The Depth Distribution—A New Characterization for Linear Codes

Tuvi Etzion, *Member, IEEE*

***Abstract*—We apply the well-known operator of sequences, the derivative D, on codewords of linear codes. The depth of a codeword c is the smallest integer i such that $D^i c$ (the derivative applied i consecutive times) is zero. We show that the depth distribution of the nonzero codewords of an $[n, k]$ linear code consists of exactly k nonzero values, and its generator matrix can be constructed from any k nonzero codewords with distinct depths. Interesting properties of some linear codes, and a way to partition equivalent codes into depth-equivalence classes are also discussed.**

***Index Terms*—Depth, depth distribution, depth-equivalent, derivative, generator matrix, linear code.**

I. Introduction

Let $W = w_1 w_2 w_3 \cdots$ be a word (finite or infinite) over an alphabet of size q. The *derivative* of W is defined by $w_2 - w_1, w_3 - w_2 \cdots$ where the subtraction is done either in the additive group Z_q or in GF(q) if q is a power of a prime. The derivative was discussed by various authors [6], [7], [9] and was especially used in connection with complexity of sequences [2]–[5]. All these papers are dealing with the case where the sequences are over GF(q). Moreover, except for [2] and [4], in all these papers the sequences are over GF(2). The case where the sequences are over Z_q, q a power of a prime was discussed in [1]. In this correspondence we will connect for the first time between the derivatives of words and linear codes. An $[n, k]$ code over GF(q) is a linear subspace of dimension k of words of length n over GF(q). An $[n, k, d]$ code is an $[n, k]$ code with minimum Hamming distance d.

Henceforth, all words will be finite and over a finite field $F = \mathrm{GF}(q)$. For $\alpha \in \mathrm{GF}(q)$ let $[\alpha^i]$ denote a word with i consecutive appearances of α (distinguished from α^i which is the ith power of α). For a word $x = (x_1, x_2, \cdots, x_n)$ over GF(q) and an element $\alpha \in \mathrm{GF}(q)$, we define $\alpha x = (\alpha x_1, \alpha x_2, \cdots, \alpha x_n)$. We define two operators $\boldsymbol{E}$ and $\boldsymbol{G}$ from F^n to F^{n-1} as follows:

$$\boldsymbol{E}: \quad (x_1, x_2, \cdots, x_n) \rightarrow (x_2, x_3, \cdots, x_n)$$
$$\boldsymbol{G}: \quad (x_1, x_2, \cdots, x_n) \rightarrow (x_1, x_2, \cdots, x_{n-1}).$$

The *derivative* $\boldsymbol{D}$: $F^n \rightarrow F^{n-1}$ is defined as $\boldsymbol{D} = \boldsymbol{E} - \boldsymbol{G}$, i.e.,

$$\boldsymbol{D}(x_1, x_2, \cdots, x_n) = (x_2 - x_1, x_3 - x_2, \cdots, x_n - x_{n-1}).$$

Note, that $\boldsymbol{D}$ is a linear operator, i.e.,

$$\boldsymbol{D}(x + y) = \boldsymbol{D}(x) + \boldsymbol{D}(y)$$

and

$$\boldsymbol{D}(\alpha x) = \alpha \boldsymbol{D} x$$

for $x, y \in F^n$ and $\alpha \in F$.

Manuscript received June 26, 1996; revised December 12, 1996. This research was supported in part by the fund for the promotion of sponsored research at the Technion.

The author is with the Computer Science Department, Technion–Israel Institute of Technology, Haifa 32000, Israel.

Publisher Item Identifier S 0018-9448(97)03449-4.

Definition 1: The depth of a word c of length n, depth(c), is the smallest integer i such that $\boldsymbol{D}^i c = [0^{n-i}]$. If no such i exists, then the depth of c is defined to be n.

As an immediate consequence of the definitions, we have that the depth of a word c of length n is i if and only if $\boldsymbol{D}^{i-1} c = [\alpha^{n-i+1}]$, for a nonzero element $\alpha \in \mathrm{GF}(q)$. It is also clear that the depth of a word of length n is at most n.

Definition 2: Given a code C of length n, let D_i be the number of codewords of depth i. The numbers $D_0, D_1, \cdots, D_n$ are called the depth distribution of C.

