On the minimum distance of cyclic codes

On the Minimum Distance of Cyclic Codes

JACOBUS H. VAN LINT AND RICHARD M. WILSON

Abstract—**The main result is a new lower bound for the minimum distance of cyclic codes that includes earlier bounds (i.e., BCH bound, HT bound, Roos bound). This bound is related to a second method for bounding the minimum distance of a cyclic code, which we call shifting. This method can be even stronger than the first one. For all binary cyclic codes of length < 63 (with two exceptions), we show that our methods yield the true minimum distance. The two exceptions at the end of our list are a code and its even-weight subcode. We treat several examples of cyclic codes of length ≥ 63.**

I. Introduction

IN THIS PAPER we shall study the relation between the zeros of codewords in a cyclic code and the minimum distance of that code. In many cases the results are considerably stronger than previously known lower bounds for the minimum distance. We use standard terminology from coding theory. For example, a cyclic code C of length n over the alphabet $\mathbb{F}_q$ will be identified with the corresponding ideal (also denoted by C) in the ring $\mathbb{F}_q[x]/(x^n - 1)$. This ideal C is generated by a polynomial $g(x)$ (which divides $x^n - 1$). The *minimum distance* of C is denoted by d. If α is a primitive nth root of unity in an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$, then $g(x)$ is a product of polynomials $m_i(x)$, where $m_i(x)$ denotes the minimal polynomial for α^i over $\mathbb{F}_q$. It will be convenient for us to use the following terminology. If $A = \{\alpha^{i_1}, \alpha^{i_2}, \cdots, \alpha^{i_l}\}$ is a set of nth roots of unity such that

$$c(x) \in C \Leftrightarrow \forall_{\xi \in A}[c(\xi) = 0],$$

then we shall say that A is a *defining set* for C (or that C is determined by A). If A is the maximal defining set for C, we shall call A *complete*.

Definition 1: We denote by $M(A)$ or $M(\alpha^{i_1}, \alpha^{i_2}, \cdots, \alpha^{i_l})$ the matrix of size l by n that has $1, \alpha^{i_k}, \alpha^{2i_k}, \cdots, \alpha^{(n-1)i_k}$ as its kth row; that is,

$$M(\alpha^{i_1}, \alpha^{i_2}, \cdots, \alpha^{i_l}) = \begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \cdots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \cdots & \alpha^{(n-1)i_2} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 1 & \alpha^{i_l} & \alpha^{2i_l} & \cdots & \alpha^{(n-1)i_l} \end{pmatrix}$$

Manuscript received June 14, 1983; revised November 2, 1984. This work was supported in part by the National Science Foundation under Grant MCS 8217596. The paper was written while the first author was a Fairchild Scholar at the California Institute of Technology. This paper was presented in part at the 14th Southeastern Conference on Combinatorics, Graph Theory and Computing, Florida Atlantic University, February 1983 and at the IEEE-IT 1984 Workshop, Caesarea, July 1984.

J. H. van Lint was with the California Institute of Technology, Pasadena. He is now with the Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, Eindhoven, The Netherlands.

R. M. Wilson is with the Department of Mathematics, California Institute of Technology, Pasadena, CA 91125.

IEEE Log Number 8406086.

If we consider this matrix as a parity check matrix for a cyclic code C^* over $\mathbb{F}_{q^m}$, then C is the corresponding subfield subcode. We refer to $M(A)$ as the *parity check matrix* corresponding to the set A. If we write each element of $M(A)$ in its representation as a column vector over $\mathbb{F}_q$, then we obtain the usual parity check matrix of size lm by n for the code C (which may have rank less than lm). If A is a defining set for a cyclic code C, then we denote the minimum distance of C by d_A.

If M is a matrix with n columns and $J \subseteq \{1, 2, \cdots, n\}$, then M_J is the submatrix of M consisting of the columns indexed by elements of J. Often J will be the *support* of a codeword $\mathbf{c}$, that is, $J = \{j | c_j \neq 0, 1 \leq j \leq n\}$.

Definition 2: A set $A = \{\alpha^{i_1}, \alpha^{i_2}, \cdots, \alpha^{i_l}\}$ will be called a *consecutive set* of length l if a primitive nth root of unity β and an exponent i exist such that $A = \{\beta^i, \beta^{i+1}, \cdots, \beta^{i+l-1}\}$.

A very well-known lower bound for the minimum distance of cyclic codes is the so-called Bose–Chaudhuri–Hocquenghem (BCH) bound.

Theorem 1 (BCH Bound): If a defining set A for a cyclic code contains a consecutive set of length $\delta - 1$, then $d_A \geq \delta$.

One of the proofs (cf. [4], [5]) of this theorem depends on the following lemma.

Lemma 1: If β is a primitive nth root of unity and $|J| = \delta - 1$, then $M(\beta^i, \beta^{i+1}, \cdots, \beta^{i+\delta-2})_J$ has rank $\delta - 1$.

We shall frequently use the following corollary of this lemma.

Corollary 1: If β is a primitive nth root of unity, $i_1 < i_2 < \cdots < i_k = i_1 + t - 1$ and $|J| = t$, then $M(\beta^{i_1}, \beta^{i_2}, \cdots, \beta^{i_k})_J$ has rank k.

The BCH bound was generalized by Hartmann and Tzeng [2]. Their result, which we call the *HT bound*, was slightly modified (and given an easy proof) by Roos (cf. [4, theorem 6.6.3] or [9]).

Theorem 2 (HT Bound): If $A = \{\alpha^{i_1}, \alpha^{i_2}, \cdots, \alpha^{i_l}\}$ is a defining set for a cyclic code and if β is a primitive nth root of unity such that A contains the consecutive sets $\{\beta^{i+ja}, \beta^{i+1+ja}, \cdots, \beta^{i+\delta-2+ja}\}$, $0 \leq j \leq s$, and if $(a, n) < \delta$, then $d_A \geq \delta + s$.

Our investigation was motivated by an extremely interesting generalization of Theorem 2 which was found recently by Roos [8]. Roughly speaking, the generalization says that if the conditions of Theorem 2 are satisfied, not for all j between 0 and s but for sufficiently many, then $d_A \geq \delta + s' - 1$ where s' is the number of values of j for

0018-9448/86/0100-0023$01.00

which the condition holds. To be more precise, we introduce the notation

$$AB = \{\xi\eta | \xi \in A, \eta \in B\}.$$

This notion of a product of sets will be the main element in Section II. If $B = \{\beta^{i_1}, \beta^{i_2}, \cdots, \beta^{i_t}\}$, where $i_1 < i_2 < \cdots < i_t$, then we denote by $\bar{B}$ the consecutive set with β^{i_1} as first element and β^{i_t} as last element.

Theorem 3 (Roos Bound): If A is a defining set for a cyclic code with minimum distance d_A and if B is a set of nth roots of unity such that $|\bar{B}| \leq |B| + d_A - 2$, then the code with defining set AB has minimum distance $d \geq |B| + d_A - 1$.

In the next section we shall give a proof of this theorem that is simpler than the original proof by Roos. Note that both the BCH bound and the original HT bound (with the condition $(a, n) = 1$) are special cases of Theorem 3. It is useful to give an example. (This example occurs in [8], but there it is only shown that $d \geq 7$.)

Example 1: Let C be the binary cyclic code of length 21 with generator $g(x) = m_1(x)m_3(x)m_7(x)m_9(x)$. The complete defining set of C is $R = \{\alpha^i | i = 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 14, 15, 16, 18\}$. Now take $A = \{\alpha^3, \alpha^4\}$. Then $d_A \geq 3$. Let $\beta = \alpha^4$, and take $B = \{\beta^j | j = 0, 1, 2, 3, 5, 6\}$. Then $|\bar{B}| = 7 \leq |B| + d_A - 2$. Since $AB \subseteq R$ we find from Theorem 3 that $d \geq 8$. (In fact, the minimum distance of this code is eight.)

In Section II we shall give a further generalization of Theorem 3. Our proof of this generalization is actually easier than the proof of Theorem 3 in [8]. The idea again is to find sets A and B such that AB is in the defining set of the code C. The theorem on the minimum distance of C depends on the ranks of $M(A)_I$ and $M(B)_I$ for certain subsets I of $\{1, 2, \cdots, n\}$. Therefore, after a section devoted to the relation between the distances of a cyclic code and certain subcodes, in Section IV we study the problem of determining the rank of a submatrix of a parity check matrix. Our new bound (Theorem 5) has led us to a technique that we call "*shifting*," which is treated in Section V. It seems to be more powerful than any of the earlier methods. Contrary to Theorem 3 and our generalization, it does not depend on the AB idea. As a first application of the methods of this paper, we study several generalizations of two-error-correcting BCH codes in Section VI. The main applications can be found in Section VII. There we consider all cyclic codes of length ≤ 57 for which the true minimum distance exceeds the BCH bound. In all cases but two (related ones), we find this true minimum distance by applying our results, which are based only on the defining set. This means that we do not use the square root bound for quadrature residue (QR) codes (cf. [5]). However, in a few cases we do need a theorem of a different nature, namely, a result due to McEliece [6]; luckily, this theorem also depends only on the zeros of the generator $g(x)$.

Section VIII was added at the request of one of the referees. In that section we treat several examples of codes with length ≥ 63 to show that our methods are still useful beyond the failure at $n = 57$.

II. Lower Bounds for the Minimum Distance of Cyclic Codes

We shall first consider a product operation for matrices that will be applied in the special situation where the matrices are parity check matrices of the form $M(A)$ defined in Definition 1. If $\boldsymbol{a} = (a_1, a_2, \cdots, a_n)$ and $\boldsymbol{b} = (b_1, b_2, \cdots, b_n)$ are vectors (words), then we define the product $\boldsymbol{a} * \boldsymbol{b} = (a_1b_1, a_2b_2, \cdots, a_nb_n)$. For an $m \times n$ matrix $\boldsymbol{A}$ with entries $a_{ij} (1 \leq i \leq m, 1 \leq j \leq n)$ and a matrix $\boldsymbol{B}$ with columns $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n$, we define

$$\boldsymbol{A} * \boldsymbol{B} = \begin{pmatrix} a_{11}\boldsymbol{b}_1 & a_{12}\boldsymbol{b}_2 & \cdots & a_{1n}\boldsymbol{b}_n \\ a_{21}\boldsymbol{b}_1 & a_{22}\boldsymbol{b}_2 & \cdots & a_{2n}\boldsymbol{b}_n \\ \cdot & \cdot & \cdots & \cdot \\ a_{m1}\boldsymbol{b}_1 & a_{m2}\boldsymbol{b}_2 & \cdots & a_{mn}\boldsymbol{b}_n \end{pmatrix},$$

that is, $\boldsymbol{A} * \boldsymbol{B}$ is a matrix that has as rows all the products $\boldsymbol{a} * \boldsymbol{b}$, where $\boldsymbol{a}$ is a row of $\boldsymbol{A}$ and $\boldsymbol{b}$ is a row of $\boldsymbol{B}$.

Theorem 4: If a linear combination, with *nonzero* coefficients, of the columns of $\boldsymbol{A} * \boldsymbol{B}$ is $\boldsymbol{0}$, then

$$\operatorname{rank}(\boldsymbol{A}) + \operatorname{rank}(\boldsymbol{B}) \leq n.$$

Proof: If

$$\sum_{j=1}^{n} \lambda_j a_{ij} \boldsymbol{b}_j = \boldsymbol{0}, \qquad 1 \leq i \leq m,$$

where $\lambda_j \neq 0$ $(1 \leq j \leq n)$, then every row of $\boldsymbol{A}$ is orthogonal to every row of $\boldsymbol{B}' = (\lambda_1\boldsymbol{b}_1, \lambda_2\boldsymbol{b}_2, \cdots, \lambda_n\boldsymbol{b}_n)$. Therefore, $\operatorname{rank}(\boldsymbol{A}) + \operatorname{rank}(\boldsymbol{B}') \leq n$. Since $\boldsymbol{B}$ and $\boldsymbol{B}'$ have the same rank, we are done.

The following theorem is an immediate corollary of Theorem 4.

Theorem 5: Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be matrices with entries from the field $\mathbb{F}$, and let $\boldsymbol{A} * \boldsymbol{B}$ be a parity check matrix for the code C over $\mathbb{F}$. If I is the support of a codeword in C, then

$$\operatorname{rank}(\boldsymbol{A}_I) + \operatorname{rank}(\boldsymbol{B}_I) \leq |I|.$$

In particular, C has minimum distance $\geq \delta$ if $\operatorname{rank}(\boldsymbol{A}_I) + \operatorname{rank}(\boldsymbol{B}_I) > |I|$ for every subset I of $\{1, 2, \cdots, n\}$ for which $|I| < \delta$.

This theorem is one of the main tools in our analysis of cyclic codes. In the applications we have $\boldsymbol{A} = M(A)$, $\boldsymbol{B} = M(B)$. The idea is as follows. First, observe that if A and B are sets of nth roots of unity, then every row of $M(A) * M(B)$ is also a row of $M(AB)$. Next, remark that we know from Corollary 1 that if β is a primitive nth root of unity and $S = A \cap \{\beta^i, \beta^{i+1}, \cdots, \beta^{i+t-1}\}$ and $|I| \geq t$, then $\operatorname{rank}(M(A)_I) \geq |S|$. If R is the defining set of a cyclic code, we try to find suitable sets A and B such that $AB \subseteq R$. The observations made above and Theorem 5 yield a lower bound for d_R.

Example 2: We illustrate the method by proving Theorem 3. Let A and B be the sets mentioned in the theorem. Then we have

$$\operatorname{rank}(M(A)_I) = \begin{cases} |I|, & \text{for } |I| < d_A \\ \geq d_A - 1, & \text{for } |I| \geq d_A. \end{cases}$$

From Corollary 1 and the condition on B and $\bar{B}$, we find

$$\operatorname{rank}(M(B)_I) \geq \begin{cases} 1, & \text{for } |I| < d_A \\ |I| - d_A + 2, & \text{for } d_A \leq |I| \leq |B| + d_A - 2. \end{cases}$$

Therefore,

$$\operatorname{rank}(M(A)_I) + \operatorname{rank}(M(B)_I) > |I| \quad \text{for } |I| \leq |B| + d_A - 2,$$

and the result follows from Theorem 5.

The following example displays the strength of the new bound compared with earlier results.

Example 3: In [8] Roos shows that it follows from Theorem 3 that the dual of the five-error-correcting BCH code of length 127 has minimum distance ≥ 22 (this could have been increased to 24 by applying Theorem 6 given later). This example had the nice feature that the result is stronger than the Carlitz–Uchiyama bound (cf. [3] or [5], where the same code is used to display the strength of the CU bound!). In fact, for the code in question the BCH bound gives $d \geq 16$, the HT bound gives $d \geq 18$, and CU gives $d \geq 20$. We now shall show that our method proves that $d \geq 30$. If we then apply McEliece's theorem (Theorem 6 of this paper) we find $d \geq 32$. Since the code contains the shortened second-order Reed–Muller code $\mathscr{R}(2,7)$, it follows that the minimum distance is equal to 32 (note that the code has 64 times as many words as $\mathscr{R}(2,7)$). To apply our method, we consider the defining set R of the code and observe that it contains the sets $\{\alpha^i | 81 \leq i \leq 95\}$, $\{\alpha^i | 98 \leq i \leq 111\}$, $\{\alpha^i | 113 \leq i \leq 127\}$, where α is a primitive 127th root of unity. Let

$$A = \{\alpha^i | 83 \leq i \leq 95\} \cup \{\alpha^i | 98 \leq i \leq 111\}$$
$$B = \{\beta^j | j = -7, 0, 1\}, \qquad \beta = \alpha^{16}.$$

Then $R \supseteq AB$. The set A contains 14 consecutive powers of α, and furthermore, it is a subset of a set of 29 consecutive powers of α, with the powers α^{96} and α^{97} missing. So, from Lemma 1 and Corollary 1 we find

$$\operatorname{rank}(M(A)_I) \geq \begin{cases} |I|, & \text{for } 1 \leq |I| \leq 14 \\ 14, & \text{for } 14 \leq |I| \leq 16 \\ |I| - 2, & \text{for } 17 \leq |I| \leq 29. \end{cases}$$

In the same way, we find

$$\operatorname{rank}(M(B)_I) \geq \begin{cases} |I|, & \text{for } 1 \leq |I| \leq 2 \\ 2, & \text{for } 2 \leq |I| \leq 8 \\ 3, & \text{for } |I| \geq 9. \end{cases}$$

By Theorem 5 we have $d_R \geq 30$. To show that the minimum distance of the code is in fact 32, we must apply either form of a theorem due to McEliece [6] stated later. The (more general) first form of the theorem will be used a number of times in Section VII. The proof is hard but a special case can be proved using a well-known argument that also occurs in the proof of the square-root bound [4, theorem 6.9.2 (iii)].

