On integer-valued rational polynomials and depth distributions of binary codes

Chris J. Mitchell (cjm@dcs.rhbnc.ac.uk)[*], *Member IEEE*

1st January 1998

Abstract

The notion of the depth of a binary sequence was introduced by Etzion. In this paper we show that the set of infinite sequences of finite depth corresponds to a set of equivalence classes of rational polynomials. We go on to characterize infinite sequences of finite depth in terms of their periodicity. We conclude by giving the depth distributions for all linear cyclic codes.

Index terms: depth, depth distribution, derivative, cyclic code, linear complexity

1 Introduction

In this paper we are concerned with considering the *depths* of binary sequences, where depth is as defined by Etzion, [1]. Etzion showed that a linear code of dimension k contains codewords of k distinct depths, and also gave the distribution of codeword depths for

[*] Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, U.K.

certain classes of codes.

We firstly show that the set of infinite sequences of finite depth corresponds to a set of equivalence classes of rational polynomials. We secondly establish an equivalence between infinite sequences of finite depth and sequences of specified periodicity. Thirdly we give the depth distributions for all linear cyclic codes, generalising the results in [1].

2 Definitions and preliminary remarks

2.1 Binary sequences

Suppose $\mathbf{s} = (s_i)$ $(i \geq 0)$ is a binary sequence (either finite or infinite). Then we say $\mathbf{s}$ is periodic with period t $(t > 0)$ if $s_i = s_{i+t}$ for every i $(i \geq 0)$. If t is the smallest positive integer for which $\mathbf{s}$ is periodic with period t, then $\mathbf{s}$ is said to have least period t (in which case $\mathbf{s}$ has period t' if and only if $t|t'$).

We write $\mathbf{0}$ and $\mathbf{1}$ for the sequences of all zeros and all ones respectively. If $\mathbf{x}$ and $\mathbf{y}$ are two binary sequences, then we write $\mathbf{x}+\mathbf{y}$ for the sequence obtained as the term by term modulo 2 sum of the elements of the two sequences. Finally, in a binary sequence, we define a 0-run of length k to be a subsequence containing k consecutive zeros.

2.2 Depths of binary sequences

Suppose $\mathbf{s} = (s_i)$ $(i \geq 0)$ is a binary sequence (either finite or infinite). The *derivative* of $\mathbf{s}$, denoted $D\mathbf{s}$, is defined to be the sequence $\mathbf{t} = (t_i)$ where $t_i = s_{i+1} - s_i$, and $D^i\mathbf{s}$ is defined to be the result of i applications of D to $\mathbf{s}$. Note that if $\mathbf{s}$ is finite of length n then $\mathbf{t}$ is finite of length $n-1$. Note also that, for a finite sequence $\mathbf{s}$ of length n, $D^i\mathbf{s}$ is only defined if $0 \leq i < n$.

As defined by Etzion, [1], the *depth* of a sequence $\mathbf{s}$ is then simply the smallest integer i (if one exists) such that $D^i\mathbf{s} = \mathbf{0}$. If no such i exists then, for a finite sequence of length n the depth is defined to be n, and for an infinite sequence the depth is defined to be infinite. Note that sequences of infinite depth certainly exist — consider, for example, the infinite sequence

$$(0, 1, 1, 0, 1, 1, 0, 1, 1, \ldots).$$

Observe that, as given in [1], if $\mathbf{s}$ has depth d, then $D^{d-1}\mathbf{s} = \mathbf{1}$.

Let S be the set of all infinite binary sequences, i.e.

$$S = \{(s_i) \ : \ i \geq 0; \ s_i \in \{0, 1\} \text{ for every } i \geq 0\}.$$

We then define S^* to be the subset of S consisting only of sequences of finite depth. As we have already noted $S \setminus S^*$ is certainly not empty; however it is simple to see that for any sequence $(s_i) \in S$ and any integer N, there exists a sequence $(s_i^*) \in S^*$ such that $s_i = s_i^*$ for every $i \leq N$.

We next make an important, albeit trivial, observation.

