On the minimum distance of ternary cyclic codes

Citation for published version (APA):

Eupen, van, M. J. M., & van Lint, J. H. (1993). On the minimum distance of ternary cyclic codes. *IEEE Transactions on Information Theory*, 39(2), 409-422. <https://doi.org/10.1109/18.212272>

DOI:

[10.1109/18.212272](https://doi.org/10.1109/18.212272)

Document status and date:

Published: 01/01/1993

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

Take down policy

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

openaccess@tue.nl

providing details and we will investigate your claim.

On the Minimum Distance of Ternary Cyclic Codes

Marijn van Eupen and Jacobus H. van Lint

Abstract—There are many ways to find lower bounds for the minimum distance of a cyclic code, based on investigation of the defining set. Some new theorems are derived. These and earlier techniques are applied to find lower bounds for the minimum distance of ternary cyclic codes. Furthermore, the exact minimum distance of ternary cyclic codes of length less than 40 is computed numerically. A table is given containing all ternary cyclic codes of length less than 40 and having a minimum distance exceeding the BCH bound. It seems that almost all lower bounds are equal to the minimum distance. Especially shifting, which is also done by computer, seems to be very powerful. For length $40 \leq n \leq 50$, only lower bounds are computed. In many cases (derived theoretically), however, these lower bounds are equal to the minimum distance.

Index Terms—Ternary cyclic code, minimum distance, shifting, selforthogonal, contraction.

1. INTRODUCTION

A CYCLIC CODE C of length n over the alphabet $\text{GF}(q)$ ($\gcd(n, q) = 1$) can be characterized as an ideal in the ring $\text{GF}(q)[x]/(x^n - 1)$ with generator $g(x)$ (say), which is a divisor of $x^n - 1$. A codeword of C will be written either as $c(x) \in \text{GF}(q)[x]/(x^n - 1)$ or as the vector c of length n having as i th entry the coefficient of x^i in $c(x)$. If α is a primitive n th root of unity in some extension field of $\text{GF}(q)$, then all zeros of $x^n - 1$ can be written as α^j ($0 \leq j \leq n - 1$). If $g(x)$ is not constant, then $g(x)$ has some zero α^{j_0} since $g(x)$ divides $x^n - 1$. But because $g(x)$ is a polynomial over $\text{GF}(q)$, it also has $\alpha^{qj_0}, \alpha^{q^2j_0}, \dots$ as its zeros (we will say: $m_{j_0}(x)$ divides $g(x)$, where $m_{j_0}(x)$ is the minimal polynomial of α^{j_0} , i.e., the monic polynomial that only has zeros $\alpha^{j_0}, \alpha^{qj_0}, \alpha^{q^2j_0}, \dots$). So we can characterize $g(x)$ (and also C) by the set $G := \{j_0 | m_{j_0}(x) \text{ divides } g(x)\}$ (here we use that $\gcd(n, q) = 1$, and so every zero of $x^n - 1$ (and so every zero of $g(x)$) has multiplicity one). Mostly we will characterize C by its defining set $R := \{j | \alpha^j \text{ is a zero of } g(x)\}$ (and sometimes by $\bar{R}$, which is the set of integers modulo n that are not in R). We define the check polynomial $h_1(x)$ as the reciprocal polynomial of $h(x) := (x^n - 1)/g(x)$ ($h_1(x)$ is the generator polynomial of the dual code). Of course every $c(x) \in C$ has zeros α^j , $j \in R$, and this is the same as saying: c has inner product zero with the vector $(1 \alpha^j \alpha^{2j} \dots \alpha^{(n-1)j})$. So a parity check matrix

of C is

$$M(\{j_1, j_2, \dots, j_t\}) := \begin{pmatrix} 1 & \alpha^{j_1} & \alpha^{2j_1} & \dots & \alpha^{(n-1)j_1} \\ 1 & \alpha^{j_2} & \alpha^{2j_2} & \dots & \alpha^{(n-1)j_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{j_t} & \alpha^{2j_t} & \dots & \alpha^{(n-1)j_t} \end{pmatrix},$$

where $R = (j_1, j_2, \dots, j_t)$ is the defining set of C (we do not require that a parity check matrix has independent rows). For purposes that will become clear soon, we will define, for $I \subset \{0, 1, \dots, n-1\}$, $M(R)_I$ as the submatrix of $M(R)$ consisting of the i th columns of $M(R)$, where $i \in I$. One can see immediately that if R contains a consecutive set of length s , then $M(R)_I$ contains a Vandermonde $s \times s$ submatrix and so $\text{rank}(M(R)_I) = s$, whenever $|I| = s$. So if we define for every codeword $c \in C$ its support I as the set of positions where c is nonzero, then a codeword c with support I , $|I| \leq s$ (i.e., the weight of c ($= \text{wt}(c) := |I|$) is at most s) cannot occur since $M(R)_I$ has full rank. So the minimum distance $d = d(C) := \min_{c \in C} \text{wt}(c)$ is at least $s + 1$. We call this bound the BCH bound (cf. [3], [4]), and we will write $d_{\text{BCH}} = s + 1$, if s is the largest integer having the property that there is a code equivalent to C with a defining set containing a consecutive subset of size s (notice that R depends on the choice of α ; we call two codes equivalent if their defining sets are the same up to multiplication with some integer coprime to n). The first generalization of the BCH bound was given by Hartmann and Tzeng [5]. They prove that if the consecutive sets $\{i + ja, i + 1 + ja, \dots, i + \delta - 2 + ja\}$ ($0 \leq j \leq s$) are contained in R , and if $(a, n) < \delta$, then the minimum distance of the code with defining set R is at least $\delta + s$. Roos [6] generalized this by proving that if the statement is true for sufficiently many (say s') values of j , then the minimum distance is at least $\delta + s' - 1$. A last generalization can be found in [1] and is called the *AB-method*. It says that if $A, B \subset \{0, 1, \dots, n-1\}$ are such that $A + B := \{a + b \bmod n | a \in A, b \in B\}$ is a subset of R , then the code with defining set R has minimum distance at least δ , if $\text{rank}(M(A)_I) + \text{rank}(M(B)_I) > |I|$ for every subset I of $\{0, 1, \dots, n-1\}$ for which $|I| < \delta$.

If C_0 is a subcode of C , then we will write $C_0 \leq C$. If R_0 is the defining set of C_0 , then we must have $R \subset R_0$. Moreover we have: $d(C) \leq d(C_0)$. If $C_0 \leq C$ and $C_0 \neq C$, then we write $C_0 < C$ (and we say: C_0 is a proper subcode of C). A cyclic code C is called minimal if $C \neq \{0\}$ (0 denotes the zero word) and if $\{0\} \leq C_0 < C$ implies that $C_0 = \{0\}$. The generator of a minimal code is $(x^n - 1)/m_j(x)$ for some j .

In Section II, we first give some theorems, that give good lower bounds for the minimum distance. The first one is called *shifting* and turned out to be very powerful. We used

Manuscript received July 8, 1991. This work was presented in part at Coding and Information Theory Conference, Essen, Germany, December 15–17, 1991.

M. van Eupen is with Eindhoven University of Technology, Eindhoven, The Netherlands, HG 987.

J. H. van Lint is with Eindhoven University of Technology, Eindhoven, The Netherlands, BG 335. He is also with Philips Research Laboratories, P.O. Box 80000, 5600 JA Eindhoven, The Netherlands.

IEEE Log Number 9203861.

a computer to compute the shifting bounds and for length less than 40 this bound was for approximately 95% of the codes equal to the minimum distance. Where the shifting bound did not equal the minimum distance we were often (but unfortunately not always) able to find a bound that did equal the minimum distance. Of course for many codes it is possible to find a lower bound more quickly by hand using other theorems than shifting (including the AB-method). But to avoid a long list of tedious examples, we only used other theorems where it was necessary (i.e., where the shifting bound did not equal the minimum distance). The results can be found in Table I.

In Section III, we treat the lengths $40 \leq n \leq 50$. Because shifting is in the worst case exponential in n , the computer could in some cases not find the shifting bound in reasonable time. Fortunately other theorems were powerful enough to find almost all minimum distances. The results can be found in Table II and Table III.

II. LOWER BOUNDS

The technique of *shifting* was introduced in 1986 by Van Lint and Wilson [1]. It gives very good lower bounds for the minimum distance of cyclic codes. We now give a definition of the shifting bound $d_{\text{SHIFT}}(C)$ of a cyclic code C , that is slightly different from the definition in [1], but easier to implement on a computer.

Definition 1: Suppose C is a cyclic code of length n with defining set R . We define the shifting bound $d_{\text{SHIFT}}(C)$ inductively.

- a) If C is a minimal cyclic code and $r_1, r_2, \dots, r_\omega$ is the longest sequence of different integers (mod n) such that
 - 1) $\{r_1 r_2, \dots, r_\omega\} \subset R$,
 - 2) There is a sequence $a_1, a_2, \dots, a_\omega$ such that for all i : $\{a_i + r_1, \dots, a_i + r_{i-1}\} \subset R$ and $a_i + r_i \notin R$ (all additions taken modulo n), then $d_{\text{SHIFT}}(C) = \omega + 1$.
- b) If C is not a minimal code and

$$\bar{d}_{\text{SHIFT}}(C) := \min_{C_0 < C} d_{\text{SHIFT}}(C_0),$$

and $r_1, r_2, \dots, r_\omega$ is the longest sequence of different integers with $\omega \leq \bar{d}_{\text{SHIFT}}(C) - 1$ satisfying conditions 1) and 2) in a), then $d_{\text{SHIFT}}(C) = \omega + 1$.

Theorem 1 (Shifting): Suppose C is a cyclic code with minimum distance d . Then, $d_{\text{SHIFT}}(C) \leq d$.

Proof: By induction w.r.t. the number of irreducible factors in the check polynomial.

- 1) Let C be a minimal code (i.e., there is one irreducible factor in the check polynomial) and $r_1, r_2, \dots, r_\omega$ ($\omega > 0$) a sequence satisfying conditions 1) and 2) in Definition a). Suppose $c(x) \in C$ is of weight ω and has support I . Then, we have for all $1 \leq i \leq \omega$:

$$\begin{aligned} \text{rank}(M(r_1, r_2, \dots, r_i)_I) \\ &= \text{rank}(M(a_i + r_1, a_i + r_2, \dots, a_i + r_i)_I) \\ &= \text{rank}(M(a_i + r_1, \dots, a_i + r_{i-1})_I) + 1 \\ &= \text{rank}(M(r_1, r_2, \dots, r_{i-1})_I) + 1. \end{aligned}$$

The first equality follows from the fact that the rank of a matrix stays invariant under multiplication with $\text{diag}(1, \alpha^{a_i}, \alpha^{2a_i}, \dots, \alpha^{(n-1)a_i})$. To prove the second equality, we recall that

$$\begin{aligned} M(a_i + r_1, \dots, a_i + r_i) \\ &= \begin{pmatrix} 1 & \alpha^{a_i + r_1} & \alpha^{2(a_i + r_1)} & \dots & \alpha^{(n-1)(a_i + r_1)} \\ 1 & \alpha^{a_i + r_2} & & \dots & \alpha^{(n-1)(a_i + r_2)} \\ \vdots & \vdots & & & \vdots \\ 1 & \alpha^{a_i + r_i} & & \dots & \alpha^{(n-1)(a_i + r_i)} \end{pmatrix} \end{aligned}$$

and see that c (the vector of length n corresponding to $c(x)$) is orthogonal to the first $i - 1$ rows of this matrix, but is not orthogonal to the last row (since otherwise $c(x)$ would have $\alpha^{a_i + r_i}$ as a zero, but $a_i + r_i \notin R$ and C is a minimal code, so this would imply that $c(x) \equiv 0$). So the last row is linearly independent from the other rows and the equality follows (notice that we may restrict ourselves to the columns corresponding to support I). The third equality is as obvious as the first one. So $\text{rank}(M(r_1, r_2, \dots, r_\omega)_I) = \text{rank}(M(r_1, r_2, \dots, r_{\omega-1})_I) + 1 = \dots = \text{rank}(M(r_1)_I) + \omega - 1 = \omega$. But this means that $M(r_1, r_2, \dots, r_\omega)_I$ has full rank and so $c(x)$ cannot be a codeword. This implies that $d_{\text{SHIFT}}(C) \leq d$.