Theorem 6: I) Let C be a binary cyclic code of length n with complete defining set R. Let R' be the set of nth roots of unity that are not in R. If l is the smallest number of elements of R' (with repetitions allowed) that have product one, then the weight of every codeword in C is divisible by 2^{l-1}. II) If C is a primitive BCH code of length $n = 2^m - 1$ with designed distance $\delta < 2^{r+1} - 1$, then all weights in $C^\perp$ are divisible by $2^{\lfloor m/r \rfloor - 1}$.

Proof: I) We only prove the case $l = 3$. We then have $1 \in R$, and for each nth root of unity γ we have $\gamma \in R$ or $\gamma^{-1} \in R$. Let $c(x) = x^{i_1} + x^{i_2} + \cdots + x^{i_k}$ be a codeword. Since $1 \in R$, it follows that k is even. Since $c(x)c(x^{-1})$ is zero for every nth root of unity, it is zero in $\mathbb{F}_2[x]/(x^n - 1)$. However, if $x^{i-j} = x^{l-m}$, then $x^{j-i} = x^{m-l}$, that is, the terms cancel four at a time. Therefore, $k(k-1) \equiv 0 \pmod 4$, and hence $4 | k$.

II) Actually, the second assertion is a corollary of I), but it is not difficult to give a direct proof, as follows. The zeros of C are of the form α^i, where the integer i written in binary representation has at most r ones. Replacing α by α^{-1} and then considering $C^\perp$, we see that the zeros of $C^\perp$ all have the form α^j, where j written in binary representation has at most $m - r - 1$ ones. Hence $C^\perp$ is a subcode of the even-weight subcode of $\mathscr{R}(r, m)^*$. The result now follows from well-known theorems on Reed–Muller codes (cf. [3, theorem 6.2.3]).

Remark: Let C be a cyclic code of length n with generator $g(x)$ such that $g(1) \neq 0$. Suppose the even-weight subcode of C satisfies the conditions of Theorem 6-I. The code C contains the all-one word; therefore, a word of odd weight w must have $w \equiv n \pmod{2^{l-1}}$.

We conclude this section with two further theorems on parity check matrices that have the form $\boldsymbol{A} * \boldsymbol{B}$. In these theorems the matrices are binary. The theorems will not be used in the following sections.

Theorem 7: Let $\boldsymbol{A}$ be a binary matrix in which all the columns are different and not $\boldsymbol{0}$. Let $\boldsymbol{B}$ be the binary parity check matrix of a code with minimum distance d. Then $\boldsymbol{A} * \boldsymbol{B}$ is the parity check matrix of a code with minimum distance $\geq 2d - 1$.

Proof: 1) We shall first show that a binary code C of length n with minimum distance $\delta \geq (1/2)n + 1$ has a dual code $C^\perp$ that has minimum distance $\delta^\perp \leq 2$. To show this, consider a generator matrix G of C with a codeword of weight δ as its first row. Without loss of generality we can write G as

$$G = \left(\begin{array}{c|c} 11\cdots1 & 00\cdots0 \\ * & G' \end{array}\right),$$

where G' is the generator matrix of a code with length $n' = n - \delta$ and minimum distance $\delta' \geq \delta/2$. Therefore, $\delta' \geq (1/2)n' + 1$. Continuing in this way, we ultimately find a code with generator G^*, $\delta^* = n^*$, and $\delta^* \geq (1/2)n^* + 1$. Hence $n^* \geq 2$, and therefore G has two identical columns. This proves the assertion. (We could also have used an induction argument.)

2) Now consider the code with $A * B$ as parity check matrix. Suppose there is a set I with $|I| \leq 2d - 2$ that supports a codeword. As we saw in the proof of Theorem 4 the row space of A_I is contained in the dual of the row space of B_I. Since any $d - 1$ columns of B are linearly independent, it follows that the dual of the row space of B_I has distance $\geq d$. So by 1) the row space of B_I has minimum distance ≤ 2, contradicting the fact that it is contained in the dual of the row space of A_I, which clearly has distance at least three.

The following theorem extends the result of Theorem 7. We give a proof which uses the idea of Theorem 5.

Theorem 8: Let A be the binary parity check matrix of a code of length n with distance $d_A \geq 4$. Let B be the binary parity check matrix of a code of the same length with distance d_B, where $2 \leq d_B \leq (1/2)n$. Then $A * B$ is a parity check matrix for a code with minimum distance $d_{A*B} \geq 2d_B$.

Proof: We apply Theorem 5. First, let $I \subset \{1, 2, \cdots, n\}$ and suppose $|I| = l \leq d_B$. Then

$$\operatorname{rank}(A_I) + \operatorname{rank}(B_I) \geq \min\{l, 3\} + \min\{l, d_B - 1\} > l = |I|.$$

Next, assume $d_B < l < 2d_B$. Since A_I is a parity check matrix for a code of length l and distance ≥ 4, we must have

$$\operatorname{rank}(A_I) \geq 1 + \log l$$

(here the base of the logarithm is two). (To see this, assume that A_I has k linearly independent rows. If a is the first column of A_I and b is any column of A_I, then $a + b$ is not a column of A_I. Hence A_I has at most 2^{k-1} columns.) The matrix B_I is a parity check matrix for a code of length l and distance d_B. By the Plotkin bound (cf. [4, theorem 5.24]), this code has at most $2d_B/(2d_B - l)$ words, so it has at most $2d_B$ words. Therefore,

$$\operatorname{rank}(B_I) \geq l - 1 - \log d_B.$$

It follows that

$$\operatorname{rank}(A_I) + \operatorname{rank}(B_I) \geq l + \log \frac{l}{d_B} > l = |I|.$$

So by Theorem 5 the proof is complete.

Remark: Theorem 7 can also be proved in the same way as Theorem 8 was proved.

Corollary 2: The rth order Reed–Muller code $\mathcal{R}(r, m)$ of length $n = 2^m$ has minimum distance 2^{m-r}.

Proof: Take A to be the parity check matrix for an extended Hamming code. Then $A * A * \cdots * A$ ($m - r - 1$ factors) is a parity check matrix for $\mathcal{R}(r, m)$.

The main result of this section is Theorem 5. To apply it successfully, we shall have to develop methods to find the rank of a matrix $M(A)_I$. This will be done in Section IV. First, however, we must deal with another difficulty, namely, the problem that could arise from looking at binary codes defined by a parity check matrix over an extension field $\mathbb{F}$. In this case, one must distinguish the code over $\mathbb{F}$ and the subfield subcode. This question and so-called contracted codes are considered in Section III.

III. Subcodes and Contracted Codes

When we apply the theorems of Sections I and II to cyclic codes over some field $\mathbb{F}_q$, we shall always consider the parity check matrix, say $M(A)$, as a parity check matrix for a code over the proper extension field $\mathbb{F}_{q^m}$ and subsequently consider the subfield subcode. If we take the defining set $A \subseteq \mathbb{F}_{q^m}$ to be complete, then the two codes have the same minimum distance, as shown by the following theorem.

Theorem 9: Let $A = \{\alpha^{i_1}, \alpha^{i_2}, \cdots, \alpha^{i_k}\} \subseteq \mathbb{F}_{q^m}$ be a set of nth roots of unity such that $\forall_{\gamma \in A}[\gamma^q \in A]$. Then the cyclic code over $\mathbb{F}_{q^m}$ with parity check matrix $M(A)$ and its subfield subcode over $\mathbb{F}_q$ have the same minimum distance.

Proof: Let c_i ($1 \leq i \leq n$) be the ith column of $M(A)$. Let $x = (x_1, x_2, \cdots, x_n)$ be a codeword in the code over $\mathbb{F}_{q^m}$ with A as defining set, that is, $\sum_{i=1}^n x_i c_i = 0$. The condition on A then implies that $\sum_{i=1}^n x_i^q c_i = 0$, and hence $\sum_{i=1}^n \operatorname{tr}(x_i) c_i = 0$ where tr denotes the trace from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. All scalar multiples of x are also codewords, so we may assume $\operatorname{tr}(x_1) \neq 0$. If x is a word of minimal weight, then we must have $\operatorname{tr}(x_i) \neq 0$ for all i for which $x_i \neq 0$ ($1 \leq i \leq n$). In that case, $(\operatorname{tr}(x_1), \operatorname{tr}(x_2), \cdots, \operatorname{tr}(x_n))$ is a word of minimal weight in the subfield subcode.

The following theorem will be useful in our analysis of binary cyclic codes in Section VII.

Theorem 10: Let $n = ln_0$. Let d be the minimum distance of the binary cyclic code C of length n for which the defining set contains $\alpha^{li_1}, \alpha^{li_2}, \cdots, \alpha^{li_k}$ (where α is a primitive nth root of unity). Let d_0 be the minimum distance of the cyclic code $\hat{C}$ of length n_0 (a "contraction" of C) with defining set $\{\zeta^{i_1}, \zeta^{i_2}, \cdots, \zeta^{i_k}\}$, $(\zeta = \alpha^l)$. Then d is even or $d \geq d_0$.

Proof: Note that ζ is a primitive n_0th root of unity. If $c = (c_0, c_1, \cdots, c_{n-1}) \in C$, then $\sum_{j=0}^{n-1} c_j (\alpha^{li_\nu})^j = 0$ ($1 \leq \nu \leq k$), and hence $\sum_{j=0}^{n_0-1} b_j (\zeta^{i_\nu})^j = 0$ ($1 \leq \nu \leq k$), where $b_j = c_j + c_{j+n_0} + c_{j+2n_0} + \cdots$. Therefore, $(b_0, b_1, \cdots, b_{n_0-1}) \in \hat{C}$. If $b_j = 0$ for $0 \leq j \leq n_0 - 1$, then c has even weight. Otherwise, at least d_0 of the coordinates c_j are one.

Example 4: Consider the binary cyclic code of length 35 with generator $m_5(x)m_7(x)$. The defining set for this code is $A = \{\alpha^i | i = 5, 7, 10, 14, 20, 21, 28\}$. By the BCH bound $d \geq 3$ (from α^{20}, α^{21}), and all the other theorems in Sections I and II cannot improve this. If we take $l = 7$, $n_0 = 5$ in Theorem 10, we find that d is even or $d \geq 5$ because the contracted code is clearly the repetition code of length five. Therefore, $d \geq 4$. (The minimum distance of this code is, in fact, four; cf. Theorem 13.)

Remark: A direct proof that the code of Example 4 has $d \geq 4$ can be given as follows. Suppose there is a word of weight three. This would imply the existence of two 35th roots of unity ξ, η, such that $1 + \xi^5 + \eta^5 = 0$ and $1 + \xi^7 + \eta^7 = 0$. Since $1 + \eta^7 + \eta^{14} + \eta^{21} + \eta^{28} = 0$ and $(1 + \eta^7)^5 = \xi^{35} = 1$, that is, $1 + \eta^7 + \eta^{28} + \eta^{35} = 1$, we find $\eta^{14} = \eta^{21}$—a contradiction.

Example 5: Consider the binary cyclic code of length 45 with generator $g(x) = m_1(x)m_3(x)m_5(x)m_{15}(x)$. The defining set for this code contains $\{\alpha^i | 1 \leq i \leq 6\}$. Hence $d \geq 7$ by the BCH bound. Again apply Theorem 10, now with $l = 5$, $n_0 = 9$. The contracted code of length $n_0 = 9$ has the zeros $\{\zeta^i | 1 \leq i \leq 8\}$, $(\zeta = \alpha^5)$. So we find $d_0 = 9$. Therefore, $d \geq 8$ (which is the true minimum distance). This method works as soon as $m_5(x)m_{15}(x) | g(x)$. We did not succeed in showing that $d \geq 8$ by any of the other theorems in Sections I and II. We consider this same code in Example 8. Further applications of Theorem 10 will occur in the analysis of cyclic codes with $n \leq 57$ in Section VII.

IV. On the Rank of Submatrices of $M(A)$

In this section we shall prove a number of lemmas concerning the ranks of parity check matrices of type $M(A)$ and their submatrices. These lemmas will be used in several applications of Theorem 5. Let us first show, by example, how the lemmas of this section can prove useful. Suppose the defining set of a code contains a consecutive set of length $l + 1$ starting with α^i and a consecutive set of length l starting with α^{i+t}. Both the BCH bound and the HT bound (if it can be applied) show that $d \geq l + 2$. We would like to show that $d \geq l + 3$. We could try to use Theorem 5 with $A = \{\alpha^i, \alpha^{i+1}, \cdots, \alpha^{i+l-1}\}$, $B = \{1, \alpha, \alpha^t\}$. To succeed we would need to know that rank $(M(B)_I) \geq 3$ if $|I| \geq l + 2$. Lemma 3 is a typical example of a result of this kind.

Lemma 2: Let $A = \{\alpha^{i_1}, \alpha^{i_2}, \cdots, \alpha^{i_k}\}$ be a set of roots of unity (where α is a primitive nth root of unity). Let $l \leq k$, and suppose that for some set $I \subset \{1, 2, \cdots, n\}$ the matrix $M(A)_I$ has rank $< l$. Then there is a polynomial $m(x)$ dividing $x^n - 1$, with degree $m(x) = m \triangleq |I|$, such that any l of the monomials $x^{i_1}, x^{i_2}, \cdots, x^{i_k}$ are linearly dependent elements in the algebra $\mathcal{A} = \mathbb{F}[x]/(m(x))$.

Proof: The matrix $M_I = M(A)_I$ has the form

$$M_I = \begin{pmatrix} \xi_1^{i_1} & \xi_2^{i_1} & \cdots & \xi_m^{i_1} \\ \xi_1^{i_2} & \xi_2^{i_2} & \cdots & \xi_m^{i_2} \\ \cdot & \cdot & \cdots & \cdot \\ \xi_1^{i_k} & \xi_2^{i_k} & \cdots & \xi_m^{i_k} \end{pmatrix}.$$

Define $m(x) \triangleq \prod_{j=1}^{m}(x - \xi_j)$. Any l of the rows of M_I are dependent. This is equivalent to the assertion of the lemma.

The idea of this lemma is used in the proofs of several of the following lemmas on ranks.

Lemma 3: If α is a primitive nth root of unity in $\mathbb{F}_{2^r}$ and $\sigma = 2^i$ generates the same group as 2 mod n, then any three columns of $M(1, \alpha, \alpha^\sigma)$ have rank 3.

Proof: Suppose the assertion is false. Then by Lemma 2 the monomials $1, x, x^\sigma$ are dependent in $\mathcal{A} = \mathbb{F}_{2^r}[x]/(m(x))$ for some polynomial $m(x)$ of degree three. So we have

$$x^\sigma \in \text{span}\{1, x\} \text{ in } \mathcal{A}.$$

Now, if $y \in \text{span}\{1, x\}$ in $\mathcal{A}$, then $y^\sigma \in \text{span}\{1, x^\sigma\} = \text{span}\{1, x\}$, and inductively it follows that $y^{\sigma^j} \in \text{span}\{1, x\}$ for every j. This implies that $x^2 \in \text{span}\{1, x\}$. This means that $m(x)$ divides $x^2 + ax + b$ for some $a, b \in \mathbb{F}_{2^r}$, a contradiction.