Remark 2.1 *If* $\mathbf{s} = (s_0, s_1, \ldots, s_{n-1})$ *is a finite binary sequence of depth* d*, say, (*$0 \leq d \leq n$*), then the addition of an additional element (0 or 1) to the end of* $\mathbf{s}$ *will either leave the depth unchanged or will increase the depth to* $n + 1$*. Hence any finite binary sequence of depth* d *can be uniquely extended to an infinite binary sequence of depth* d*.*

2.3 Linear codes and depth distributions

We are concerned here exclusively with (n, k) linear codes, i.e. subspaces of dimension k of the n-dimensional vector space over $\mathbf{Z}_2$. We also refer to codewords of length n, by which we mean elements of the n-dimensional vector space over $\mathbf{Z}_2$.

A *cyclic code* C of length n is an ideal in the ring $\mathbf{Z}[x]/(x^n-1)$. This ring is a Principal Ideal Domain, and hence C has a generator g. We can associate with g a polynomial $g(x) \in \mathbf{Z}_2[x]$, where $g(x)$ has degree at most n and $g(x)|x^n-1$. If $g(x)$ has degree $n-k$, we can then write

$$C = \{c(x)g(x) \ : \ c(x) \in \mathbf{Z}_2[x]; \text{ deg } c(x) < k\}$$

and regard C as a set of polynomials of degree at most $n-1$. C is then an (n,k) linear code, where with each polynomial $a(x) = \sum_{i=0}^{n-1} a_{n-i-1}x^i$ we associate the n bit sequence $(a_0, a_1, \ldots, a_{n-1})$.

For background information on cyclic codes see, for example, Chapter 7 of [2]. Again following Etzion, [1], given a code C of length n, let D_i denote the number of codewords in C of depth i ($i > 0$), and the *depth distribution* of C is simply the tuple of numbers $(D_1, D_2, \ldots, D_n)$.

Result 2.2 (Theorem 1 of [1]) *The depth distribution of an* (n,k) *linear code contains exactly* k *non-zero values.*

We refer to the set of values of i for which D_i is non-zero as the *depth spectrum* of a code, which, by Result 2.2, must contain exactly k integers.

3 Rational polynomials and binary sequences

We now consider a special class of rational polynomials. We show that, under a simple equivalence relation, the equivalence classes of these polynomials have a direct correspondence with infinite binary sequences of finite depth. Moreover the depth of a binary sequence simply corresponds to the minimal degree of all polynomials in the corresponding equivalence class.

These results were inspired by corresponding results for sequences over the reals. The use of the Δ operator to find a polynomial of minimal degree which matches a given set of data points dates back to Newton, and such methods can be found in any elementary text on Numerical Analysis, e.g. Chapter 6 of [3]. What is perhaps surprising is the usefulness of the field $\mathbf{Q}$ in this context, instead of finite fields as used in analogous work in [4].

Let $\mathbf{Q}[x]$ be the set of all polynomials over the rationals $\mathbf{Q}$. Further let $\mathbf{Q_Z}[x]$ be the subset of $\mathbf{Q}[x]$ containing those polynomials which are integer-valued for all integers x, i.e.

$$\mathbf{Q_Z}[x] = \{f(x) \in \mathbf{Q}[x] \; : \; f(i) \in Z \text{ for every } i \in Z\}.$$

If $f(x), g(x) \in \mathbf{Q_Z}[x]$ then we define the equivalence relation $\simeq$ by $f(x) \simeq g(x)$ if and only if $f(i) \equiv g(i) \pmod 2$ for every $i \in Z$. For any polynomial $f(x)$ we write $\overline{f(x)}$ for the equivalence class containing $f(x)$. Let $\overline{\mathbf{Q_Z}[x]}$ denote the set of equivalence classes under $\simeq$. For the purposes of this paper we are almost exclusively concerned with these equivalence classes.

Remark 3.1 *Note that $\mathbf{Z}[x]$ is a subset of $\mathbf{Q_Z}[x]$, but is rather an uninteresting subset from our viewpoint, since if $f(x) \in \mathbf{Z}[x]$ then $\overline{f(x)} \in \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$, i.e. all polynomials in $\mathbf{Z}[x]$ fall into one of just four equivalence classes in $\overline{\mathbf{Q_Z}[x]}$.*

Conversely, $\mathbf{Q_Z}[x] \setminus \mathbf{Z}[x]$ contains infinitely many equivalence classes, e.g. $\overline{x^2/2 + x/2}$ and $\overline{x^3/6 + x^2/2 + x/3}$ (see Lemma 3.7 below).