In this correspondence we show that the depth distribution is an interesting parameter of linear codes. In Section II we will show that the nonzero codewords of each $[n, k]$ code have exactly k nonzero values in their depth distribution. We also show that any k codewords from distinct nonzero depths can be chosen as the rows of a generator matrix for the code. In Section III we discuss the depth distribution of some binary codes, self-dual codes, the Hamming code, the extended Hamming code, and the first-order Reed–Muller code. Finally, we show how the set of equivalent codes can be partitioned into depth-equivalence classes.

II. On the Depth Distribution of a Linear Code

The main result of this section is a proof that the depth distribution of the nonzero codewords of an $[n, k]$ code consists of exactly k nonzero values. This fact will enable us to obtain some interesting results in this and the next section.

Lemma 1: If c_1 is a word of length n and depth i, and c_2 is a word of length n and depth $j, j < i$, then $c = c_1 + c_2$ is a word with depth i.

Proof: Since c_1 is of depth i, it follows that $\boldsymbol{D}^{i-1} c_1 = [\alpha^{n-i+1}]$. Since c_2 is of depth $j, j < i$, it follows by definition that $\boldsymbol{D}^{i-1} c_2 = [0^{n-i+1}]$. Thus $\boldsymbol{D}^{i-1}(c_1 + c_2) = [\alpha^{n-i+1}]$, and hence we have that $c = c_1 + c_2$ has depth i. □

Lemma 2: If c_1 is a word of length n over GF(q) and α is a nonzero element of GF(q) then αc_1 and c_1 have the same depth.

Proof: This is an immediate observation from the fact that by definition of the derivative we have $\boldsymbol{D}(\alpha c_1) = \alpha \boldsymbol{D} c_1$. □

The immediate consequence of Lemmas 1 and 2 is the following corollary.

Corollary 1: If $c_1, c_2, \cdots, c_k$ are words of length n and distinct depths then $c_1, c_2, \cdots, c_k$ are linearly independent.

Lemma 3: Let c_1 and c_2 be two words of length n and depth i over GF(q). If α is a primitive element in GF(q) then there exists an integer $j, 0 \le j \le q-2$, such that $c_1 + \alpha^j c_2$ is of depth $m, m < i$.

Proof: By the definition of the depth, $\boldsymbol{D}^{i-1} c_1 = [\beta_1^{n-i+1}]$ for some nonzero $\beta_1 \in \mathrm{GF}(q)$ and $\boldsymbol{D}^{i-1} c_2 = [\beta_2^{n-i+1}]$ for some nonzero $\beta_2 \in \mathrm{GF}(q)$. Let j_1 and j_2 be two integers such that $0 \le j_1, \ j_2 \le q-2, \beta_1 = \alpha^{j_1}$, and $-\beta_2 = \alpha^{j_2}$. Let j_3 be an integer such that $0 \le j_3 \le q-2$ and $j_3 \equiv j_1 - j_2 \pmod{q-1}$. Since $\alpha^{j_3}\alpha^{j_2} = \alpha^{j_1}$, it follows that $\boldsymbol{D}^{i-1}(c_1 + \alpha^{j_3} c_2) = [0^{n-i+1}]$ and hence $c_1 + \alpha^{j_3} c_2$ has depth less than i. □

Theorem 1: The depth distribution of the nonzero codewords of an $[n, k]$ linear code consists of exactly k nonzero values.

Proof: By Corollary 1, the depth distribution of the nonzero codewords of an $[n, k]$ code consists of at most k nonzero values. Assume that the depth distribution of the nonzero codewords of an $[n, k]$ code C over GF(q) consists of $m, m < k$, nonzero values. Let C_1 be the subcode that consists of the q^m linear combinations of m

nonzero codewords $c_1, c_2, \cdots, c_m$, where

$$\text{depth } (c_m) > \text{depth } (c_{m-1}) > \cdots > \text{depth } (c_2) > \text{depth } (c_1).$$

Let c be a codeword in $C \setminus C_1$ with the smallest depth. Without loss of generality we can assume that $\text{depth } (c) = \text{depth } (c_i)$, for some $i, 1 \le i \le m$. If α is a primitive element in GF (q) then clearly, $\alpha^j c_i + c$ is a codeword in $C \setminus C_1$ for all $0 \le j \le q-2$. By Lemma 3 there exists an integer $r, 0 \le r \le q-2$, such that $\text{depth } (\alpha^r c_i + c) < \text{depth } (c)$, a contradiction to the assumption that c is a codeword with the smallest depth in $C \setminus C_1$. Thus the depth distribution of the nonzero codewords of C consists of exactly k nonzero values. □

An immediate consequence from Theorem 1 and Corollary 1 is

Corollary 2: Any k codewords of an $[n, k]$ code over GF (q) with distinct nonzero depths can form a generator matrix of the code.

