Quasi-Cyclic Dyadic Codes in the Walsh–Hadamard Transform Domain

B. Sundar Rajan, *Senior Member, IEEE,* and
Moon Ho Lee, *Senior Member, IEEE*

***Abstract*—A code is s-quasi-cyclic (s-QC) if there is an integer s such that cyclic shift of a codeword by s-positions is also a codeword. For $s = 1$, cyclic codes are obtained. A dyadic code is a code which is closed under all dyadic shifts. An s-QC dyadic (s-QCD) code is one which is both s-QC and dyadic. QCD codes with $s = 1$ give codes that are cyclic and dyadic (CD). In this correspondence, we obtain a simple characterization of all QCD codes (hence of CD codes) over any field of odd characteristic using Walsh–Hadamard transform defined over that finite field. Also, it is shown that dual a code of an s-QCD code is also an s-QCD code and s-QCD codes for a given dimension are enumerated for all possible values of s.**

***Index Terms*—Discrete Fourier transform (DFT), dyadic codes, quasi-cyclic (QC) codes, Walsh–Hadamard transform (WHT).**

I. Introduction

An s-quasi-cyclic (s-QC) code is a code with the property that cyclic shift of any codeword by s positions gives another codeword. Cyclic codes are 1-QC codes. The class of QC codes contains asymptotically good codes in the sense of meeting a version of Varshamov–Gilbert bound [1] and includes several well-known codes [2].

Dyadic codes are defined only for length n, a power of 2, say $n = 2^r$, as follows. For any integer $i \in \{0, 1, \ldots, 2^r - 1\}$, let

$$\lceil i \rceil = \lceil i_{r-1}, i_{r-2}, \ldots, i_1, i_0 \rceil$$

denote its radix-2 representation, where

$$i = i_{r-1}2^{r-1} + i_{r-2}2^{r-2} + \cdots + i_1 2 + i_0$$

and $i_j = 0, 1$ for $j = 0, 1, \ldots, r-1$. Radix-2 addition of two numbers i and j denoted by $i \oplus j$ or $\lceil i \rceil \oplus \lceil j \rceil$ is defined by

$$i \oplus j = \lceil i \rceil \oplus \lceil j \rceil = \lceil k \rceil$$

where $k_l = (i_l + j_l) \bmod 2$, for $l = 0, 1 \ldots, r-1$. The m-dyadic shift, $m = 0, 1, \ldots, n-1$, of a vector $(a_0, a_1, \ldots, a_{n-1})$ is the vector

$$(a_{0\oplus m}, a_{1\oplus m}, \ldots, a_{(n-1)\oplus m})$$

[3], [4].

Definition 1: We call a linear code of length $n = 2^r$ over a field a *dyadic code* if the m-dyadic shift of every codeword is also a codeword for all $m = 0, 1, \ldots, n-1$.

The class of dyadic codes is a special case of the class of Abelian group codes [5]–[8], which is briefly discussed in the next section. A linear cyclic code has the additional structure of being closed under all cyclic shifts apart from linearity. Similarly, a dyadic code has the additional structure of being closed under all dyadic shifts in addition to the linearity of the code.

Definition 2: We define a dyadic code of length $n = 2^r$ to be a *quasi-cyclic dyadic (QCD) code* if there is an integer t such that every cyclic shift of a codeword by t places is also a codeword. If t is the smallest such integer, say $t = 2^s$ for some $s = 0, 1, \ldots, r-1$, we call the code a 2^s-QCD code. A 2^0-QCD code will be referred as a *cyclic-dyadic (CD) code*.

Example 1: Consider the following ternary length-4 code $\mathcal{C}_0$ with nine codewords:

$$\mathcal{C}_0 = \{(0000), (1122), (2211), (1212), (2001), (0120), (2121), (0210), (1002)\}.$$

By inspection, $\mathcal{C}_0$ is closed under all dyadic shifts but not closed under cyclic shift, whereas codes $\mathcal{C}_3$ and $\mathcal{C}_4$ in Table II are codes with identical parameters and are closed under all dyadic shifts as well as cyclic shifts. That is, $\mathcal{C}_0$ is a dyadic code whereas $\mathcal{C}_3$ and $\mathcal{C}_4$ are CD codes.