- 2) Suppose C is not a minimal code. By induction, we know that $\bar{d}_{\text{SHIFT}}(C) \leq \bar{d}(C) := \min_{C_0 < C} d(C_0)$. Suppose $r_1, r_2, \dots, r_\omega$ satisfy conditions 1) and 2) and $\omega \leq \bar{d}_{\text{SHIFT}}(C) - 1 \leq \bar{d}(C) - 1$. Again let $c(x)$ be a codeword of weight ω (> 0). We see that if $\alpha^{a_i + r_i}$ is a zero of $c(x)$, then $c(x)$ is in a proper subcode of C , since $a_i + r_i \notin R$. This contradicts the fact that $0 < \omega \leq \bar{d}(C) - 1$. So again the last row of $M(a_i + r_1, a_i + r_2, \dots, a_i + r_i)$ is linearly independent of the others and in the same way as in 1), we have $\text{rank}(M(r_1, r_2, \dots, r_\omega)_I) = \omega$ and $c(x)$ cannot be a codeword. $\square$

In some cases shifting is not powerful enough and we have to improve the lower bound, using some other theorems. The first theorem is very useful and is also a consequence of a theorem of McEliece [7].

Theorem 2: Suppose C is a ternary cyclic code of length n with defining set R . Suppose that if $i \notin R$, then $n - i \in R$. Then, C is selforthogonal (or equivalently: $\text{wt}(c(x)) \equiv 0 \pmod{3}$ for all $c(x) \in C$).

Proof: Suppose $c(x), c'(x) \in C$ and α is a primitive n th root of unity. If $c(\alpha^i) \neq 0$, then $i \notin R$ so by assumption $n - i \in R$ and $c'(\alpha^{-i}) = 0$. This is true for all i , so $c(x)c'(x^{-1}) \equiv 0 \pmod{x^n - 1}$. Looking at the coefficient of x^{n-1} in $c(x)c'(x^{-1})$, we get $\langle c(x), c'(x^{-1}) \rangle \equiv 0 \pmod{3}$ ($\langle c(x), c'(x) \rangle$ denotes the inner product of $c(x)$ and $c'(x)$ in $\text{GF}(3)$). So C is selforthogonal (and because $\langle c(x), c'(x) \rangle \equiv \langle c(x), c(x) \rangle + \langle c'(x), c'(x) \rangle + 2\langle c(x) + c'(x), c(x) + c'(x) \rangle$, this is equivalent to saying that all weights in C are divisible by 3). $\square$

Example 11.1: $n = 11$, $R = \{0, 2, 6, 7, 8, 10\}$. This code satisfies the condition in Theorem 2. Here $d_{\text{SHIFT}} = 5$, but because weights are divisible by 3, we have $d \geq 6$.

Example 22.1: $n = 22$, $\bar{R} = \{2, 6, 8, 10, 18\}$. Here, $d_{\text{SHIFT}} = 10$ and by Theorem 2 we have $d \geq 12$.

Example 22.2: $n = 22$, $R = \{0, 4, 7, 11, 12, 13, 14, 16, 17, 19, 20, 21\}$. Here, $d_{\text{SHIFT}} = 7$ and by Theorem 2 we have $d \geq 9$.

Example 22.3: $n = 22$, $R = \{0, 2, 6, 7, 8, 10, 11, 13, 17, 18, 19, 21\}$. Here, $d_{\text{SHIFT}} = 5$ and by Theorem 2 we have $d \geq 6$.

Example 23.1: $n = 23$, $R = \{0, 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$. Here, $d_{\text{SHIFT}} = 7$ and by Theorem 2 we have $d \geq 9$.

Example 26.1: $n = 26$, $\bar{R} = \{1, 2, 3, 6, 9, 18\}$. Here, $d_{\text{SHIFT}} = 13$ and by Theorem 2 we have $d \geq 15$.

Example 26.2: $n = 26$, $\bar{R} = \{1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 19\}$. Here, $d_{\text{SHIFT}} = 8$ and by Theorem 2 we have $d \geq 9$.

Example 26.3: $n = 26$, $\bar{R} = \{1, 2, 3, 4, 6, 7, 9, 10, 11, 12, 18, 21\}$. Here, $d_{\text{SHIFT}} = 8$ and by Theorem 2 we have $d \geq 9$.

Theorem 3 (Orthogonal Subcode Representation): Suppose C and C_0 are ternary cyclic codes of length n generated by

$$g(x) = \prod_{j=1}^s m_{i_j}(x) \quad \text{and} \quad g_0(x) = \prod_{j=1}^t m_{i_j}(x),$$

respectively, where $t > s$. Suppose that if γ is a zero of $g_0(x)/g(x)$, then γ^{-1} is a zero of $g_0(x)$. Then every $c(x) \in C$ can be written as $c(x) = c_0(x) + c_1(x)$, where $c_0(x) \in C_0$ and $c_1(x)$ is an element of the code C_1 , that is generated by

$$g_1(x) = \frac{x^n - 1}{\left(\frac{g_0(x)}{g(x)}\right)}.$$

Moreover, $\text{wt}(c(x)) \equiv \text{wt}(c_0(x)) + \text{wt}(c_1(x)) \pmod{3}$.

Proof: It is easy to see that $\gcd(g_0(x), g_1(x)) = g(x)$. So $g(x) = a(x)g_0(x) + b(x)g_1(x)$ for certain polynomials $a(x), b(x) \in \text{GF}(3)[x]/(x^n - 1)$. So also $c(x) = c_0(x) + c_1(x)$ for certain $c_0(x) \in C_0$ and $c_1(x) \in C_1$. Furthermore $g_0(x)g_1(x^{-1}) \equiv 0 \pmod{(x^n - 1)}$, because if γ is not a zero of $g_0(x)$, then by assumption it is not a zero of $g_0(x^{-1})/g(x^{-1})$ (i.e., γ is a zero of $g_1(x^{-1})$). But now we have $c_0(x)c_1(x^{-1}) \equiv 0 \pmod{(x^n - 1)}$, and this means that $\langle c_0(x), c_1(x) \rangle \equiv 0 \pmod{3}$. So

$$\begin{aligned} \text{wt}(c(x)) &\equiv \langle c(x), c(x) \rangle \\ &\equiv \langle c_0(x) + c_1(x), c_0(x) + c_1(x) \rangle \\ &\equiv \langle c_0(x), c_0(x) \rangle + 2\langle c_0(x), c_1(x) \rangle + \langle c_1(x), c_1(x) \rangle \\ &\equiv \langle c_0(x), c_0(x) \rangle + \langle c_1(x), c_1(x) \rangle \\ &\equiv \text{wt}(c_0(x)) + \text{wt}(c_1(x)) \pmod{3}. \end{aligned} \quad \square$$

Corollary 1: Suppose C is a ternary cyclic code of length n with defining set R not containing 0. Also suppose that the code C_0 corresponding to $R \cup \{0\}$ is selforthogonal. Then, the following holds for all $c(x) \in C$:

- a) $\text{wt}(c(x)) \equiv \text{mod } 3$ or $\text{wt}(c(x)) \equiv n \pmod{3}$,
- b) if $\text{wt}(c(x)) \equiv 0 \pmod{3}$, then $c(x) \in C_0$.

Proof: C_0 is generated by $g_0(x) = (x - 1)g(x)$. The condition in Theorem 3 is satisfied. We see that C_1 is generated by $(x^n - 1)/(x - 1) = x^{n-1} + x^{n-2} + \dots + 1$. So all nonzero codewords in C_1 are of weight n . Applying Theorem 3 and using the fact that $\text{wt}(c_0(x)) \equiv 0 \pmod{3}$ (by assumption), we get a). Moreover, if $\text{wt}(c(x)) \equiv 0 \pmod{3}$, then by Theorem 3 also $\text{wt}(c_1(x)) \equiv 0 \pmod{3}$, i.e., $c_1(x) \equiv 0$ (since $n \not\equiv 0 \pmod{3}$). This proves statement b). $\square$

Example 11.2: $n = 11$, $R = \{2, 6, 7, 8, 10\}$. The conditions in Corollary 1 are satisfied (see Example 11.1). Using shifting we get $d \geq 4$. But because $\text{wt}(c(x)) \equiv 0$ or $\text{wt}(c(x)) \equiv 2$ for all codewords $c(x)$, we have $d \geq 5$.

Example 22.4: $n = 22$, $\bar{R} = \{0, 2, 6, 8, 10, 18\}$. The conditions in Corollary 1 are satisfied (see Example 22.1) and $d_{\text{SHIFT}} = 8$. By Corollary 1 a) we have $d \geq 9$. But Corollary 1 b) says that if a codeword $c(x)$ of weight 9 occurs, then $c(x)$ is an element of the code in Example 22.1, which has $d \geq 12$. This is a contradiction and so $d \geq 10$.

Example 22.5: $n = 22$, $R = \{4, 7, 11, 12, 13, 14, 16, 17, 19, 20, 21\}$. The conditions in Corollary 1 are satisfied (see Example 22.2) and $d_{\text{SHIFT}} = 6$. Using Corollary 1 b) and the fact that the code in Example 22.2 has $d \geq 9$, we get $d \geq 7$.

Example 22.6: $n = 22$, $R = \{2, 6, 7, 8, 10, 11, 13, 17, 18, 19, 21\}$. The conditions in Corollary 1 are satisfied (see Example 22.3) and $d_{\text{SHIFT}} = 5$. Using Corollary 1 a) we get $d \geq 6$.

Example 22.7: $n = 22$, $R = \{4, 7, 12, 13, 14, 16, 17, 19, 20, 21\}$. Here $d_{\text{SHIFT}} = 6$. We wish to apply Theorem 3 to prove that $d \geq 7$. Let the code C with defining set R be generated by $g(x)$. Let C_0 be generated by $g(x)(x - 1)(x + 1)$. Then the condition in Theorem 3 is satisfied. C_0 is the code of Example 22.2 and is selforthogonal and has $d \geq 9$. Furthermore, C_1 is generated by $(x^{22} - 1)/(x^2 - 1)$ and $c_1(x) \in C_1$ can only have a weight divisible by 3 if $c_1(x) \equiv 0$. Now suppose $c(x) \in C$ has weight 6. Write $c(x) = c_0(x) + c_1(x)$, where $c_0(x) \in C_0$ and $c_1(x) \in C_1$. Then by the congruence relation $\text{wt}(c(x)) \equiv \text{wt}(c_0(x)) + \text{wt}(c_1(x)) \pmod{3}$, and from the observations previously made we have $c_1(x) \equiv 0$. So $c(x) \in C_0$, which is a contradiction, since C_0 has no codewords of weight 6. So $d \geq 7$.

Example 23.2: $n = 23$, $R = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$. The conditions of Corollary 1 are satisfied (see Example 23.1) and $d_{\text{SHIFT}} = 6$. Suppose a codeword of weight 6 occurs, then by Corollary 1 b) it is in the code of Example 23.1, which has $d \geq 9$. A contradiction, so $d \geq 7$. Applying Corollary 1 a), we get $d \geq 8$ (this is also shown in [8]).

Example 26.4: $n = 26$, $\bar{R} = \{0, 1, 2, 3, 6, 9, 18\}$. The conditions of Corollary 1 are satisfied (see Example 26.1). Here $d_{\text{SHIFT}} = 12$, but by Corollary 1 b) we must have $d \geq 13$ (see Example 26.1). And by Corollary 1 a) we get $d \geq 14$.

Example 26.5: $n = 26$, $R = \{7, 8, 11, 13, 14, 16, 17, 20, 21, 22, 23, 24, 25\}$. Here $d_{\text{SHIFT}} = 7$, and by Corollary 1 a) we have $d \geq 8$ (see Example 26.2).

Since our codes are ternary, 3 is not a divisor of n . So if n is not too big (say $n \leq 50$), then 2 is a divisor of n , unless n is a prime or $n = 25, 35$, or 49 . But if 2 divides n , then

we can use knowledge of the cyclic codes of length $n/2$ to find better lower bounds.

Definition 2: Suppose C is a ternary cyclic code of length m . Then the code of length $2m$ defined by:

$$C^2 := \{c(x^2) + xc'(x^2) | c(x), c'(x) \in C\}$$

is called the square of C .

It is easy to see that C^2 is a ternary cyclic code again, which has the same minimum distance as C . Moreover the following holds.

Theorem 4: A ternary cyclic code D of length $n = 2m$ is a square, if and only if $R = m + R$, where R is the defining set of D and $m + R := \{m + r \bmod n | r \in R\}$.