III. More Properties and Applications

An important tool in the understanding of the properties of words of certain depths, and for using the depth as a tool is an algorithm for computing the depth of a word. We will give the algorithm for words over GF (2). This algorithm is a generalization of the algorithm of Games and Chan [5] for computing the linear complexity of a cyclic word of length 2^n. A generalization for GF $(q), q > 2$, is quite simple and will follow the lines presented in [4]. The algorithm which follows is presented in a recursive way.

Algorithm A: Let $V = (v_1, v_2, \cdots, v_n)$ be a binary word of length n and let r be the largest integer such that $2^r < n$. Let

$$V' = (v_1, v_2, \cdots, v_{2^r})$$

and

$$U = (v_1 + v_{2^r+1}, v_2 + v_{2^r+2}, \cdots, v_{n-2^r} + v_n).$$

We compute the function $d(V)$ recursively as follows:

If $V = [0^n]$ then $d(V) = 0$.

If $V = [1^n]$ then $d(V) = 1$.

If $U = [0^{n-2^r}]$ then $d(V) = d(V')$.

If $U \ne [0^{n-2^r}]$ then $d(V) = 2^r + d(U)$

Theorem 2: If $V = (v_1, v_2, \cdots, v_n)$ is a binary word then in Algorithm A we have $d(V) = \text{depth } (V)$.

Proof: If $V = [0^n]$ then obviously $\text{depth } (V) = 0$ and if $V = [1^n]$ then obviously $\text{depth } (V) = 1$. Let r, U, and V' be defined as in the algorithm. We remind that $\text{depth } (V) \le n$ and $\text{depth } (V) = d$ if and only if$(\boldsymbol{E}\text{-}\boldsymbol{G})^{d-1} = [1^{n-d+1}]$. Also note that over GF (2) we have $(\boldsymbol{E} - \boldsymbol{G})^{2^m} = \boldsymbol{E}^{2^m} - \boldsymbol{G}^{2^m}$ since $\binom{2^m}{k}$ is even for $1 \le k \le 2^m - 1$. Therefore, clearly $U \ne [0^{n-2^r}]$ if and only if $\text{depth } (V) > 2^r$ and hence $\text{depth } (V) = 2^r + \text{depth } (U)$. $U = [0^{n-2^r}]$ if and only if $\text{depth } (V) \le 2^r$. We distinguish between two cases.

Case 1: $\text{depth } (V) > 2^{r-1}$. Let

$$\begin{aligned} V^* &= (v_1, v_2, \cdots, v_n, v_{n-2^r+1}, v_{n-2^r+2}, \cdots, v_{2^r}) \\ &= (X_1, X_2, X_3, X_4), \end{aligned}$$

where $X_i, 1 \le i \le 4$, is a word of length 2^{r-1}. Since $U = [0^{n-2^r}]$ and by the definition of V^* it follows that $X_1 = X_3$ and $X_2 = X_4$. Hence

$$\begin{aligned} (\boldsymbol{E} - \boldsymbol{G})^{2^{r-1}} V^* &= (X_1 - X_2, X_2 - X_3, X_3 - X_4) \\ &= (X_1 - X_2, X_1 - X_2, X_1 - X_2) \end{aligned}$$

and thus $\text{depth } (V) = \text{depth } (V')$.

Case 2: $\text{depth } (V) \le 2^{r-1}$. Let

$$\begin{aligned} V^* &= (v_1, v_2, \cdots, v_n, v_{n-2^r+1}, v_{n-2^r+2}, \cdots, v_{2^r}) \\ &= (X_1, X_2, X_3, X_4) \end{aligned}$$

where $X_i, 1 \le i \le 4$, is a word of length 2^{r-1}. Since $\text{depth } (V) \le 2^{r-1}$, it follows that

$$(\boldsymbol{E} - \boldsymbol{G})^{2^{r-1}} V^* = (\boldsymbol{E}^{2^{r-1}} - \boldsymbol{G}^{2^{r-1}}) V^* = [0^{2^r + 2^{r-1}}]$$

and hence $X_1 = X_2, X_2 = X_3$, and $X_3 = X_4$. Thus $\text{depth } (V) = \text{depth } (V')$.