The transform domain characterization of cyclic codes over a finite field is given in terms of the discrete Fourier transform (DFT) defined over an extension of that field [9]. Extension of this transform domain characterization to the general class of Abelian codes [8] and to cyclic codes over integer residue rings have been studied [10], [11]. The transform domain description of codes is useful for encoding and decoding [9], [12]. The DFT approach for cyclic codes of arbitrary length is discussed in [13] and for repeated-root cyclic codes [14], [15] in [16]. QC codes over finite fields have been studied using a slightly modified version of DFT by Tanner [17].

In this correspondence, we characterize all QCD codes (hence CD codes) in the Walsh–Hadamard transform (WHT) domain. Our characterization does not need extension of the field. Notice that if a cyclic code over F_q of length n is to be described in the transform domain using the DFT then it is necessary that the DFT is defined in the extension field F_{q^m}, where m is the least integer such that n divides $q^m - 1$. Similarly, the DFT domain study of QC codes by Tanner is also carried out using an extension field. The main result of this correspondence is that if such a QC code is dyadic as well, i.e., if the code is QCD, then using the WHT it can be described without field extension. As a special case, CD codes also get described using the WHT without field extension. Since algebraic decoding generally takes place in the extension field, such an approach may lead to simpler/more efficient decoding.

The content of this correspondence is organized as follows. In Section II, we review the well-known DFT characterization of cyclic codes, briefly discuss dyadic codes as a special case of Abelian codes, and the WHT as a special case of the generalized DFT, used in [8] to study Abelian codes, and present the WHT domain characterization of dyadic codes. In Section III, we present the main result which is a transform domain characterization of QCD codes using the WHT and discuss several examples. Using this characterization, in Section IV, we discuss dual codes of QCD codes and carry out enumeration of QCD codes of all possible dimensions. Section V consists of a summary of the results and concluding remarks.

II. Transform Domain Characterization of Dyadic Codes

We start by describing the well-known transform domain characterization of cyclic codes. Let $\vec{a} = (a_0, a_1, \ldots, a_{n-1}) \in F_q^n$, where $(n, q) = 1$. Also let r be the smallest positive integer such that $n|(q^r -$

Manuscript received May 23, 2000; revised January 24, 2002. The work of B. S. Rajan was supported in part by CSIR, India, under Research Grant (22(0298)/99/EMR-II).

B. S. Rajan is with the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore 560 012, India (e-mail: bsrajan@ece.iisc.ernet.in).

M. H. Lee is with the Institute of Information and Communication, Chonbuk National University, Chonju 561-756, Korea (e-mail: moonho@moak.chonbuk.ac.kr).

Communicated by R. M. Roth, Associate Editor for Coding Theory.
Publisher Item Identifier 10.1109/TIT.2002.800475.

1) and $\alpha \in F_{q^r}$ be an element of multiplicative order n. The DFT of $\vec{a}$ is defined to be $\vec{A} = (A_0, A_1, \ldots, A_{n-1}) \in F_{q^r}^n$, where

$$A_j = \sum_{i=0}^{n-1} \alpha^{ij} a_i, \qquad j = 0, 1, \ldots, n-1. \tag{1}$$

A_j is called the jth DFT coefficient or the jth transform component of $\vec{a}$. The following restriction on the values of DFT coefficients holds:

$$A_{qj \bmod n} = A_j^q.$$

This constraint implies $A_j \in F_{q^{r_j}} \subset F_{q^r}$, where r_j is the smallest positive integer such that $jq^{r_j} \equiv j \bmod n$. So, the set of transform components $\{A_j, A_{qj}, A_{q^2 j}, \ldots, A_{q^{(r_j-1)}j}\}$ are related.

Let $\mathcal{C} \subseteq F_q^n$ be a code of length n over F_q. We say, A_j takes values from

$$\left\{ \sum_{i=0}^{n-1} \alpha^{ij} a_i | \vec{a} \in \mathcal{C} \right\} \subseteq F_{q^r}.$$

For any $j \in [0, n-1]$, the *cyclotomic coset modulo* n of j is defined as $[j]_n^q = \{i \in [0, n-1] | j \equiv iq^t \bmod n$ for some nonnegative integer $t\}$. Notice that the conjugacy constraint relates only the components of the transform vector indexed by elements of the same q-cyclotomic coset. Now, the extensively studied linear cyclic codes over F_q are characterized in the transform domain as follows.