We define the *depth* of an equivalence class of polynomials $\overline{f(x)}$ to be one greater than the minimum degree amongst the polynomials in $\overline{f(x)}$. We show below how this corresponds directly to the notion of the depth of a binary sequence. We also define the meaning of the Δ operator for polynomials: if $f(x) \in \mathbf{Q_Z}[x]$ then $\Delta f(x) = (f(x+1) - f(x)) \in \mathbf{Q_Z}[x]$.

Note that, for convenience, we refer to the zero polynomial as having degree -1.

Remark 3.2 *There is only one equivalence class of polynomials of depth 0, and only one equivalence class of polynomials of depth 1, namely $\overline{0}$ and $\overline{1}$ respectively. This holds because the only polynomial in $\mathbf{Q_Z}[x]$ of degree -1 is 0, and the only polynomials in $\mathbf{Q_Z}[x]$ of degree 0 are those equal to an integer. The even integer polynomials all belong to $\overline{0}$, and the odd integer polynomials all belong to $\overline{1}$.*

We can now state the following well-known result:

Result 3.3 (Section 6.8 of [3]) *Suppose $f(x) \in \mathbf{Q_Z}[x]$ has degree $d \geq 0$, and hence let*

$$f(x) = \sum_{i=0}^{d} f_i x^i.$$

Then

$$\Delta f(x) = \sum_{i=0}^{d-1} g_i x^i.$$

where

$$g_j = \sum_{i=j+1}^{d} \binom{i}{j} f_i, \quad 0 \leq j < d.$$

I.e. $\Delta f(x)$ has degree exactly $d-1$.

We next define Δ^{-1} as follows. If $g(x) \in \mathbf{Q_Z}[x]$ then

$$\Delta^{-1} g(x) = \{f(x) \in \mathbf{Q_Z}[x] \; : \; \Delta f(x) = g(x)\}.$$

We now establish the following simple result, which coincides with corresponding results for derivatives and integrals.

Lemma 3.4 *If $g(x) \in \mathbf{Q_Z}[x]$ with leading coefficient r and degree $d-1$, then $\Delta^{-1}g(x)$ is a non-empty set with the property that if $f(x) \in \Delta^{-1}g(x)$ then:*

(i) $f(x) - f^*(x)$ is a constant polynomial if and only if $f^*(x) \in \Delta^{-1}g(x)$, and

(ii) $f(x)$ has leading coefficient r/d and degree d.

Proof Suppose $g(x) \in \mathbf{Q_Z}[x]$ has degree $d-1$, and let

$$g(x) = \sum_{i=0}^{d-1} g_i \binom{x}{i}$$

(this is the *standard form* for an Integer Valued Polynomial). Now define the degree d polynomial $f(x) \in \mathbf{Q_Z}[x]$ by:

$$f(x) = \sum_{i=1}^{d} g_{i-1} \binom{x}{i}$$

It follows immediately that $\Delta f(x) = g(x)$, and so $\Delta^{-1}g(x)$ is non-empty.

Now suppose $f(x) \in \Delta^{-1}g(x)$.

(i) By Result 3.3 it should be clear that if $f(x), f^*(x) \in \Delta^{-1}g(x)$, then $f(x) - f^*(x)$ is equal to a constant. Moreover, if $f(x) - f^*(x)$ is equal to a constant, then, again by Result 3.3, $\Delta f(x) = \Delta f^*(x)$.

(ii) By Result 3.3 it should be clear that $f_d = g_{d-1}/d$, and the result now follows. □

We now abuse our notation slightly and also consider Δ as a mapping from $\overline{\mathbf{Q_Z}[x]}$ into $\overline{\mathbf{Q_Z}[x]}$. This is well defined since if $f(x) \simeq h(x)$ then

$$\Delta f(x) = f(x+1) - f(x) \simeq h(x+1) - h(x) = \Delta h(x).$$

It also follows that $\Delta \overline{f(x)} = \overline{\Delta f(x)}$.

