

 Open access • Journal Article • DOI:10.1109/18.75250

## Repeated-root cyclic codes — Source link

J.H. van Lint





**Institutions:** Philips

**Published on:** 01 Mar 1991 - IEEE Transactions on Information Theory (IEEE)

**Topics:** Linear code, Block code, Expander code, Hamming code and Cyclic code

Related papers:

- [On repeated-root cyclic codes](#)
- [Cyclic and negacyclic codes over finite chain rings](#)
- [Polynomial weights and code constructions](#)
- [The  \$\mathbb{Z}/4\$ -linearity of Kerdock, Preparata, Goethals, and related codes](#)
- [On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions](#)

Share this paper:    

View more about this paper here: <https://typeset.io/papers/repeated-root-cyclic-codes-87f83qkupf>

## Repeated-root cyclic codes

**Citation for published version (APA):**

van Lint, J. H. (1991). Repeated-root cyclic codes. *IEEE Transactions on Information Theory*, 37(2), 343-345.  
<https://doi.org/10.1109/18.75250>

**DOI:**

[10.1109/18.75250](https://doi.org/10.1109/18.75250)

**Document status and date:**

Published: 01/01/1991

**Document Version:**

Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

**Please check the document version of this publication:**

- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

[Link to publication](#)

**General rights**

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

[www.tue.nl/taverne](http://www.tue.nl/taverne)

**Take down policy**

If you believe that this document breaches copyright please contact us at:

[openaccess@tue.nl](mailto:openaccess@tue.nl)

providing details and we will investigate your claim.

# Correspondence

## Repeated-Root Cyclic Codes

J. H. van Lint

**Abstract**—In the theory of cyclic codes, it is common practice to require that  $(n, q) = 1$ , where  $n$  is the word length and  $\mathbb{F}_q$  is the alphabet. This ensures that the generator  $g(x)$  of the cyclic code has no multiple zeros (= repeated roots). Furthermore it makes it possible to use an idempotent element as generator. However, much of the theory also goes through without the restriction on  $n$  and  $q$ . Recently, the author was asked whether dropping the restriction could produce any good codes or that they would always be bad (in some sense), in which case making the restriction right after the definition, as most authors do, would be justified. This question led to the results below. We shall show that a binary cyclic code of length  $2n$  ( $n$  odd) can be obtained from two cyclic codes of length  $n$  by the well known  $|u|u + v|$  construction. This leads to an infinite sequence of optimal cyclic codes with distance 4. Furthermore, it shows that for these codes low complexity decoding methods can be used. The structure theorem generalizes to other characteristics and to other lengths. Independently, Castagnoli *et al.* have studied the same question. Some of their results are similar to these results, but their methods are different. Some comparisons of the methods using earlier examples are also given.

**Index Terms**—Binary cyclic codes of even length, shortened Hamming codes.

### I. BINARY CYCLIC CODES OF LENGTH $2n$ ( $n$ ODD)

Let  $n$  be odd and  $x^n - 1 = f_1(x)f_2(x) \cdots f_t(x)$  the factorization of  $x^n - 1$  into irreducible factors in  $\mathbb{F}_2[x]$ .

We define  $g_1(x) := f_1(x) \cdots f_k(x)$ ,  $g_2(x) := f_{k+1}(x) \cdots f_t(x)$ , where  $k < l < t$ . Let  $r_1 := \deg g_1$ ,  $r_2 := \deg g_2$ .

Let  $C_1$  be the cyclic code of length  $n$  and dimension  $n - r_1$  with generator  $g_1(x)$ , and let  $C_2$  be the cyclic code of length  $n$  and dimension  $n - r_2$  with generator  $g_2(x)$ , and let  $d_i$  be the minimum distance of  $C_i$  ( $i = 1, 2$ ). Clearly  $d_2 \geq d_1$ .