Thus by the recursive definition of the function $d(V)$ in Algorithm A we have $d(V) = \text{depth } (V)$. □

If $n = 2^m$ then Algorithm A for computing the depth coincides with the Games and Chan algorithm [5] for finding the linear complexity of a cyclic sequence. Hence we have the following corollary.

Corollary 3:: If V is a binary word of length 2^n then its depth as a noncyclic word is equal its linear complexity as a cyclic word.

In all the following lemmas we consider only binary words and codes, unless stated otherwise. The first lemma characterizes some of the properties of words with length 2^n (cyclic or noncyclic) and certain depths. Some of these properties are well known [3] and all of them can be easily derived from Algorithm A for computing the depth of a word or the Games and Chan algorithm [5].

Lemma 4:: Let v be a word of length 2^n.

1) v has depth 2^n if and only if v has odd weight, where the weight of a word v is the number of nonzero entries in v.
2) v has depth $2^i + 1$ if and only if v has the form $(X\overline{X}X\overline{X} \cdots X\overline{X})$, where X is a word of length 2^i, and $\overline{X}$ is the binary complement of X.
3) v has weight two only if v has depth $\Sigma_{i=m}^{n-1} 2^i = 2^n - 2^m$, for some $m, 0 \le m \le n-1$.

Next, we intend to show a characterization of the depth distribution for certain kinds of codes.

Definition 3: If C is an $[n, k]$ code over GF (q), its dual or orthogonal code $C^\perp$ is the set of vectors which are orthogonal to all the codewords of C. If $C = C^\perp$ then C is called a self-dual code.

In the next lemma we make use of Corollary 3, i.e., the fact that the depth and the linear complexity of a binary word of length 2^n coincide. First, we extend the definitions of the operators $\boldsymbol{E}$ and $\boldsymbol{D}$. For a binary word $x = (x_1, x_2, \cdots, x_{2^n})$, the *shift operator* $\tilde{\boldsymbol{E}}$ is defined by

$$\tilde{\boldsymbol{E}} x = (x_2, x_3, \cdots, x_{2^n}, x_1)$$

and the operator $\tilde{\boldsymbol{D}}$ is defined by

$$\tilde{\boldsymbol{D}} = (\tilde{\boldsymbol{E}} + \boldsymbol{1}) x = (x_2 + x_1, x_3 + x_2, \cdots, x_{2^n} + x_{2^n - 1}, x_1 + x_{2^n}).$$

The linear complexity of a binary word x of length 2^n is c if $(\tilde{\boldsymbol{E}} + \boldsymbol{1})^{c-1} x = [1^{2^n}]$.

Lemma 5: Let v be a nonzero word of length 2^n and depth $i, 1 \le i \le 2^{n-1}$, and u be a word of length 2^n and depth $2^n + 1 - i$. Then u and v are not orthogonal.

Proof: We will prove that for each i, $1 \le i \le 2^{n-1}$, each word of length 2^n and depth i is not orthogonal to any word of length 2^n and depth $2^n + 1 - i$. The proof is by induction. The basis is $i = 1$; the only word of depth 1, is $[1^{2^n}]$, and by Lemma 4 1), a word of length 2^n has depth 2^n if and only if it has odd weight. Hence, the claim follows. Assume the claim is true for i, $1 \le i \le 2^{n-1} - 1$, i.e., each word of length 2^n and depth i is not orthogonal to any word of length 2^n and depth $2^n + 1 - i$. Let $v = (v_1, v_2, \cdots, v_{2^n})$ be a word of length 2^n and depth $i+1$, and $u = (u_1, u_2, \cdots, u_{2^n})$ be a word of length 2^n and depth $2^n - i$. By definition

$$\tilde{\boldsymbol{D}}v = (v_1 + v_2, v_2 + v_3, \cdots, v_{2^n-1} + v_{2^n}, v_{2^n} + v_1)$$

and by Lemma 4 1) we have that $\Sigma_{j=1}^{2^n} u_j$ is even, and hence there exist two words Y and $\overline{Y}$ such that $\tilde{\boldsymbol{D}}Y = \tilde{\boldsymbol{D}}\overline{Y} = u$, where

$$Y = \left(\sum_{j=1}^{2^n} u_j, u_1, u_1 + u_2, u_1 + u_2 + u_3, \cdots, \sum_{j=1}^{2^n-1} u_j\right).$$