We then immediately have:

Corollary 3.5 *Suppose $\overline{f(x)} \in \overline{\mathbf{Q_Z}[x]}$ has depth $d > 0$. Then $\Delta \overline{f(x)}$ has depth $d-1$.*

Proof Since $\overline{f(x)} \in \overline{\mathbf{Q}_{\mathbf{Z}}[x]}$ has depth $d > 0$, there exists a polynomial $h(x) \in \overline{f(x)}$ of degree $d-1$ (and no polynomial of smaller degree). Now, by definition, $\Delta h(x)$ (which has degree $d-2$ by Result 3.3) is an element of $\Delta\overline{f(x)}$, and hence $\Delta\overline{f(x)}$ has depth at most $d-1$.

Now suppose $h(x) \in \Delta\overline{f(x)}$ has depth less than $d-2$. Then there exists a polynomial $m(x) \in \overline{f(x)}$ such that $\Delta m(x) = h(x)$; hence, by Result 3.3, $m(x)$ has degree less than $d-1$. This contradicts our assumption that $\overline{f(x)}$ has depth d. □

We can also define the action of Δ^{-1} on an element of $\overline{\mathbf{Q}_{\mathbf{Z}}[x]}$. We then have:

Lemma 3.6 *Suppose* $\overline{h(x)} \in \overline{\mathbf{Q}_{\mathbf{Z}}[x]}$. *Then* $\Delta^{-1}\overline{h(x)}$ *contains precisely two elements of* $\overline{\mathbf{Q}_{\mathbf{Z}}[x]}$.

Proof Suppose $f_1(x), f_2(x) \in \mathbf{Q}_{\mathbf{Z}}[x]$ satisfy $\Delta f_1(x) \simeq \Delta f_2(x)$. Then, if $m(x) = \Delta(f_1(x) - f_2(x))$, by definition we have:

$$m(i) \equiv 0 \pmod 2$$

for every integer $i \geq 0$. Hence $m(x) \simeq 0$, i.e. $\overline{\Delta(f_1(x) - f_2(x))}$ has depth 0. Hence, by Corollary 3.5, $\overline{f_1(x) - f_2(x)}$ has depth 0 or 1. Now, by Remark 3.2, this means that $\overline{f_1(x) - f_2(x)} \in \{\overline{0}, \overline{1}\}$, i.e. either $f_1(x) - f_2(x) \simeq 0$ or $f_1(x) - f_2(x) \simeq 1$.

Hence either $f_1(x) \simeq f_2(x)$ or $f_1(x) \simeq f_2(x) + 1$. Thus either $\overline{f_1(x)} = \overline{f_2(x)}$ or $\overline{f_1(x)} = \overline{f_2(x) + 1}$, and hence $\Delta^{-1}\overline{h(x)}$ either contains zero or two elements. But, by Lemma 3.4, $\Delta^{-1}\overline{h(x)}$ cannot be empty, and the result follows. □

We also have the following lemma establishing some basic properties of $\overline{\mathbf{Q}_{\mathbf{Z}}[x]}$.

Lemma 3.7 *(i) The number of equivalence classes in* $\overline{\mathbf{Q}_{\mathbf{Z}}[x]}$ *which have depth* d $(d > 0)$ *is precisely* 2^{d-1}.

(ii) Suppose $\overline{g(x)} \in \overline{\mathbf{Q}_{\mathbf{Z}}[x]}$ *has depth* $d+1$ $(d \geq 0)$*. Then there exists* $f(x) \in \overline{g(x)}$ *of degree* d *with leading coefficient equal to* $(1/d!)$*.*

Proof We establish both results by induction on the depth d.

(i) By Remark 3.2, the result holds for $d = 1$. Suppose that the result holds for all depths less than d, for some $d > 1$. Now, by Lemma 3.6, if $\overline{g(x)}$ has depth $d-1$, then there exist precisely two equivalence classes $\overline{f(x)}$ with the property that $\Delta\overline{f(x)} = \overline{g(x)}$. Moreover, both these equivalence classes will have depth d by Corollary 3.5. By the inductive hypothesis, there are 2^{d-2} such equivalence classes $\overline{g(x)}$, each having two such equivalence classes $\overline{f(x)}$ of depth d. All these 2^{d-1} equivalence classes will be distinct, and they will include all possible equivalence classes of depth d (again by Corollary 3.5). The result now follows.