We are interested in the cyclic code  $C$  of length  $2n$  and dimension  $2n - r_1 - r_2$  with generator  $g(x) := g_1^2(x)g_2(x)$ . We claim that this code has the following structure:

Let  $a = (a_0, a_1, \dots, a_{n-1}) \in C_1$  and  $c = (c_0, c_1, \dots, c_{n-1}) \in C_2$ . Define  $b := a + c$ . Since  $n$  is odd, we can define words that belong to  $C$  by

$$w := (a_0, b_1, a_2, \dots, b_{n-2}, a_{n-1}, b_0, a_1, \dots, a_{n-2}, b_{n-1}),$$

and in this way we find *all* words of  $C$ . The last assertion is a consequence of dimension arguments. We prove the first assertion as follows. Write

$$\begin{aligned} a(x) &= a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \\ &= (a_0 + a_2x^2 + \cdots + a_{n-1}x^{n-1}) \\ &\quad + x(a_1 + \cdots + a_{n-2}x^{n-3}) \\ &= a_e(x^2) + xa_o(x^2), \end{aligned}$$

Manuscript received December 19, 1989.

The author is with Philips Research Laboratories, P.O. Box 80000-5600 JA, Eindhoven, The Netherlands and the Department of Mathematics and Computing Science, Eindhoven University of Technology, Eindhoven, The Netherlands.

IEEE Log Number 9041643.

and analogously for  $c(x)$  and  $b(x)$ . We then have the following two (equivalent) representations for the polynomial  $w(x)$  corresponding to the codeword  $w$ :

$$w(x) = \{a_e(x^2) + x^{n+1}a_o(x^2)\} + \{xb_o(x^2) + x^n b_e(x^2)\} \quad (1.1)$$

and

$$w(x) = \{a(x) + x(x^n + 1)a_o(x^2)\} + \{b(x) + (x^n + 1)b_e(x^2)\}. \quad (1.2)$$

Both terms in (1.2) are divisible by  $g_1(x)$ . From (1.1) we see that the first term only contains even powers of  $x$ , the second one only odd powers of  $x$ . Since  $g_1(x)$  has no multiple factors, this implies that both terms are actually divisible by  $g_1^2(x)$ .

From (1.2) we find

$$w(x) = (x^n + 1)a(x) + c(x) + (x^n + 1)c_e(x^2) \quad (1.3)$$

in which every term is divisible by  $g_2(x)$ .

Since  $b = a + c$ , the word  $w$  is a permutation of the word  $|a|a + c|$ , (cf. [4, p. 76]). We have proved the following theorem.

**Theorem 1:** Let  $C_1$  be a binary cyclic code of length  $n$  (odd) with generator  $g_1(x)$ , and let  $C_2$  be a binary cyclic code of length  $n$  with generator  $g_1(x)g_2(x)$ . Let  $d_i$  be the minimum distance of  $C_i$ ,  $i = 1, 2$ . Then the binary cyclic code  $C$  of length  $2n$  with generator  $g_1^2(x)g_2(x)$  is equivalent to the  $|u|u + v|$  sum of  $C_1$  and  $C_2$ . Therefore  $C$  has minimum distance  $\min\{2d_1, d_2\}$ .

**Example 1:** Take  $n = 7$ . We have

$$x^7 - 1 = (x^3 + x + 1)(x^3 + x^2 + 1)(x + 1).$$

Define  $g_1(x) := (x^3 + x + 1)$ ,  $g_2(x) := (x + 1)$ . Then

$$a(x) := g_1(x) = 1 + x + x^3 = 1 + x(1 + x^2),$$

$$c(x) := g_1(x)g_2(x) = 1 + x^2 + x^3 + x^4 = 1 + x^2 + x^4 + x(x^2);$$

so,  $a = (1101000)$  and  $b = (0110100)$ . We find

$$w = (11000000111100),$$

i.e.,

$$\begin{aligned} w(x) &= 1 + x + x^8 + x^9 + x^{10} + x^{11} \\ &= (1 + x + x^3)^2(1 + x)(1 + x^2 + x^4). \end{aligned}$$

It was shown by Best and Brouwer [1] that the three times shortened binary Hamming codes are optimal. In fact, they showed that, if  $A(n, d)$  is the maximal cardinality of binary codes with length  $n$  and minimum distance  $d$ , then

$$A(m + 1, 4) = A(m, 3) \leq 2^m / (m + 4 - i),$$

$$\text{if } m \equiv i \pmod{4}, \quad 0 \leq i \leq 3. \quad (1.4)$$

We now consider the even-weight subcode of a shortened Hamming code. With  $m = 2^l - 1$  we have an  $[m - 1, m - l - 2, 4]$  code, which is optimal by (1.4). The following theorem gives a, perhaps surprising, property of these optimal codes.