Lemma 4: If α is a primitive nth root of unity in $\mathbb{F}_{2^r}$ and if $\sigma = 2^i$ generates the same group as 2 mod n, then

1) any four columns of $M(\alpha, \alpha^\sigma, \alpha^{\sigma^2})$ have rank 3,
2) any five columns of $M(1, \alpha, \alpha^\sigma, \alpha^{\sigma^2})$ have rank 4,
3) any eight columns of $M(\alpha, \alpha^\sigma, \alpha^{\sigma^2}, \alpha^{\sigma^3})$ have rank 4.

Proof: 1) Arguing as in the proof of Lemma 3, we find that x, x^2, and x^4 are in span $\{x, x^\sigma\}$ in an algebra $\mathcal{A} = \mathbb{F}_{2^r}[x]/(m(x))$ for some polynomial $m(x)$ of degree four. This contradicts Corollary 1. Parts 2) and 3) are done in the same way.

Although we have no example of a useful application of the following proposition, it is a typical example of the ideas of this section.

Proposition 1: If α is a primitive nth root of unity in $\mathbb{F}_{2^r}$ and $t > 1$, then either 1) any $t + 2$ columns of $M(1, \alpha, \alpha^{2^t-1})$ have rank 3, or 2) the *binary* code with $M(1, \alpha, \alpha^{2^t-1})$ as parity check matrix has minimum distance $\leq t + 2$.

Proof: Consider a three-by-$(t + 2)$ submatrix of $M(1, \alpha, \alpha^{2^t-1})$, say

$$M_1 = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \xi_1 & \xi_2 & \cdots & \xi_{t+2} \\ \xi_1^{\sigma-1} & \xi_2^{\sigma-1} & \cdots & \xi_{t+2}^{\sigma-1} \end{pmatrix}, \qquad \sigma = 2^t.$$

If the rows of M_1 are dependent, then so are the rows of

$$M_2 = \begin{pmatrix} \xi_1 & \xi_2 & \cdots & \xi_{t+2} \\ \xi_1^2 & \xi_2^2 & \cdots & \xi_{t+2}^2 \\ \xi_1^\sigma & \xi_2^\sigma & \cdots & \xi_{t+2}^\sigma \end{pmatrix}.$$

Hence the elements ξ_i $(1 \leq i \leq t + 2)$ are zeros of some polynomial $x^\sigma + ax^2 + bx$. The zeros of this (linearized) polynomial form a t-dimensional space over $\mathbb{F}_2$. Therefore, a subset of $t + 2$ of these zeros contains a subset of even cardinality with sum zero, say, without loss of generality, $\xi_1 + \xi_2 + \cdots + \xi_k = 0$. Since k is even, we have $\xi_1^0 + \xi_2^0 + \cdots + \xi_k^0 = 0$, and therefore we must also have $\xi_1^{\sigma-1} + \xi_2^{\sigma-1} + \cdots + \xi_k^{\sigma-1} = 0$. We therefore have found a word of weight $k \leq t + 2$ in the binary code with $M(1, \alpha, \alpha^{2^t-1})$ as parity check matrix.

In some applications of Theorem 5, it will be necessary to prove results similar to those of this section ad hoc (cf. Examples 26 and 53).

Remark: We shall often use the fact that for $I \subset \{1, 2, \cdots, n\}$ the numbers rank $M(\alpha^{i_1}, \alpha^{i_2}, \cdots, \alpha^{i_k})_I$ and rank $M(\alpha^{i_1+j}, \alpha^{i_2+j}, \cdots, \alpha^{i_k+j})_I$ are equal.

V. Shifting

The lemmas about ranks of matrices $M(A)_I$ that were proved in the previous section were based only on the cardinality of I. Sometimes we can do more if we restrict ourselves to sets $I \subseteq \{1, 2, \cdots, n\}$ that support codewords in the code defined by A. We shall prove a lemma on the rank of $M(A)_I$ based on this assumption. It is possible to rephrase this result in such a way that it yields a *direct* method for finding bounds on the minimum distance of cyclic codes (i.e., a method that does not involve the product method of Section II). This method, which we call shifting, is the main topic of this section.

Lemma 5: Let C be a code with defining set R, and let $\mathbf{c} \in C$ be a codeword with support $\subseteq I$ such that $\mathbf{c}$ does not belong to the code with defining set $R \cup \{\alpha^j\}$. Then for any set $\{\alpha^{i_1}, \alpha^{i_2}, \cdots, \alpha^{i_k}\} \subset R$ we have

$$\operatorname{rank}\left(M(\alpha^{i_1}, \alpha^{i_2}, \cdots, \alpha^{i_k}, \alpha^j)_I\right) = 1 + \operatorname{rank}\left(M(\alpha^{i_1}, \cdots, \alpha^{i_k})_I\right).$$

Proof: The word $\mathbf{c}$ yields a linear combination of the columns of $M(\alpha^{i_1}, \cdots, \alpha^{i_k})_I$, which is $\mathbf{0}$. The same linear combination of columns of this matrix extended by the row $(1, \alpha^j, \alpha^{2j}, \cdots, \alpha^{(n-1)j})_I$ is not $\mathbf{0}$. Therefore, the last row of $M(\alpha^{i_1}, \cdots, \alpha^{i_k}, \alpha^j)_I$ does not belong to the span of the other rows.

Example 6: We treat an example that shows how Lemma 5 can be used, but it is mainly intended as an introduction to the remainder of this section. Let C be the binary code of length 51 with generator $g(x) = m_1(x)m_3(x)m_{19}(x)$. This code has defining set $R = \{\alpha^i | i = 1, 2, 3, 4, 6, 8, 12, 13, 16, 19, 24, 25, 26, 27, 32, 35, 38, 39, 43, 45, 47, 48, 49, 50\}$. We wish to show that C has minimum distance $d \geq 9$. First, consider the even-weight subcode. We must add zero to the set R, and since we then have nine consecutive powers of α, the even-weight subcode has minimum distance ≥ 10. Next, observe that R contains $\{\alpha^i | i = 1, 2, 3, 4\} \cdot \{\alpha^j | j = 0, 23, 46\}$; therefore, we find $d \geq 7$ by the HT bound (Theorem 2). Therefore, it suffices to show that $d \neq 7$. Suppose $|I| = 7$ and that I is the support of a codeword in C. Note that if we add α^5 to R we may also add $\alpha^{5 \cdot 2^5} = \alpha^7$. This yields eight consecutive powers of α, and therefore we know from the BCH bound that I is not the support of a codeword with $R \cup \{\alpha^5\}$ as defining set.

Now we apply Lemma 5 and the remark at the end of Section IV:

$$\begin{aligned}
&\operatorname{rank}\left(M(\alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^{24})_I\right) \\
&\quad = \operatorname{rank}\left(M(\alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^{25})_I\right) \\
&\quad = 1 + \operatorname{rank}\left(M(\alpha^2, \alpha^3, \alpha^4, \alpha^{25})_I\right) \\
&\quad = 1 + \operatorname{rank}\left(M(\alpha^3, \alpha^4, \alpha^5, \alpha^{26})_I\right) \\
&\quad = 2 + \operatorname{rank}\left(M(\alpha^3, \alpha^4, \alpha^{26})_I\right) \\
&\quad = 2 + \operatorname{rank}\left(M(\alpha^4, \alpha^5, \alpha^{27})_I\right) \\
&\quad = 3 + \operatorname{rank}\left(M(\alpha^4, \alpha^{27})_I\right) = 5.
\end{aligned}$$

If we take $A = \{\alpha^i | i = 1, 2, 3, 4, 24\}$, $B = \{\alpha^j | j = 0, 23, 46\}$, then rank $(M(B)_I) = 3$ by Lemma 1. Theorem 5 now shows us that we have found a contradiction. This proves the assertion. Why we call the method shifting has become clear. In the following we avoid the use of Theorem 5.

We shall introduce the concept of the "independent set." The reader should have no difficulty recognizing it as the same thing as shifting. Let S be a subset of a field $\mathbb{F}$. We inductively define a family of subsets of $\mathbb{F}$, which we call independent with respect to S, as follows.

1) $\varnothing$ is independent with respect to S.

2) If A is independent with respect to S, $A \subseteq S$, $b \notin S$, then $A \cup \{b\}$ is independent with respect to S.

3) If A is independent with respect to S and $c \in \mathbb{F}$, $c \neq 0$, then cA is independent with respect to S.

Theorem 11: Let $f(x)$ be a polynomial with coefficients in $\mathbb{F}$, and let $S = \{a \in \mathbb{F} | f(a) = 0\}$. Then the weight $\operatorname{wt}(f)$ of $f(x)$ satisfies

$$\operatorname{wt}(f) \geq |A|$$

for every subset A of $\mathbb{F}$ that is independent with respect to S.

Proof: Write

$$f(x) = \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_k x^{i_k},$$

where $\lambda_i \neq 0$ $(1 \leq i \leq k)$, $k = \operatorname{wt}(f)$. We shall show inductively that if A is independent with respect to S, then the vectors in the set

$$V(A) = \{(a^{i_1}, a^{i_2}, \cdots, a^{i_k}) | a \in A\}$$

are (distinct and) linearly independent over $\mathbb{F}$. This will prove $|A| \leq k$ and hence the theorem. By 1) our assertion is true for $A = \varnothing$. Suppose the vectors in $V(A)$ are linearly independent and that $A \subseteq S$. Let $b \notin S$. By 2) the set $A \cup \{b\}$ is independent with respect to S. Since each element of A is a zero of $f(x)$ but $f(b) \neq 0$, the vector $(\lambda_1, \lambda_2, \cdots, \lambda_k)$ has inner product zero with the vectors in $V(A)$, but not with $(b^{i_1}, b^{i_2}, \cdots, b^{i_k})$. Hence this latter vector is not in the span of $V(A)$, and thus the vectors in $V(A \cup \{b\})$ are linearly independent. Finally, suppose the vectors in $V(A)$ are linearly independent and $0 \neq c \in \mathbb{F}$. Since $V(cA)$ is obtained from $V(A)$ by application of the linear transformation with matrix $\operatorname{diag}(c^{i_1}, c^{i_2}, \cdots, c^{i_k})$, it also consists of linearly independent vectors.

To demonstrate the strength of Theorem 11, we shall show that it implies that the binary Golay code has $d = 7$. Of course, this is a well-known fact, but as far as we know this has not been explained on the basis of the zeros of codewords only.

Example 7 (the Binary Golay Code): We consider the binary cyclic code C of length 23 with generator $g(x) = m_1(x)$. The defining set R of this code is $R = \{\alpha^i | i = 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$. Observe that $x^{23} - 1 = (x - 1)m_1(x)m_5(x)$. Let $f(x) \in C$, and let $S = \{a \in \mathbb{F}_{2^{11}} | f(a) = 0\}$. If $m_5(x) | f(x)$, then either $f(x) = 0$ or $f(x) = (x^{23} - 1)/(x - 1)$, which has weight 23. So we may assume S contains no zeros of $m_5(x)$. We construct a sequence $A_0, A_1, A_2, \cdots$ of subsets of $\mathbb{F}_{2^{11}}$ that are inde-

pendent with respect to S (shifting):

$$A_0 = \emptyset; \quad \text{for each } i > 0,\ a_iA_i \subseteq S,$$
$$b_i \notin S \text{ and } A_{i+1} = a_iA_i \cup \{b_i\}:$$

$$a_0 = 1,\ b_0 = \alpha^5 \mapsto A_1 = \{\alpha^5\},$$
$$a_1 = \alpha^{-1},\ b_1 = \alpha^5 \mapsto A_2 = \{\alpha^4, \alpha^5\},$$
$$a_2 = \alpha^{-3},\ b_2 = \alpha^5 \mapsto A_3 = \{\alpha^1, \alpha^2, \alpha^5\},$$
$$a_3 = \alpha^7,\ b_3 = \alpha^{14} \mapsto A_4 = \{\alpha^8, \alpha^9, \alpha^{12}, \alpha^{14}\},$$
$$a_4 = \alpha^4,\ b_4 = \alpha^5 \to A_5 = \{\alpha^{12}, \alpha^{13}, \alpha^{16}, \alpha^{18}, \alpha^5\},$$
$$a_5 = \alpha^{-10},\ b_5 = \alpha^5 \mapsto A_6 = \{\alpha^2, \alpha^3, \alpha^6, \alpha^8, \alpha^{18}, \alpha^5\}.$$

It follows from Theorem 11 that $\mathrm{wt}(f) \geq |A_6| = 6$. Suppose $\mathrm{wt}(f) = 6$. Then $(x-1)|f(x)$, i.e., $\alpha^0 \in S$. Then $\alpha^{-2}A_6 \subseteq S$, and therefore $A_7 = \alpha^{-2}A_6 \cup \{\alpha^5\}$ is independent with respect to S, contradicting Theorem 11. It follows that $\mathrm{wt}(f) \geq 7$.

It is interesting to observe that the BCH bound is a corollary of Theorem 11. To show this, consider a consecutive set of zeros of a codeword $f(x)$, say $\{\alpha^i, \alpha^{i+1}, \cdots, \alpha^{i+\delta-1}\}$. Let $f(\alpha^{i+\delta}) \neq 0$. In this case, we shift as follows:

$$\emptyset \mapsto \{\alpha^{i+\delta}\} \mapsto \{\alpha^{i+\delta-1}, \alpha^{i+\delta}\} \mapsto \cdots \mapsto \{\alpha^i, \alpha^{i+1}, \cdots, \alpha^{i+\delta}\},$$

showing that $\mathrm{wt}(f) > \delta$. In the same way, the HT bound can be obtained as a corollary of Theorem 11 (cf. [10]).

The following example (also considered in Example 5) shows the relation between shifting and the product method of Theorem 5.

Example 8: Let C be the binary cyclic code of length 45 with generator $g(x) = m_1(x)m_3(x)m_5(x)m_{15}(x)$. The defining set of this code is

$$R = \{\alpha^i | i = 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 19, 20, 23, 24, 25, 30, 31, 32, 34, 35, 38, 40\}.$$

Note that the zeros of $m_7(x)$ are $\{\alpha^i | i = 7, 11, 13, 14, 22, 26, 28, 29, 37, 41, 43, 44\}$. If C has a word $f(x)$ of weight seven then $f(x)$ is not divisible by $m_7(x)$ (by the BCH bound). Let S be the zero set of $f(x)$. As in the previous example, we construct a sequence $A_1, A_2, \cdots$ of subsets of $\mathbb{F}_{2^{12}}$ that are independent with respect to S. For each $i > 0$, $a_iA_i \subseteq S$, $b_i \notin S$, and $A_{i+1} = a_iA_i \cup \{b_i\}$:

$$A_1 = \{\alpha^1, \alpha^2, \alpha^3\},$$
$$a_1 = 1,\ b_1 = \alpha^{22} \mapsto A_2 = \{\alpha^1, \alpha^2, \alpha^3, \alpha^{22}\},$$
$$a_2 = \alpha,\ b_2 = \alpha^{29} \mapsto A_3 = \{\alpha^2, \alpha^3, \alpha^4, \alpha^{23}, \alpha^{29}\},$$
$$a_3 = \alpha,\ b_3 = \alpha^{11} \mapsto A_4 = \{\alpha^3, \alpha^4, \alpha^5, \alpha^{24}, \alpha^{30}, \alpha^{11}\},$$
$$a_4 = \alpha,\ b_4 = \alpha^{14} \mapsto A_5 = \{\alpha^4, \alpha^5, \alpha^6, \alpha^{25}, \alpha^{31}, \alpha^{12}, \alpha^{14}\},$$
$$a_5 = \alpha^{26},\ b_5 = \alpha^7 \mapsto A_6 = \{\alpha^{30}, \alpha^{31}, \alpha^{32}, \alpha^6, \alpha^{12}, \alpha^{38}, \alpha^{40}, \alpha^7\}.$$

Since the independent set A_6 has cardinality eight we have a contradiction, and hence C has minimum distance ≥ 8. The sequence of independent sets immediately shows us two sets A and B such that $AB \subset R$, namely, $A = A_1 = \{\alpha^1, \alpha^2, \alpha^3\}$ and $B = \{a_1, a_1a_2, a_1a_2a_3, \cdots\} = \{1, \alpha, \alpha^2, \alpha^3, \alpha^{29}\}$. So, in principle, we can now apply Theorem 5 by trying to show that if $I \subseteq \{1, 2, \cdots, 45\}$ and $|I| = 7$, then $\mathrm{rank}(M(B)_I) = 5$. However, this is false! If we take I from the multiples of five, then the rows of $M(B)_I$ corresponding to α^2 and α^{29} are identical. So, we must use in some way the fact that I is the support of a codeword.