- A cyclic code is the set of inverse DFT vectors of all the vectors of an F_q-subspace of DFT $(F_q^n) \subset F_{q^r}^n$, in which transform components in $[j]_n^q$, $j = 0, 1, \ldots, n-1$, either take only the zero value or all the values of $F_{q^{r_j}}$, and transform components in disjoint $[j_1]_n^q$ and $[j_2]_n^q$ take values independently.

From the above characterization, it is clear that to specify a cyclic code, it is sufficient to specify the set of cyclotomic cosets in which the transform components of all the codewords is zero.

It is important to notice that this characterization demands extension of the field (unless $n = q-1$) over which the code is defined and this is also true for the case of QC codes [17]. Now we proceed to present similar characterization for dyadic codes viewing them as a special case of Abelian group codes.

Let G be an Abelian group of order n and F_q the finite field with q elements. The group algebra of G over F_q, denoted by F_qG, is the set

$$F_qG = \left\{ \sum_{g \in G} a_g g | a_g \in F_q \right\}$$

with addition and multiplication operations, defined by

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$$

and

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{h \in G} b_h h \right) = \sum_{k \in G} c_k k \tag{2}$$

where $c_k = \sum_{gh=k} (a_g b_h)$.

There is a natural 1–1 correspondence between F_q^n, the set of n-tuples over F_q, and F_qG. The subsets of F_q^n that correspond to ideals of F_qG are called Abelian codes [5]–[7]. It is easily seen that when G is a cyclic group, the multiplication in F_qG given by (2) represents the cyclic convolution of two length n vectors over F_q and ideals of F_qG are cyclic codes. For general Abelian groups, the multiplication given by (2) represents a generalized convolution determined by the structure of the Abelian group and accordingly Abelian codes over F_q are linear codes with the property that the set of codewords is closed under this generalized convolution. When the group G is an elementary Abelian group which is a direct product of r cyclic groups each of order 2, the resulting convolution is the dyadic convolution and the corresponding Abelian codes are precisely the dyadic codes given in Definition 1. To be explicit, the dyadic convolution of two length-n vectors $\vec{a} = (a_0, a_1, \ldots, a_{n-1})$ and $\vec{b} = (b_0, b_1, \ldots, b_{n-1})$ is the vector $\vec{c} = (c_0, c_1, \ldots, c_{n-1})$ given by

$$c_k = \sum_{i,\, j;\, i \oplus j = k} a_i b_j = \sum_{i=0}^{n-1} a_i b_{i \oplus k}, \qquad k = 0, 1, \ldots, n-1.$$

In terms of dyadic convolution, dyadic codes can be defined as linear codes with the property that dyadic convolution of a codeword with an arbitrary vector results in another codeword.

The well-known WHT [3], [4] transforms a length n real vector $(a_0, a_1, \ldots, a_{n-1})$ to another length n real vector $(A_0, A_1, \ldots, A_{n-1})$, and is given by

$$A_j = \sum_{i=0}^{n-1} (-1)^{\langle j, i \rangle} a_i, \qquad j = 0, 1, \ldots, n-1$$

where the modulo-2 inner product $\langle j, i \rangle$ is given by

$$\langle j, i \rangle = j_{r-1} i_{r-1} + j_{r-2} i_{r-2} + \cdots + j_0 i_0 \pmod 2. \tag{3}$$

The transform kernel -1 is an element of order 2 in the complex and real field, and in our case, since we will be working with vectors over a field F_q of characteristic p, an odd prime, the element $p-1$ in the field is an element of order 2, and can be used as the transform kernel. We will continue to use -1 to denote an element of order 2 in F_q.