**Theorem 2:** The even weight subcode of a shortened binary Hamming code is cyclic (for a suitable ordering of the symbols).

*Proof:* It is not difficult to see that it makes no difference on which position the code is shortened (all resulting codes are equivalent). Let  $n = 2^s - 1$ . Let  $m_1(x)$  denote the minimal polynomial of a primitive element  $\alpha$  of  $\mathbb{F}_{2^s}$ . Then  $m_1(x)$  is the generator polynomial of the  $[n, n-s]$  Hamming code and  $(x+1)m_1(x)$  is the generator polynomial of the corresponding even weight subcode. In Theorem 1 we take  $g_1(x) = (x+1)$  and  $g_2(x) = m_1(x)$ . We then find a cyclic code  $C$  of length  $2n$ , dimension  $2n-s-2$  with minimum distance 4. It follows from the  $|u|u+v|$  construction that all weights in  $C$  are even. Therefore  $C$  has a parity check matrix with a top row of 1's and all columns distinct. Hence  $C$  is equivalent to the even weight subcode of a shortened Hamming code (see Example 4).  $\square$

A simple decoding method for the  $|u|u+v|$  codes is known. It is in fact an example of the method of Blokh and Zyablov [3]. Besides being simple the method has the advantage that it sometimes corrects error patterns beyond half the minimum distance. Recently, Forney [5] introduced the "squaring construction" of which the  $|u|u+v|$  construction is an example. Forney's trellis decoding method for these codes again provides a low complexity decoder for our cyclic codes of length  $2n$ . This is a possible advantage of these codes.

## II. CYCLIC CODES OF LENGTH $q^n n$ OVER $\mathbb{F}_q$ WITH $(n, q) = 1$

The situation for the general case (mentioned in the title of this section) can be handled in the same way as we did in Section I. However, the generalization of (1.2) and (2.1) below to the general case leads to formulas that show that in the general case the approach used by Castagnoli *et al.* [6] is much easier. So, it is only for lengths  $2n$ ,  $3n$ , and  $4n$  that we really gain some more insight by the generalized  $|u|u+v|$  construction. We illustrate the idea for  $q^r = 3$  and give a brief sketch for  $q^r = 4$ .

Let  $(n, 3) = 1$ . We consider the factorization of  $x^n - 1$  into irreducible factors in  $\mathbb{F}_3[x]$ :

$$x^n - 1 = f_1(x)f_2(x) \cdots f_i(x).$$

We now take  $g_1(x) = f_1(x) \cdots f_k(x)$ ,  $g_2(x) = f_{k+1}(x) \cdots f_i(x)$ , and  $g_3(x) = f_{i+1}(x) \cdots f_m(x)$ . We consider three ternary cyclic codes  $C_i$ , ( $i = 1, 2, 3$ ) of length  $n$  with generator polynomials  $g_1(x)$ ,  $g_1(x)g_2(x)$ , and  $g_1(x)g_2(x)g_3(x)$ . Using the same notation as in the previous section, we denote the dimension of  $C_i$  by  $n - r_i$  and its minimum distance by  $d_i$ . Let  $g(x) := \{g_1(x)\}^3 \{g_2(x)\}^2 \{g_3(x)\}$  be the generator polynomial of a cyclic code  $C$  of length  $3n$ .

A polynomial  $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$  is written as

$$\begin{aligned} a(x) &= (a_0 + a_3x^3 + \cdots) + x(a_1 + a_4x^3 + \cdots) \\ &\quad + x^2(a_2 + a_5x^3 + \cdots) \\ &= a^{(0)}(x^3) + xa^{(1)}(x^3) + x^2a^{(2)}(x^3). \end{aligned}$$