Proof: $\Rightarrow$: Suppose $D = C^2$, where C is a cyclic code of length m . Suppose α is a primitive n th root of unity. Then obviously $\alpha^m = -1$ and so $\alpha^{m+i} = -\alpha^i$ for all i . Let $i \in R$. Because D is a square of C , we know that $c(\alpha^{2i}) + \alpha^i c'(\alpha^{2i}) = 0$, for all $c(x), c'(x) \in C$. But then also $c(\alpha^{2i}) - \alpha^i c'(\alpha^{2i}) = 0$, for all $c(x), c'(x) \in C$, since $c'(x) \in C$ implies $-c'(x) \in C$. So we also have $c((-\alpha^i)^2) + (-\alpha^i)c'((-\alpha^i)^2) = 0$, for all $c(x), c'(x) \in C$, and so $-\alpha^i = \alpha^{m+i}$ is a zero of all elements of D . This means that also $m + i \in R$. $\Leftarrow$: Again α is a primitive n th root of unity. We write $\beta := \alpha^2$ and β is a primitive m th root of unity. We shall prove that if $R = m + R$, then $D = C^2$, where C has defining set $R' = R \bmod m$. Take $d(x) \in D$ and write $d(x) + d(-x) = a(x^2)$, $d(x) - d(-x) = xb(x^2)$, where $a(x), b(x) \in \text{GF}(3)[x]/(x^m - 1)$. We have $d(\alpha^i) = d(-\alpha^i) = 0$ for all $i \in R$. So also $a(\alpha^{2i}) = b(\alpha^{2i}) = 0$ for all $i \in R$. But this means that $a(\beta^i) = b(\beta^i) = 0$ for all $i \in R'$ so $a(x), b(x) \in C$ and so $d(x) = 2((d(x) + d(-x)) + (d(x) - d(-x))) = 2(a(x^2) + xb(x^2)) \in C^2$. On the other hand, if $c(\beta^i) = c'(\beta^i) = 0$ for all $i \in R'$ (i.e., $c(x), c'(x) \in C$), then $c(\alpha^{2i}) \pm \alpha^i c'(\alpha^{2i}) = 0$ for all $i \in R'$. But then $c(x^2) + xc'(x^2)$ has zeros α^i and $-\alpha^i = \alpha^{m+i}$ for all $i \in R'$. So $c(x^2) + xc'(x^2) \in D$. $\square$

Notice that the code of Example 22.3 is the square of the code of Example 11.1.

Example 22.8: $n = 22$, $R = \{2, 6, 7, 8, 10, 13, 17, 18, 19, 21\}$. By Theorem 4, this code is the square of the code of Example 11.2. So $d \geq 5$. This also explains why the code has no words of weight 7 or 21.

In the explanation of Table III, the following theorem will be quite useful. We dedicate it to Paris, since it was proved (at night) in a hotel room in that city.

Theorem 5 ("Paris by Night"): Suppose C is a ternary cyclic code of length $n = 2m$ and defining set R . Let C_L be the cyclic code of length n with defining set $R \cup (m + R)$ (the so called lower square of C) and C_U the cyclic code of length n with defining set $R \cap (m + R)$ (the upper square of C). Call d_L and d_U the minimum distances of C_L and C_U , respectively. Then, for the minimum distance d of C , we have $d \geq \min\{d_L, 2d_U\}$.

Proof: Notice that C_L and C_U are ternary cyclic codes. Moreover, using Theorem 4, it is easy to see that C_L and C_U

are squares. Of course $C_L \leq C \leq C_U$. Suppose $c(x) \in C$ and $c(x) \notin C_L$. Then $c(x)$ is nonzero both on the even positions and on the odd positions, since otherwise $c(\alpha^i) = 0$ would imply $c(\alpha^{-i}) = c(\alpha^{m+i}) = 0$, and $c(x)$ would be an element of C_L . But $c(x)$ is also in the square C_U . So $\text{wt}(c(x)) \geq 2d_U$. $\square$

Corollary 2: If $d_L \leq 2d_U$, then $d = d_L$.

Proof: From Theorem 5 we have: $d \geq d_L$. But $C_L \leq C$, so we also have: $d \leq d_L$. $\square$

Example 22.9: $n = 22$, $R = \{2, 4, 6, 7, 8, 10, 12, 13, 14, 16, 17, 18, 19, 20, 21\}$. C_U is the code of Example 22.8 and so $d_U \geq 5$. C_L has defining set $\{0, 11\}$ and so $d_L = 11$. Using Theorem 5, we get: $d \geq 10$.

Theorem 6: Suppose C is a ternary cyclic code of length $n = 2m$ with defining set R . Let C_E be the cyclic code of length n with defining set $R \cup \{j | j \equiv 0 \bmod 2\}$ and C_O the cyclic code of length n with defining set $R \cup \{j | j \equiv 1 \bmod 2\}$. Then every element of C can be written as $(\mathbf{a} + \mathbf{b}, -\mathbf{a} + \mathbf{b})$, where $(\mathbf{a}, -\mathbf{a}) \in C_E$, and $(\mathbf{b}, \mathbf{b}) \in C_O$ ($\mathbf{a}$ and $\mathbf{b}$ are of length m), and

- $\text{wt}((\mathbf{a} + \mathbf{b}, -\mathbf{a} + \mathbf{b})) = 3(m - l_{00}) - \text{wt}(\mathbf{a}) - \text{wt}(\mathbf{b})$, where $l_{00} := |\{i | a_i = b_i = 0\}|$,
- $\text{wt}((\mathbf{a} + \mathbf{b}, -\mathbf{a} + \mathbf{b})) \geq 2 \max\{\text{wt}(\mathbf{a}), \text{wt}(\mathbf{b})\} - \min\{\text{wt}(\mathbf{a}), \text{wt}(\mathbf{b})\}$,
- $\text{wt}((\mathbf{a} + \mathbf{b}, -\mathbf{a} + \mathbf{b})) \geq \min\{d_E, d_O, \max\{d_E/2, d_O/2\}\}$, where d_E and d_O are the minimum distances of C_E and C_O , respectively, and $(\mathbf{a} + \mathbf{b}, -\mathbf{a} + \mathbf{b}) \neq \mathbf{0}$.

Proof: By Theorem 3, we can write every codeword of C as the sum of a codeword of C_E and a codeword of C_O . But every codeword of C_E is of the form $(\mathbf{a}, -\mathbf{a})$ and every codeword of C_O is of the form $(\mathbf{b}, \mathbf{b})$ (since $x^m - 1$ and $x^m + 1$ are divisors of their respective generators). Now, define for given $\mathbf{a}$ and $\mathbf{b}$ in $\text{GF}(3)^m$: $l_{rs} := |\{i | a_i = r \text{ and } b_i = s\}|$ ($r, s = 0, 1, 2$). Then, we have

$$\begin{aligned} & \text{wt}(\mathbf{a}) + \text{wt}(\mathbf{b}) + \text{wt}(\mathbf{a} + \mathbf{b}) + \text{wt}(-\mathbf{a} + \mathbf{b}) \\ &= \sum_{r \neq 0} \sum_s l_{rs} + \sum_r \sum_{s \neq 0} l_{rs} + \sum_r \sum_{s \neq -r} l_{rs} \\ & \quad + \sum_r \sum_{s \neq r} l_{rs} \\ &= \sum_{r \neq 0} \left(\sum_s l_{rs} + \sum_{s \neq 0} l_{rs} + \sum_{s \neq -r} l_{rs} + \sum_{s \neq r} l_{rs} \right) \\ & \quad + 3 \sum_{s \neq 0} l_{0s} \\ &= \sum_{r \neq 0} \left(\sum_s l_{rs} + 2 \sum_s l_{rs} \right) + 3 \sum_{s \neq 0} l_{0s} \\ &= 3 \left(\sum_{r \neq 0} \sum_s l_{rs} + \sum_{s \neq 0} l_{0s} \right) \\ &= 3 \left(\sum_r \sum_s l_{rs} - l_{00} \right) \\ &= 3(m - l_{00}). \end{aligned}$$

And so

$$\begin{aligned}
\text{wt}((\mathbf{a} + \mathbf{b}, -\mathbf{a} + \mathbf{b})) &= \text{wt}(\mathbf{a} + \mathbf{b}) \\
&\quad + \text{wt}(-\mathbf{a} + \mathbf{b}) \\
&= 3(m - l_{00}) \\
&\quad - \text{wt}(\mathbf{a}) - \text{wt}(\mathbf{b}) \\
&\geq 3 \max\{\text{wt}(\mathbf{a}), \text{wt}(\mathbf{b})\} \\
&\quad - \text{wt}(\mathbf{a}) - \text{wt}(\mathbf{b}) \\
&= 2 \max\{\text{wt}(\mathbf{a}), \text{wt}(\mathbf{b})\} \\
&\quad - \min\{\text{wt}(\mathbf{a}), \text{wt}(\mathbf{b})\} \\
&\geq \max\{\text{wt}(\mathbf{a}), \text{wt}(\mathbf{b})\}.
\end{aligned}$$

So a) and b) have been proved. To prove c), we observe that there are three possibilities:

- 1) $\text{wt}(\mathbf{a}) = 0$; then $\text{wt}((\mathbf{a} + \mathbf{b}, -\mathbf{a} + \mathbf{b})) \geq d_O$;
- 2) $\text{wt}(\mathbf{b}) = 0$; then $\text{wt}((\mathbf{a} + \mathbf{b}, -\mathbf{a} + \mathbf{b})) \geq d_E$;
- 3) $\text{wt}(\mathbf{a}) \neq 0$, $\text{wt}(\mathbf{b}) \neq 0$; then $\max\{\text{wt}(\mathbf{a}), \text{wt}(\mathbf{b})\} \geq \max\{d_E/2, d_O/2\}$. $\square$

Example 22.10: $n = 22$, $\bar{R} = \{0, 1, 3, 5, 9, 15\}$. C_E is equivalent to the code of Example 22.1 and so $d_E \geq 12$. C_O has defining set $\{0\}$ and so $d_O = 22$. Applying Theorem 6c) we get $d \geq 11$. But a codeword of weight 11 cannot occur by Corollary 1 a). So $d \geq 12$.

Theorem 5 and Theorem 6 will be used more optimally in the next section. We shall now discuss the relationship between Theorem 6 and *contraction*. The method of contraction was introduced in [1]. For the parameters that we shall treat in this paper, we could actually do without the method. However, one special case is so often quite useful that we mention it here.

Lemma 1: Let C be a cyclic code of length $2m$ with defining set R , containing as even integers the set $2R'$ (where $R' \subset \{0, 1, \dots, m-1\}$). Define the contraction C' as

$$\{(c_0 + c_m, c_1 + c_{m+1}, \dots, c_{m-1} + c_{2m-1}) | \mathbf{c} \in C\}$$

and write $c'_i := c_i + c_{m+i}$ ($0 \leq i < m$). Then C' is a cyclic code of length m with defining set R' .

Proof: Let α be a primitive $(2m)$ th root of unity and $\beta = \alpha^2$ a primitive m th root of unity. Then

$$\begin{aligned}
\sum_{i=0}^{m-1} c'_i (\beta^j)^i &= \sum_{i=0}^{m-1} (c_i + c_{m+i}) (\alpha^{2j})^i \\
&= \sum_{i=0}^{m-1} c_i (\alpha^{2j})^i + \sum_{i=m}^{2m-1} c_i (\alpha^{2j})^i = 0,
\end{aligned}$$

if $j \in R'$ (and hence $2j \in R$). $\square$

We use this as follows. If $\mathbf{c}' \in C'$ and $\mathbf{c}' \neq 0$, then $\text{wt}(\mathbf{c}) \geq \text{wt}(\mathbf{c}')$. If $\mathbf{c}' = 0$, then $\text{wt}(\mathbf{c})$ is even and furthermore 0 belongs to the defining set of C (in other words $\mathbf{c}$ is in the even-like subcode of C).

Example: $n = 26$, $R = \{2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24\}$. We see that $R' = \{0\}$ (see Lemma 1). So if $\mathbf{c}$ is a codeword and $\mathbf{c}'$ its contraction, then either $\text{wt}(\mathbf{c}') = 13$ (and

so $\text{wt}(\mathbf{c}) \geq 13$) or $\text{wt}(\mathbf{c}') = 0$. So, if $\text{wt}(\mathbf{c}) < 13$, then $\text{wt}(\mathbf{c})$ is even. This is also obvious if we use Theorem 6 and observe that C_O has defining set $\{0\}$.