VI. Generators with Few Factors

In general, a binary cyclic code with defining set $A = \{\alpha^i\}$ will not be very good. For example, if the code is a primitive BCH code (i.e., $n = 2^m - 1$), then the code has $d = 2$ or $d = 3$. In this section we wish to study codes that have a defining set of the form $A = \{\alpha^i, \alpha^j\}$. From the BCH bound we know that if $(i, j) = (1, 3)$ then the code has $d \geq 5$. Our main interest will be in finding other pairs with this property. If $n + 1$ is not a power of two, no interesting general statements can be made. For example, we have seen that for $n = 23$ the polynomial $m_1(x)m_5(x)$ generates the repetition code. So, we usually consider only codes with $n = 2^m - 1$. We shall first prove two theorems that show that we should not expect too much.

Theorem 12: Let $n = 2^m - 1$, $m \geq 4$, m odd. The minimum distance of the binary cyclic code of length n generated by $m_1(x)m_t(x)$ is at most five if $(t, n) = 1$ and at most four otherwise.

Proof: We remark that $d \leq 6$ by the Hamming bound. First, assume $(n, t) = 1$. Let $\mathbb{F} = \mathrm{GF}(2^m)$. We define

$$H = \{\alpha^t + \beta^t | \alpha + \beta = 1 \text{ in } \mathbb{F}, \{\alpha, \beta\} \neq \{0, 1\}\}.$$

So, $|H| = (n-1)/2$ if $d > 4$. From now on assume that $d > 3$.

1) We consider triples $T = \{\alpha, \beta, \gamma\} \subset \mathbb{F}^*$. We call T a triple of type (a, b) if $\alpha + \beta + \gamma = a$, $\alpha^t + \beta^t + \gamma^t = b$. The number of triples T with $\alpha + \beta + \gamma = 0$ is $n(n-1)/6$ and the same holds for triples T with $\alpha^t + \beta^t + \gamma^t = 0$. These triples are different since $d > 3$. Therefore, there are $[(n-1)(n-4)]/6$ triples of types $(1, b)$, $(b \neq 0)$. If a triple of type $(1, b)$ with $b \in H \cup \{1\}$ occurs, we have a codeword of weight ≤ 5. So, assume this does not happen. We have $(n-1)/2$ possibilities for b. So, for these values of b, the average number of triples of type $(1, b)$ is $(n-4)/3$. If two triples of type $(1, b)$ are not disjoint, we find a codeword of weight four. If there were $(n-1)/3$ disjoint triples of type $(1, b)$ then, since these triples do not contain zero or one, the sum of the elements of $\mathbb{F}$ is one, a contradiction. Therefore, for each type $(1, b)$ that occurs, there are exactly $(n-4)/3$ triples of this type.

2) Consider triples $S = \{\xi, \eta, \zeta\} \subset \mathbb{F}^*$ of type $(0, b)$. We know that $b = 0$ does not occur (since $b = 0$ would imply the existence of a codeword of weight three). Therefore, for each $b \neq 0$, there are $(n-1)/6$ triples of type $(0, b)$. If two such triples are not disjoint, then we find a

codeword of weight four. None of these triples contains one.

3) Consider a triple T of type $(1, b)$ and triple S of type $(0, b+1)$. If these overlap, then from S, T, and $\{1\}$ we find a codeword of weight ≤ 5. If the triples T of type $(1, b)$ and the triples S of type $(0, b+1)$ do not overlap, then by counting the cardinality of their union, we find

$$3\left\{\frac{n-4}{3}+\frac{n-1}{6}\right\} \leq n-1,$$

i.e., $n \leq 7$.

4) If $(t, n) > 1$, then there are more than $[(n-1)(n-4)]/6$ triples of types $(1, b)$ with $b \neq 0$. The argument given in 1) then shows we must have a codeword of weight ≤ 4.

Remark: The first assertion (i.e., $d \leq 5$) is also true if m is even (consider a subfield).

Theorem 13: Let p and q be two integers with $(p, q) = 1$. A binary cyclic code of length $n = pq$ with generator $m_p(x)m_q(x)$ has minimum distance ≤ 4.

Proof: Let α be a primitive nth root of unity, $\zeta_p = \alpha^q$, $\zeta_q = \alpha^p$. By the Chinese Remainder theorem, an integer $a < n$ exists such that $a \equiv 0 \pmod p$, $a \equiv 1 \pmod q$, and an integer $b < n$ exists such that $b \equiv 1 \pmod p$, $b \equiv 0 \pmod q$. The polynomial $f(x) = 1 + x + x^a + x^b$ satisfies $f(\zeta_p) = f(\zeta_q) = 0$. That is, $f(x)$ is a codeword.

The following lemma will be used several times.

Lemma 6: Let C be a binary cyclic code of length $n = 2^m - 1$ with generator $g(x) = m_1(x)\prod_{i \in K} m_i(x)$, where each $i \in K$ is of the form $i = 1 + 2^k$ for some k. Then the minimum weight of C is odd.

Proof: Let the positions ξ_j $(j \in J)$ correspond to a codeword of even weight w. Then $\sum_j \xi_j^0 = \sum_j \xi_j^1 = 0$ and also $\sum_j \xi_j^i = 0$ $(i \in K)$. For any η and $i = 1 + 2^k$, we have

$$\begin{aligned}(\xi_j + \eta)^i &= (\xi_j + \eta)^{1+2^k} \\ &= \xi_j^i + \xi_j^{2^k}\eta + \xi_j\eta^{2^k} + \eta^i\end{aligned}$$

and therefore $\sum_j (\xi_j + \eta)^i = 0$. This means that the positions $\xi_j + \eta (j \in J)$ also correspond to a codeword. Taking $\eta = \xi_1$ yields a codeword of weight $w - 1$.

We now give a first generalization of two-error-correcting BCH codes (cf. [1]).

Theorem 14: Let $n = 2^m - 1$, $(i, m) = 1$, $\sigma = 2^i$. The binary cyclic code of length n with generator $g(x) = m_1(x)m_{\sigma+1}(x)$ has minimum distance five.

Proof: By Theorem 12 we have $d \leq 5$. We give three different proofs of $d \geq 5$.

1) Since $\{\alpha^j | j = 1, 2, \sigma, \sigma + 1\}$ is a defining set, we have $d \geq 4$ by the HT bound. The result then follows from Lemma 6.

2) Let $A = \{\alpha^0, \alpha^1\}$ and $B = \{\beta, \beta^\sigma, \beta^{\sigma^2}\}$, where $\beta = \alpha^{2^{m-i}}$. Then the defining set for the code contains AB. Since $(\sigma - 1, n) = 1$ any two columns of $M(B)$ have rank two. By Lemma 4-1) any four columns of $M(B)$ have rank three. So we are finished by Theorem 5.

3) Lemma 2 also provides us with a way to prove Theorem 14. Take $A = \{1, \alpha, \alpha^2, \alpha^\sigma, \alpha^{\sigma+1}\}$ and $l = 4$ in the lemma. Then $1, x, x^2, x^3$ is a basis for $\mathscr{A}$ and by the lemma, we must have $x^\sigma = ax^2 + bx + c$ in $\mathscr{A}$. This implies that $x^{\sigma+1} = ax^3 + bx^2 + cx$, but since $x^{\sigma+1} \in \text{span}\{1, x, x^2\}$ we see that $a = 0$, that is, $x^\sigma \in \text{span}\{1, x\}$. In the same way as in the proof of Lemma 3, this implies that $x^{\sigma^j} \in \text{span}\{1, x\}$ for all j and hence $x^2 \in \text{span}\{1, x\}$, a contradiction.

The next theorem also gives a class of two-error-correcting codes (cf. [5, ch. 9 § 11], [1], [8]).

Theorem 15: Let $n = 2^m - 1$, m odd. Let $t = \lfloor m/4 \rfloor$ and $\sigma = 2^t$. Then the binary cyclic code of length n with generator $g(x) = m_{\sigma+1}(x)m_{2\sigma+1}(x)$ has minimum distance five (except if $m = 3$, in which case the distance is seven).

Proof: By Theorem 12 we know that $d \leq 5$ for $m > 3$. We distinguish between $m \equiv 1 \pmod 4$ and $m \equiv 3 \pmod 4$.

Case 1, $m = 4t + 1$: We apply Theorem 5. A defining set for the code contains AB, where $A = \{\alpha, \alpha^{\sigma^2}\}$, $B = \{\alpha^\sigma, \alpha^{\sigma^3}, \alpha^{2\sigma^3}\} = \{\beta, \beta^\tau, \beta^{\tau^2}\}$ with $\beta = \alpha^{2\sigma^3}$, $\tau = \sigma^2$. Since $(\sigma^2 - 1, n) = 1$ any two columns of $M(A)$ have rank two. By Lemma 4-1) any four columns of $M(B)$ have rank three, and we are done.

Case 2, $m = 4t + 3$: Now a defining set contains AB, where $A = \{\alpha, \alpha^{2\sigma^2}\}$, $B = \{\alpha^\sigma, \alpha^{2\sigma}, \alpha^{4\sigma^3}\} = \{\beta, \beta^\tau, \beta^{\tau^2}\}$ with $\beta = \alpha^{2\sigma}$, $\tau = 2\sigma^2$, and again Lemma 4-1) settles it.

Remark: It is, of course, possible to replace the generator in Theorem 15 by one of the form $m_1(x)m_s(x)$ (e.g., in Case 1 we would have $s = \sigma^2 - \sigma + 1$), but then it is harder to show that $d = 5$.

We now consider the situation of Theorem 15 once more, but we now add α to the defining set. Just as in the case of BCH codes, this extra zero increases the distance by two. From Lemma 6 we know that the new code has odd minimum distance, so all we have to prove is that $d \geq 6$.

Theorem 16: Let n, t, and σ be as in Theorem 15. The binary cyclic code of length n with generator $g(x) = m_1(x)m_{\sigma+1}(x)m_{2\sigma+1}(x)$ has minimum distance seven.

Proof: Since d is odd (by Lemma 6), the Hamming bound guarantees $d \leq 7$. In the proof of Theorem 15 replace A by $A' = A \cup \{1\}$. Then for the new code we find $d \geq 6$ (using Lemma 3).

Remark: We did not need the fact that d is odd. In the proof of Theorem 15 we could have replaced B by $B' = B \cup \{1\}$, and then Lemma 4-2) shows that $d \neq 6$.

The following theorem again produces two infinite classes of codes with minimum distance five (resp. 7) and the same dimension as the corresponding BCH codes. In fact, Theorems 15 and 16 are special cases of Theorem 17.

Theorem 17: Let $n = 2^m - 1$, m odd. Let $0 < s < m$, $(s, m) = 1$, and define $\sigma = 2^s$. Then the binary cyclic

codes with generator $g(x) = m_{\sigma+1}(x)m_{\sigma^3+1}(x)$ (resp. $m_1(x)m_{\sigma+1}(x)m_{\sigma^3+1}(x)$) have minimum distance five (resp. 7).

Proof: The proof is the same as for the previous two theorems, where we now take $A = \{\alpha^\sigma, \alpha^{\sigma^3}\}$, $B = \{\alpha, \alpha^\tau, \alpha^{\tau^2}\}$ with $\tau = \sigma^2$.

Example 9: If m is odd then the binary cyclic code of length $n = 2^m - 1$ with generator $g(x) = m_1(x)m_{13}(x)$ has minimum distance five. This follows from Theorem 17 by taking $s = 2$ and considering $\beta = \alpha^5$ as a new primitive root.

Example 10: In [1] it was shown that the Goethals codes can be defined in a simple way and that the minimum distance of these codes (which is eight) follows from properties of the binary cyclic code with generator $g(x) = m_r(x)m_s(x)$, where $r = 2^{t-1} + 1$, $s = 2^t + 1$, $m = 2t + 1$, $n = 2^m - 1$. Theorem 17 shows an even simpler construction. In the definition of the Goethals codes (cf. [1, definition 2]), replace r by three and s by nine and thus obtain a code with $d = 8$.

It is well-known that the Golay code, even though it has generator $m_1(x)$, has a very large minimum distance; in fact, it is perfect. The known proofs of this fact have used more information than the defining set alone (e.g., the square-root bound [4, theorem 6.9.2]). In Example 7 we showed by shifting that knowledge of the defining set suffices. In the following example we show this in another way using methods like those used earlier.

Example 11 (the Golay Code): We shall show that the method of Theorem 17 can also be used if n is not $2^m - 1$. Let $n = 23$ and $g(x) = m_1(x)$. The defining set is $\{\alpha^i | i = 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$. Take $A = \{1, \alpha^2, \alpha^8\}$, $B = \{\alpha, \alpha^4, \alpha^{16}\}$. Then AB is a subset of the defining set. Since $\operatorname{rank}(M(A)_I) = \operatorname{rank}(M(\alpha, \alpha^3, \alpha^9)_I)$, we find from Lemma 4-1) that any four columns of $M(A)$ have rank three. Similarly, any four columns of $M(B)$ have rank three. Hence by Theorem 5 we have $d \geq 6$. For the even-weight subcode we can add one to the defining set, and then we may replace B by $B' = B \cup \{1\}$. Then apply Lemma 4-2). We find $d \geq 7$.

Example 12: To illustrate the results of this section, we now consider all the binary cyclic [127, 113] codes. By changing primitive elements, it is easy to show that the code with generator $m_1(x)m_s(x)$ is equivalent to the code with generator $m_1(x)m_{s'}(x)$, where $ss' \equiv 1 \pmod{127}$. This leaves as (possibly) inequivalent codes those with generator $m_1(x)m_s(x)$, where $s \in \{3, 5, 7, 9, 11, 19, 21, 23, 63\}$. We know from Theorem 12 that $d \leq 5$ for all these codes. In each case, $d \geq 4$ by the HT bound. By Lemma 6 we have $d = 5$ if $s = 3$, 5, or 9. The code with generator $m_1(x)m_{11}(x)$ is equivalent to the code with generator $m_1(x)m_{13}(x)$, which has $d = 5$, as shown in Example 9. By Theorem 17 the code with generator $m_9(x)m_5(x)$ has $d = 5$ (take $\sigma = 8$). This code is equivalent to the one with generator $m_1(x)m_{23}(x)$. The code with generator $m_1(x)m_{-1}(x)$ has $d = 5$ because the even-weight subcode has $d \geq 6$ by the BCH bound. This leaves us with the generators $m_1(x)m_s(x)$ with $s \in \{7, 19, 21\}$ for which the theorems of this section do nothing. The reason for this is that they all have $d = 4$. Let the primitive 127th root of unity satisfy $\alpha^7 + \alpha + 1 = 0$. In each case, we exhibit a set $S \subseteq \mathbb{F}_{27}$ such that $\Sigma_{x \in S} x = \Sigma_{x \in S} x^s = 0$:

1) $s = 7$, $S = \{\alpha, \alpha^3, \alpha^7, \alpha^{63}\}$,
2) $s = 19$, $S = \{\alpha, \alpha^7, \alpha^{96}, \alpha^{111}\}$,
3) $s = 21$, $S = \{\alpha^3, \alpha^{17}, \alpha^{43}, \alpha^{63}\}$.