(ii) $1 \in \overline{1}$ (which has leading coefficient 1), and hence the result holds for $d = 0$. Now suppose it holds for all depths less than or equal to d, and suppose $\overline{g(x)}$ has depth $d+1$. Now, by Corollary 3.5, $\Delta\overline{g(x)}$ has depth d. Choose $h(x) \in \Delta\overline{g(x)}$ with degree $d-1$ and leading coefficient $1/d!$ (which exists by the inductive hypothesis). Now, by Lemma 3.4(ii), if $f(x) \in \Delta^{-1}h(x)$, then $f(x)$ has degree d and leading coefficient $1/(d+1)!$, and the result follows. □

Next define the function $\Phi : \mathbf{Q}_{\mathbf{Z}}[x] \rightarrow S$ as follows.

Definition 3.8 $\Phi(f(x)) = (s_i)$, $i \geq 0$, *where* $s_i = f(i) \bmod 2$ *for every* i*.*

We then immediately have the following result.

Lemma 3.9 Φ *has the following properties.*

(i) Φ *is a group homomorphism from* $(\mathbf{Q}_{\mathbf{Z}}[x], +)$ *into* $(S, +)$*.*

(ii) Φ *commutes with* D/Δ, *i.e.* $\Phi(\Delta f(x)) = D\Phi(f(x))$, *for every* $f(x) \in \mathbf{Q_Z}[x]$.

As we did with the Δ operator, we now abuse our notation slightly and also consider Φ as a mapping from $\overline{\mathbf{Q_Z}[x]}$ into S. This is well defined by the definition of $\simeq$.

We then have the following results.

Lemma 3.10 *If* $\overline{f(x)} \in \overline{\mathbf{Q_Z}[x]}$, *then the depth of* $\overline{f(x)}$ *equals the depth of the sequence* $\Phi(\overline{f(x)})$.

Proof Suppose $f(x) \in \mathbf{Q_Z}[x]$ and suppose the infinite binary sequence $\Phi(f(x))$ has depth d, i.e.

$$D^{d-1}\Phi(f(x)) = \mathbf{1}.$$

Hence, by Lemma 3.9(ii):

$$\Phi(\Delta^{d-1}f(x)) = \mathbf{1}$$

i.e. $\Delta^{d-1}f(i) \equiv 1 \pmod 2$ for every integer i. Hence $\overline{\Delta^{d-1}f(x)} = \overline{1}$ (the unique equivalence class of polynomials of depth 1). Hence, by Corollary 3.5, $\overline{f(x)}$ has depth precisely d, and the result follows. □

Theorem 3.11 Φ *is a group isomorphism of* $(\overline{\mathbf{Q_Z}[x]}, +)$ *onto* $(S^*, +)$.

Proof We first show that Φ always maps an element of $\overline{\mathbf{Q_Z}[x]}$ into an element of S^*. Suppose $\overline{f(x)} \in \overline{\mathbf{Q_Z}[x]}$, and hence $\overline{f(x)}$ has depth d (for some integer d). Then, by Lemma 3.10, $\Phi(\overline{f(x)})$ also has finite depth d and so $\Phi(\overline{f(x)}) \in S^*$.

By Lemma 3.9(i), we need only show that Φ is a bijection. First suppose $\Phi(\overline{f_1(x)}) = \Phi(\overline{f_2(x)})$. Hence $g_1(i) \equiv g_2(i) \pmod 2$ for any $g_1(x) \in \overline{f_1(x)}$ and any $g_2(x) \in \overline{f_2(x)}$. Hence $\overline{f_1(x)} = \overline{f_2(x)}$, and we have shown that Φ is injective.

We show that Φ is surjective by induction on the depths of elements in S^*. First observe that $\mathbf{0}$ is the unique sequence of depth 0, and $\Phi(\overline{0}) = \mathbf{0}$. Now suppose that every binary sequence of depth less than d has a pre-image in $\overline{\mathbf{Q}_{\mathbf{Z}}[x]}$ under Φ. Suppose that $\mathbf{x}$ is a binary sequence of depth d.