It is easy to see that

$$(\tilde{\boldsymbol{D}}v) \cdot (\tilde{\boldsymbol{E}}Y) = (\tilde{\boldsymbol{D}}v) \cdot (\tilde{\boldsymbol{E}}\overline{Y}) = \sum_{j=1}^{2^n} v_j u_j$$

$\mathrm{depth}\,(u) = \mathrm{depth}\,(\tilde{\boldsymbol{E}}u)$ since u is of length 2^n and by Corollary 3 its depth is equal its linear complexity as a cyclic word. Since $\mathrm{depth}\,(u) = \mathrm{depth}\,(\tilde{\boldsymbol{E}}u)$, it follows that $\tilde{\boldsymbol{D}}v$ and Y are orthogonal if and only if v and u are orthogonal. But, by the induction assumption we have that $\tilde{\boldsymbol{D}}v$ and Y are not orthogonal (since $\tilde{\boldsymbol{D}}v$ has depth i and Y has depth $2^n + 1 - i$) and hence v and u are not orthogonal. □

Corollary 4:: If $\{D_{i_0}, D_{i_1}, \cdots, D_{i_{2^n-1}}\}$ is the set of nonzero values of the depth distribution of a self-dual binary code of length 2^n then for any two integer j and $m, i_j + i_m \neq 2^n + 1$.

Corollary 5: In a self-dual code of length 2^n we have $D_0 = 1$ and for each $i, 1 \leq i \leq 2^{n-1}$, either $D_i = 0$ and $D_{2^n+1-i} \neq 0$, or $D_i \neq 0$ and $D_{2^n+1-i} = 0$.

The first-order Reed–Muller code in an $[2^n, n+1, 2^{n-1}]$ linear code. This code is unique, i.e, all linear codes with the same parameters are equivalent to the first-order Reed–Muller code.

Lemma 6: For any given n, any generator matrix with $n+1$ rows, where row $i, 1 \leq i \leq n$, is any word of length 2^n and depth $2^{i-1}+1$, and row $n+1$ is the only word of length 2^n and depth 1, is a generator matrix of the $[2^n, n+1, 2^{n-1}]$ first-order Reed–Muller code.

Proof: By Corollary 1 all the $n+1$ rows are linearly independent. By Theorem 1 the depths of the nonzero codewords are 1 and $2^j + 1, 0 \leq j \leq n-1$. Therefore, by Lemma 4 2), the weights of all codewords, which are not $[0^{2^n}]$ and $[1^{2^n}]$ is 2^{n-1} and the lemma follows. □

The Hamming code is the unique $[2^n - 1, 2^n - n - 1, 3]$ code. The extended Hamming code is the unique $[2^n, 2^n - n - 1, 4]$ code. The code which is orthogonal to the extended Hamming code is the first-order Reed–Muller code. For more information on these codes the reader is referred to [8].

Lemma 7: For any given n, any generator matrix with $2^n - n - 1$ rows which contains any word of length 2^n and depth i for each i, $1 \leq i \leq 2^n - 1$, $i \neq 2^n - 2^j$, for each j, $0 \leq j \leq n-1$, as a row, is a generator matrix of the $[2^n, 2^n - n - 1, 4]$ extended Hamming code.

Proof: Follows immediately by Lemmas 1 and 4 3). □

Similarly to Lemma 7 we can obtain the following lemma.

Lemma 8: For any given n, any generator matrix with $2^n - n - 1$ rows which contains any word of length $2^n - 1$ and depth i for each i, $1 \leq i \leq 2^n - 1$, $i \neq 2^n - 2^j$, for each j, $0 \leq j \leq n-1$, as a row, is a generator matrix of the $[2^n - 1, 2^n - n - 1, 3]$ Hamming code.

