A Novel Method for Obtaining the Pattern of Low-Weight Codeword Components of Recursive Systematic Convolutional Codes

Bohulu Kwame Ackah and Chenggao Han
Graduate School of Informatics and Engineering,
The University of Electro-Communications,
1-5-1 Chofugaoka, Chofu-shi, Tokyo, 182–8585, Japan
Email: {bohulu, han.ic}@uec.ac.jp

Abstract

In this paper, we present a novel low-complexity method for determining the pattern of the low-weight codeword components of any RSC code as well as the distance spectrum. Using our method, we list the partial distance spectrum for selected RSC codes up to a cut-off weight $d_{\max}$ and compare the simulation results to the bounds obtained via our novel method and the transfer function method.

I. PRELIMINARIES

A polynomial in x, with degree M is an expression of the form

$$v(x) = \sum_{m=0}^{M} v_m x^m$$

where $v_m,\ 0 \leq m \leq M$, are called the *coefficients* and $v_m \neq 0$. If $v_M = 1,\ v(x)$ is called a *monic* polynomial. Moreover, the *Hamming weight* of $v(x)$, which is denoted by $w_H(v(x))$, is defined as the total number of non-zero coefficients. For two polynomials $v(x),\ \deg(v(x)) = M$ and $w(x),\ \deg(w(x)) = N$, the sum and product of $v(x)$ and $w(x)$ are defined as

$$v(x) + w(x) = \sum_{m=0}^{map\{M,N\}} (v_m + w_n)x^m$$

$$v(x)w(x) = \sum_{m=0}^{M+N} \sum_{i=0}^{m} (v_i w_{m-i})x^m$$

respectively.

For a prime number p, the Galois field with p elements, denoted as GF(p) is the set of integers $\{0, 1, p-1\}$ integers where addition and multiplication of 2 elements are carried out modulo-p. If the coefficients $v_m, 0 \leq m \leq M$ are elements of GF(p), $v(x)$ is called a polynomial over GF(p). Let $v(x)$ and $w(x)$ are both polynomials over GF(p), $w(x) \neq 0$. Then there exists polynomials $q(x)$ and $r(x)$ over GF(p) such that $v(x) = w(x)q(x) + r(x)$ and $r(x) = 0$ or deg $r(x) <$ deg $w(x)$. $q(x)$ and $r(x)$ are called the *quotient polynomial* and *remainder polynomials*, respectively of the division of $v(x)$ by $w(x)$.

A monic polynomial which cannot be factorised into lower degree polynomials over GF(p) is called a *prime polynomial*. Let $v(x)$ be a prime polynomial with degree $M > 1$. Then, we can define a set of p^M polynomials with degree less than M over GF(p). If within this set, addition and multiplication operations are carried out modulo-$v(x)$ over GF(p), we obtain what is called an *extension field* of GF(p), which is denoted by GF(p^M). Addition and multiplication modulo-$v(x)$ over GF(p) means all addition and multiplication operations on the polynomials and their coefficients are carried out modulo-$v(x)$ and modulo-p respectively, and to perform multiplication modulo-$v(x)$, means to divide the polynomial product by $v(x)$ and find the remainder polynomial.

Elements in GF(p^M) can be represented by a power notation, *i.e.* $X^m,\ 0 \leq m \leq p^M - 1$, where X^2 may be used in place of $1+x$, for example. Through out this paper, the power notation

will be used more often for the sake of convenience, with the appropriate conversion between the power and polynomial notation made known where necessary.

Let X be a non-zero element of GF(p^M).Then, ϵ denotes the *order* of X, and is defined as the least positive integer value such that $X^\epsilon = 1$, and X is called a *primitive element* iff $\epsilon = p^M - 1$. Let $v(x)$ be a prime polynomial with degree M. If $v(x)$ generates GF(p^M) such that X is a primitive element in GF(p^M), then $v(x)$ is called a *primitive polynomial*.

Finally, the root of $v(x)$, denoted by β, is any non-zero element in GF(p^M) such that $v(\beta) = 0$. The order of β is defined similarly to that of X and is also denoted by ϵ, and if $\beta^\epsilon = 1$, then all $\beta^i,\ 0 \leq i \leq \epsilon - 1$ are distinct. If $v(x)$ is a primitive polynomial, then β is a primitive element, *i.e.* $\epsilon = p^M - 1$, otherwise $\epsilon < p^M - 1,\ \epsilon | p^M - 1$.

Example 1. $f(x) = 1 + x + x^2$.