Definition 3 (WHT): Let $\vec{a} = (a_0, a_1, \ldots, a_{n-1})$ be a length-n vector over F_q, a field with odd characteristic p, and $n = 2^r$. The WHT of $\vec{a}$ is defined to be the length-n vector $\vec{A} = (A_0, A_1, \ldots, A_{n-1})$ over F_q, given by

$$A_j = \sum_{i=0}^{n-1} (-1)^{\langle j, i \rangle} a_i, \qquad j = 0, 1, \ldots, n-1 \tag{4}$$

where $\langle j, i \rangle$ is given by (3). A_j will be referred to as the jth transform component or the jth spectral component of $\vec{a}$.

It can be easily verified that the inverse transform is given by

$$a_i = \frac{1}{(n \bmod p)} \sum_{j=0}^{n-1} (-1)^{\langle j, i \rangle} A_j, \qquad i = 0, 1, \ldots, n-1.$$

Notice that since p is an odd prime and n is a power of 2, n cannot be zero modulo p and since every nonzero element is invertible in a field, the inverse transform exists. This is the reason for restricting our discussion to codes over fields with odd characteristic.

The WHT given in Definition 3 is a special case of the generalized DFT given in [8] and consequently the following properties hold.

Convolution Property: The WHT defined over F_q given by (4) establishes an algebra isomorphism of F_q^n to itself where addition operation is mapped onto addition and dyadic convolution is mapped onto point-wise product, i.e., if $\vec{a}$, $\vec{b}$, and $\vec{c}$ are n-tuples over F_q such that

$$c_i = \sum_{k=0}^{n-1} a_{i \oplus k} b_k, \qquad i = 0, 1, \ldots, n-1$$

then their WHT coefficients satisfy the relation $C_j = A_j B_j$, $j = 0, 1, \ldots, n-1$.

Conjugate Symmetry Property: From the conjugate symmetry property of the generalized DFT proved in [8] there is no extension of the field required for (4) and, consequently, all transform components are independent. Combining this observation with [8, Theorem 1 and Definition 2] gives the following theorem.

Theorem 1: Let $\mathcal{C}$ be a length-$n = 2^r$ linear code over F_q where q is a power of an odd prime p and for $i \in \{0, 1, \ldots, n-1\}$, let $\boldsymbol{C}_i$ denote the set of values taken by the ith WHT component of all the codewords of $\mathcal{C}$. If $\boldsymbol{C}_i = 0$ for all $i \in \boldsymbol{Z}$, a subset of $\{0, 1, \ldots, n-1\}$ and $\boldsymbol{C}_i = F_q$ for all $i \notin \boldsymbol{Z}$ with values from F_q taken independently then $\mathcal{C}$ is dyadic and, conversely, for every linear dyadic code there is a set $\boldsymbol{Z} \subset \{0, 1, \ldots, n-1\}$ such that $\boldsymbol{C}_i = 0$ for all $i \in \boldsymbol{Z}$ and for all other values of $i \notin \boldsymbol{Z}$, $\boldsymbol{C}_i = F_q$ with values from F_q taken independently.

Notice that in Theorem 1, if $\mathcal{C}$ is dyadic, then it is completely characterized by the subset $\boldsymbol{Z}$ of $\{0, 1, \ldots, n-1\}$. Henceforth, we will refer to this subset as *the defining set of* $\mathcal{C}$.

Remark 1: It is important to notice the term *independently* in Theorem 1 as well as in the transform domain characterization of cyclic codes (bullet) in Section II. This essentially means that if A_i and A_j are two spectral components taking all values from F_q then for every particular value for A_i, say $A_i = x$, the set of values A_j takes is the entire F_q. In other words, the value taken by A_i does not determine the value taken by A_j and *vice versa*. Recently, it has been shown that if two nonzero spectral components are related (do not take values independently) say, by $A_j = \sigma(A_i)$ where σ is an appropriate map that determines the relation, then the code is not cyclic and can be a QC or a group code depending upon the map σ [18].

From Theorem 1 it follows that corresponding to every subset of $\{0, 1, \ldots, n-1\}$ there is a dyadic code with that subset as the defining set of the code. Hence we have the following corollary.

Corollary 1: Including the two trivial codes (F_q^n and the all-zero codeword) there are 2^{2^r} dyadic codes of length 2^r.

