{E}_i = \langle \Theta \rangle \sum \langle M_5 \oplus M_5 \rangle$. By Theorem 2.9, the nonzeros of the concatenated code...
of length 39 has minimum distance 12 and from the Jensen cyclic code of length 39 with generator \( z_0 \) set contains of length 13 over \( S \).

The outer code bound we find that the distance is at least \( 2d(z_0) \).

In Case 1, let \( w(t) = b \). Let \( S = \{ 1, 2, 3, 4 \} \subseteq F_{10} \). We shall write \( \omega = z \). The mapping \( \tau \) maps \( \beta \) to its subfield subcode over \( F_2 \). This is in fact a quadratic residue code of length 13 over \( F_2 \). The nonzero elements of \( F_{10} \) occur in the sets \( z(S_10) \leq i \leq 4 \). The nonzero elements of \( F_{10} \) with trace 0 form the set \( S \). Since \( \tau(b) = 7 \), there must be two nonzero symbols in \( b \) corresponding to the same value of \( i \). By considering a suitable multiple of \( b \), we may assume that this is \( i = 0 \). It follows that \( \tau(b) \) has weight \( \leq 5 \), which implies that \( \tau(b) = 0 \).

So all seven nonzero symbols of \( b \) must be in \( S \). Since the sum of these seven symbols is 0, all three elements of \( S \) must occur. From this we see that any word of weight 7 has as its nonzero symbols all three elements of one of the sets \( S_5 \), and exactly one of these elements is heavy.

In Case 2, let \( w(t) = b \). By a suitable multiplication we can see to it that at least one nonzero coordinate is in \( S \). By the same argument as above, this implies that \( \tau(b) = 0 \), i.e. all nonzero symbols are in \( S \). Now we are done if we can show that each element of \( S \) occurs twice. Since the sum of the nonzero symbols is 0, the only other possibilities are the following.

1) All nonzero symbols are the same. In this case there would be a word of weight 6 in the subcode over \( F_2 \), but this code is \( [0] \). So this is impossible.

2) Two symbols of \( S \) occur, one twice and the other four times. In that case \( \beta \) contains a word \( b(y) \) of the form

\[
\begin{align*}
b(y) &= \omega p_1(y) + \omega^2 p_2(y), \\
p_1(y) &= 1 + y', \\
p_2(y) &= y^2 + y + y'.
\end{align*}
\]

If we write

\[
b(y) = \omega^2 p_2(y) + \omega p_1(y),
\]

then \( b \) is in the quadratic residue code with zeros \( \{ y' \} \subseteq \{ 0, 2, 5, 6, 7, 8, 11 \} \) and hence \( b(y) \) \( b(y) \) must be 0. However,

\[
b(y) = p_1(y) + p_2(y) + p_3(y),
\]

a sum of 14 powers of \( y \), namely, \( y_1 \) with

\[
j = 0, 2, 1, 2, a, 2b, 2c, 2d, a, b, c, d, a + i, b + i, c + i, d + i.
\]

Since these powers must add up to 0, each exponent must occur an even number of times. It is a simple exercise to show that this is impossible (without loss of generality one can assume that \( i = 1 \); the second occurrence of 0 forces \( a = -1 \); since \( 2i = 2 \), we may assume \( b = 2 \), etc.). So again we have an impossibility.

We have shown that indeed \( d \geq 16 \).

Example 3.3: Let \( C_2 = (m_1, m_2, m_3) \). We shall show that the minimum distance of this code is at least 10. The nonzero of \( C_2 \) are those of \( C_3 \), and also the zeros of \( m_3(x) \), i.e., all 12th roots of unity \( \neq 1 \) (powers of \( y \)). Hence

\[
C_2 = C_3 \ominus (\theta_0) \ominus M.
\]

where \( M \) is the even weight code of length 13. So the matrices of the last component in the direct sum have columns of zeros and an even number of columns with ones (i.e., only ones).

We saw in Example 3.2 that the matrices of \( (\theta_0) \ominus M \) have

1) six columns, exactly two of which are heavy;
2) seven columns, at least two of which are light;
3) or at least eight nonzero columns.

In Case 1, adding a matrix of \( (\theta_0) \ominus M \) can change a heavy column into one of weight 1, whereas a light column can keep weight 2 or get weight 3. So we obtain a word with weight at least \( 2 + 1 + 4 \cdot 2 = 10 \).

In Case 2, we find a matrix of weight at least \( 5 \cdot 1 + 3 + 2 = 10 \), since not all seven columns can be altered.

The only way to find a matrix of weight \( < 10 \) in case (3) is from a word \( b \) in \( C_3 \) with eight heavy columns. If this were possible, then without loss of generality two of these heavy columns would correspond to the symbol 1, the only heavy symbol with trace 0. As before, \( \tau(b) = 0 \) is impossible and therefore \( \tau(b) \) is a word of weight 6 in the code \( \beta \), with all its nonzero elements equal to \( \omega \) or \( \omega^2 \). We saw in Example 3.2 that such words do not exist.

IV. CONCLUSION

Our methods show that the Jensen bound can be a powerful tool for the analysis of cyclic codes if it is possible to obtain information on the distribution of symbols in low-weight code-words of codes over extensions of \( F_2 \). In his paper Jensen gives several examples of codes that are better than BCH codes. For all of them, the bound as given in Definition 2.8 is used for the analysis. So, it is possible that an extension of his ideas by the methods of Example 3.2 could yield even better codes.

The first author has applied the ideas of this correspondence to several other binary cyclic codes. For those codes, shifting also yields the minimum distance but it was often much easier to use the concatenated structure.

REFERENCES