We now use the same idea of stretching this polynomial (= word) to length  $3n$  (as in Section I) as follows. We must distinguish between  $n \equiv 1 \pmod{3}$  and  $n \equiv 2 \pmod{3}$ . We define

$$\bar{a}(x) := \begin{cases} a^{(0)}(x^3) + x^{n+2}a^{(2)}(x^3) + x^{2n+1}a^{(1)}(x^3), & \text{if } n \equiv 1, \pmod{3}, \\ a^{(0)}(x^3) + x^{n+1}a^{(1)}(x^3) + x^{2n+2}a^{(2)}(x^3), & \text{if } n \equiv 2, \pmod{3}. \end{cases}$$

Clearly all monomials in  $\bar{a}(x)$  have an exponent divisible by 3, i.e.,  $\bar{a}(x)$  is the third power of some polynomial. Note that

$$\bar{a}(x) \equiv a(x), \pmod{x^n - 1}$$

and therefore  $f_i(x)|a(x)$  implies that  $f_i^3(x)|\bar{a}(x)$ .

The next step is also a generalization of the idea of Section I. Let  $a \in C_1$ ,  $b \in C_2$ ,  $c \in C_3$ . We generalize the  $|u|u+v|$  construction and form a codeword that is a permutation of  $|a|a-b|a+b+c|$  as follows. We define

$$w(x) := (x^n - 1)^2 \bar{a}(x) + x^n(x^n - 1)\bar{b}(x) + x^{2n}\bar{c}(x), \pmod{(x^{3n} - 1)}. \quad (2.1)$$

This definition ensures that  $g(x)$  divides  $w(x)$ . For example  $g_2^3(x)$  divides the second and third term in (2.1) by the observation just made and  $g_2^2(x)$  clearly divides the first term. A trivial dimension argument shows that we obtain all the words of  $C$  in this way. A generalization of the minimum distance argument of the  $|u|u+v|$  construction shows that the minimum distance  $d$  of  $C$  is equal to  $\min\{3d_1, 2d_2, d_3\}$ . Here we take  $d_3 = \infty$  if  $C_3 = \{0\}$ .

For binary cyclic codes of length  $4n$  ( $n$  odd), one proceeds in the same way. As generalization of (2.1) one finds

$$w(x) = \sum_{m=1}^4 x^{(m-1)n} (x^n - 1)^{4-m} \bar{a}_m(x), \pmod{(x^{4n} - 1)}.$$

The right-hand side is a vector of the form  $(a, a+b, a+c, a+b+c+d)$ , and repeated application of the rule  $wt(x) + wt(y) \geq wt(x+y)$  leads to  $d_{\min} = \min\{4d_1, 2d_2, 2d_3, d_4\}$  in the obvious notation.

*Example 2:* Let  $n = 8$ . We have

$$\begin{aligned} x^8 - 1 &= (x-1)(x+1)(x^2+1)(x^2+x+2)(x^2+2x+2) \\ &= m_0(x)m_4(x)m_2(x)m_1(x)m_5(x), \end{aligned}$$

(where  $m_i(x)$  is the minimal polynomial of  $\alpha^i$ ,  $\alpha$  a primitive element of  $\mathbb{F}_{3^2}$ ). Take  $g_1(x) = m_0(x)$ ,  $g_2(x) = m_1(x)$ , and  $g_3(x) = m_2(x)m_4(x)$ . Then the codes  $C_i$  are  $[8, 7, 2]$ ,  $[8, 5, 3]$ , and  $[8, 2, 6]$  respectively. We find a ternary cyclic code that is a  $[24, 14, 6]$  code. If we compare with BCH codes, then there is a  $[26, 16, 6]$  code that can be shortened to yield the same parameters. Note that there is a  $[24, 12, 9]$  ternary extended quadratic residue code (cf. [4]) while the best we can do to obtain  $d = 9$ , using the construction of this section, is to take  $g_1(x) = m_0(x)m_1(x)$ ,  $g_2(x) = m_2(x)$ , and  $g_3(x) = m_4(x)m_5(x)$ , which yields a code of dimension 8.

Bloemen *et al.* [2] analyzed ternary cyclic codes of length  $3n$  with  $n \leq 8$ . The only "good" code that they found was a  $[24, 20, 3]$  code ( $g_1(x) = 1$ ,  $g_2(x) = m_0(x)$ ,  $g_3(x) = m_1(x)$ ). There is no  $[24, k, d]$  code with  $d = 3$ ,  $k > 20$  or  $k = 20$ ,  $d > 3$  (by the Hamming bound).