The main result of this correspondence (Theorem 4) and Theorem 6 answer the following question:

- Among these 2^{2^r} dyadic codes how many are 2^s-QC, and how can they by recognized (characterized) for every $s = 0, 1, \ldots, r-1$?

III. QCD Codes in the WHT Domain

In this section, we present the main result of this correspondence which gives the constraints among the spectral components to be satisfied for a dyadic code to be a 2^s-QCD code.

Definition 4: For a vector $\vec{a}$, $\vec{a}^{(l)}$ will denote the 2^l-cyclic shifted version of $\vec{a}$ and the corresponding WHT vector will be denoted by $\vec{A}^{(l)}$.

Definition 5: A *constraint* $\mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_2 \cup \cdots \cup \mathcal{D}_l$ is a partition of $\{0, 1, \ldots, n-1\}$. If $i \in \mathcal{D}_j$ and $|\mathcal{D}_j| = 1$, then i is called a free spectral component. If not, it is said to be a constrained spectral component. The spectral components belonging to $\mathcal{D}_j$, $j = 1, 2, \ldots, l$, are said to form a constrained set of spectral components. Let $\mathcal{C}$ be a length-$n = 2^r$ linear code over F_q where q is a power of an odd prime p and for $i \in \{0, 1, \ldots, n-1\}$, let $\boldsymbol{C}_i$ denote the set of values taken by the ith WHT component of all the codewords of $\mathcal{C}$. The code $\mathcal{C}$ *is said to satisfy the constraint* $\mathcal{D}$ if $\boldsymbol{C}_{i_1} = \boldsymbol{C}_{i_2}$ whenever $i_1, i_2 \in \mathcal{D}_j$ for some $1 \le j \le l$. Equivalently, $\mathcal{C}$ *is said to satisfy the constraint* $\mathcal{D}$ if its defining set is a union of some $\mathcal{D}_j$.

Remark 2: It is important to notice that the above definition means that if two spectral components, say i_1 and i_2 are in a constrained set then either $\boldsymbol{C}_{i_1} = \boldsymbol{C}_{i_2} = 0$ or $\boldsymbol{C}_{i_1} = \boldsymbol{C}_{i_2} = F_q$ and it does not mean that they are related as mentioned in Remark 1.

Definition 6: For every $j = [j_{r-1}, j_{r-2}, \ldots, j_0]$ and $0 \le s \le r-2$

$$[j_{r-1}, j_{r-2}, \ldots, j_{s+1}, j_s \oplus j_{s+1}, j_{s-1}, j_{s-2}, \ldots, j_0]$$

will be denoted by $j^{(s)}$.

Note that $j^{(s)}$ is equal to j if j_{s+1} is zero, otherwise, $j^{(s)}$ and j differ by 2^s: if $j_s = 0$, then $j^{(s)} - j = 2^s$ and if $j_s = 1$, then $j - j^{(s)} = 2^s$. Also observe that $(j^{(s)})^{(s)} = j$.

Theorem 2: All length $n = 2^r$ dyadic codes are 2^{r-1}-QCD codes.

Proof: This follows from the fact that cyclic shift of a codeword by 2^{r-1} positions is the same as the 2^{r-1}-dyadic shift of the codeword and a dyadic code is closed under all dyadic shifts. □

Next, we consider the case $s = r-2$. This can be made part of Theorem 4, but we discuss it separately so that the idea in the main theorem leading to a certain constrained set (Definition 7) of spectral components characterizing 2^s-QCD codes can be seen without notational complications. Furthermore, this case will be used as the induction base in the main theorem.

Theorem 3: A length-$n = 2^r$ dyadic code is 2^{r-2}-QCD, if it satisfies the constraint

$$\mathcal{D} = \bigcup_{j=0}^{2^{r-1}-1} \{j\} \bigcup_{(j_{r-3}, j_{r-4}, \ldots, j_0)} \{[1, x, j_{r-3}, \ldots, j_0] | x = 0, 1\}.$$

In other words, j is free for $0 \le j \le 2^{r-1} - 1$ and for all $2^{r-1} \le j \le 2^r - 1$, any two spectral components differing only in j_{r-2} form a constrained set of spectral components.