Suppose C is a ternary cyclic code of length $n = 2m$ and $\mathbf{c} = (\mathbf{a} + \mathbf{b}, -\mathbf{a} + \mathbf{b})$, where $(\mathbf{a}, -\mathbf{a}) \in C_E$ and $(\mathbf{b}, \mathbf{b}) \in C_O$, is a codeword of C . Then obviously $\mathbf{c}' = 2\mathbf{b}$ (see Lemma 1) and so $\text{wt}(\mathbf{c}') = \text{wt}(\mathbf{b})$. So actually $d_O/2$ equals the minimum distance of C' . One could also define $C'' := \{(c_0 - c_m, -c_1 + c_{m+1}, \dots, \pm c_{m-1} \mp c_{2m-1}) | \mathbf{c} \in C\}$ and derive something similar for $d_E/2$, but unfortunately C'' need not be cyclic. We shall not go into detail about this. The reader can verify easily that in the ternary case Theorem 6 is always at least as powerful as contraction to length $n/2$. A ternary code of length $n = 2m$ is called *double* if $\{j | j \equiv 1 \pmod{2}\} \subset R$, and it is easy to see that the minimum distance of a double code is twice the minimum distance of its contraction.

Special Cases

Example 26.6: $n = 26$, $R = \{1, 2, 3, 6, 8, 9, 17, 18, 20, 23, 24, 25\}$. $d_{\text{SHIFT}} = 6$. We wish to prove that $d \geq 7$. Suppose $\mathbf{c}(x)$ is a codeword of weight 6. Obviously we have

$$(c(x) + c(-x))^2 - (c(x) - c(-x))^2 = c(x)c(-x). \quad (1)$$

Notice that $c(x)c(-x)$ is in the code with defining set $\{0, 13\}$. Moreover, $\gcd(c(x), x^2 - 1) = \gcd(c(-x), x^2 - 1) = 1$ (since the codes corresponding to $R \cup \{1\}$ and $R \cup \{-1\}$ have $d \geq 8$), and so $c(x)c(-x)$ is equal to $(x^{26} - 1)/(x^2 - 1)$, up to cyclic shift or multiplication by 2. We wish to prove that this is not possible for any w_0, w_1 , where $w_0 := \text{wt}(c(x) + c(-x))$ and $w_1 := \text{wt}(c(x) - c(-x)) = 6 - w_0$. First, we have to make some preparations. We apply Theorem 3 to get $c(x) = c_0(x) + c_1(x)$, where $c_0(x)$ is in the code with defining set $R \cup \{0, 13\}$ and $c_1(x)$ is in the code with defining set $\{0, 13\}$. We do this because looking at the zeros of $c_0(x)$ and $c_1(x)$ we have $c_0(x)c_0(-x) \equiv 0$ and $c_0(x)c_1(-x^{-1}) \equiv 0$, and so $\langle c_0(x), c_0(-x) \rangle = \langle c_0(x), c_1(-x) \rangle = \langle c_0(-x), c_1(x) \rangle = 0$. So $w_0 \equiv \langle c(x) + c(-x), c(x) + c(-x) \rangle = 2\langle c(x), c(-x) \rangle = 2\langle c_0(x) + c_1(x), c_0(-x) + c_1(-x) \rangle = 2(\langle c_0(x), c_0(-x) \rangle + \langle c_0(x), c_1(-x) \rangle + \langle c_1(x), c_0(-x) \rangle + \langle c_1(x), c_1(-x) \rangle) = 2\langle c_1(x), c_1(-x) \rangle$. But, again by Theorem 3, we can write $c_1(x) = a_1 l(x) + a_2 l(-x)$, where $l(x) = x^{25} + x^{24} + \dots + x + 1 = (x^{26} - 1)/(x - 1)$ and $a_1, a_2 \in \text{GF}(3)$. Then, since $\langle l(x), l(-x) \rangle = 0$, we have that $\langle c_1(x), c_1(-x) \rangle = a_1 a_2$ and moreover $c(1) = \langle c_1(x), l(x) \rangle = 2a_1$ and $c(-1) = \langle c_1(x), l(-x) \rangle = 2a_2$. So $w_0 \equiv 2\langle c_1(x), c_1(-x) \rangle = 2c(1)c(-1)$. We know that $c(1) \neq 0$ and $c(-1) \neq 0$. So we must be in one of the following cases.

- 1) $c(1) + c(-1) = 0$ (i.e., 1 is a zero of $c(x) + c(-x)$). This means that $c(1)c(-1) = 2$ or equivalently that $w_0 \equiv 1 \pmod{3}$ and $w_1 \equiv 2 \pmod{3}$.
- 2) $c(1) - c(-1) = 0$ (i.e., 1 is a zero of $c(x) - c(-x)$). This means that $c(1)c(-1) = 1$ or equivalently that $w_0 \equiv 2 \pmod{3}$ and $w_1 \equiv 1 \pmod{3}$.

So certainly $w_0 \not\equiv 0 \pmod{3}$. If $w_0 = 1$, then 1 is not a zero of $c(x) + c(-x)$ and so we are in case 2, which is a contradiction, since $w_0 \not\equiv 2 \pmod{3}$. So essentially there is just one case left, and that is the case where $w_0 = 2$ and both

nonzero coefficients in $c(x) + c(-x)$ have the same sign (if they have different sign, then 1 is a zero of $c(x) + c(-x)$ and $w_0 \equiv 1 \pmod{3}$). In that case $(c(x) + c(-x))^2$ has weight at most 3, and

$$\text{wt}((c(x) + c(-x))^2) \leq 4 + \binom{4}{2} = 10.$$

Looking at (1), we see that there cannot be any overlap between $(c(x) + c(-x))^2$ and $(c(x) - c(-x))^2$, since the weight of their sum must be 13. But also by (1), we must then have that all nonzero coefficients in $(c(x) + c(-x))^2$ have the same sign. This is a contradiction, since the nonzero coefficients in $c(x) + c(-x)$ have the same sign. So $c(x)$ cannot have weight 6 and so $d \geq 7$.

Example 26.7: $n = 26$, $R = \{0, 13, 14, 16, 17, 22, 23, 25\}$. Here, $d_{\text{SHIFT}} = 5$ and the Roos bound equals 6 (which is rather remarkable). To prove this, observe that the consecutive sets $\{13 + 3j, 14 + 3j\}$ are contained in R if $j \in \{0, 1, 3, 4\}$. By Roos [6], this means that $d \geq 3 + 4 - 1 = 6$.

Explanation of Table I

By computer we calculated the minimum distance of all ternary cyclic codes with length < 40 . In many cases this minimum distance is equal to the BCH bound. In Table I we give the minimum distance of all ternary cyclic codes of length < 40 , and minimum distance not equal to the BCH bound. So the minimum distances of all other ternary cyclic codes of length < 40 can easily be found by computing the BCH bound. Also by computer we calculated the d_{SHIFT} (see Definition 1) of the codes listed in Table I. We see from Table I that in many cases the minimum distance equals the d_{SHIFT} . In the other cases, some minimum distances are equal to bounds given by other theorems in this section (or belong to the special cases). In these cases we refer to an example in this section. Unfortunately some minimum distances are left, that could not be derived theoretically by us. These are indicated by a question mark. By the shifting certificate we mean the sequence $r_1, r_2, \dots, r_{d_{\text{SHIFT}}-1}$, which has been put in the order of Definition 1.

Of course we did not mention codes that were equivalent to a code that was already in the list. We saw that we could call two codes equivalent, if their defining sets were the same up to multiplication with an integer coprime to n . But if $n = 2m$, we can also call two codes equivalent, if their defining sets are the same up to a shift over m (this corresponds to a substitution of x by $-x$ in the codewords $c(x)$, and so the minimum distance stays invariant). So we call two codes equivalent if their defining sets can be obtained from each other by some combination of multiplying with an integer coprime to n and shifting over m (where $n = 2m$).

To find the defining sets of the codes in Table I and to find equivalent codes, we refer to the Appendix.

III. LONGER CODES

In this section, ternary cyclic codes will be studied with $40 \leq n \leq 50$. Computing exact minimum distances for these

codes is very time consuming, so we only computed lower bounds. Of course, first of all we used shifting, since this method seems to be very powerful as we saw in Section II. But, for some codes, shifting also took too much time and so we had to compute a lower bound using one of the other theorems in Section II. Of course, we also tried to improve the d_{SHIFT} using one of the other theorems.

$n = 40$

There are too many ternary cyclic codes of length 40 to give a list of all of them. So for each dimension k we computed the best of the lower bounds for the minimum distance of all codes of dimension k , and only listed the corresponding codes (Table II). For some codes in Table II we were able to find an upper bound for the minimum distance (just by computing some codewords), that equaled the lower bound for its minimum distance. This is indicated by a boldface entry in the column " $d_{\text{max}} \geq$." In the last column of Table II, an explanation is given for the lower bound. If this lower bound is not the BCH bound and is not explained in some example, then the bound equals the d_{SHIFT} and the sequence $r_1, r_2, \dots, r_{d_{\text{SHIFT}}-1}$ is given.

Example 40.1: $n = 40$, $\bar{R} = \{1, 3, 9, 27\}$. We will use Theorem 5 to prove that $d \geq 24$. Notice that C_L has as defining set all integers modulo 40, and so we may take d_L infinite. C_U is the square of the code of length 20 with defining set $\{0, 2, 4, 5, 6, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19\}$, which has minimum distance at least 12 by the BCH bound. So by Theorem 5 we have $d \geq 24$.

Example 40.2: $n = 40$, $\bar{R} = \{0, 1, 3, 9, 27\}$. Again we will use "Paris by night" to prove that $d \geq 22$. Also again d_L is infinite. C_U is the square of the code of length 20 with defining set $\{0, 1, 3, 7, 9\}$, which has minimum distance at least 11 by the BCH bound. So by Theorem 5, we have $d \geq 22$.

$40 < n \leq 50$

In Table III, we give a complete list of all ternary cyclic codes of length $40 < n \leq 50$, having a lower bound for the minimum distance more than the BCH bound. Again we also computed upper bounds and if the lower bound equals the upper bound, we indicate this with a boldface entry in the column " $d \geq$." In the last column one can find an explanation for the lower bound for d . If shifting gives the best bound, then a shifting certificate is given. Otherwise we either refer to a theorem ("Paris" means Theorem 5) or to an example. Sometimes we also give an explanation for the upper bound, by giving a subcode with a known minimum distance contained in our code (e.g., " $\supset nr.13$ "). The " $\simeq$ "-sign denotes "a code equivalent to." If the code is double or a square, then the minimum distance can be calculated from Table I and there is nothing else to explain. Notice that not for all codes the shifting bound is given in Table III. Here the computer spent too much time to compute the shifting bound. Because we need lower bounds for the minimum distance of all proper subcodes of a code to compute the shifting bound, we have put other lower bounds in the computer where shifting bound was not known. Notice that this means that the entries in the column