Example 13: We carried out the same calculations (by computer) for the binary cyclic codes of length 511 with a generator of the form $m_1(x)m_s(x)$. We found that if the methods of this paper do not demonstrate that $d = 5$, then d is always four with one exception! The code with generator $m_1(x)m_{19}(x)$ has $d = 5$, and we have shown that it is not possible to show this by the methods of this paper. In fact, the only way we could prove it was to determine $H = \{\alpha^{19} + \beta^{19} | \alpha + \beta = 1 \text{ in } \mathbb{F}_{2^9}, \alpha\beta \neq 0\}$ and show that $|H| = 255$.

VII. Analysis of Binary Cyclic Codes with $n < 63$

In [7] a list is given of binary cyclic codes with $n \leq 65$ and their minimum distance d (found by computer) resp. the BCH bound d_{BCH} for the minimum distance. In Table I we consider the sublist consisting only of those codes with $n < 63$ for which $d > d_{\text{BCH}}$. (For codes with $n \geq 63$ see Section VIII.) For each of these codes, we give a lower bound for the minimum distance, which is equal to d (except in two cases) either from the HT bound or the Roos bound or from one of our theorems. For those codes for which it is necessary to give the details of the calculation, we do so in this section. For all the codes in the list, this work can be carried out by hand, but as n increases the work becomes quite tedious. The reader should clearly see (by reading this section) how one could design a computer program to continue the list. The construction of the product sets AB may be time-consuming for a computer. Visually, it was, in general, not difficult.

Explanation of Table I

In many cases Table I only gives an indication how to find the bound. The following examples will clarify our notation.

a) If the HT bound (Theorem 2) or the Roos bound (Theorem 3) can be applied, this will be indicated by specifying the sets A and B such that AB is in the defining set R of the code. For example, code 1 in the list has $R = \{\alpha^i | i = 3, 5, 6, 9, 10, 12\}$. The HT bound with $A = \{\alpha^5, \alpha^6\}$, $B = \{\alpha^0, \alpha^4\}$ yields $d \geq 4$. This is indicated by HT(5, 6*0, 4).

b) If d_{BCH} is even, one can consider the even-weight subcode of the code in question and see if some bound exists that increases the estimate. For example, code 13 in the list has $d_{\text{BCH}} = 4$. For the even-weight subcode, the defining set contains $\{1, \alpha, \alpha^2\}\{1, \alpha^8\}$, and therefore it has distance ≥ 6 by the HT bound. This is indicated as

TABLE I
TABLE OF CYCLIC CODES OF LENGTH $n \langle 63$ WITH $d \rangle d_{BCH}$

Number	n	k	d	d_{BCH}	G	Lower Bound for d
1	15	9	4	3	3,5	HT (5, 6 * 0, 4)
2	15	8	4	3	0,3,5	d even
3	17	9	5	4	1	HT (1, 2 * 0, 7, 14); SQRT
4	21	15	4	3	0,3,7	d even
5	21	13	4	3	3,7,9	HT (6, 7 * 0, 8)
6	21	12	4	3	0,3,7,9	d even
7	21	9	6	5	1,3,9	Example 14
8	21	9	8	6	0,1,3,7	Example 15
9	21	7	8	5	1,3,7,9	Roos (3, 4 * 0, 4, 8, 12, 20, 24); Example 1
10	21	6	8	6	0,1,3,7,9	subcode of 9
11	23	12	7	5	1	Examples 7, 11; SQRT
12	23	11	8	6	0,1	even-weight subcode of 11
13	31	21	5	4	1,5	if even HT (0, 1, 2 * 0, 8)
14	31	21	5	4	1,7	$\cong 13$ ($\beta = \alpha^{-6}$)
15	31	20	6	4	0,1,5	even-weight subcode of 13
16	31	20	6	4	0,1,7	$\cong 15$ ($\beta = \alpha^{-6}$)
17	31	16	7	5	1,5,7	Example 16
18	31	15	8	5	0,1,5,7	even-weight subcode of 17
19	31	11	11	7	1,3,5,11	Example 17
20	31	11	11	7	1,3,7,11	$\cong 19$ ($\beta = \alpha^{11}$)
21	31	10	12	10	0,1,3,5,11	even-weight subcode of 19
22	31	10	12	10	0,1,3,7,11	even-weight subcode of 20
23	33	21	4	3	3,11	HT (11, 12 * 0, 10); Theorem 10
24	33	20	4	3	0,3,11	d even
25	33	13	10	5	1,3	Example 18
26	33	11	11	8	1,3,11	Example 19
27	33	10	12	10	0,1,3,11	even-weight subcode of 26
28	35	28	4	3	5,7	Example 4
29	35	27	4	3	0,5,7	d even
30	35	25	4	3	5,7,15	HT (14, 15 * 0, 6)
31	35	24	4	3	0,5,7,15	d even
32	35	20	6	5	1,5	Example 20
33	35	19	6	5	0,1,5	d even
34	35	17	6	5	1,5,15	subcode of 32
35	35	16	6	5	0,1,5,15	d even
36	35	16	7	6	1,5,7	Roos (7, 8, 9, 10 * 0, 36, 48)
37	35	15	8	6	0,1,5,7	even-weight subcode of 36
38	35	13	8	6	1,5,7,15	Example 21
39	35	12	8	6	0,1,5,7,15	subcode of 38
40	35	7	14	12	0,1,3,5	Example 22
41	39	26	6	4	0,1	Example 23
42	39	25	4	3	3,13	HT (12, 13 * 0, 14); Theorem 10
43	39	24	4	3	0,3,13	d even
44	39	24	6	4	0,1,13	subcode of 41
45	39	15	10	7	1,3	Example 24
46	39	14	10	8	0,1,3	subcode of 45
47	39	13	12	7	1,3,13	Example 25
48	39	12	12	8	0,1,3,13	subcode of 47
49	41	21	9	6	1	Example 26
50	41	20	10	6	0,1	even-weight subcode of 49
51	43	29	6	4	1	Roos (21, 41 * 0, 6, 18, 24)
52	43	15	13	7	1,3	Example 27
53	45	35	4	3	5,9	HT (9, 10 * 0, 26); Theorem 10
54	45	35	4	3	3,5	HT (5, 6 * 0, 19)
55	45	34	4	3	0,5,9	d even
56	45	34	4	3	0,3,5	d even
57	45	33	4	3	5,9,15	subcode of 53
58	45	32	4	3	0,5,9,15	d even
59	45	31	4	3	3,5,9	subcode of 53
60	45	31	4	3	3,5,21	subcode of 54
61	45	30	4	3	0,3,5,9	d even
62	45	30	4	3	0,3,5,21	d even
63	45	29	4	3	3,5,9,15	subcode of 53
64	45	28	4	3	0,3,5,9,15	d even
65	45	28	6	5	0,1,9	d even
66	45	28	6	5	0,1,21	d even
67	45	27	4	3	3,5,9,21	subcode of 53
68	45	27	6	5	1,3,15	Roos (15, 16 * 0, 8, 16, 32)
69	45	26	4	3	0,3,5,9,21	d even
70	45	25	4	3	3,5,9,15,21	subcode of 53
71	45	24	4	3	0,3,5,9,15,21	d even
72	45	24	6	5	0,1,9,21	d even
73	45	23	7	6	1,5,21	Example 28

TABLE I (*Continued*)

74	45	22	8	6	0,1,5,21	even-weight subcode of 73
75	45	21	8	7	1,5,9,15	Example 5
76	45	21	8	7	1,3,5,15	Example 5
77	45	21	8	7	1,5,15,21	Example 5
78	45	20	8	7	0,1,5,9,15	d even
79	45	20	8	7	0,1,5,15,21	d even
80	45	18	8	7	0,1,5,9,21	d even
81	45	17	8	7	1,3,5,9,15	HT (1,2,3,4,5,6∗0,14)
82	45	17	8	7	1,3,5,15,21	HT (1,2,3,4,5,6∗0,29)
83	45	16	10	8	0,1,3,7	Example 29
84	45	15	9	8	1,3,7,15	if even then subcode of 83
85	45	15	10	8	1,7,9,15	Roos (13,14,15,16,17,18∗0,13,91,104)
86	45	14	10	8	0,1,7,9,15	subcode of 85
87	45	14	10	8	0,1,3,7,15	subcode of 83
88	45	12	10	8	0,1,3,7,9	subcode of 83
89	45	11	9	8	1,3,7,15,21	subcode of 84
90	45	9	12	9	1,5,7,9,15	Example 30
91	45	8	12	9	0,1,5,7,9,15	subcode of 90
92	47	24	11	5	1	Example 31
93	47	23	12	6	0,1	even-weight subcode of 93
94	51	41	4	3	3,17	HT (12,17∗0,22); Theorem 10
95	51	40	4	3	0,3,17	d even
96	51	35	5	4	1,9	HT (1,2∗0,7,14)
97	51	34	6	4	0,1,9	even-weight subcode of 96
98	51	34	6	4	0,1,5	Example 32
99	51	33	4	3	3,9,17	subcode of 94
100	51	33	6	5	1,3,17	Example 33
101	51	33	6	5	1,9,17	Example 34
102	51	32	4	3	0,3,9,17	d even
103	51	32	6	5	0,1,9,17	d even
104	51	32	6	4	0,1,5,17	subcode of 98
105	51	27	5	4	1,9,19	subcode of 96
106	51	27	8	5	1,3,9	Example 35
107	51	27	9	5	1,5,9	Example 36
108	51	27	9	5	1,3,19	Example 37
109	51	26	8	6	0,1,3,9	subcode of 106
110	51	26	10	6	0,1,5,9	even-weight subcode of 107
111	51	25	8	5	1,3,9,17	subcode of 106
112	51	25	10	9	1,3,5,17	Example 38
113	51	25	10	7	1,5,9,17	Example 39
114	51	25	10	5	1,3,17,19	Example 40
115	51	24	8	6	0,1,3,9,17	subcode of 106
116	51	24	10	7	0,1,5,9,17	subcode of 110
117	51	19	10	6	1,3,9,19	subcode of 108 + Theorem 10
118	51	19	10	9	1,5,9,19	Example 41
119	51	19	14	11	1,3,5,9	Example 42
120	51	18	14	12	0,1,3,5,9	subcode of 119
121	51	17	12	6	1,3,9,17,19	Example 43
122	51	17	14	9	1,3,5,17,19	Example 44
123	51	17	14	10	1,5,9,17,19	Example 45
124	51	17	16	11	1,3,5,9,17	Example 46
125	51	16	12	10	0,1,3,9,17,19	subcode of 121
126	51	16	14	10	0,1,5,9,17,19	subcode of 123
127	51	16	16	12	0,1,3,5,9,17	subcode of 124
128	51	11	15	9	1,3,5,11,19	Example 47
129	51	11	15	9	1,5,9,11,19	$\cong 128\ (\alpha = \beta^{11})$
130	51	9	15	12	1,3,5,11,17,19	subcode of 128
131	51	9	15	12	1,5,9,11,17,19	subcode of 128
132	51	8	24	20	0,1,3,5,9,17,19	Example 48
133	55	41	4	3	5,11	Theorem 10
134	55	40	4	3	0,5,11	d even
135	55	35	5	4	1	HT (7,8,9∗0,9)
136	55	34	8	4	0,1	Example 49
137	55	30	10	5	0,1,11	Example 50
138	55	25	11	7	1,5	Example 52
139	55	24	12	7	0,1,5	even-weight subcode of 138
140	55	21	15	8	1,5,11	Example 51
141	55	20	16	8	0,1,5,11	Example 51
142	57	37	4	3	3,19	Theorem 10
143	57	36	4	3	0,3,19	d even
144	57	21	14	6	1,3	Example 53
145	57	20	14	10	0,1,3	Example 53
146	57	19	16	9	1,3,19	$d \geq 14$ by Example 53
147	57	18	16	10	0,1,3,19	$d \geq 14$ by Example 53

follows: if even, HT(0, 1, 2*0, 8). The conclusion of course is that $d \geq 5$.

c) If α^0 is in the defining set, then d must be even. This is indicated by d even.

d) For the sake of completeness, we indicate by SQRT those quadratic residue codes for which the square-root bound gives the true minimum distance. In all cases there is some other reference.

e) The list in [7] includes some codes that are equivalent to other codes in the list. For example, Code 20 in the list has $g(x) = m_1(x)m_3(x)m_7(x)m_{11}(x)$. If we take $\beta = \alpha^{11}$ as a new primitive root, then we find the code with generator $m_1(x)m_3(x)m_5(x)m_{11}(x)$, which is Code 19. We indicate this by $\cong 19$ ($\beta = \alpha^{11}$).

Remark (added in proof): In [11, p. 447] Downie and Sloane point out that the entries with numbers 14, 16, 20, and 22 in Table I have errors in the columns d and G. For each of the corrected entries it is easy to check that our methods give the correct value of d.

Table I gives each code a number, gives the length n, dimension k, true distance d, BCH bound d_{BCH}, the set G such that $g(x) = \Pi_{i \in G} m_i(x)$ (in other words, $R = \{\alpha^i | i \in G\}$ is a defining set); finally, Table I indicates how to find a lower bound equal to d. Of course, to establish the true value of d, one must also have upper bounds for d. In some cases these are provided by the Hamming bound [4, theorem 5.2.7] or the Griesmer bound [4, theorem 5.2.6], for example, Code 8 in the list. For several codes Theorems 12 and 13 give the necessary upper bound. However, in most cases one has to find a word of weight d as we did in Example 12. We do not indicate the upper bounds in the table.

The following examples of the methods of this paper treat the codes of the table that require explanation. The entry Example 14 refers to Example 14 to follow. For each code, R will denote the complete defining set. In the examples where we specify A and B such that $AB \subseteq R$ and then apply Theorem 5 the matrices A and B of that theorem are, respectively, $M(A)$ and $M(B)$. When shifting is applied, we consider a codeword $c(x)$ and assume that it has weight d. If we need the fact that $c(\alpha^i) \neq 0$, we observe that $c(\alpha^i) = 0$ would imply $c(\alpha^j) = 0$ for every zero α^j of $m_i(x)$. This contradicts some bound. If this is easily checked, we omit the details. In several examples, we use the fact that we know that d is even. Usually, one can find d without using this extra information (see, e.g., Example 15).

Example 14: Let $n = 21$, $g(x) = m_1(x)m_3(x)m_9(x)$. Then $R \supseteq AB$, where $A = \{\alpha^i | i = 1, 3, 4\}$, $B = \{\beta^j | j = -2, 0, 1\}$, $\beta = \alpha^8$. Apply Theorem 5 and Corollary 1. We find $d \geq 6$.

Example 15: Let $n = 21$, $g(x) = m_0(x)m_1(x)m_3(x)m_7(x)$. Then $R = \{\alpha^i | i = 0, 1, 2, 3, 4, 6, 7, 8, 11, 12, 14, 16\}$. We have $d_{\text{BCH}} = 6$ and d is even. Let $A = \{\alpha^i | i = 1, 2, 3, 6\}$ and $|I| = 6$. Then $\text{rank}(M(A)_I) = 4$ by Corollary 1. Let $B = \{\alpha^j | j = 0, 1, 5\}$, Then $\text{rank}(M(B)_I) = 3$. Since $AB \subseteq R$ we find from Theorem 5 that $d \neq 6$. Hence $d \geq 8$. For this code we could also have applied Theorem 6-I, which shows that $d \equiv 0 \pmod 4$. It is also possible to show that $d \geq 8$ by taking $A = B = \{\alpha^i | i = 0, 1, 2, 6\}$ and applying Theorem 5 again.

Example 16: Let $n = 31$, $g(x) = m_1(x)m_5(x)m_7(x)$. There are several ways to show that $d \geq 7$. Of course, the square root bound for QR codes is the easiest. We could also use the remark following Theorem 6, which shows that $d \equiv 3 \pmod 4$. Two successive applications of Theorem 5 and Corollary 1 also do the job. We have $R \supset AB$, where $A = \{\alpha^i | i = 8, 9, 10\}$, $B = \{\beta^j | j = 0, 1, 3\}$, $\beta = \alpha^{10}$. So from Theorem 3 we find $d \geq 6$. However, for the even-weight subcode we can apply Theorem 5 with $A = \{\alpha^i | i = 4, 7, 8, 9\}$, $B = \{\beta^j | j = 0, 3, 4\}$, $\beta = \alpha^8$. If $|I| = 6$ then $\text{rank}(M(A)_I) = 4$ and $\text{rank}(M(B)_I) = 3$ by Corollary 1; therefore weight six does not occur. Hence $d \geq 7$.