Proof: For any codeword $\vec{a}$ we have

$$\begin{aligned}
A_j^{(2^{r-2})} &= \sum_{i=0}^{n-1} (-1)^{\langle j, i \rangle} a_i^{(2^{r-2})} \\
&= \sum_{i=0}^{n-1} (-1)^{\langle j, i \rangle} a_{i-2^{r-2}} \\
&= \sum_{i=0}^{n-1} (-1)^{\langle j, i+2^{r-2} \rangle} a_i \\
&= \sum_{i=0}^{n-1} (-1)^{j_{r-1}(i_{r-1} \oplus i_{r-2}) \oplus j_{r-2}(i_{r-2} \oplus 1) \bigoplus_{l=r-3}^{0} j_l i_l} a_i \\
&= (-1)^{j_{r-2}} \sum_{i=0}^{n-1} (-1)^{j_{r-1} i_{r-1} \oplus (j_{r-1} \oplus j_{r-2}) i_{r-2} \bigoplus_{l=r-3}^{0} j_l i_l} a_i \\
&= (-1)^{j_{r-2}} A_{j^{(r-2)}}. \qquad (5)
\end{aligned}$$

From (5), it follows that A_j and $A_{j^{(r-2)}}$ do not differ if j_{r-1} is zero, in which case, j is a free spectral component, and if j_{r-1} is 1 then they differ only in j_{r-2}, in which case j and $j^{(r-2)}$ form a constrained set of spectral components. □

To extend Theorem 3 to cases $s \le r-3$, we generalize the constrained set $\{[1, x, j_{r-3}, \ldots, j_0] | x = 0, 1\}$ of Theorem 3 as follows.

Definition 7: For a given s, $0 \le s \le r-2$, for every μ, $(s+1 \le \mu \le r-1)$, and a fixed $(j_{s-1}, j_{s-2}, \ldots, j_0)$, the set of $2^{\mu-s}$ spectral components consisting of those j's where

$$j = [0, 0, \ldots, 0, 1 = j_\mu, j_{\mu-1}, j_{\mu-2}, \ldots, j_{s+1}, j_s, j_{s-1}, \ldots, j_0]$$

is denoted by $J(\mu, s, j_{s-1}, j_{s-2}, \ldots, j_0)$.

Example 2: For each $r = 2, 3$, and 4 corresponding to each $s = 0, 1, \ldots, r-1$, the sets $J(\mu, s, j_{s-1}, \ldots, j_0)$ for all possible values of μ are shown in Table I. The set of j's for which the entry is the same letter among $A, B, C, \ldots$ form one such set.

The main result of this correspondence follows.

TABLE I
CONSTRAINED SETS OF SPECTRAL COMPONENTS FOR $n = 2^r$, $r = 2, 3$, AND 4 CORRESPONDING TO EXAMPLE 2

Constrained sets of spectral components for $n = 2^2$.

$j \rightarrow$	$< 00 >$	$< 01 >$	$< 10 >$	$< 11 >$
$s = 0$	A	B	C	C
$s = 1$	A	B	C	D

Constrained sets of spectral components for $n = 2^3$.

$j \rightarrow$	$< 000 >$	$< 001 >$	$< 010 >$	$< 011 >$	$< 100 >$	$< 101 >$	$< 110 >$	$< 111 >$
$s = 0$	A	B	C	C	D	D	D	D
$s = 1$	A	B	C	D	E	F	E	F
$s = 2$	A	B	C	D	E	F	G	H

Constrained sets of spectral components for $n = 2^4$.

$j \rightarrow$	$< 0000 >$	$< 0001 >$	$< 0010 >$	$< 0011 >$	$< 0100 >$	$< 0101 >$	$< 0110 >$	$< 0111 >$	$< 1000 >$	$< 1001 >$	$< 1010 >$	$< 1011 >$	$< 1100 >$	$< 1101 >$	$< 1110 >$	$< 1111 >$
$s = 0$	A	B	C	C	D	D	D	D	E	E	E	E	E	E	E	E
$s = 1$	A	B	C	D	E	F	E	F	G	H	G	H	G	H	G	H
$s = 2$	A	B	C	D	E	F	G	H	I	J	K	L	I	J	K	L
$s = 3$	A	B	C	D	E	F	G	H	I	J	K	L	M	M	O	P