By definition, $D\mathbf{x}$ has depth $d-1$, and hence by the inductive hypothesis, there exists a polynomial $f(x) \in \mathbf{Q}_{\mathbf{Z}}[x]$ such that:

(a) $\overline{f(x)}$ has depth $d-1$, and

(b) $\Phi(\overline{f(x)}) = D\mathbf{x}$.

Now, by Lemma 3.6, $\Delta^{-1}\overline{f(x)}$ contains precisely two elements of $\overline{\mathbf{Q}_{\mathbf{Z}}[x]}$. Additionally, by Lemma 3.9(ii),

$$\Phi(\Delta^{-1}\overline{f(x)}) \subset D^{-1}\Phi(\overline{f(x)}) = D^{-1}D\mathbf{x}.$$

But $D^{-1}D\mathbf{x}$ contains two elements, namely $\mathbf{x}$ and $\mathbf{x}+\mathbf{1}$, and hence $\Phi(\Delta^{-1}\overline{f(x)}) = D^{-1}D\mathbf{x}$. The result now follows. □

We conclude by observing that if $\overline{f_1(x)}, \overline{f_2(x)} \in \overline{\mathbf{Q}_{\mathbf{Z}}[x]}$, then, $\overline{f_1(x)+f_2(x)}$ will clearly have depth equal to the greater of the depths of $\overline{f_1(x)}$ and $\overline{f_2(x)}$, given they are different. If they have the same depth, d say, then $\overline{f_1(x)+f_2(x)}$ will have depth less than d (this follows immediately from Lemma 3.7(ii)). This provides the basis of an alternative proof for Result 2.2.

Before proceeding we give some elementary results about the depths and periodicity of infinite binary sequences. We first have the following simple result, which follows immediately from Lemma 3.7(i) and Theorem 3.11.

Lemma 3.12 *If $d > 0$ then there are precisely 2^{d-1} infinite binary sequences of depth d.*

We can also establish results characterising binary sequences of finite depth in terms of their period. We first have the following trivial result, whose proof follows immediately from the definition of D.

Lemma 3.13 *If* $\mathbf{x}$ *is a binary sequence of finite depth* $d > 0$*, and* $D\mathbf{x}$ *is periodic with least period* t*, then* $\mathbf{x}$ *is periodic with least period either* t *or* $2t$*.*

We can now establish:

Lemma 3.14 *If* $\mathbf{x}$ *and* $\mathbf{y}$ *are binary sequences of finite depth* $d > 0$*, then* $\mathbf{x}$ *and* $\mathbf{y}$ *are periodic, and have the same period which must be equal to a power of 2.*

Proof Since $\mathbf{1}$ is the unique sequence of depth 1 and has period $2^0 = 1$, Lemma 3.13 immediately implies that every sequence of finite depth must have finite period equal to a power of 2. The result then follows from Etzion's observation in [1] that, for a finite sequence of length 2^i (for some $i > 0$), the notion of depth corresponds precisely to the linear equivalence of the corresponding infinite sequence of period 2^i. $\Box$

Finally, given the above-mentioned correspondence between depth and linear equivalence, we can also give the following result, well-known in the context of the linear equivalence of sequences.

Theorem 3.15 *The set* S^* *of infinite binary sequences with finite depth is equal to the set of infinite binary sequences of period* 2^i *for some* $i \geq 0$*. Moreover, if* $\mathbf{s} \in S$ *has depth* d*, then the least period of* $\mathbf{s}$ *is* $2^{\lfloor \log_2 d \rfloor + 1}$*, i.e. the set of sequences having depths from* $\{2^i + 1, 2^i + 2, \ldots, 2^{i+1}\}$ *is equal to the set of sequences of period* 2^{i+1} *(*$i \geq 0$*).*

Remark 3.16 *It is interesting to note that we have established a relationship between the linear equivalence of sequences having period a power of 2, and the degrees of polynomials* *in the corresponding equivalence classes of rational polynomials.*

4 Depth distributions of linear cyclic codes

In this section we characterise the depth distributions of all linear cyclic codes. The key observation that we use to establish this characterisation is that, if $\mathbf{x}$ is a codeword of a linear cyclic code, and $\mathbf{1}$ is *not* a codeword of C, then $D^s\mathbf{x}$ must be equal to a substring of some non-zero codeword.

We first need the following elementary observation.