We give one more example of the construction of binary cyclic codes of length  $4n$ ,  $n$  odd. This example generalizes Theorem 2. It is also due to Bloemen *et al.*

*Example 3:* Let  $n = 2^s - 1$ . Take as generator for a cyclic code  $C$  of length  $4n$  the polynomial  $g(x) = (x-1)^3 m_1(x)$ . Here  $m_1(x)$  is the minimal polynomial of a primitive element  $\alpha$  of  $\mathbb{F}_{2^s}$ . Using the terminology of previous examples we have  $g_1(x) = 1$ ,  $g_2(x) = (x-1)$ ,  $g_3(x) = 1$ , and  $g_4(x) = m_1(x)$ . The ingredients are now four cyclic codes of length  $n$  with minimum distances 1, 2, 2, 4 respectively. The minimum distance of  $C$  is  $\min\{4 \cdot 1, 2 \cdot 2, 1 \cdot 4\} = 4$ . Let  $s = a + 2$ . We find a binary cyclic  $[2^s - 4, 2^s - s - 5, 4]$  code. This is not bad, since by (1.4) the  $[2^s - 4, 2^s - 4, 3]$  code is optimal.

## III. COMPARISON WITH OTHER METHODS

The ideas and results of the previous sections were discussed with J. L. Massey at a meeting in Oberwolfach in 1989. It turned out that he and some of his students were working on the same problem and that they had several similar results (and the general case) but that their methods were different. He kindly sent a preprint of the paper. Below we shall compare our results and their methods. For more details the reader is referred to Castagnoli *et al.* [6]. There the authors treat repeated-root cyclic codes using parity check matrices that are based on the properties of the so-called *Hasse derivative* of a function.

**Definition:** If  $f(x) = \sum_{i=0}^n f_i x^i \in \mathbb{F}_q[x]$ , then the  $k$ th Hasse derivative  $f^{(k)}(x)$  is defined by

$$f^{(k)}(x) := \sum_{i=k}^n \binom{i}{k} f_i x^{i-k}. \quad (3.1)$$

It is an elementary exercise to prove the following lemma (use (3.1) to generalize Leibnitz's rule).

**Lemma 1:** If  $\alpha$  is a zero of  $f(x)$  in some extension field of  $\mathbb{F}_q$ , with multiplicity  $s$ , then  $\alpha$  is a zero of  $f^{(k)}(x)$  for  $k < s$  but not for  $k = s$ .

Let us see what this lemma shows for some of the examples previously given.

**Example 4:** Consider the code of Theorem 2. The generator has 1 as a zero with multiplicity 2 and  $\alpha$  is a zero with multiplicity 1. This means that if  $c(x) = \sum c_i x^i$  is a codeword, then

$$\sum c_i = 0, \quad \sum i c_i = 0, \quad \text{and} \quad \sum c_i \alpha^i = 0,$$

i.e.,

$$H_1 := \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 0 & 1 & \cdots & 0 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & \cdots & 0 & 1 \\ \alpha^n & \alpha^{n+1} & \cdots & \alpha^{2n-2} & \alpha^{2n-1} \end{pmatrix}$$

is a parity check matrix for  $C$ ; here the second row is obtained by applying the lemma. Note that  $\alpha^n = 1$ . Hence the matrix  $H_1$  consists of all possible columns with a 1 at the top, except for  $(100 \cdots 0)^T$  and  $(110 \cdots 0)^T$ , i.e., the code is indeed equivalent to the even weight subcode of a shortened Hamming code.

**Example 5:** Consider the  $[24, 20, 3]$  ternary code  $C$  mentioned after Example 2. It has as generator  $m_0^2(x)m_1(x)$ . Let  $\alpha$  be a primitive element of  $\mathbb{F}_9$ . By the same argument as in the previous example we find a parity check matrix for this code:

$$H_2 := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 1 \\ 0 & 1 & 2 & \cdots & 0 & 1 & 2 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{21} & \alpha^{22} & \alpha^{23} \end{pmatrix}.$$

So, it is clear that  $C$  is equivalent to a twice shortened  $[26, 22, 3]$  BCH code (the columns of  $H_2$  are all possible  $(1, \xi)^T$  with  $\xi \in \mathbb{F}_{27} \setminus \mathbb{F}_3$ ).