Theorem 4: A dyadic code $\mathcal{C}$ of length $n = 2^r$ is 2^s-QCD, $0 \leq s < r - 2$, if it satisfies the constraint

$$\mathcal{D} = \bigcup_{j=0}^{2^{s+1}-1} \{j\} \bigcup_{(j_{s-1}, j_{s-2}, \ldots, j_0)} \bigcup_{\mu=s+1}^{r-1} J(\mu, s, j_{s-1}, j_{s-2}, \ldots, j_0).$$

In other words, $\mathcal{C}$ is 2^s-QCD, if

i) for all $0 \leq j \leq 2^{s+1} - 1$, the spectral component j is free;

ii) among all $j \geq 2^{s+1}$, every $J(\mu, s, j_{s-1}, j_{s-2}, \ldots, j_0)$ forms a constrained set of spectral components.

Proof for the "Only if" Part: Let $\mathcal{C}$ be a 2^s-QCD code and $\vec{a} = (a_0, a_1, \ldots a_{n-1}) \in \mathcal{C}$. Then, we have $A_j^{(s)}$ given by (6) displayed at the bottom of this page. If $0 \leq j \leq 2^{s+1} - 1$, we have $j_{r-1} = j_{r-2} = \cdots = j_{s+1} = 0$, and (6) becomes

$$A_j^{(s)} = (-1)^{j_s} \sum_{i=0}^{n-1} (-1)^{\langle j, i \rangle} a_i = (-1)^{j_s} A_j.$$

The preceding equation implies that for all j, $0 \leq j \leq 2^{s+1} - 1$ the spectral component j is free. This proves condition i).

For $2^{s+1} \leq j \leq 2^r - 1$, we continue with (6) and obtain (7) and (8) also displayed at the bottom of this page.

Note that in (8), D depends only on $j_{r-1}, j_{r-2}, \ldots, j_{s+2}$ among all the components of j.

Let μ be the largest integer, $s + 1 \leq \mu \leq r - 1$, such that $j_\mu = 1$; that is, $j_{r-1} = j_{r-2} = \cdots = j_{\mu+1} = 0$. Then, after a few manipulations, (7) reduces to (9) and (8) reduces to (10), both displayed at the bottom of this page. Equation (9) shows that $A_j^{(s)}$ is related to $A_{j^{(s)}}$

$$\begin{aligned} A_j^{(s)} &= \sum_{i=0}^{n-1} (-1)^{\langle j, i \rangle} a_{i-2^s} = \sum_{i=0}^{n-1} (-1)^{\langle j, i+2^s \rangle} a_i \\ &= \sum_{i=0}^{n-1} (-1)^{j_{r-1}(i_{r-1} \oplus \prod_{\lambda=s}^{r-2} i_\lambda) \oplus \cdots \oplus j_{s+2}(i_{s+2} \oplus \prod_{\lambda=s}^{s+1} i_\lambda) \oplus j_{s+1}(i_{s+1} \oplus i_s) \oplus j_s(i_s \oplus 1) \oplus j_{s-1} i_{s-1} \oplus \cdots \oplus j_0 i_0} a_i. \end{aligned} \tag{6}$$

$$\begin{aligned} A_j^{(s)} &= (-1)^{j_s} \sum_{i=0;\, i_{s+1} i_s \neq 1}^{n-1} (-1)^{\langle j^{(s)}, i \rangle} a_i + (-1)^{j_s} \sum_{i=0;\, i_{s+1} i_s = 1}^{n-1} (-1)^{\langle j^{(s)}, i \rangle} (-1)^D a_i \\ &= (-1)^{j_s} A_{j^{(s)}} + (-1)^{j_s} \sum_{i=0;\, i_{s+1} i_s = 1}^{n-1} (-1)^{\langle j^{(s)}, i \rangle} \left[(-1)^D - 1 \right] a_i \end{aligned} \tag{7}$$