Weight-2 PCs: For this case, since $x^1 = x$, $x^2 \equiv 1 + x$, and $x^3 \equiv 1 \bmod f(x)$, the order of the root β_0 is $\epsilon_0 = 3$ and a should be a multiple of 3. The corresponding values for $a(x)$ and $h(x)$ are shown in Table I for the first four valid values of a.

TABLE I: $f(x) = 1 + x + x^2$

$a(x)$	$h(x)$
$1 + x$	$1 + x^3$
$1 + x + x^3 + x^4$	$1 + x^6$
$1 + x + x^3 + x^4 + x^6 + x^7$	$1 + x^9$
$1 + x + x^3 + x^4 + x^6 + x^7 + x^9 + x^{10}$	$1 + x^{12}$

We may write the weight-2 PCs in general form as $h(x) = 1+x^{3\ell},\ \ell > 1$ and the corresponding $a(x)$ is given by

$$a(x) = \sum_{\ell=0}^{L-1} x^{3\ell}(1 + x)$$

Weight-3 PCs: The elements of GF(2^2) are shown in Table II and it is obvious that $\mathcal{Z} = \{(1, 2)\}$. This means that $(a, b) \in \{3\ell + 1,\ 3n + 2\},\ l = n = \{0, 1, ...\}$. The corresponding values for $a(x)$ and $h(x)$ are shown in Table X below for the first four valid values of (a, b).

TABLE II: Non-zero Elements of GF(2^2) generated by $f(x) = 1 + x + x^2$

power representation	actual value
$X^0 = X^3 = 1$	1
X	x
X^2	$1 + x$

We may write the weight-3 PCs in general form as $h(x) = 1 + x^{3\ell+1} + x^{3n+2},\ \ell,\ n \geq 0$

Example 2. $f(x) = 1 + x + x^2 + x^3 + x^4$

Weight-2 PCs: We can confirm that the order of β_0 is $\epsilon_0 = 5$. This means that a should be a multiple of 5. The corresponding values for $a(x)$ and $h(x)$ are shown in Table IV with general forms for $\ell > 1$

TABLE III: $f(x) = 1 + x + x^2$

$a(x)$	$h(x)$
1	$1 + x + x^2$
$1 + x + x^2$	$1 + x^2 + x^4$
$1 + x + x^3$	$1 + x^4 + x^5$
$1 + x^2 + x^3$	$1 + x + x^5$

TABLE IV: $f(x) = 1 + x + x^2 + x^3 + x^4$

$a(x) = \sum_{\ell=0}^{L-1} x^{5\ell}(1 + x)$	$h(x) = 1 + x^{5\ell}$
$1 + x$	$1 + x^5$
$1 + x + x^5 + x^6$	$1 + x^{10}$
$1 + x + x^5 + x^6 + x^{10} + x^{11}$	$1 + x^{15}$
$1 + x + x^5 + x^6 + x^{10} + x^{11} + x^{15} + x^{16}$	$1 + x^{20}$

Weight-3 PCs: We refer to Table V and it is obvious that $\mathcal{Z} = \{\}$ and therefore, there are no weight-3 PCs for $f(x)$

TABLE V: Non-zero Elements of GF(2^4) generated by $f(x) = 1 + x + x^2 + x^3 + x^4$

power representation	actual value
$X^0 = X^5 = X^{10} = X^{15}$	1
$X = X^6 = X^{11}$	x
$X^2 = X^7 = X^{12}$	x^2
$X^3 = X^8 = X^{13}$	x^3
$X^4 = X^9 = X^{14}$	$1 + x + x^2 + x^3$

Example 3. $f(x) = 1 + x^2$

Weight-2 PCs: Since

$$f(x) = (1 + x)^2$$

and the order of the root $\beta_0 = 1$ is $\epsilon_0 = 1$, we obtain from (**??**) and (**??**)

$$(\beta_0)^a = 1 \tag{1}$$

$$a(\beta_0)^{(a-1)} = 0 \tag{2}$$

Although (1) indicates a can be any positive integer, we can see from (2) that a should be an even number. The corresponding values for $a(x)$ and $h(x)$ are shown in Table VI with general forms for $\ell > 1$.

TABLE VI: $f(x) = 1 + x^2$

$a(x) = \sum_{\ell=0}^{L-1} x^{2\ell}$	$h(x) = 1 + x^{2\ell}$
1	$1 + x^2$
$1 + x^2$	$1 + x^4$
$1 + x^2 + x^4$	$1 + x^6$
$1 + x^2 + x^4 + x^6$	$1 + x^8$

Weight-3 PCs: Given that there is a single non-zero element in GF(2) which is generated by $1 + x$ we can conclude that there are no weight-3 PCs associated with $f(x)$.