TABLE I
(PART 1)

nt	n	k	d	d_{SHIFT}	d_{RCH}	G	Shifting certificate	Expl.
1	8	4	4	4	3	0,4,5	4,7,0	
2	11	5	6	5	4	0,2	7,10,6,0	Ex. 11.1
3	11	6	5	4	4	2	6,7,2	Ex. 11.2
4	13	6	6	6	5	0,4,7	10,11,7,12,0	
5	13	6	6	6	5	0,2,7	6,0,11,5,2	
6	16	4	8	8	6	0,1,5,8,10	7,13,8,14,9,0,1	
7	16	7	6	6	5	4,5,8,10	4,7,12,13,5	
8	16	8	4	4	3	0,4,5,8	4,7,0	
9	16	9	5	5	4	5,8,10	7,14,13,5	
10	16	9	4	4	3	4,5,8	4,7,5	
11	20	6	8	8	6	0,2,4,10,11	10,16,11,17,12,13,0	
12	20	7	8	8	6	2,4,10,11	10,11,16,12,17,13,2	
13	20	8	8	8	5	0,4,5,10,11	11,4,16,12,15,10,0	
14	20	9	6	6	5	4,5,10,11	11,15,10,4,5	
15	20	10	6	6	5	0,4,10,11	11,12,19,10,0	
16	20	12	4	4	3	0,5,10,11	10,19,0	
17	20	12	4	4	3	0,4,5,10	4,15,0	
18	20	13	4	4	3	5,10,11	11,17,5	
19	20	13	4	4	3	4,5,10	4,15,5	
20	20	13	4	4	3	2,5,10	14,5,2	
21	20	14	4	4	3	0,10,11	10,19,0	
22	20	14	4	4	3	4,5	4,15,5	
23	20	15	4	4	3	10,11	11,17,0	
24	22	5	12	10	8	0,1,4,7,11	13,19,14,20,11,12,3,0,1	Ex. 22.1
25	22	6	12	10	7	2,4,7,11	10,17,12,19,11,6,16,7,2	Ex. 22.10
26	22	6	10	8	8	1,4,7,11	11,12,13,14,3,4,1	Ex. 22.4
27	22	7	10	8	7	2,4,7	12,6,17,16,18,7,2	Ex. 22.9
28	22	10	9	7	5	0,4,7,11	11,12,20,19,13,0	Ex. 22.2
29	22	10	6	5	4	0,2,7,11	7,10,6,0	Ex. 22.3
30	22	11	7	6	5	4,7,11	11,12,19,13,4	Ex. 22.5
31	22	11	6	5	4	2,7,11	6,17,7,2	Ex. 22.6
32	22	12	7	6	4	4,7	16,13,12,19,4	Ex. 22.7
33	22	12	5	4	4	2,7	6,7,2	Ex. 22.8
34	22	15	4	4	3	0,7,11	19,11,0	
35	22	16	4	4	3	4,11	12,14,4	
36	23	11	9	7	6	0,5	14,10,21,19,20,0	Ex. 23.1
37	23	12	8	6	5	5	14,10,21,19,5	Ex. 23.2
38	26	6	15	13	11	0,4,5,7,8,13,14,17	11,12,13,22,10,19,20,21,14,15,4,0	Ex. 26.1
39	26	6	12	12	10	0,1,5,7,8,13,14,17	19,21,13,23,20,22,14,24,7,0,1	
40	26	6	12	12	10	0,1,2,4,8,13,14,17	24,12,8,22,25,13,9,23,0,1,4	
41	26	7	14	12	9	4,5,7,8,13,14,17	10,11,12,13,21,20,19,14,15,4,5	Ex. 26.4
42	26	7	12	12	10	2,4,7,8,13,14,17	16,6,12,20,10,21,22,11,23,7,2	
43	26	7	12	12	8	1,2,4,8,13,14,17	1,9,3,13,17,24,23,12,8,2,4	
44	26	8	11	11	8	4,5,7,8,14,17	19,22,10,23,20,14,15,21,4,5	
45	26	8	10	10	6	1,2,4,8,14,17	1,9,17,22,3,24,23,2,4	
46	26	9	9	9	8	0,4,7,8,13,14,17	10,22,21,20,11,12,7,0	
47	26	9	9	9	8	0,2,7,8,13,14,17	20,21,22,16,24,6,7,0	
48	26	9	9	9	7	0,1,4,8,13,14,17	22,12,8,25,23,24,0,1	
49	26	9	11	10	9	0,1,2,8,13,14,17	22,24,25,0,16,1,23,2,3	?
50	26	10	9	9	7	4,7,8,13,14,17	10,11,22,21,20,12,7,4	
51	26	10	9	9	7	2,7,8,13,14,17	20,16,6,22,21,23,7,2	
52	26	10	8	8	7	1,7,8,13,14,17	7,23,21,20,22,8,1	
53	26	10	9	9	6	1,4,8,13,14,17	23,16,9,13,12,8,3,1	
54	26	10	10	10	8	1,2,8,13,14,17	22,17,8,23,1,13,24,2,3	
55	26	10	10	10	9	4,5,7,13,14,17	12,13,21,15,11,10,14,4,5	
56	26	10	9	9	7	1,4,7,13,14,17	10,3,16,22,12,11,9,1	
57	26	11	8	8	7	2,7,8,14,17	20,16,6,23,21,7,2	
58	26	11	6	6	5	2,4,8,14,17	22,16,23,17,2	
59	26	11	7	7	6	1,4,8,14,17	22,9,24,3,8,1	
60	26	11	7	7	5	1,2,8,14,17	22,23,1,16,2,3	
61	26	12	9	8	8	0,7,8,13,14,17	20,21,22,23,24,7,0	Ex. 26.2
62	26	12	9	8	6	0,5,8,13,14,17	13,22,14,23,15,16,0	Ex. 26.3
63	26	12	8	8	7	0,1,8,13,14,17	23,24,13,0,22,8,1	
64	26	12	9	8	6	0,4,7,13,14,17	11,12,16,25,21,10,0	?
65	26	12	6	6	5	0,1,7,13,14,17	22,13,0,16,1	
66	26	12	6	6	5	0,1,4,13,14,17	9,0,12,3,1	
67	26	12	6	6	5	0,4,7,8,13,17	10,11,7,12,0	
68	26	13	8	7	7	7,8,13,14,17	20,21,22,23,7,8	Ex. 26.5
69	26	13	8	8	6	5,8,13,14,17	13,14,22,15,23,16,5	
70	26	13	6	6	5	4,8,13,14,17	22,12,23,13,4	
71	26	13	8	7	5	1,8,13,14,17	23,16,13,24,8,1	?
72	26	13	7	7	6	4,7,13,14,17	12,21,10,11,13,4	
73	26	13	6	6	4	1,7,13,14,17	22,16,21,13,1	
74	26	13	8	8	7	4,5,13,14,17	13,14,22,16,12,4,5	
75	26	13	6	6	5	2,4,13,14,17	12,13,17,16,2	
76	26	13	6	6	5	1,4,13,14,17	9,13,22,3,1	
77	26	13	8	8	5	1,2,13,14,17	1,17,13,2,16,22,3	

" d_{SHIFT} " need not equal the d_{SHIFT} of Definition 1 (but it is easy to see that the d_{SHIFT} from Table III is still at most d).

Example 44.1: $n = 44$, $\bar{R} = \{2, 6, 10, 11, 18, 30, 33\}$. We shall use Theorem 5 to prove that $d \geq 22$. C_L has defining set $\{11, 33\}$ and so $d_L = 22$. C_U is the square of the code of length 22 with defining set $\{0, 1, 3, 4, 5, 7, 9, 12, 13, 14, 15, 16, 17, 19, 20, 21\}$, which has minimum distance 12, since it is equivalent to the code of

Example 22.10. So also $d_U = 12$. By Theorem 5, we have $d \geq 22$. By Corollary 2, we have $d = 22$.

Example 44.2: $n = 44$, $\bar{R} = \{0, 2, 6, 10, 11, 18, 30, 33\}$. We wish to apply Theorem 6 to prove that 21 is the best lower bound for the minimum distance that we can find (notice that "Paris by Night" gives $d \geq 20$). Suppose $c = (a + b, -a + b)$ is a nonzero element of the code of weight less than 21, where $(a, -a) \in C_E$ and $(b, b) \in C_O$. If $c \in C_E$ or $c \in C_O$, then

TABLE I
(PART 2)

nr.	n	k	d	d_{SHIFT}	d_{RCH}	G	Shifting certificate	Expl.
78	26	13	6	6	5	4,7,8,13,17	10,23,11,7,4	
79	26	13	6	6	5	1,7,8,13,17	20,8,24,7,1	
80	26	14	7	7	5	5,8,14,17	14,15,23,22,16,5	
81	26	14	6	6	5	4,8,14,17	16,24,22,23,4	
82	26	14	6	6	5	2,8,14,17	22,16,23,17,2	
83	26	14	7	7	5	1,8,14,17	23,16,8,24,22,1	
84	26	14	7	6	5	4,7,14,17	11,16,10,21,4	?
85	26	14	6	6	4	1,7,14,17	21,23,7,1,3	
86	26	14	6	6	4	1,7,8,17	20,24,8,7,1	Ex. 26.6
87	26	14	7	6	4	1,2,8,17	23,24,2,1,3	
88	26	15	6	6	5	0,7,13,14,17	13,22,21,16,0	
89	26	15	6	6	4	0,4,13,14,17	22,13,12,16,0	
90	26	15	6	6	5	0,7,8,13,17	23,24,7,20,0	
91	26	15	6	6	5	0,4,8,13,17	12,25,23,24,0	
92	26	16	6	6	4	7,13,14,17	22,16,21,13,7	
93	26	16	6	6	4	4,13,14,17	12,10,23,14,4	
94	26	16	6	6	5	2,13,14,17	22,17,16,13,2	
95	26	16	6	6	4	1,13,14,17	14,1,25,23,3	
96	26	16	6	6	4	7,8,13,17	7,24,23,20,8	
97	26	16	6	6	4	4,8,13,17	8,20,4,13,10	
98	26	16	6	6	5	1,8,13,17	23,13,9,20,1	
99	26	16	6	6	5	4,7,13,17	10,23,21,11,4	
100	26	16	6	6	5	2,4,13,17	10,4,2,23,6	
101	26	17	5	5	4	4,14,17	12,10,14,4	
102	26	17	6	5	4	2,8,17	17,24,23,2	?
103	26	18	6	5	3	0,13,14,17	13,22,16,0	Ex. 26.7
104	26	18	4	4	3	0,7,13,17	23,11,0	
105	26	19	5	5	3	13,14,17	13,22,16,14	
106	26	19	4	4	3	0,7,17	23,21,0	
107	26	20	4	4	3	14,17	22,16,14	
108	28	6	12	12	10	0,2,4,5,7,14	4,14,5,15,10,11,12,13,6,7,0	
109	28	7	12	12	10	2,4,5,7,14	4,14,10,12,20,11,13,5,6,7,2	
110	28	8	12	12	6	2,4,5,7	10,5,11,6,16,15,4,20,21,7,2	
111	28	10	7	7	5	2,4,5	11,4,22,10,5,2	
112	28	18	4	4	3	0,4,7,14	20,7,0	
113	28	19	4	4	3	4,7,14	20,7,4	
114	28	19	4	4	3	2,7,14	6,21,2	
115	28	20	4	4	3	4,7	20,7,4	
116	32	4	16	16	12	0,1,2,5,10,16,20	13,25,14,26,15,27,16,28,17,18,19,0,1,2,3	
117	32	7	12	12	10	1,5,8,10,16,20	7,13,23,25,27,24,26,8,9,10,1	
118	32	8	8	8	6	0,1,5,8,10,16	7,13,8,14,9,0,1	
119	32	9	10	10	8	1,5,10,16,20	13,27,25,14,28,26,9,10,1	
120	32	9	8	8	6	1,5,8,10,16	7,23,13,8,9,10,1	
121	32	13	6	6	5	2,5,10,16,20	13,20,5,6,2	
122	32	14	6	6	5	0,1,4,10,16,20	9,11,0,3,1	
123	32	14	6	6	5	4,5,8,10,20	4,7,12,13,5	
124	32	15	6	6	5	5,8,10,16,20	13,28,14,7,5	
125	32	15	6	6	5	1,4,10,16,20	9,25,10,3,1	
126	32	16	4	4	3	0,4,5,8,16,20	4,7,0	
127	32	16	6	6	5	0,1,10,16,20	25,9,26,0,1	
128	32	16	6	6	5	5,8,10,20	13,29,28,7,5	
129	32	17	4	4	3	4,5,8,16,20	4,7,5	
130	32	17	6	6	5	5,10,16,20	13,28,14,15,5	
131	32	17	6	6	5	1,10,16,20	25,9,26,10,1	
132	32	17	6	6	5	2,5,16,20	21,5,20,6,2	
133	32	18	4	4	3	0,5,8,16,20	20,7,0	
134	32	18	4	4	3	0,4,5,16,20	4,15,0	
135	32	18	4	4	3	4,5,8,20	4,7,5	
136	32	18	5	5	4	0,1,10,16	9,10,0,1	
137	32	18	5	5	4	5,8,10	7,14,13,5	
138	32	19	4	4	3	5,8,16,20	20,7,5	
139	32	19	4	4	3	1,8,16,20	8,19,1	
140	32	19	4	4	3	4,5,16,20	4,15,5	
141	32	19	5	5	4	1,10,16	9,25,10,1	
142	32	20	4	4	3	0,5,16,20	20,15,0	
143	32	20	4	4	3	5,8,20	20,7,5	
144	32	21	4	4	3	5,16,20	20,15,5	
145	32	21	4	4	3	1,16,20	16,19,1	
146	35	12	12	12	10	0,2,5,7	18,21,30,24,22,6,19,20,5,7,0	
147	35	13	12	11	10	2,5,7	18,19,20,21,23,5,22,6,7,2	?
148	35	16	8	8	6	0,2,5	18,24,23,30,22,5,0	
149	35	17	7	7	6	2,5	18,30,22,23,5,2	
150	35	18	8	7	5	0,2,7	18,23,21,31,6,0	?
151	35	22	6	6	4	0,2	34,23,31,18,0	
152	35	23	5	5	4	2	31,23,18,2	
153	35	24	4	4	3	0,5,7	20,14,0	
154	35	25	4	4	3	5,7	20,14,5	
155	37	18	11	8	5	0,2	13,18,14,19,31,5,0	?
156	37	19	10	8	5	2	13,18,14,19,31,5,2	?