Lemma 4.1 *Suppose $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ is a binary codeword of length n, with corresponding polynomial:*

$$c(x) = c_0x^{n-1} + c_1x^{n-2} + \cdots c_{n-1}.$$

Then the $n-i$ elements of $D^i\mathbf{c}$ equal the first $n-i$ terms (i.e. the terms for x^{n-1}, x^{n-2}, $\ldots$, x^i) of the polynomial $c(x)(x-1)^i \bmod (x^n-1)$.

Proof We prove this result by induction on i. It is trivially true for $i = 0$. Now suppose it is true for all $i < r$, for some $r > 0$, i.e. we know that $D^{r-1}\mathbf{c}$ corresponds to the first $n-r+1$ terms of the polynomial $c(x)(x-1)^{r-1} \bmod (x^n-1)$. Suppose $D^{r-1}\mathbf{c} = (b_0, b_1, \ldots, b_{n-r})$ and hence

$$b_0x^{n-1} + b_1x^{n-2} + \cdots + b_{n-r}x^{r-1}$$

is equal to the first $n-r+1$ terms of $c(x)(x-1)^{r-1} \bmod (x^n-1)$. Thus

$$D^r\mathbf{c} = (b_1 - b_0, b_2 - b_1, \ldots, b_{n-r} - b_{n-r-1})$$

and, working modulo (x^n-1):

$$c(x)(x-1)^r \quad = \quad (x-1)(b_0x^{n-1} + b_1x^{n-2} + \cdots + b_{n-r}x^{r-1} + f(x))$$

$$= \quad (b_1 - b_0)x^{n-1} + (b_2 - b_1)x^{n-2} + \cdots + (b_{n-r} - b_{n-r-1})x^r + f'(x)$$

where $f(x)$ and $f'(x)$ are polynomials of degrees at most $r-2$ and $r-1$ respectively.

The result now follows. □

We can now establish:

Lemma 4.2 *Suppose C is a linear cyclic code of length n with the property that $\mathbf{1}$ is not a codeword. Suppose also that the maximum length of a 0-run in a codeword of $C - \{\mathbf{0}\}$ is L. Then all the non-zero codewords in C have depth at least $n - L$.*

Proof Suppose $\mathbf{x}$ is a non-zero codeword from C, and choose $s = n - L - 1$. Then, since C is a linear cyclic code, $D^s\mathbf{x}$ is equal to $n - s$ consecutive bits of a non-zero codeword. This follows by induction, since $D\mathbf{x}$ is simply $n-1$ consecutive bits of the sum of $\mathbf{x}$ with a copy of $\mathbf{x}$ cyclically shifted by one position. Now, since C is linear and cyclic, $D\mathbf{x}$ is equal to $n-1$ bits of a codeword, which is non-zero since $\mathbf{x} \neq \mathbf{1}$.

Moreover, the $n-s$ consecutive bits of $D^s\mathbf{x}$ cannot all be zero since $n - s = L + 1 > L$. Hence $\mathbf{x}$ has depth greater than $s = n - L - 1$, and the result follows. □

Corollary 4.3 *If $g(x)$ is the generator polynomial for an (n,k) linear cyclic code C, and $(x-1) \not| (x^n - 1)/g(x)$, then C has depth spectrum $\{n, n-1, \ldots, n-k+1\}$.*

Proof In such a linear cyclic code, if a codeword contains a 0-run of length k then it must be the all-zero codeword. Moreover, $\mathbf{1}$ cannot be a codeword since $(x-1) \not| (x^n-1)/g(x)$. The result now follows from Result 3.3 and Lemma 4.2. □

Lemma 4.4 *Suppose $(x-1)^s | (x^n - 1)$, and let C be an (n,s) linear cyclic code. Then C has generator polynomial $(x^n-1)/(x-1)^s$ if and only if the depth spectrum of C is $\{1, 2, \ldots, s\}$.*

Proof Suppose that $(x^n-1)/(x-1)^s$ is the generating polynomial for C, and hence

$$C = \{f(x)(x^n-1)/(x-1)^s \bmod x^n-1 \ : \ \deg(f(x)) < s\}.$$

If $\mathbf{c} \in C$ is a codeword with corresponding polynomial $c(x)$ then, by Lemma 4.1, $D^s\mathbf{c}$ corresponds to the first $n-s$ terms of $(x-1)^s c(x)$. But, by our assumption, $c(x) = c'(x).(x^n-1)/(x-1)^s \bmod x^n-1$, for some polynomial $c'(x)$. Hence $D^s\mathbf{c}$ corresponds to the first $n-s$ terms of $(x-1)^s c'(x)(x^n-1)/(x-1)^s = 0 \bmod x^n-1$, i.e. $\mathbf{c}$ has depth at most s, and hence, by Result 3.3, the depth spectrum is $\{1,2,\ldots,s\}$.