Example 17: Let $n = 31$, $g(x) = m_1(x)m_3(x)m_5(x)m_{11}(x)$. We have

$$R = \{\alpha^i | i = 1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 16, 17, 18, 20, 21, 22, 24, 26\}.$$

Here the HT bound shows us that $d \geq 8$. By the remark following Theorem 6, we must have $d \geq 11$. We can also prove this using our methods. First, observe that if d is even, then $d \geq 10$ by the BCH bound on the consecutive set $\{\alpha^{11k+9} | 0 \leq k \leq 8\}$. Now take $A = \{\alpha^i | i = 10, 11, 12, 13, 17, 18\}$, $B = \{\alpha^{-i} | i = 0, 1, 7, 8, 9\}$. If $|I| = 9$ or 10, then by Corollary 1 we have $\text{rank}(M(A)_I) = 6$ and $\text{rank}(M(B)_I) = |I| - 5$. Therefore, the code has no words of weight nine or ten.

Example 18: Let $n = 33$, $g(x) = m_1(x)m_3(x)$. This is a very nice example of Theorem 10. Taking $l = 3$, $n_0 = 11$, we find that d is even or $d \geq 11$. If d is even then $d \geq 10$ by the BCH bound.

Example 19: Let $n = 33$, $g(x) = m_1(x)m_3(x)m_{11}(x)$. From the previous example we know that $d \geq 10$. This example shows that sometimes, when one is doing the work visually, it is useful to change primitive roots. The set R for this code does not show any promising choices for A and B. We take $\alpha = \beta^{10}$ and find a new defining set $R^* = \{\beta^i | i = 3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 18, 19, 20, 21, 22, 23, 24, 26, 27, 28, 30\}$. Here one quickly sees that $R^* \supseteq AB$, where $A = \{\beta^i | i = 5, 6, 9, 10, 11, 12, 13, 14\}$ and $B = \{\beta^i | i = 0, 1, 9\}$. An application of Theorem 5 and Corollary 1 with $|I| = 10$ shows that $d \neq 10$.

Example 20: Let $n = 35$, $g(x) = m_1(x)m_5(x)$. Then $R \supseteq AB$, where $A = \{\alpha^i | i = 2, 4, 5\}$, $B = \{\beta^j | j = 0, 1, 3\}$, $\beta = \alpha^6$. By Theorem 5 and Corollary 1, we have $d \geq 6$.

Example 21: Let $n = 35$, $g(x) = m_1(x)m_5(x)m_7(x)m_{15}(x)$. This code is a subcode of code 36. Therefore, $d \geq 7$. We have $R \supseteq AB$, where $A = \{\alpha^i | i = 4, 8, 9, 10\}$, $B = \{\beta^j | j = 0, 1, 2, 6\}$, $\beta = \alpha^6$. Therefore, we have $d \neq 7$ by Theorem 5 and Corollary 1.

Example 22: Let $n = 35$, $g(x) = m_0(x)m_1(x)m_3(x)m_5(x)$. Since d is even and $d_{\text{BCH}} = 12$ it suffices to show that $d \neq 12$. We have $R \supseteq AB$, where $A = \{\alpha^i | i = 0, 1, 2, 3, 4, 8, 9, 10, 11\}$, $B = \{\alpha^j | j = 0, 1, 2, 8, 9\}$. So, Theorem 5 and Corollary 1 actually show that words of weight k with $9 \leq k \leq 13$ do not occur.

Example 23: Let $n = 39$, $g(x) = m_0(x)m_1(x)$. Here $R = \{\alpha^i | i = 0, 1, 2, 4, 5, 8, 10, 11, 16, 20, 22, 25, 32\}$. This is the first example of this section where Corollary 1 does not help us in applying Theorem 5. We have $R \supseteq AB$, where $A = \{\alpha^0, \alpha^1\}$, $B = \{\alpha^0, \alpha^1, \alpha^4\}$. We know d is even and wish to show that $d \neq 4$. Therefore, we need to know that $\operatorname{rank}(M(B)_I) = 3$ for $|I| = 4$. However, it is sufficient to show this under the assumption that I is the support of a codeword. Now shifting will do the trick. Since α^{14} is a zero of $m_{-1}(x)$, it cannot be a zero of a codeword of weight four. We find from Lemma 5

$$\operatorname{rank}\left(M(\alpha^0, \alpha^1, \alpha^4)_I\right) = \operatorname{rank}\left(M(\alpha^{10}, \alpha^{11}, \alpha^{14})_I\right)$$
$$= 1 + \operatorname{rank}\left(M(\alpha^{10}, \alpha^{11})_I\right) = 3.$$

So, by Theorem 5 we have a contradiction, and hence $d \geq 6$.

Example 24: Let $n = 39$, $g(x) = m_1(x)m_3(x)$. Here $d_{\mathrm{BCH}} = 7$. We know from Theorem 10 that d is even or $d \geq 13$. So, it suffices to show that $d \neq 8$. We have $R \supseteq AB$, where $A = \{\alpha^i | i = 1, 2, 3, 4, 5, 8\}$, $B = \{\alpha^j | j = 0, 1, 7\}$. Therefore, Theorem 5 and Corollary 1 show that $d \neq 8$.

Example 25: Let $n = 39$, $g(x) = m_1(x)m_3(x)m_{13}(x)$. By Theorem 10 d is even or $d \geq 13$. So, consider the even-weight subcode. The defining set contains AB, where $A = \{\alpha^i | i = 0, 1, 2, 3, 8, 9\}$, $B = \{\alpha^j | j = 0, 1, 2, 3, 24\} = \{\beta^k | k = 0, 2, 4, 6, 9\}$, $\beta^2 = \alpha$. From Theorem 5 and Corollary 1, we find $d \geq 12$.

Example 26: Let $n = 41$, $g(x) = m_1(x)$. The square-root bound for this QR code shows that $d \geq 7$ but the true minimum distance is nine. We shall first show a distinction between the HT bound and our AB method. The code is equivalent to the code with generator $m_3(x)$. For the latter code the defining set contains $\{\alpha^i | 11 \leq i \leq 15\} \cup \{\alpha^i | 26 \leq i \leq 30\}$, and so $d \geq 7$ by the HT bound. Now consider this set as $\{\alpha^i | 11 \leq i \leq 14\}\{\alpha^j | j = 0, 1, 15, 16\}$. Now $B = \{\alpha^j | j = 0, 1, 15, 16\} = \{\beta^k | k = 0, 3, 4, 7\}$, $\beta = \alpha^{14}$. Therefore, if we can show that any seven columns of $M(B)$ have rank four, it follows from Theorem 5 that $d \geq 8$. (By cheating and using the fact that d is odd for QR codes, we would be finished.) Suppose that there are seven columns of $M(B)$ that have rank < 4. By Lemma 2 there are 41st roots of unity $\xi_1, \xi_2, \cdots, \xi_7$ such that $\prod(x - \xi_i) = x^7 + ax^4 + bx^3 + c$. Therefore, $\sum \xi_i = 0$ and hence $\sum \xi_i^{2^j} = 0$ for every j, in particular $\sum \xi_i^2 = \sum \xi_i^5 = \sum \xi_i^9 = 0$. From $x^2 \prod (x - \xi_i) = x^9 + ax^6 + bx^5 + cx^2$, it then follows that either $a = 0$ or $\sum \xi_i^6 = 0$. The latter possibility would imply $\sum \xi_i^k = 0$ for every $k \neq 0$, which is absurd. Therefore, $a = 0$. A second application of this kind of argument leads to a contradiction. The reader will have realized that the foregoing is actually the shifting principle at work! Therefore, we should settle the question just by shifting.

The defining set for the code with generator $m_3(x)$ is

$$R = \{\alpha^i | i = 3, 6, 7, 11, 12, 13, 14, 15, 17, 19,$$
$$22, 24, 26, 27, 28, 29, 30, 34, 35, 38\}$$

and a codeword with any other α^j as a zero is **0** or **1**. We proceed as in Example 7. Let us first find a large enough set that allows three shifts. Inspection of R quickly reveals the candidate $A = \{\alpha^i | i = 6, 12, 26, 27, 29, 34\}$, which allows multiplication by 1, α, and α^{29}. We postpone the problem of showing that A is independent with respect to the set of zeros of a codeword $c(x)$. Suppose this has been done. Let us find a $\gamma \notin R$ such that $\alpha\gamma$ and $\alpha^{29}\gamma$ are in R. We readily see that $\gamma = \alpha^5$ works. Hence $A \cup \{\alpha^5\}$ is independent and $(\alpha A \cup \{\alpha^6\}) \subset S$. Now we take γ' such that $\gamma' \notin R$ and $\alpha^{28}\gamma' \in R$, say $\gamma' = \alpha$. We find the independent set $(\alpha^{29}A \cup \{\alpha^{34}\} \cup \{\alpha^{29}\}) \subset R$. By adjoining any element not in R we find an independent set of size nine. So, to show that $d \geq 9$ it remains to show that A is independent. This can be done by working our way back. Find α^j such that $\alpha^j A$ has exactly one element that is not in R. Deleting this element, etc., we find the sequence

$$A_1 = A,$$
$$\alpha^{26}A_1 = \{\alpha^{32}, \alpha^{38}, \alpha^{11}, \alpha^{12}, \alpha^{14}, \alpha^{19}\},\ A_2 = \alpha^{26}A_1 \setminus \{\alpha^{32}\},$$
$$\alpha^{33}A_2 = \{\alpha^{30}, \alpha^3, \alpha^4, \alpha^6, \alpha^{11}\},\ A_3 = \alpha^{33}A_2 \setminus \{\alpha^4\},$$
$$\alpha^{16}A_3 = \{\alpha^5, \alpha^{19}, \alpha^{22}, \alpha^{27}\},\ A_4 = \alpha^{16}A_3 \setminus \{\alpha^5\},$$
$$\alpha^{31}A_4 = \{\alpha^9, \alpha^{12}, \alpha^{17}\},\ A_5 = \alpha^{31}A_4 \setminus \{\alpha^9\}.$$

Now A_5 is easily seen to be independent, and therefore all A_i, $1 \leq i \leq 5$ are independent completing the proof that $d \geq 9$.

Example 27: Let $n = 43$, $g(x) = m_1(x)m_3(x)$. For this code we have

$$R = \{\alpha^i | i = 1, 2, 3, 4, 5, 6, 8, 10, 11, 12,$$
$$16, 19, 20, 21, 22, 23, 24, 27,$$
$$31, 32, 33, 35, 37, 38, 39, 40, 41, 42\}.$$

We see at one glance that $d \geq 9$ by the HT bound and that the even-weight subcode has $d \geq 14$ by the BCH bound. We show that $d \geq 13$ by applying Theorem 5. Observe that $R \supseteq AB$, when $A = \{\alpha^i | 0 \leq i \leq 3 \wedge 18 \leq i \leq 21\} = \{\beta^{2i} | 0 \leq i \leq 3 \wedge 18 \leq i \leq 21\}$, $(\beta^2 = \alpha)$, and $B = \{\alpha^j | j = 1, 2, 3, 19, 20, 21\}$. To determine $\operatorname{rank}(M(A)_I)$, we can use Corollary 1. We are done if we can show that $\operatorname{rank}(M(B)_I) = 6$ if I is the support of a codeword. Apply shifting as in Lemma 5. Observe that no element not in R is a zero of a codeword of weight < 14, since the only subcodes are the even-weight subcode and the repetition code. We find $\operatorname{rank}(M(\alpha^4, \alpha^5, \alpha^6)_I) = 3$, $\operatorname{rank}(M(\alpha^4, \alpha^5, \alpha^6, \alpha^{29})_I) = 4$, $\operatorname{rank}(M(\alpha^2, \alpha^3, \alpha^4, \alpha^{27}, \alpha^{29})_I) = 5$, $\operatorname{rank}(M(\alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{35}, \alpha^{37}, \alpha^{36})_I) = 6$, and hence $\operatorname{rank}(M(B)_I) = 6$.

Example 28: Let $n = 45$, $g(x) = m_1(x)m_5(x)m_{21}(x)$. We have $R \supseteq AB$ with $A = \{\alpha^i | i = 1, 2, 4\}$, $B = \{\beta^j | j = 0, 1, 2, 4\}$, $\beta = \alpha^{19}$. Apply theorem 5 and Corollary 1.

Example 29: Let $n = 45$, $g(x) = m_0(x)m_1(x)m_3(x)m_7(x)$. We have $R \supseteq AB$, where $A = \{\alpha^i | i = -2, -1, 0, 1, 3, 4\}$, $B = \{\beta^j | j = -2, 0, 3\}$, $\beta = \alpha^{16}$. By Theorem 5 and Corollary 1, we find $d \geq 9$. Since d is even, $d \geq 10$.

Example 30: Let $n = 45$, $g(x) = m_1(x)m_5(x)m_7(x)m_9(x)m_{15}(x)$. We have $R \supseteq AB$, where $A = \{\alpha^i | i = 13,$

14, 15, 16, 17, 18, 19, 22}, $B = \{\beta^j | j = 0, 3, 4, 7\}$, $\beta = \alpha^{34}$. By Theorem 5 and Corollary 1 we have $d \geq 12$.

Example 31: Let $n = 47$, $g(x) = m_1(x)$. For this QR code the square-root bound shows that $d = 11$. By the remark following Theorem 6, we have $d \equiv 3 \pmod 4$, and therefore if we wish to show that $d \geq 11$ by our methods, we need only prove that $d \geq 8$. For this code

$$R = \{\alpha^i | i = 1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42\}.$$

The HT bound shows that $d \geq 6$. Let I be the support of a codeword ($|I| \geq 6$). We have $R \supseteq AB$, where $A = \{\alpha^i | i = 0, 1, 15\} = \{\beta^j | j = 0, 3, -2\}$, $\beta^3 = \alpha$, $B = \{\alpha^j | j = 2, 3, 6, 27, 36\}$. It follows from Corollary 1 that $\operatorname{rank}(M(A)_I) = 3$. For B we apply Lemma 5. If a codeword has a zero $\alpha^i \notin R (i \neq 0)$, then it is 1. We have

$$\begin{aligned}\operatorname{rank}(M(B)_I) &= \operatorname{rank}(M(\alpha^{24}, \alpha^{25}, \alpha^{28}, \alpha^2, \alpha^{11})_I) \\ &= 1 + \operatorname{rank}(M(\alpha^{24}, \alpha^{25}, \alpha^{28}, \alpha^2)_I) \\ &= 1 + \operatorname{rank}(M(\alpha^8, \alpha^9, \alpha^{12}, \alpha^{33})_I) \\ &= 2 + \operatorname{rank}(M(\alpha^8, \alpha^9, \alpha^{12})_I) = 5.\end{aligned}$$

Example 32: Let $n = 51$, $g(x) = m_0(x)m_1(x)m_5(x)$. This is a tricky example. We shall show that the code with generator $m_1(x)m_5(x)$, which has $d = 3$, does not have any words of weight four. To do this observe that $R \supseteq AB$, where $A = \{\alpha^i | i = 1, 2, 4\}$, $B = \{\alpha^j | j = 0, 3, 6\}$. If $|I| = 4$ then $\operatorname{rank}(M(A)_I) = 3$. With B we have to be careful since three divides the length of the code. The only thing we can say is that $\operatorname{rank}(M(B)_I) \geq 2$, but this is enough for our purpose. Theorem 5 shows that weight four does not occur.