$wt(c) \geq 22$ (C_E has defining set $\{11, 33\}$ and C_O is the code number 7 in Table III). If $wt(a) = 22$, then by Theorem 6b) we also have $wt(c) \geq 22$. So we can assume that $wt(a) = 11$. Now we can say immediately that $wt(c) \equiv 2wt(a) + 2wt(b) \equiv 1 + 2wt(b) \not\equiv 2 \pmod{3}$ (since b is an element of the code of Example 22.10 and so $wt(b) \not\equiv 2 \pmod{3}$) and so $wt(c) \neq 20$ so $d \geq 21$. We shall show that we cannot improve this bound

by using Theorem 6. Let $b(x)$ be the polynomial corresponding to b . Notice that $b(x) \pm b(-x)$ is an element of the code of Example 22.8 (minimum distance 5) and cannot be the zero word (since otherwise $wt(c) \geq 22 + 10 = 32$ or $c \in C_L$, which has minimum distance 22). Since a is either zero on the even or zero on the odd positions, we have $l_{00} \leq 11 - 5 = 6$. So $22 - l_{00} \geq 22 - 6 = 16$ and, by Theorem 6a), we have

TABLE II

k	$d_{\max} \geq$	G	Explanation
1	40	1,2,4,5,7,8,10,11,13,20,22,25	BCH
2	30	0,1,2,4,7,8,10,11,13,20,22,25	BCH
3	25	1,2,4,7,8,10,11,13,20,22,25	BCH
4	24	0,2,4,5,7,8,10,11,13,20,22,25	Example 40.1
5	22	2,4,5,7,8,10,11,13,20,22,25	Example 40.2
6	24	0,1,4,7,8,10,11,13,20,22,25	BCH
7	22	1,4,7,8,10,11,13,20,22,25	BCH
8	20	1,4,7,8,10,11,13,22,25	BCH
9	18	4,5,7,8,10,11,13,20,22,25	19,20,33,32,29,30,21,34,28,31,24,15,11,22,10,4,5
10	18	0,4,7,8,10,11,13,20,22,25	28,31,32,19,33,29,20,34,30,21,35,22,36,10,11,7,0
11	16	2,7,8,10,11,13,20,22,25	30,6,24,32,33,29,21,19,37,18,17,16,22,7,2
12	16	0,4,7,8,11,13,20,22,25	31,32,19,35,36,23,37,34,11,24,33,20,21,7,0
13	14	1,4,5,8,10,13,20,22,25	8,27,4,12,37,31,35,30,26,24,9,3,1
14	14	0,7,8,10,11,13,20,22,25	29,20,23,24,38,30,37,33,32,21,19,7,0
15	14	1,2,5,8,13,20,22,25	BCH
16	12	0,5,7,8,10,13,20,22,25	20,21,22,30,38,29,37,24,23,7,0
17	12	5,7,8,10,13,20,22,25	23,24,15,31,7,29,21,30,22,20,5
18	11	0,7,8,10,13,20,22,25	37,24,38,30,21,22,20,23,7,0
19	11	7,8,10,11,20,22,25	19,20,23,32,22,33,24,21,7,8
20	10	0,7,8,13,20,22,25	22,23,31,7,39,20,25,21,0
21	9	8,11,13,20,22,25	34,16,37,38,19,32,24,0
22	8	0,10,11,13,20,22,25	19,10,37,34,30,25,0
23	8	10,11,13,20,22,25	30,10,37,33,19,25,11
24	8	0,1,10,13,20,22	26,30,9,39,37,0,1
25	8	7,11,20,22,25	21,25,34,22,19,20,7
26	7	4,13,22,25	BCH
27	6	5,7,20,22,25	21,34,22,20,5
28	6	0,13,20,22,25	37,38,25,39,0
29	6	7,20,22,25	21,34,22,20,7
30	5	0,13,20,22	BCH
31	5	7,20,22	BCH
32	4	5,22,25	34,25,5
33	4	20,22,25	34,25,20
34	4	22,25	34,25,22
35	3	13,20	BCH

$\text{wt}(\mathbf{c}) \geq 3 * 16 - \text{wt}(\mathbf{a}) - \text{wt}(\mathbf{b}) = 37 - \text{wt}(\mathbf{b})$. We have three cases.

- 1) $\text{wt}(\mathbf{b}) \leq 15$: $\text{wt}(\mathbf{c}) \geq 37 - 15 = 22$.
- 2) $\text{wt}(\mathbf{b}) = 16$: $\text{wt}(\mathbf{c}) \geq 37 - 16 = 21$, and also by Theorem 6b): $\text{wt}(\mathbf{c}) \geq 2 * 16 - 11 = 21$.
- 3) $\text{wt}(\mathbf{b}) > 16$: $\text{wt}(\mathbf{c}) > 21$ by Theorem 6b).

Example 44.3: $n = 44$, $\bar{R} = \{2, 4, 6, 10, 11, 12, 16, 18, 20, 30, 33, 36\}$. We wish to apply Theorem 6 to prove that $d \geq 16$. Suppose $\mathbf{c} = (\mathbf{a} + \mathbf{b}, -\mathbf{a} + \mathbf{b})$ is a nonzero codeword of weight less than 16, where $(\mathbf{a}, -\mathbf{a}) \in C_E$ (having defining set $\{11, 33\}$) and $(\mathbf{b}, \mathbf{b}) \in C_O$ (code number 14). As in Example 44.2, we may assume that $\text{wt}(\mathbf{a}) = 11$. If $b(x)$ is the polynomial corresponding to $\mathbf{b}$, then $b(x) \pm b(-x)$ is an element of the code of length 22 with defining set $\{0, 11\}$ and we may assume that $b(x) \pm b(-x) \neq 0$ (since otherwise $\text{wt}(\mathbf{b}) = 0$ and so $\text{wt}(\mathbf{c}) = 22$). So $l_{00} \leq 11 - 2 = 9$ and $22 - l_{00} \geq 13$. So by Theorem 6a), we have $\text{wt}(\mathbf{c}) \geq 3 * 13 - \text{wt}(\mathbf{a}) - \text{wt}(\mathbf{b}) = 28 - \text{wt}(\mathbf{b})$. But $\text{wt}(\mathbf{b}) \equiv 0 \pmod{3}$ (by Theorem 2) and we must be in one of the following two cases.

- 1) $\text{wt}(\mathbf{b}) \leq 12$: $\text{wt}(\mathbf{c}) \geq 28 - 12 = 16$.
- 2) $\text{wt}(\mathbf{b}) \geq 15$: $\text{wt}(\mathbf{c}) \geq 2 * 15 - 11 = 19$ by Theorem 6b).

So $d \geq 16$.

Example 44.4: $n = 44$, $\bar{R} = \{1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 16, 18, 20, 23, 25, 27, 30, 31, 36, 37\}$. This code satisfies the condition of Theorem 2, and so $d \equiv 0 \pmod{3}$. $d_{\text{SHIFT}} = 10$ and so $d \geq 12$. Moreover $d = 12$, since this code contains number 13 in Table III.

Example 44.5: $n = 44$, $\bar{R} = \{0, 1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 16, 18, 20, 23, 25, 27, 30, 31, 36, 37\}$. This code satisfies the conditions of Corollary 1 a) (see Example 44.4). Here

$d_{\text{SHIFT}} = 10$, so we have by Corollary 1 c) that $d \geq 11$.

Example 44.6: $n = 44$, $R = \{0, 7, 8, 13, 14, 17, 19, 21, 22, 24, 26, 28, 29, 32, 34, 35, 38, 39, 40, 41, 42, 43\}$. We wish to apply Theorem 6 to prove that $d \geq 10$. Suppose $\mathbf{c} = (\mathbf{a} + \mathbf{b}, -\mathbf{a} + \mathbf{b})$ is a nonzero codeword of weight less than 10, where $(\mathbf{a}, -\mathbf{a}) \in C_E$ (number 19) and $(\mathbf{b}, \mathbf{b}) \in C_O$ (number 14). Notice that C_E is a square with minimum distance 10, i.e., if $\text{wt}(\mathbf{a}, -\mathbf{a}) < 20$, then $(\mathbf{a}, -\mathbf{a})$ (and also $\mathbf{a}$) is either zero on the even or on the odd positions (and if it is zero both on the even and on the odd positions, then $\text{wt}(\mathbf{c}) \geq 18$). Let $b(x)$ be the polynomial corresponding to $\mathbf{b}$, then $b(x) \pm b(-x)$ has zeros 1 and -1 and so $\mathbf{b}$ must have weight at least 2 on both the even and the odd positions (if $\mathbf{b}$ is zero on either the even or on the odd positions, then $\mathbf{b} = \mathbf{0}$ and $\text{wt}(\mathbf{c}) \geq 10$). We have three cases.

- 1) $\text{wt}(\mathbf{a}) > 9$ or $\text{wt}(\mathbf{b}) > 9$. Then, $\text{wt}(\mathbf{c}) \geq 10$ by Theorem 6b).
- 2) $\text{wt}(\mathbf{a}) < 9$ and $\text{wt}(\mathbf{b}) = 9$. Then, $\text{wt}(\mathbf{c}) \geq 10$ by Theorem 6b).
- 3) $\text{wt}(\mathbf{a}) = 9$ and $\text{wt}(\mathbf{b}) = 9$. Then by the observations just made $l_{00} \leq 2 + (11 - 2) = 11$ and so by Theorem 6a) we have: $\text{wt}(\mathbf{c}) \leq 3 * 11 - 9 - 9 = 15$.

So $d \geq 10$, and since code nr.19 in Table III is contained in this code, we have $d = 10$.

Example 44.7: $n = 44$, $R = \{1, 3, 5, 8, 9, 11, 15, 22, 23, 24, 25, 27, 28, 31, 32, 33, 37, 40\}$. We wish to apply Theorem 6 to prove that $d \geq 8$. Suppose $\mathbf{c} = (\mathbf{a} + \mathbf{b}, -\mathbf{a} + \mathbf{b})$ is a nonzero codeword of weight < 8 , where $(\mathbf{a}, -\mathbf{a}) \in C_E$ (equivalent to number 13) and $(\mathbf{b}, \mathbf{b}) \in C_O$ (number 38). C_E is selforthogonal and has minimum distance 12, so $\text{wt}(\mathbf{c})$ can only be