Now suppose every codeword has depth at most $s < n$ (the case $s = n$ is trivial since every depth must occur). Using the converse argument, we see that for any $c(x)$ corresponding to a codeword $\mathbf{c}$, the first $n-s$ terms of $(x-1)^s c(x)$ must all be zero. But, since C is cyclic, every cyclic shift of $(x-1)^s c(x)$ must equal $(x-1)^s c'(x)$ for some other polynomial $c'(x)$ corresponding to a codeword. Hence $(x-1)^s c(x) = 0$ for every $c(x)$, i.e.

$$(x^n-1)|(x-1)^s c(x)$$

for every $c(x)$. The result now follows. □

We are now ready to state the main result of this part of the paper, which provides a complete characterisation of the depth spectra of linear cyclic codes.

Note that in the next theorem we use $||$ to denote 'exactly divides', in the sense that $a(x)^r||b(x)$ if and only if $a(x)^r|b(x)$ and $a(x)^{r+1} \not| b(x)$.

Theorem 4.5 *Suppose C is an (n,k) linear cyclic code, and let $g(x)$, of degree $n-k$, be the generator polynomial for C. Then*

$$(x-1)^s||(x^n-1)/g(x)$$

if and only if C has depth spectrum $\{1,2,\ldots,s\} \cup \{n, n-1, \ldots, n-k+s+1\}$.

Proof Suppose $g(x)$, the generator polynomial for C, satisfies

$$(x-1)^s || (x^n-1)/g(x).$$

We define two related linear cyclic codes: C_0, an (n,s) code with generator polynomial $(x^n-1)/(x-1)^s$, and C_1, an $(n,k-s)$ code with generator polynomial $g(x)(x-1)^s$. By Lemma 4.4, C_0 has depth spectrum $\{1,2,\ldots,s\}$, and by Corollary 4.3, C_1 has depth spectrum $\{n,n-1,\ldots,n-k+s+1\}$.

Now, since both C_0 and C_1 have generator polynomials which are a multiple of $g(x)$, both C_0 and C_1 are subcodes of C. Hence, by Result 2.2, C has depth spectrum $\{1,2,\ldots,s\} \cup \{n,n-1,\ldots,n-k+s+1\}$.

The converse follows from the simple observation that, for any $g(x)$, there exists an s such that $(x-1)^s || (x^n-1)/g(x)$ □

5 Concluding remark

Many of the results concerning infinite sequences can probably be generalised to the ring of integers modulo c ($\mathbf{Z}_c$) for arbitrary c. Similarly, the results on finite sequences and codes are likely to be capable of generalisation to arbitrary finite fields GF(q).

Acknowledgements

The author would like to acknowledge the valuable comments and suggestions of T. Etzion, G.A. Kabatyanskii, K.G. Paterson, and two anonymous referees. Additionally, without the support of the EPSRC, under Grant Number GR/L07260, for Tuvi Etzion's visit to Royal Holloway during the summer of 1996, this paper would not have been written.

References

[1] T. Etzion, “The depth distribution — A new characterization for linear codes,” *IEEE Transactions on Information Theory*, vol. **43**, pp. 1361–1363, 1997.

[2] F. MacWilliams and N. Sloane, *The theory of error-correcting codes.* North-Holland, Amsterdam, 1977.

[3] R. Hamming, *Introduction to applied numerical analysis.* McGraw-Hill, New York, NY, 1971.

[4] S. Blackburn, T. Etzion, and K. Paterson, “Permutation polynomials, de Bruijn sequences and linear complexity,” *Journal of Combinatorial Theory (Series A)*, vol. **76**, pp. 55–82, 1996.