Example 33: Let $n = 51$, $g(x) = m_1(x)m_3(x)m_{17}(x)$. We have

$$R = \{\alpha^i | i = 1, 2, 3, 4, 6, 8, 12, 13, 16, 17, 24, 26, 27, 34, 39, 45, 48\}.$$

Suppose $c(x)$ is a codeword of weight five with zero-set S. Then $\alpha^7 \notin S$ (by the BCH bound), $\alpha^{15} \notin S$ (by the HT bound). We find the following sequence of sets that are independent with respect to S: $\{\alpha^2, \alpha^3\}$, $\{\alpha^2, \alpha^3, \alpha^7\}$, $\{\alpha, \alpha^2, \alpha^6, \alpha^{15}\}$, $\{\alpha^3, \alpha^4, \alpha^8, \alpha^{17}, \alpha^7\}$, $\{\alpha^{12}, \alpha^{13}, \alpha^{17}, \alpha^{26}, \alpha^{16}, \alpha^7\}$. This contradicts Theorem 11. Hence $d \geq 6$.

Example 34: Let $n = 51$, $g(x) = m_1(x)m_9(x)m_{17}(x)$. We have

$$R = \{\alpha^i | i = 1, 2, 4, 8, 9, 13, 15, 16, 17, 18, 21, 26, 30, 32, 33, 34, 36, 42\}.$$

Suppose $c(x)$ is a codeword of weight five with zero-set S. Then $\alpha^0 \notin S$, $\alpha^{25} \notin S$, $\alpha^{31} \notin S$ (by the BCH bound). The following sequence of sets is independent with respect to S: $\{\alpha^{15}, \alpha^{16}\}$, $\{\alpha^{15}, \alpha^{16}, \alpha^0\}$, $\{\alpha^{32}, \alpha^{33}, \alpha^{17}, \alpha^{31}\}$, $\{\alpha^{33}, \alpha^{34}, \alpha^{18}, \alpha^{32}, \alpha^{25}\}$, $\{\alpha^{16}, \alpha^{17}, \alpha, \alpha^{15}, \alpha^8, \alpha^0\}$. This contradicts Theorem 11. Hence $d \geq 6$.

Example 35: Let $n = 51$, $g(x) = m_1(x)m_3(x)m_9(x)$. By Theorem 10 we have $d \geq 17$ or d is even. Since $d_{\mathrm{BCH}} = 5$ we can show $d \geq 8$ by proving that there is no codeword $c(x)$ of weight six. For the even-weight subcode

$$R = \{\alpha^i | i = 0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 15, 16, 18, 21, 24, 26, 27, 30, 32, 33, 39, 45, 48\}.$$

We have $R \supseteq AB$, where $A = \{\alpha^i | i = 0, 2, 3\}$, $B = \{\alpha^j | j = 0, 1, 6, 13\}$. Let I be the support of $c(x)$. Then

$$\begin{aligned}\operatorname{rank}(M(B)_I) &= \operatorname{rank}(M(\alpha^{32}, \alpha^{33}, \alpha^{38}, \alpha^{45})_I) \\ &= 1 + \operatorname{rank}(M(\alpha^{32}, \alpha^{33}, \alpha^{45})_I) \\ &= 1 + \operatorname{rank}(M(\alpha^0, \alpha^1, \alpha^{13})_I),\end{aligned}$$

because α^{38} cannot be a zero of $c(x)$ by the HT bound. For any set of size five, we have $\operatorname{rank}(M(\alpha^0, \alpha^1, \alpha^{13})_1) = \operatorname{rank}(M(\beta^0, \beta^4, \beta)_1) = 3$, ($\beta^4 = \alpha$).

Example 36: Let $n = 51$, $g(x) = m_1(x)m_5(x)m_9(x)$. The defining set is

$$R = \{\alpha^i | i = 1, 2, 4, 5, 7, 8, 9, 10, 13, 14, 15, 16, 18, 20, 21, 26, 28, 29, 30, 32, 33, 36, 40, 42\}.$$

We find from Roos (7, 8, 9∗0, 7, 21) that $d \geq 6$. If d is even then we find from Roos (0, 1, 2∗0, 7, 14, 28) that $d > 6$. Suppose I is a set of size seven or eight that supports a codeword $c(x)$. By the BCH bound α^{12}, α^{19}, and α^{23} are not zeros of $c(x)$. We find for $B = \{\alpha^j | j = 0, 6, 7, 8, 13\}$ from Lemma 5

$$\begin{aligned}\operatorname{rank}(M(B)_I) &= \operatorname{rank}(M(\alpha^{13}, \alpha^{19}, \alpha^{20}, \alpha^{21}, \alpha^{26})_I) \\ &= 1 + \operatorname{rank}(M(\alpha^{13}, \alpha^{20}, \alpha^{21}, \alpha^{26})_I) \\ &= 1 + \operatorname{rank}(M(\alpha^5, \alpha^{12}, \alpha^{13}, \alpha^{18})_I) \\ &= 2 + \operatorname{rank}(M(\alpha^5, \alpha^{13}, \alpha^{18})_I) \\ &= 2 + \operatorname{rank}(M(\alpha^{15}, \alpha^{23}, \alpha^{28})_I) \\ &= 3 + \operatorname{rank}(M(\alpha^{15}, \alpha^{28})_I) \\ &= 3 + \operatorname{rank}(M(\alpha^0, \alpha^{13})_I) = 5.\end{aligned}$$

If $|I| = 7$ we can apply Theorem 5 with $A = \{\alpha^i | i = 1, 2, 7\}$; if $|I| = 8$ we take $A' = \{\alpha^i | i = 1, 2, 7, 8\}$. It follows that there is no codeword of weight seven or eight.

Example 37: Let $n = 51$, $g(x) = m_1(x)m_3(x)m_{19}(x)$. This example was treated in complete detail as Example 6. To show how we shall abbreviate the shifting method in the following examples, the reader should compare Example 6 with the following abbreviated form:

$$\begin{aligned}(1, 2, 3, 4, 24) &\to (2, 3, 4, 5, 25) \to (2, 3, 4, 25) \\ &\to (3, 4, 5, 26) \to (2, 4, 26) \\ &\to (4, 5, 27) \to (4, 27).\end{aligned}$$

Example 38: Let $n = 51$, $g(x) = m_1(x)m_3(x)m_5(x)m_{17}(x)$. We have

$$R = \{\alpha^i | i = 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 13, 14, 16, 17, 20, 24, 26, 27, 28, 29, 32, 34, 39, 40, 45\}.$$

The argument is similar to the previous examples. Let

$A = \{\alpha^i | i = 0, 1, 2, 27\} = \{\beta^j | j = 0, 2, 4, 3\}$, $\beta^2 = \alpha$. Then $\operatorname{rank}(M(A)_I) = 4$ for $|I| \geq 6$. Let $B = \{\alpha^j | j = 1, 2, 5, 12, 26, 27\}$. $R \supseteq AB$. We again abbreviate the shifting argument:

$$\begin{aligned}(1,2,5,12,26,27) &\to (6,7,10,17,31,32)\\ &\to (6,7,10,17,32)\\ &\to (16,17,20,27,42)\\ &\to (16,17,20,27) \to (5,6,9,16)\\ &\to (5,6,16) \to (0,1,11).\end{aligned}$$

Then we use $\operatorname{rank} M(1, \alpha, \alpha^{11})_I = \operatorname{rank} M(1, \gamma^5, \gamma^4)_I = 3$, $\gamma^5 = \alpha$.

Example 39: Let $n = 51$, $g(x) = m_1(x)m_5(x)m_9(x)m_{17}(x)$. We have

$$\begin{aligned}R = \{\alpha^i | i = {} & 1,2,4,5,7,8,9,10,13,14,\\ & 15,16,17,18,20,21,26,28,\\ & 29,30,32,33,34,36\,40,42\}.\end{aligned}$$

Here $R \supseteq AB$, where $A = \{\alpha^i | i = 1, 7, 8, 9\}$, $B = \{\alpha^j | j = 0, 1, 6, 7, 8, 9\}$. Suppose I supports a codeword of weight < 11. We shall show that $\operatorname{rank}(M(B)_I) = 6$. We abbreviate the shifting as earlier:

$$\begin{aligned}(0,1,6,7,8,9) &\to (20,21,26,27,28,29)\\ &\to (20,21,26,28,29)\\ &\to (4,5,10,12,13) \to (4,5,10,13)\\ &\to (15,16,21,24) \to (15,16,21).\end{aligned}$$

Example 40: Let $n = 51$, $g(x) = m_1(x)m_3(x)m_{17}(x)m_{19}(x)$. Then

$$\begin{aligned}R = \{\alpha^i | i = {} & 1,2,3,4,6,8,12,13,16,17,\\ & 19,24,25,26,27,32,34,35,\\ & 38,39,43,45,47,48,49,50\}.\end{aligned}$$

$R \supseteq AB$ where $A = \{\alpha^i | i = \pm 1, \pm 6\}$, $B = \{\alpha^j | j = \pm 2, \pm 7, \pm 18\}$. For both matrices we use shifting (abbreviated):

$$\begin{aligned}A\colon\ (-6,-1,1,6) &\to (48,2,4,9) \to (48,2,4)\\ &\to (49,3,5) \to (49,3) \to (2,7) \to (2)\end{aligned}$$

$$\begin{aligned}B\colon\ (-7,-2,-18,7,2,18) &\to (3,8,43,17,12,28)\\ &\to (3,8,43,17,12)\\ &\to (49,3,38,12,7)\\ &\to (49,3,38,12)\\ &\to (8,13,48,22)\\ &\to (8,13,48)\\ &\to (48,2,37)\\ &\to (48,2) \to (2,7).\end{aligned}$$

Example 41: Let $n = 51$, $g(x) = m_1(x)m_5(x)m_9(x)m_{19}(x)$. We have

$$\begin{aligned}R = \{\alpha^i | i = {} & 1,2,4,5,7,8,9,10,13,14,15,16,\\ & 18,19,20,21,25,26,28,29,30,32,\\ & 33,35,36,38,40,42,43,47,49,50\}.\end{aligned}$$

Take $A = \{\alpha^i | i = 1, 2, 7, 8, 13\}$, $B = \{\alpha^j | j = 0, 6, 7, 8, 13\}$. Assume $|I| = 9$. We abbreviate the shifting as earlier:

$$\begin{aligned}A\colon\ (1,2,7,8,13) &\to (3,4,9,10,15) \to (4,9,10,15)\\ &\to (3,8,9,14) \to (8,9,14) \to (0,1,6)\end{aligned}$$

$$\begin{aligned}B\colon\ (0,6,7,8,13) &\to (12,18,19,20,25)\\ &\to (18,19,20,25) \to (0,1,2,7).\end{aligned}$$

Example 42: Let $n = 51$, $g(x) = m_1(x)m_3(x)m_5(x)m_9(x)$. We have

$$\begin{aligned}R = \{\alpha^i | {} & 1 \leq i \leq 10, 12 \leq i \leq 16, i = 18,20,21,24,\\ & 26,27,28,29,30,32,33,36,39,40,42,45,48\}.\end{aligned}$$

From Theorem 10 we have $d \geq 17$ or d even. If d is even then $d \geq 12$ by the BCH bound. To show that $d \neq 12$ take $A = \{\alpha^i | 0 \leq i \leq 4\}$, $B = \{\alpha^j | j = 0, 1, 2, 3, 4, 5, 12, 26\}$. Shift as follows:

$$\begin{aligned}(6,7,8,9,10,11,18,32) &\to (6,7,8,9,10,18,32)\\ &\to (12,13,14,15,16,24,38)\\ &\to (12,13,14,15,16,24)\\ &\to (26,27,28,29,30,38)\\ &\to (26,27,28,29,30).\end{aligned}$$

Example 43: Let $n = 51$, $g(x) = m_1(x)m_3(x)m_9(x)m_{17}(x)m_{19}(x)$. As in the previous example $d \geq 17$ or d is even. We know from Code 114 that $d \geq 10$. We show that $d \neq 10$. Take $A = B = \{\alpha^i | i = 1, 12, 15, 24, 33, 42\}$. Shift as follows:

$$\begin{aligned}(33,42,15,24,12,1) &\to (39,48,21,30,18,7)\\ &\to (39,48,21,30,18)\\ &\to (43,1,25,34,22)\\ &\to (43,1,25,34) \to (50,8,32,41)\\ &\to (50,8,32) \to (38,47,20)\\ &\to (38,47) \to (44,2) \to (2).\end{aligned}$$

Example 44: Let $n = 51$, $g(x) = m_1(x)m_3(x)m_5(x)m_{17}(x)m_{19}(x)$. Here $R \supseteq AB$, $A = \{\alpha^i | i = 1, 2, 3, 4, 24, 25\}$, $B = A \cup \{\alpha^{23}, \alpha^{46}\}$. Take B in the order $(25, 46, 3, 23, 24, 1, 4, 2)$ and at each shift move the last element to 33 and then remove 33.

Example 45: Let $n = 51$, $g(x) = m_1(x)m_5(x)m_9(x)m_{17}(x)m_{19}(x)$. $R \supset AB$ with $A = \{\alpha^i | i = 1, 2, 5, 7\}$, $B = \{\alpha^j | j = 0, 3, 8, 12, 13, 27, 28, 31, 33, 48\}$. Take B in the order (48, 3, 13, 12, 31, 33, 27, 28, 8, 0) and shift the last element to (respectively) 22, 45, 44, 22, 37, 44, 24, 24, 11 (and at each stage remove the element $\notin R$).

Example 46: Let $n = 51$, $g(x) = m_1(x)m_3(x)m_5(x)m_9(x)m_{17}(x)$. $R \supseteq AB$, where $A = B = \{\alpha^i | i = 1, 3, 6, 9, 12, 15, 27, 33\}$. Take B in the order (33, 27, 3, 9, 6, 15, 12, 1) and shift the last element to (respectively): 31, 11, 22, 31, 35, 35, 11.

Example 47: Let $n = 51$, $g(x) = m_1(x)m_3(x)m_5(x)m_{11}(x)m_{19}(x)$. Here $R \supseteq AB$, where $A = \{\alpha^i | i = 2 \wedge 44 \leq i \leq 49\}$, $B = \{\beta^j | j = 0, 1, 3, 5, 6, 8, 11\}$, $\beta = \alpha^{10}$. Apply Theorem 5 and Corollary 1. We find $d \geq 14$. If d is even then $d \geq 18$ by the BCH bound. So $d \geq 15$.

Example 48: Let $n = 51$, $g(x) = (x^n - 1)/m_1(x)$. It is clear that the condition of Theorem 6-I is satisfied with $l = 4$. Therefore, $d = 24$.

Example 49: Let $n = 55$, $g(x) = m_0(x)m_1(x)$. We have $d \geq 5$ by the HT bound and d is even. To show that $d \neq 6$ take $A = \{\alpha^0, \alpha^7, \alpha^{16}\} = \{\beta^0, \beta^3, \beta^{-1}\}$, $(\beta^{24} = \alpha)$, and $B = \{\alpha^0, \alpha^1, \alpha^2, \alpha^{36}\}$. Shift as follows:

$$(0,1,2,36) \to (13,14,15,49) \to (13,14,49)$$
$$\to (35,36,16) \to (36,16) \to (1,36).$$

Example 50: Let $n = 55$, $g(x) = m_0(x)m_1(x)m_{11}(x)$. We have $R \supseteq AB$ with A as in the previous example, $B = \{\beta^j | j = -3,0,1,2\}$, $\beta = \alpha^{16}$. Apply Theorem 5 and Corollary 1.

Example 51: Let $n = 55$, $g(x) = (x^n - 1)/m_1(x)$. From Code 137 we know $d \geq 10$ and by Theorem 6 we have $d \equiv 0 \pmod 8$. So $d \geq 16$. The remark following Theorem 6 shows that $d \geq 15$ if we take the code with generator $(x^n - 1)/m_0(x)m_1(x)$.