TABLE III
(PART 1)

nr.	n	k	d >	d _{SHIFT}	d _{BCH}	G	Explanation
1	41	8	20	20	16	0,2,4,7,8	28,34,30,36,17,5,23,19,7,25,15,10,12,18,20,16,4,6,0
2	41	9	18	18	13	2,4,7,8	4,33,21,5,34,22,23,17,16,15,20,10,18,19,6,7,2
3	41	17	12	12	7	4,7,8	7,21,16,11,20,15,25,29,4,10,5
4	41	24	8	8	7	0,2,8	0,33,31,39,8,6,2
5	41	25	8	8	5	7,8	7,21,16,30,19,10,8
6	44	5	24		16	0,1,4,7,8,11,14,22	double
7	44	6	24		14	1,4,7,8,11,14,22	double
8	44	6	20		16	1,2,7,8,11,14,22	double
9	44	7	22		13	0,1,4,7,8,14,22	Example 44.1
10	44	7	20		14	1,4,7,8,11,14	double
11	44	8	21		12	1,4,7,8,14,22	Example 44.2
12	44	8	20		13	1,2,7,8,14,22	'Paris', Dnr.8
13	44	10	12		8	0,2,4,7,8,11,14,22	square
14	44	10	18		10	0,1,7,8,11,14,22	double
15	44	10	12	10	8	0,1,4,7,11,14,22	double
16	44	11	12	10	8	2,4,7,8,11,14,22	'Paris', Dnr.13
17	44	11	14		10	1,7,8,11,14,22	double
18	44	11	12	10	8	1,4,7,11,14,22	double
19	44	12	10	8	8	0,2,4,7,8,14,22	square
20	44	12	16		10	0,1,7,8,14,22	Example 44.3
21	44	12	12	10	7	0,1,4,7,14,22	square
22	44	12	12	10	7	2,4,7,8,11,14	square
23	44	12	14		8	1,7,8,11,14	double
24	44	12	10		8	1,4,7,11,14	double
25	44	13	10	8	8	2,4,7,8,14,22	'Paris', Dnr.19
26	44	13	14	14	10	1,7,8,14,22	21,22,24,25,27,13,41,37,39,23,7,8,1, Dnr.17
27	44	13	12	10	7	1,4,7,14,22	'Paris', Dnr.21
28	44	14	10	8	7	2,4,7,8,14	square
29	44	14	11	11	8	1,7,8,14	23,37,24,38,25,39,26,7,8,1
30	44	14	10	10	7	1,4,7,14	square
31	44	15	12	10	8	0,4,7,8,11,14,22	'Paris', Dnr.13
32	44	15	12	10	8	0,2,7,8,11,14,22	'Paris', Dnr.13
33	44	15	8	8	6	0,1,7,11,14,22	double
34	44	16	12	10	7	4,7,8,11,14,22	'Paris', Dnr.13
35	44	16	12	10	7	2,7,8,11,14,22	'Paris', Dnr.13
36	44	16	12	10	8	1,4,8,11,14,22	'Paris', Dnr.13
37	44	16	12	10	8	1,2,8,11,14,22	'Paris', Dnr.13
38	44	16	8	8	6	1,7,8,11,22	double
39	44	17	10	8	8	0,4,7,8,14,22	'Paris', Dnr.19
40	44	17	10	8	8	0,2,7,8,14,22	'Paris', Dnr.19
41	44	17	8	8	6	0,1,7,14,22	37,21,13,25,42,0,1, Dnr.33
42	44	17	12	10	7	4,7,8,11,14	'Paris', Dnr.22
43	44	17	12	10	7	2,7,8,11,14	'Paris', Dnr.22
44	44	18	10	8	7	4,7,8,14,22	'Paris', Dnr.19
45	44	18	10	8	7	2,7,8,14,22	'Paris', Dnr.19
46	44	18	10	8	8	1,4,8,14,22	'Paris', Dnr.19
47	44	18	10	8	8	1,2,8,14,22	'Paris', Dnr.19
48	44	18	8	8	6	1,7,8,22	21,39,23,27,7,8,1, Dnr.38
49	44	19	10	8	7	4,7,8,14	'Paris', Dnr.28
50	44	19	10	8	7	2,7,8,14	'Paris', Dnr.28
51	44	20	12	10	8	0,7,8,11,14,22	Example 44.4
52	44	20	9	7	5	0,4,7,11,14,22	square
53	44	20	8	8	5	0,2,7,11,14,22	10,18,38,43,41,6,0
54	44	20	6	5	4	0,1,4,11,14,22	square
55	44	21	11	10	7	7,8,11,14,22	Example 44.5
56	44	21	9	7	5	4,7,11,14,22	'Paris', Dnr.52
57	44	21	6	5	4	1,4,11,14,22	'Paris', Dnr.54
58	44	21	8	8	5	4,7,8,11,22	32,21,40,16,19,7,4
59	44	22	10	8	8	0,7,8,14,22	Example 44.6
60	44	22	7	6	5	0,4,7,14,22	square
61	44	22	8	8	5	0,2,7,14,22	38,13,34,17,6,21,0, Dnr.53
62	44	22	6	5	4	0,1,4,14,22	square
63	44	22	8	8	7	7,8,11,14	38,39,32,40,33,7,8
64	44	22	7	6	5	4,7,11,14	square
65	44	22	6	5	4	1,4,11,14	square
66	44	23	8	8	7	7,8,14,22	38,39,13,28,34,7,8
67	44	23	7	6	5	4,7,14,22	'Paris', Dnr.60
68	44	23	6	5	4	1,4,14,22	'Paris', Dnr.62
69	44	23	8	8	5	4,7,8,22	16,35,12,20,39,7,4, Dnr.58
70	44	24	8	8	7	7,8,14	38,39,13,28,34,7,8
71	44	24	7	6	4	4,7,14	square
72	44	24	5	4	4	1,4,14	square
73	44	25	8	7	5	0,7,11,14,22	'Paris', Dnr.33
74	44	25	6	5	4	0,1,11,14,22	'Paris', Dnr.54
75	44	26	6	5	4	7,8,11,22	Theorem 6 (iii), Dnr.54
76	44	26	8	7	5	1,8,11,22	Example 44.7
77	44	27	7	6	5	0,7,14,22	'Paris', Dnr.60

smaller than 8 if $\text{wt}(\mathbf{a}) = 6$ (if $\text{wt}(\mathbf{a}) = 0$, then $\mathbf{c} \in C_O$, which has minimum distance 8). But if $\text{wt}(\mathbf{a}) = 6$, then $\mathbf{a}$ is zero on either the even or the odd positions. By Theorem 6b) $\text{wt}(\mathbf{c})$ can only be smaller than 8 if $\text{wt}(\mathbf{b}) \leq 6$. So we have two cases.

- 1) $m - l_{00} = 6$. Then $\mathbf{c}$ is in the lower square C_L by the observations just made ($\mathbf{c}$ is zero on either the even or the odd positions). But $d_L = 9$, so this is impossible.

- 2) $m - l_{00} \geq 7$. Then, by Theorem 6a), we have: $\text{wt}(\mathbf{c}) \geq 21 - 6 - 6 = 9$.

So $d \geq 8$, and since code number 38 is contained in it, we have $d = 8$.

Example 44.8: $n = 44$, $R = \{7, 8, 13, 17, 19, 21, 22, 24, 28, 29, 32, 35, 39, 40, 41, 43\}$. We wish to apply Theorem 6 to prove that $d \geq 6$. Suppose $\mathbf{c} = (\mathbf{a} + \mathbf{b}, -\mathbf{a} + \mathbf{b})$ is a nonzero codeword of weight < 6 , where $(\mathbf{a}, -\mathbf{a}) \in C_E$ (number 19)

TABLE III
(PART 2)

nr.	n	k	d	d _{SHIFT}	d _{BCH}	G	Explanation
78	44	27	6	5	4	0,1,14,22	'Paris', $\supset$ nr.62
79	44	28	6	5	4	7,8,22	Example 44.8
80	44	28	7	6	5	1,8,22	Example 44.9
81	44	30	4	4	3	0,4,11,14,22	square
82	44	30	4	4	3	0,2,11,14,22	10,33,0
83	44	30	4	4	3	0,7,11,22	square
84	44	31	4	4	3	4,11,14,22	11,33,4
85	44	31	4	4	3	2,11,14,22	10,33,2
86	44	31	4	4	3	4,8,11,22	32,11,4
87	44	31	4	4	3	7,11,22	19,11,7
88	44	32	4	4	3	0,7,22	square
89	44	32	4	4	3	4,11,14	square
90	44	32	4	4	3	2,11,14	10,33,2
91	44	33	4	4	3	7,22	19,17,7
92	44	35	4	4	3	0,11,14,22	38,22,0
93	44	36	4	4	3	8,11,22	28,24,8
94	44	37	4	4	3	11,14	34,38,11
95	46	11	18	18	12	0,2,5,10,23	$\simeq$ double
96	46	12	18	18	12	2,5,10,23	16,10,6,18,14,4,20,22,32,36,42,5,17,15,19,7,2, $\supset$ nr.95
97	46	12	18	18	10	1,5,10,23	double
98	46	13	18	18	10	2,5,10	'Paris', $\supset$ nr.97
99	46	22	9	7	6	0,5,10,23	square
100	46	22	9	9	6	0,1,10,23	38,27,39,22,41,0,9,1
101	46	23	9	7	6	5,10,23	'Paris', $\supset$ nr.99
102	46	23	9	8	6	1,10,23	Example 46.1
103	46	24	8	6	5	5,10	square
104	46	24	8	8	6	1,10	38,27,28,39,29,9,1
105	46	33	4	4	3	0,10,23	20,28,0
106	46	34	4	4	3	10,23	20,28,10
107	47	23	9	9	6	0,5	38,44,30,19,43,10,22,0
108	47	24	8	8	5	5	43,29,44,38,39,10,5

TABLE IV
(PART 1)

n	minimal polynomials	zeros exponents	permutations
4	1 $x+2$ 2 x^2+1 3 $x+1$	0 1,3 2	1 2 3 3 2 1
5	trivial		
7	trivial		
8	1 $x+2$ 2 x^2+x+2 3 x^2+1 4 $x+1$ 5 x^2+2x+2	0 1,3 2,6 4 5,7	1 2 3 4 5 1 5 3 4 2 4 5 3 1 2
10	1 $x+2$ 2 $x^4+2x^3+x^2+2x+1$ 3 $x^4+x^3+x^2+x+1$ 4 $x+1$	0 1,3,7,9 2,4,6,8 5	1 2 3 4 4 3 2 1
11	1 $x+2$ 2 $x^5+2x^3+x^2+2x+2$ 3 $x^5+x^4+2x^3+x^2+2$	0 1,3,4,5,9 2,6,7,8,10	1 2 3 1 3 2
13	1 $x+2$ 2 x^3+x^2+x+2 3 x^3+x^2+2 4 x^3+2x^2+2x+2 5 x^3+2x+2	0 1,3,9 2,5,6 4,10,12 7,8,11	1 2 3 4 5 1 3 4 5 2 1 4 5 2 3 1 5 2 3 4
14	1 $x+2$ 2 $x^6+2x^5+x^4+2x^3+x^2+2x+1$ 3 $x^6+x^5+x^4+x^3+x^2+x+1$ 4 $x+1$	0 1,3,5,9,11,13 2,4,6,8,10,12 7	1 2 3 4 4 3 2 1
16	1 $x+2$ 2 x^4+x^2+2 3 x^2+x+2 4 x^2+1 5 x^4+2x^2+2 6 $x+1$ 7 x^2+2x+2	0 1,3,9,11 2,6 4,12 5,7,13,15 8 10,14	1 2 3 4 5 6 7 1 5 7 4 2 6 3 6 2 7 4 5 1 3
17	trivial		
19	trivial		
20	1 $x+2$ 2 x^4+x^3+2x+1 3 $x^4+2x^3+x^2+2x+1$ 4 $x^4+x^3+x^2+x+1$ 5 x^2+1 6 $x+1$ 7 x^4+2x^3+x+1	0 1,3,7,9 2,6,14,18 4,8,12,16 5,15 10 11,13,17,19	1 2 3 4 5 6 7 1 7 3 4 5 6 2 6 7 4 3 5 1 2

and $(b, b) \in C_O$ (number 38). The only way to get $\text{wt}(c) < 6$, is to take $\text{wt}(a) = 5$ and $\text{wt}(b) = 4$ or 5. But C_E is a square and so $\text{wt}(a) = 5$ implies that a is zero on either the even or

the odd positions. We have two cases.