Example 4. $f(x) = 1 + x^2 + x^3 + x^4 + x^6$

Weight-2 PCs: $f(x)$ can be written as

$$f(x) = \prod_{k=0}^{1} f_k(x)$$

where

$$f_0(x) = 1 + x + x^2, \;\; f_1(x) = 1 + x + x^2 + x^3 + x^4$$

From Example 1 and Example 2, we know that $a_0 = 3$ and $a_1 = 5$. Hence, valid values of a should be a multiple of the least common multiples of a_0 and a_1, which means a should be a multiple of 15. The corresponding values for $a(x)$ and $h(x)$ are shown in Table VIII with general forms for $\ell > 1$.

Weight-3 PCs: From Example 1 and Example 2, we have $\mathcal{Z}_0 = \{(1, 2)\}$ and $\mathcal{Z}_1 = \{\}$. Therefore $\mathcal{Z}_0 \bigcap \mathcal{Z}_1 = \{\}$ and therefore there are no weight-3 PCs associated with $f(x)$.

TABLE VII: $f(x) = 1 + x^2 + x^3 + x^4 + x^6$

$a(x) = \sum_{\ell=0}^{L-1} x^{15\ell}(1 + x^2 + x^3 + x^6 + x^7 + x^9)$	$h(x) = 1 + x^{15\ell}$
$1 + x^2 + x^3 + x^6 + x^7 + x^9$	$1 + x^{15}$
$1 + x^2 + x^3 + x^6 + x^7 + x^9 + x^{15} + x^{17} + x^{18} + x^{21} + x^{22} + x^{24}$	$1 + x^{30}$

Example 5. $f(x) = 1 + x + x^5$

Weight-2 PCs: $f(x)$ can be written as

$$f(x) = \prod_{k=0}^{1} f_k(x)$$

where

$$f_0(x) = 1 + x + x^2,\ f_1(x) = 1 + x^2 + x^3$$

From Example 1, we know that $a_0 = 3$ and it can be confirmed that $a_1 = 7$. Hence, valid values of a should be a multiple of the least common multiples of a_0 and a_1, which means a should be a multiple of 21. The corresponding values for $a(x)$ and $h(x)$ are shown in Table VIII with general forms for $\ell > 1$.

TABLE VIII: $f(x) = 1 + x + x^5$

$a(x) = \sum_{\ell=0}^{L-1} x^{21\ell}(1 + x^2 + x^3 + x^4 + x^6 + x^8 + x^4 + x^6 + x^8 + x^{11} + x^{12} + x^{16})$	$h(x) = 1 + x^{21\ell}$
$1 + x^2 + x^3 + x^4 + x^6 + x^8 + x^4 + x^6 + x^8 + x^{11} + x^{12} + x^{16}$	$1 + x^{21}$

Weight-3 PCs: From Example 1, we have $\mathcal{Z}_0 = \{(1, 2)\}$ with $\mathcal{AB}_0 = \{(3\ell+1,\ 3n+2)\},\ \ell = n = \{0, 1, ...\}$ and from Table IX, $\mathcal{Z}_1 = \{(1, 5),\ (2, 3),\ (4, 6)\}$, with $\mathcal{AB}_1 = \{(7\ell + 1,\ 7n + 5),\ (7\ell + 2,\ 7n + 3),\ (7\ell + 4,\ 7n + 6)\},\ \ell = n = \{0, 1, ...\}$. Therefore $(a, b) \in \mathcal{AB}_0 \bigcap \mathcal{AB}_1$.

The corresponding values for $a(x)$ and $h(x)$ are shown in Table X below for the first three valid values of (a, b).

TABLE IX: Non-zero Elements of GF(2^3) generated by $1 + x^2 + x^3$

power representation	actual value
$X^0 = X^7$	1
X	x
X^2	x^2
X^3	$1 + x^2$
X^4	$1 + x + x^2$
X^5	$1 + x$
X^6	$x + x^2$

TABLE X: $f(x) = 1 + x + x^5$

$a(x)$	$h(x)$
1	$1 + x + x^5$
$1 + x + x^5$	$1 + x^2 + x^{10}$
$1 + x + x^2 + x^3 + x^4 + x^6 + x^8$	$1 + x^{11} + x^{13}$