Proof: One can verify from the algorithm for computing the depth of a word that a word of length $2^n - 1$ and weight either one or two has depth $2^n - 2^j$ for some j, $0 \leq j \leq n-1$. The lemma follows now from Lemma 1. □

Another application for the depth distribution is in partitioning and classification of equivalent codes into disjoint classes. Let F_q^n be the set of all words of length n over GF(q). Two codes $C_1, C_2 \subset F_q^n$ are said to be *isomorphic* if there exists a permutation π, such that $C_2 = \{\pi(c) \colon c \in C_1\}$. They are said to be *equivalent* if there exists a vector a and a permutation π, such that $C_2 = \{a + \pi(c) \colon c \in C_1\}$. Since we discuss linear codes, it follows that all equivalent codes can be obtained by the $n!$ permutations on the n coordinates. If r out of the $n!$ permutations result in a code equal to C_1 then there exist $n!/r$ different linear codes equivalent to C_1. If we want further to partition these $n!/r$ codes into new equivalence classes, one simple method is to use the depth distribution of the codes. We will define two linear codes as *depth-equivalent* if they are isomorphic and have the same depth distribution. This definition can give us new interesting results. For example, there are exactly four depth-equivalence classes for the $[8, 4, 4]$ extended Hamming code which is also a self-dual code. The first class has depth distribution $D_0 = 1, D_1 = 1, D_2 = 2, D_3 = 4$, and $D_5 = 8$. The second class has depth distribution $D_0 = 1, D_1 = 1, D_2 = 2, D_5 = 4$, and $D_6 = 8$. The third class has depth distribution $D_0 = 1, D_1 = 1, D_3 = 2, D_5 = 4$, and $D_7 = 8$. The fourth class has depth distribution $D_0 = 1, D_1 = 1, D_5 = 2, D_6 = 4$, and $D_7 = 8$. We do not know all the feasible depth distributions for the $[16, 11, 4]$ extended Hamming code, or any other interesting codes.

Roth [10] has observed that there are other possible alternate definitions of "depth". Let α be an element in GF(q). Let C be a linear code over GF(q), $c = (c_0, c_1, \cdots, c_{n-1})$ be a codeword in C, and $c(x) = \Sigma_{j=0}^{n-1} c_j x^j$ the polynomial associated with c. We say that c has "depth" i, if i is the smallest integer such that

$$(x - \alpha)^i c(x) \equiv 0 (\mathrm{mod}\,(x - \alpha)^n).$$

Similar results to the ones obtained in this correspondence can be obtained by using this definition for the "depth." If $\alpha = 1$ and n is a power of q then the depth of a codeword c by both definitions is the same. It is intriguing to find connections between these two definitions, more connections between the linear complexity and the depth of a word, to find the depth distribution of other interesting codes, and more applications for the concept of depth associated with linear codes.

Acknowledgment

The author wishes to thank R. Roth for his valuable suggestions, G. A. Kabatyanskii, C. Mitchell, and A. Vardy for helpful discussions, and two anonymous referees for their careful reading and important observations which amended to the presentation of this correspondence.

References

[1] R. Bar-Yehuda, T. Etzion, and S. Moran, "Rotating-table games and derivatives of words," *Theor. Comput. Sci.*, vol. 108, pp. 311–329, 1993.

[2] S. R. Blackburn, T. Etzion, and K. G. Paterson, "Permutation polynomials, de bruijn sequences and linear complexity," *J. Comb. Theory, Ser. A*, vol. 76, pp. 55–82, 1996.

[3] A. H. Chan, R. A. Games, and E. L. Key, "On the complexities of de bruijn sequences," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 233–246, 1982.

[4] C. Ding, "A fast algorithm for determining the linear complexity of sequences over GF(p^m) with period p^n," unpublished manuscript, 1990.

[5] R. A. Games and A. H. Chan, "A fast algorithm for determining the complexity of binary sequences with period 2^n," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 144–166, 1983.

[6] T. Goka, "An operator on binary sequences," *SIAM Rev.*, vol. 12, pp. 264–266, 1970.

[7] A. Lempel, "On a homomorphism of the de bruijn graph and its applications to the design of feedback shift resiters," *IEEE Trans. Comput.*, vol. C-19, pp. 1204–1209, 1970.

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

[9] M. B. Nathanson, "Derivatives of binary sequences," *SIAM J. Appl. Math.*, vol. 21, pp. 407–412, 1971.

[10] R. M. Roth, private communication.