- 1) $m - l_{00} = 5$. Then c is an element of the lower square, which has minimum distance 6,

TABLE IV
(PART 2)

n	minimal polynomials	zeros exponents	permutations
22	1 $x+2$ 2 $x^5+2x^4+2x^3+2x^2+1$ 3 $x^5+2x^3+x^2+2x+2$ 4 $x^5+x^4+2x^3+x^2+2$ 5 $x^5+2x^3+2x^2+2x+1$ 6 $x+1$	0 1,3,5,9,15 2,6,8,10,18 4,12,14,16,20 7,13,17,19,21 11	1 2 3 4 5 6 1 5 4 3 2 6 6 4 5 2 3 1
23	1 $x+2$ 2 $x^{11}+2x^8+2x^6+x^4+x^3+2x^2+2x+2$ 3 $x^{11}+x^{10}+x^9+2x^8+2x^7+x^5+x^3+2$	0 1,2,3,4,6,8,9,12,13,16,18 5,7,10,11,14,15,17,19,20,21, 22	1 2 3 1 3 2
25	1 $x+2$ 2 $x^{20}+x^{15}+x^{10}+x^5+1$ 3 $x^4+x^3+x^2+x+1$	0 {1,2,3,4} • {0,5,10,15,20} 5,10,15,20	none
26	1 $x+2$ 2 x^3+2x+1 3 x^3+x^2+x+2 4 x^3+x^2+2 5 x^3+2x^2+x+1 6 x^3+x^2+2x+1 7 x^3+2x^2+2x+2 8 $x+1$ 9 x^3+2x+2 10 x^3+2x^2+1	0 1,3,9 2,6,18 4,10,12 5,15,19 7,11,21 8,20,24 13 14,16,22 17,23,25	1 2 3 4 5 6 7 8 9 10 1 5 4 7 10 2 9 8 3 6 1 6 9 3 2 10 4 8 7 5 1 10 7 9 6 5 3 8 4 2 8 9 5 10 3 7 6 1 2 4
28	1 $x+2$ 2 $x^6+x^5+x^3+x+1$ 3 $x^6+2x^5+x^4+2x^3+x^2+2x+1$ 4 $x^6+x^5+x^4+x^3+x^2+x+1$ 5 $x^6+2x^5+2x^3+2x+1$ 6 x^2+1 7 $x+1$	0 1,3,9,19,25,27 2,6,10,18,22,26 4,8,12,16,20,24 5,11,13,15,17,23 7,21 14	1 2 3 4 5 6 7 1 5 3 4 2 6 7 7 5 4 3 2 6 1
29	trivial		
31	trivial		
32	1 $x+2$ 2 x^6+x^4+2 3 x^4+x^2+2 4 x^2+x+2 5 x^8+2x^4+2 6 x^2+1 7 x^4+2x^2+2 8 $x+1$ 9 x^2+2x+2	0 1,3,9,11,17,19,25,27 2,6,18,22 4,12 5,7,13,15,21,23,29,31 8,24 10,14,26,30 16 20,28	1 2 3 4 5 6 7 8 9 1 5 7 9 2 6 3 8 4 8 2 3 9 5 6 7 1 4
34	1 $x+2$ 2 $x^{16}+2x^{15}+x^{14}+\dots+2x+1$ 3 $x^{16}+x^{15}+x^{14}+\dots+x+1$ 4 $x+1$	0 1,3,5,7,...,33 2,4,6,8,...,32 17	1 2 3 4 4 3 2 1
35	1 $x+2$ 2 $x^{12}+2x^{11}+2x^{10}+x^9+2x^8+x^7+x^5+2x^4+x^2+1$ 3 $x^{12}+x^{10}+2x^8+x^7+x^5+2x^4+x^3+2x^2+2x+1$ 4 $x^6+x^5+x^4+x^3+x^2+x+1$ 5 $x^4+x^3+x^2+x+1$	0 1,3,4,9,11,12,13,16,17,27,29, 33 2,6,8,18,19,22,23,24,26,31, 32,34 5,10,15,20,25,30 7,14,21,28	1 2 3 4 5 1 3 2 4 5
37	1 $x+2$ 2 $x^{18}+2x^{16}+2x^{14}+2x^{13}+x^{11}+x^7+2x^5+2x^4+2x^2+1$ 3 $x^{18}+x^{17}+2x^{16}+2x^{15}+x^{14}+2x^{13}+2x^{12}+2x^{10}+2x^9+2x^8+2x^6+2x^5+x^4+2x^3+2x^2+x+1$	0 1,3,4,7,9,10,11,12,16,21, 25,26,27,28,30,33,34,36 2,5,6,8,13,14,15,17,18,19, 20,22,23,24,29,31,32,35	1 2 3 1 3 2
38	1 $x+2$ 2 $x^{18}+2x^{17}+x^{16}+\dots+2x+1$ 3 $x^{18}+x^{17}+x^{15}+\dots+x+1$ 4 $x+1$	0 1,3,5,7,...,37 2,4,6,8,...,36 19	1 2 3 4 4 3 2 1

2) $m - l_{00} \geq 6$. Then, by Theorem 6a), we have $\text{wt}(c) \geq 18 - 5 - 5 = 8$.

So $d \geq 6$, and since the lower square has minimum distance 6, we have $d = 6$.

Example 44.9: $n = 44$, $R = \{1, 3, 5, 8, 9, 15, 22, 23, 24, 25, 27, 28, 31, 32, 37, 40\}$. We wish to apply Theorem 6 to prove that $d \geq 7$. Suppose $c = (a+b, -a+b)$ is a nonzero codeword of weight < 7 , where $(a, -a) \in C_E$ (equivalent to number 19)

and $(b, b) \in C_O$ (number 38). The only way to get $\text{wt}(c) < 7$ is by taking $\text{wt}(a) = 5$ and $\text{wt}(b) = 4$ or 5 or $\text{wt}(a) = 6$ and $\text{wt}(b) = 6$. But C_E is a square and so $\text{wt}(a) < 10$ implies that a is zero on either the even or the odd positions. We have two cases.

- 1) $m - l_{00} = \text{wt}(a)$. Then, c is an element of the lower square, which has minimum distance 7.
- 2) $m - l_{00} \geq \text{wt}(a) + 1$. Then, by Theorem 6a), we have

TABLE IV
(PART 3)

n	minimal polynomials	zeros exponents	permutations
40	1 $x+2$	0	1 2 3 4 5 6 7 8 9 10 11 12 13
	2 $x^4+x^3+x^2+1$	1,3,9,27	1 6 3 4 13 2 7 8 10 9 11 12 5
	3 x^4+x^3+2x+1	2,6,14,18	1 9 12 4 5 10 7 8 2 6 11 3 13
	4 $x^4+2x^3+x^2+2x+1$	4,12,28,36	1 10 12 4 13 9 7 8 6 2 11 3 5
	5 x^2+x+2	5,15	11 6 12 7 13 2 4 8 10 9 1 3 5
	6 $x^4+2x^3+x^2+1$	7,21,23,29	
	7 $x^4+x^3+x^2+x+1$	8,16,24,32	
	8 x^2+1	10,30	
	9 x^4+x^2+2x+1	11,17,19,33	
	10 x^4+x^2+x+1	13,31,37,39	
	11 $x+1$	20	
	12 x^4+2x^3+x+1	22,26,34,38	
	13 x^2+2x+2	25,35	
41	1 $x+2$	0	1 2 3 4 5 6
	2 $x^8+2x^6+x^5+x^3+2x^2+1$	1,3,9,14,27,32,38,40	1 3 4 6 2 5
	3 $x^8+x^7+x^6+2x^4+x^2+x+1$	2,6,13,18,23,28,35,39	1 4 6 5 3 2
	4 $x^8+x^7+2x^6+2x^2+x+1$	4,5,12,15,26,29,36,37	1 5 2 3 6 4
	5 $x^8+2x^7+2x^6+2x^5+2x^3+2x^2+2x+1$	7,16,19,20,21,22,25,34	1 6 5 2 4 3
	6 $x^8+x^6+x^5+2x^4+x^3+x^2+1$	8,10,11,17,24,30,31,33	
43	trivial		
44	1 $x+2$	0	1 2 3 4 5 6 7 8 9
	2 $x^{10}+2x^8+2x^6+2x^4+1$	1,3,5,9,15,23,25,27,31,37	1 5 8 6 2 4 7 3 9
	3 $x^5+2x^4+2x^3+2x^2+1$	2,6,10,18,30	9 2 6 8 5 3 7 4 1
	4 $x^5+2x^3+x^2+2x+2$	4,12,16,20,36	
	5 $x^{10}+2x^6+2x^4+2x^2+1$	7,13,17,19,21,29,35,39,41,43	
	6 $x^5+x^4+2x^3+x^2+2$	8,24,28,32,40	
	7 x^2+1	11,33	
	8 $x^5+2x^3+2x^2+2x+1$	14,26,34,38,42	
	9 $x+1$	22	
46	1 $x+2$	0	1 2 3 4 5 6
	2 $x^{11}+2x^{10}+x^9+x^8+2x^7+x^5+x^3+1$	1,3,9,13,25,27,29,31,35,39,41	1 4 5 2 3 6
	3 $x^{11}+x^{10}+x^9+2x^8+2x^7+x^5+x^3+2$	2,4,6,8,12,16,18,24,26,32,36	6 3 2 5 4 1
	4 $x^{11}+x^8+x^6+2x^4+x^3+x^2+2x+1$	5,7,11,15,19,21,33,37,43,45	
	5 $x^{11}+2x^8+2x^6+x^4+x^3+2x^2+2x+2$	10,14,20,22,28,30,34,38,40,42,44	
	6 $x+1$	23	
47	1 $x+2$	0	1 2 3
	2 $x^{23}+x^{22}+x^{21}+x^{18}+x^{17}+x^{16}+x^{14}+2x^{13}+2x^{11}+x^8+2x^6+x^4+2x^3+2$	1,2,3,4,6,7,8,9,12,14,16,17,18,21,24,25,27,28,32,34,36,37,42	1 3 2
	3 $x^{23}+x^{20}+2x^{19}+x^{17}+2x^{15}+x^{12}+x^{10}+2x^9+2x^7+2x^6+2x^5+2x^2+2x+2$	5,10,11,13,15,19,20,22,23,26,29,30,31,33,35,38,39,40,41,43,44,45,46	
49	1 $x+2$	0	none
	2 $x^{42}+x^{35}+x^{28}+x^{21}+x^{14}+x^7+1$	$\{1,2,3,4,5,6\} \cdot \{0,7,14,21,28,35,42\}$	
	3 $x^6+x^5+x^4+x^3+x^2+x+1$	7,14,21,28,35,42	
50	1 $x+2$	0	1 2 3 4 5 6
	2 $x^{20}+x^{15}+x^{10}+2x^5+1$	$\{1,3,7,9\} \cdot \{0,10,20,30,40\}$	6 3 2 5 4 1
	3 $x^{20}+x^{15}+x^{10}+x^5+1$	$\{2,4,6,8\} \cdot \{0,10,20,30,40\}$	
	4 $x^4+2x^3+x^2+2x+1$	5,15,35,45	
	5 $x^4+x^3+x^2+x+1$	10,20,30,40	
	6 $x+1$	25	

$$\text{wt}(c) \geq 3(\text{wt}(\mathbf{a}) + 1) - \text{wt}(\mathbf{a}) - \text{wt}(\mathbf{b}) = 2\text{wt}(\mathbf{a}) - \text{wt}(\mathbf{b}) + 3 \geq 8.$$

So $d \geq 7$, and since the lower square has minimum distance 7, we have $d = 7$.

Example 46.1: $n = 46$, $R = \{1, 3, 9, 10, 13, 14, 20, 22, 23, 25, 27, 28, 29, 30, 31, 34, 35, 38, 39, 40, 41, 42, 44\}$. $d_{\text{SHIFT}} = 8$. The conditions in Corollary 1 are satisfied. By Corollary 1 a) weights are congruent to 0 or 1 mod 3. So $d \geq 9$.

APPENDIX

In Table IV, we give a complete list of all irreducible factors of $x^n - 1$, $n \leq 50$, over $\text{GF}(3)$ (a list for $n \leq 100$ can be found in [9]). We also give the exponents of the zeros of these polynomials for some chosen n th root of unity. As we saw, a cyclic code of length n can be represented by a set of irreducible factors of $x^n - 1$. In the last column, we give the permutations on the minimal polynomials, that permute

codes into equivalent codes. If $x^{n-1} + x^{n-2} + \dots + x + 1$ is an irreducible factor of $x^n - 1$, this will be denoted by "trivial."

ACKNOWLEDGMENT

The authors are very grateful to F. Bussemaker, Department of Mathematics, Eindhoven University of Technology, for writing the programs.

REFERENCES

- [1] J. H. van Lint and R. M. Wilson, "On the minimum distance of cyclic codes," *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 23-40, Jan. 1986.
- [2] M. van Eupen and C. van Eijl, "Minimum afstanden van ternaire cyclische codes," rep., Eindhoven Univ. of Technol., 1989.
- [3] J. H. van Lint, *Introduction to Coding Theory*. New York: Springer-Verlag, 1982.
- [4] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North Holland, 1977.
- [5] C. R. P. Hartmann and K. K. Tzeng, "Generalizations of the BCH bound," *Inform. Contr.*, vol. 20, pp. 489-498, 1972.
- [6] C. Roos, "A new lower bound for the minimum distance of a cyclic code," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 330-332, May 1983.
- [7] R. J. McEliece, "Weight congruences for p -ary cyclic codes," *Discrete Math.*, vol. 3, pp. 117-192, 1972.
- [8] E. F. Assmus, Jr. and H. F. Mattson, Jr., "On weights in quadratic residue codes," *Discrete Math.*, vol. 3, pp. 1-20, 1972.
- [9] R. J. McEliece, "Factorization of polynomials over finite fields," *Math. Computat.*, vol. 23, pp. 861-867, 1969.