**Example 6:** We have another look at Example 3. The code  $C$  of length  $4n$  has a parity check matrix

$$H_3 := \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \cdots & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & \cdots & 0 & 0 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{4n-4} & \alpha^{4n-3} & \alpha^{4n-2} & \alpha^{4n-1} \end{pmatrix}.$$

Since  $\alpha^n = 1$ , this matrix can be obtained from the generator matrix of the  $[2^s - 1, s]$  simplex code by deleting the three columns  $(100 \cdots 0)^T$ ,  $(010 \cdots 0)^T$ ,  $(110 \cdots 0)^T$  and then adjoining a row of 1's. If we do not adjoin the row of 1's, we see that we obtain the generator matrix of a  $[2^s - 4, s, 2^{s-1} - 2]$  code that meets the Griesmer bound with equality. This is the familiar

anticode construction (cf. [4], pp. 548–549). In our case  $H_3$  generates a  $[2^s - 4, s + 1, 2^{s-1} - 4]$  code (by the same argument as for the anticode construction). This code has the additional property of being cyclic and its minimum distance is only 2 less than the maximal possible value. If we write  $x^n - 1 = (x - 1)m_1(x)r(x)$ , then in the terminology of Section II we have  $g_1(x) = r(x)$ ,  $g_2(x) = m_1(x)$ ,  $g_3(x) = 1$ ,  $g_4(x) = x - 1$ . It follows that the minimum distance of the cyclic code is  $\min\{4 \cdot (2^{s-1} - 1), 2 \cdot (2^s - 1)\}$ , in accordance with what was just stated.

One could ask whether the code meeting the Griesmer bound could also be cyclic. Our formula for the minimum distance, i.e., the minimum of the distances  $4d_1$ ,  $2d_2$ ,  $2d_3$ , and  $d_4$ , would imply that  $d_1 \geq 2^{s-1}$ ,  $d_2 \geq 2^s - 1$ , and similarly for  $d_3$ , while  $d_4 = \infty$ . So  $C_2$  has dimension  $\leq 1$  and then  $C_1$  must have dimension  $> 1$ . This forces  $C_1$  to be the simplex code, but that does not contain the repetition code ( $= C_2$ ) as a subcode. So the answer is no.

## IV. CONCLUSION

We have found that the even weight subcodes of the shortened binary Hamming codes form a sequence of repeated-root cyclic codes that are optimal. In nearly all other cases, one does not find good cyclic codes by dropping the usual restriction that  $n$  and  $q$  must be relatively prime. This statement is based on an analysis for lengths up to 100. Theorem 1 shows why this was to be expected, but it also leads to low complexity decoding methods. This is an advantage (especially for the codes that are not much worse than corresponding codes of odd length).

## ACKNOWLEDGMENT

The author would like to thank E. W. Gaal for bringing this problem to his attention and for many helpful comments.

## REFERENCES

- [1] M. R. Best and A. E. Brouwer, "The triply shortened binary Hamming code is optimal," *Discrete Math.*, vol. 17, pp. 235–245, 1977.
- [2] A. A. F. Bloemen, G. J. J. A. N. van Houtum, and W. F. J. Verhaegh, "Over cyclische codes over alfabet  $\mathbb{F}_q$  en met lengte  $q^k n$ ," Eindhoven Univ. of Technol., Eindhoven, The Netherlands, 1989.
- [3] E. L. Blokh and V. V. Zyablov, "Coding of generalized concatenated codes," *Prob. Inform. Transm.*, vol. 10, pp. 218–222, 1974.
- [4] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North Holland, 1977.

- [5] G. D. Forney, Jr., "Coset codes—Part II," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1152–1187, 1988.
- [6] G. Castagnoli, J. L. Massey, Ph. Schoeller, and N. von Seemann, "On repeated-root cyclic codes," *IEEE Trans. Inform. Theory*, vol. 37, no. 2, pp. 337–342, Mar. 1991.