Example 52: Let $n = 55$, $g(x) = m_1(x)m_5(x)$. By theorem 10 $d \geq 11$ or d is even. Assume d is even. For the defining set R (of the even-weight subcode), we have $R \supseteq AB$, where $A = \{\alpha^i | i = 0,1,2,18,49\}$, $B = \{\alpha^j | j = 0,7,8,13,14,16\}$. We shift, using the fact that adding a zero of $m_{11}(x)$ implies weight ≥ 15 by Example 51:

A: $(0,1,2,18,49) \to (15,16,17,33,9)$
$$\to (15,16,17,9) \to (0,1,2,-6)$$
B: $(0,7,8,13,14,16) \to (36,43,44,49,50,52)$
$$\to (36,43,49,50,52)$$
$$\to (50,2,8,9,11)$$
$$\to (50,2,8,9) \to (0,7,13,14);$$
$$\{\alpha^0, \alpha^7, \alpha^{13}, \alpha^{14}\} = \{\beta^0, \beta^1, \beta^{-6}, \beta^2\}, \quad \beta = \alpha^7.$$

Example 53: Let $n = 57$, $g(x) = m_1(x)m_3(x)$. Except for the quadratic residue code of length 47 (where we were saved by Theorem 6), this is the only code in our list for which the true minimum distance exceeds $2d_{\text{BCH}}$. This causes extreme difficulties, but with a trick we can just make our method work. The reader will not find it too difficult to see that shifting (e.g., using $A = B = \{\alpha^i | i = 3,6,9,12,21,24\}$; see below) shows that $d \geq 12$. Of course, we know from Theorem 10 that d is even or $d \geq 19$. The difficult part is to show that $d \neq 12$. For the even-weight subcode we have

$$R = \{\alpha^i | i = 0,1,2,3,4,6,7,8,9,12,14,15,16,$$
$$18,21,24,25,27,28,29,30,$$
$$32,33,36,39,41,42,43,45,$$
$$48,49,50,51,53,54,55,56\}.$$

We have $R \supseteq AB$, where $A = \{\alpha^i | i = 6,9,12\}$, $B = \{\alpha^j | j = 3, 6, 9, 12, 21, 24, 44, 47, 49, 52\}$. Let I be the support of a codeword of weight 12. It is easy to show by shifting (we can now leave out the details) that $\operatorname{rank}(M(B \setminus \{\alpha^{52}\})_I) = \operatorname{rank}(M(B \setminus \{\alpha^{47}\})_I) = 9$. We must try to show that $\operatorname{rank}(M(B)_I) = 10$, which will give a contradiction. We take a closer look at I and at the proof of Theorem 10 and find that $I = I_0 + I_1$, where $|I_0| = 6$, $I_1 = \{i + 19 | i \in I_0\}$ and the positions $\xi_1, \xi_2, \cdots, \xi_6$ indexed by I_0 correspond to a codeword of weight six in the code with generator $m_1(x)$. The positions corresponding to I are $\zeta\xi_1, \cdots, \zeta\xi_6$, where $\zeta = \alpha^{19}$ and we have $\sum_{i=1}^6 \xi_i = 0$ and $\sum \xi_i^3 + \sum(\zeta\xi_i)^3 = 0$ trivially. If the rows of $M(B)_I$ are dependent, then we see by considering $M(B)_{I_0}$ and $M(B)_{I_1}$ separately that the rows of $M(\alpha^{44}, \alpha^{47}, \alpha^{49}, \alpha^{52})_{I_0}$ are dependent, that is, $M(1, \alpha^3, \alpha^5, \alpha^8)_{I_0}$ has rank three (cf. Corollary 1). The theorems in Section IV do not exclude this, but we can show ad hoc that this is false. Suppose there is a polynomial $f(x) = x^8 + ax^5 + bx^3 + c$ with coefficients in $\mathbb{F}_{2^{18}}$ such that $f(\xi_i) = 0$ $(1 \leq i \leq 6)$. Since the coefficient of x^7 in $f(x)$ is zero, we see that the remaining two zeros ξ_7, ξ_8 of f (possibly in an extension field of $\mathbb{F}_{2^{18}}$) are equal, say $\xi_7 = \xi_8 = \xi$. Therefore, $f'(\xi) = 0$ and we then find $b = a\xi^2$, $c\xi^{-2} \in \mathbb{F}_{2^{18}}$. Hence $\xi \in \mathbb{F}_{2^{18}}$, $c = \xi^8$ and hence

$$f(x) = (x + \xi)^2(x^6 + \xi^2 x^4 + ax^3 + \xi^4 x^2 + \xi^6).$$

Since the ξ_i $(1 \leq i \leq 6)$ are the roots of $(x + \xi)^6 = ax^3$, we see that $a = a_0^3$ for some $a_0 \in \mathbb{F}_{2^{18}}$. Let $S_j = \sum_{i=1}^6 \xi_i^j$. Then $0 = \sum_{i=1}^6 f(\xi_i) = S_6 + \xi^2 S_4 + aS_3 + \xi^4 S_2 + \xi^6 S_0$, and since $S_j = 0$ for $j = 1, 2, 4, 8, \cdots \pmod{57}$, we find $S_3 = a$ (because $S_6 = S_3^2$, $S_3 \neq 0$). In the same way, we find from $xf(x)$ that $S_5 = a\xi^2$ and from $x^3 f(x)$ that $S_9 = a^3$. On the other hand, $S_9 = (S_3)^{2^{13}}$ because $3 \cdot 2^{13} \equiv 9 \pmod{57}$. It follows that $a^{19} = 1$, i.e., a_0 is a 57th root of unity. This means the positions $\xi_1, \xi_2, \cdots, \xi_6, a_0$ correspond to a codeword of weight seven in the code with generator $m_3(x)$. This contradicts Theorem 10. This completes the proof that $d = 14$.

Note added in proof: It has been observed by readers of a preprint that the methods of this paper also work for this example without all the tricks that we used above.

VIII. Some Results for Longer Codes

A referee raised the question whether the methods of this paper are still fairly efficient beyond the failure, at 146 in the table. The answer is yes. Of course, there are too many codes of length 63 in the list in [7] to do by hand here, but we shall treat the only code in the list that has $n = 63$ and $d > 2d_{\text{BCH}}$ as an example. The reader shall see that this is indeed a difficult code to handle. However, we point out that a code that looks rather easy, namely, the one with $g(x) = m_1(x)m_9(x)m_{31}(x)$ is actually very hard, and in fact we did not succeed in showing that $d \neq 5$ using our methods.

The list in [7] contains 20 codes of length 65 that have $d > d_{\text{BCH}}$. The ambitious reader can try his skill on these codes as exercises. We shall give several hints that leave only a few hard problems. Again we shall treat the one example with $d > 2d_{\text{BCH}}$ in detail and three easier examples. For five of the 20 codes we do not know at present whether the methods of this paper will yield the true minimum distance.

Example 54: Consider the code C with $n = 63$, $g(x) = m_3(x)m_5(x)m_7(x)m_9(x)m_{11}(x)m_{13}(x)m_{21}(x)m_{27}(x)$

(which is equivalent to the code with factors $m_i(x)$, $i = 1$, 5, 7, 9, 15, 21, 23, 27 in the generator). This code has distance 15 but d_{BCH} is only seven. We have

$$R = \{\alpha^i | i = 3,5,6,7,9,10,11,12,13,14,17,$$
$$18,19,20,21,22,24,25,26,27,28,$$
$$33,34,35,36,37,38,40,41,42,$$
$$44,45,48,49,50,52,54,56\}.$$

The missing cyclotomic cosets in R are $(1,2,4,8,16,32)$, $(15, 30, 60, 57, 51, 39)$, $(23, 46, 29, 58, 53, 43)$, and $(31,62,61,59,55,47)$ which correspond, respectively, to $m_1(x)$, $m_{15}(x)$, $m_{23}(x)$ and $m_{31}(x)$. Denote by C_i ($i = 1, 15, 23$) the code obtained by adding the factor $m_i(x)$ to $g(x)$.

1) *The code C_1:* This code has distance ≥ 15 by the BCH bound.

2) *The code C_{15}:* Call the defining set R_{15}. If we add a zero of $m_1(x)$ or $m_{23}(x)$, we obtain a code with $d \geq 15$. We claim that C_{15} also has $d \geq 15$. This follows from Theorem 5 with $A = \{\alpha^i | i = 9, 10, 11, 12, 13, 14, 24, 56\}$ and $B = \{\alpha^j | j = 0, 1, 24, 25, 26, 27, 28\}$. To find the ranks of $M(A)_I$ and $M(B)_I$, we use shifting (in the abbreviated form; the adjoined element underlined):

$$(48) \to (\underline{16}, 48) \to (\underline{4}, 17, 49) \to (\underline{4}, 6, 19, 51)$$
$$\to (19, 21, \underline{23}, 34, 3)$$
$$\to (3, 5, 7, \underline{8}, 18, 50)$$
$$\to (7, \underline{8}, 9, 11, 12, 22, 54)$$
$$\to (13, 14, 15, \underline{16}, 17, 18, 28, 60)$$
$$\to (9, 10, 11, 12, 13, 14, 24, 56),$$

for A, and

$$(48, 49, 50) \to (\underline{46}, 48, 49, 50) \to (\underline{46}, 7, 9, 10, 11)$$
$$\to (42, 3, \underline{4}, 5, 6, 7)$$
$$\to (57, \underline{58}, 18, 19, 20, 21, 22)$$
$$\to (0, 1, 24, 25, 26, 27, 28)$$

for B.

3) *The code C_{23}:* We now have defining set R_{23}, and if we add a zero of $m_1(x)$ or $m_{15}(x)$ to R_{23}, the new code has $d \geq 15$. Again we claim that C_{23} also has $d \geq 15$. We can now take $B = \{\alpha^j | j = 9, 10, 11, 12, 13, 14\}$ and $A = \{\alpha^i | i = 0, 8, 9, 10, 11, 12, 13, 14, 15\}$. Again A is handled by shifting:

$$(23) \to (\underline{8}, 23) \to (7, \underline{15}, 22) \to (6, 14, \underline{15}, 21)$$
$$\to (29, 37, 38, \underline{39}, 44) \to (28, 36, 37, 38, \underline{39}, 43)$$
$$\to (27, 35, 36, 37, 38, \underline{39}, 42)$$
$$\to (26, 34, 35, 36, 37, 38, \underline{39}, 41)$$
$$\to (25, 33, 34, 35, 36, 37, 38, \underline{39}, 40)$$
$$\to (0, 8, 9, 10, 11, 12, 13, 14, 15).$$

4) From 1)–3) it follows that if we add a zero of $m_1(x)$, $m_{15}(x)$, or $m_{23}(x)$ to R, then the new code has $d \geq 15$. This allows us to use shifting once again. We apply Theorem 5 with $A = \{\alpha^i | i = 0, 8, 16, 24\}$ and $B = \{\alpha^j | j = 3, 9, 10, 11, 12, 17, 18, 20, 25, 26, 28\}$. For B we shift as follows:

$$(21) \to (21, \underline{29}) \to (\underline{4}, 10, 18) \to (\underline{4}, 5, 11, 19)$$
$$\to (\underline{4}, 5, 6, 12, 20) \to (19, 20, 21, 27, \underline{29}, 35)$$
$$\to (17, 18, 19, 25, 27, \underline{32}, 33)$$
$$\to (\underline{8}, 9, 10, 11, 17, 19, 24, 25)$$
$$\to (24, 25, 26, 27, \underline{32}, 33, 35, 40, 41)$$
$$\to (\underline{4}, 10, 11, 12, 13, 18, 19, 21, 26, 27)$$
$$\to (5, 11, 12, 13, 14, 19, 20, 22, 27, 28, \underline{30})$$
$$\to (3, 9, 10, 11, 12, 17, 18, 20, 25, 26, 28).$$

So $M(B)_I$ has rank 11 and we are done.

Remark: The following principles will aid the reader in treating at least half of the codes of length 65 for which $d > d_{\text{BCH}}$.

1) If $m_5(x) | g(x)$, then d is even or $d \geq 13$ by Theorem 10.
2) If $m_{13}(x) | g(x)$, then d is even or $d \geq 5$ by Theorem 10.
3) If d is even, then the even-weight subcode has the same minimum distance.

We first treat three rather easy examples and then the case where $d > 2d_{\text{BCH}}$.

Example 55: Let $n = 65$, $g(x) = m_1(x)m_5(x)$. To show that $d \geq 8$ we apply principles 1) and 3) just given. If we add α^0 to the defining set R, then we can apply HT$(63, 64*0, 17, 34, 51, 68)$.

Example 56: Let $n = 65$, $g(x) = m_0(x)m_1(x)m_7(x)$. If we add the factor $m_3(x)$ to the generator, we obtain a code with $d_{\text{BCH}} = 10$. We apply Theorem 5 and Lemma 5 with $A = B = \{\alpha^i | i = 57, 64, 0, 1\}$. Shifting (abbreviated) gives

$$(8) \to (8, \underline{17}) \to (63, \underline{6}, 7) \to (64, \underline{6}, 7, 8) \to (57, 64, 0, 1).$$

This shows that $d \geq 8$.

Example 57: Let $n = 65$, $g(x) = m_1(x)m_5(x)m_7(x)$. To show that $d \geq 12$ we apply principles 1) and 3) of the remark. So add α^0 to the defining set. The new set contains AB, where $A = \{\alpha^i | i = 0, 1, 2, 4, 5, 7, 8, 9\}$, $B = \{\alpha^j | j = 0, 28, 56\}$. Now Theorem 5 and Corollary 1 yield $d \geq 12$.

Example 58: As a final example, we treat the only code of length 65 for which $d > 2d_{\text{BCH}}$, namely, the code with generator $g(x) = m_1(x)m_3(x)m_5(x)m_{13}(x)$. If we add either α^7 or α^{11} to the defining set, then we obtain a code

with distance at least 16 by the BCH bound. The defining set contains AB, where $A = \{\alpha^i | i = 1, 2, 3, 4, 5, 10, 12, 20, 31, 32, 39, 40\}$ and $B = \{0, 29, 58\}$. To find the rank of $M(A)_I$, where I is the support of a codeword, we apply shifting:

$$
\begin{aligned}
(3,4) &\to (15,16,\underline{51}) \to (5,6,41,\underline{42}) \\
&\to (\underline{29},30,31,1,2) \to (59,60,61,\underline{23},31,32) \\
&\to (62,63,64,26,\underline{27},34,35) \\
&\to (\underline{29},30,31,32,59,60,2,3) \\
&\to (32,33,34,35,\underline{36},62,63,5,6) \\
&\to (31,32,33,34,35,\underline{42},61,62,4,5) \\
&\to (2,3,4,5,6,\underline{11},13,32,33,40,41) \\
&\to (60,61,62,63,64,4,6,\underline{14},25,26,33,34) \\
&\to (1,2,3,4,5,10,12,20,31,32,39,40).
\end{aligned}
$$

So $M(A)_I$ has rank 12 if $|I| \leq 15$, and hence $|I| \geq 15$.

REFERENCES

[1] R. D. Baker, J. H. van Lint, and R. M. Wilson, "On the preparata and Goethals codes," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 342–345, May 1983.

[2] C. R. P. Hartmann and K. K. Tzeng, "Generalizations of the BCH bound," *Inform. Contr.*, vol. 20, pp. 489–498, 1972.

[3] J. H. van Lint, *Coding Theory, Lecture Notes in Mathematics*, vol. 201. New York: Springer-Verlag, 1973.

[4] ——, *Introduction to Coding Theory*. New York: Springer-Verlag, 1982.

[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.

[6] R. J. McEliece, "Weight congruences for p-ary cyclic codes," *Discrete Math.*, vol. 3, pp. 177–192, 1972.

[7] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed. Cambridge, MA:MIT Press, 1972.

[8] 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.

[9] ——, "A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound," *J. Comb. Theory*, Ser A, vol. 33, pp. 229–232, 1982.

[10] R. M. Wilson, "A method for bounding the minimum distance of cyclic codes," in *Proc. 14th S. E. Conf. Combinatorics, Graph Theory and Computing = Congressus Numerantium*, vol. 40, pp. 429–435, 1983.

[11] D. E. Downie and N. J. A. Sloane, "The covering radius of cyclic codes of length up to 31," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 446–447, May 1985.