where

$$D = \left\langle (j_{r-1}, j_{r-2}, \ldots, j_{s+4}, j_{s+3}, j_{s+2}), \left(\prod_{\lambda=s+2}^{r-2} i_\lambda, \prod_{\lambda=s+2}^{r-3} i_\lambda, \ldots, i_{s+3} i_{s+2}, i_{s+2}, 1 \right) \right\rangle. \tag{8}$$

$$A_j^{(s)} = (-1)^{j_s} A_{j^{(s)}} + \sum_{i=0;\, i_{s+1} i_s = 1}^{2^{\mu+1}-1} (-1)^{j_\mu i_\mu \oplus j_{\mu-1} i_{\mu-1} \oplus \cdots \oplus j_{s+2} i_{s+2} \oplus j_{s-1} i_{s-1} \oplus \cdots \oplus j_0 i_0} \left[(-1)^D - 1 \right] a_i. \tag{9}$$

$$D = \left(\prod_{\lambda=s+2}^{\mu-1} i_\lambda \oplus j_{\mu-1} \prod_{\lambda=s+2}^{\mu-2} i_\lambda \oplus \cdots \oplus j_{s+4} i_{s+3} i_{s+2} \oplus j_{s+3} i_{s+2} \oplus j_{s+2} \right). \tag{10}$$

and the second term on the right-hand side (RHS) is independent of j_{s+1} and j_s.

We will prove condition ii) by induction on s. To be specific, we assume that the condition is true for $s+1$ and show that it is true for s. Since every 2^s-QC code is 2^{s+1}-QC as well, and Theorem 3 shows that the condition is true for $s = r-2$, we will be through. Toward this end, consider the following set of four equations obtained from (9) for all possible values of j_{s+1} and j_s for a fixed $(j_{\mu-1}, \ldots, j_{s+2})$:

$$A^{(s)}_{\langle 0,\ldots,0,1,j_{\mu-1},\ldots,j_{s+2},0,0,j_{s-1},\ldots,j_0\rangle} = A_{\langle 0,\ldots,0,1,j_{\mu-1},\ldots,j_{s+2},0,0,j_{s-1},\ldots,j_0\rangle} + K \tag{11}$$

$$A^{(s)}_{\langle 0,\ldots,0,1,j_{\mu-1},\ldots,j_{s+2},1,0,j_{s-1},\ldots,j_0\rangle} = A_{\langle 0,\ldots,0,1,j_{\mu-1},\ldots,j_{s+2},1,1,j_{s-1},\ldots,j_0\rangle} + K \tag{12}$$

$$A^{(s)}_{\langle 0,\ldots,0,1,j_{\mu-1},\ldots,j_{s+2},0,1,j_{s-1},\ldots,j_0\rangle} = -A_{\langle 0,\ldots,0,1,j_{\mu-1},\ldots,j_{s+2},0,1,j_{s-1},\ldots,j_0\rangle} + K \tag{13}$$

$$A^{(s)}_{\langle 0,\ldots,0,1,j_{\mu-1},\ldots,j_{s+2},1,1,j_{s-1},\ldots,j_0\rangle} = -A_{\langle 0,\ldots,0,1,j_{\mu-1},\ldots,j_{s+2},1,0,j_{s-1},\ldots,j_0\rangle} + K \tag{14}$$

where K is the value of the second term in the RHS of (8) which is independent of j_{s+1} and j_s. Since,

$$J(\mu, s, j_{s-1}, j_{s-2}, \ldots, j_0) = J(\mu, s+1, 0, j_{s-1}, \ldots, j_0) \bigcup J(\mu, s+1, 1, j_{s-1}, \ldots, j_0)$$

and by the induction hypothesis $J(\mu, s+1, 0, j_{s-1}, \ldots, j_0)$ and $J(\mu, s+1, 1, j_{s-1}, \ldots, j_0)$ are constrained sets of spectral components, if any of the four terms on the left-hand side of (11)–(14) is zero, then it is easily checked that we get $K = 0$ and then all four terms become zero. Hence $J(\mu, s, j_{s-1}, j_{s-2}, \ldots, j_0)$ is a constrained set of spectral components. This completes the proof for the "only if" part of the theorem.

Proof for the "if Part": Let $\mathcal{C}$ satisfy the constraint $\mathcal{D}$, i.e., the conditions i) and ii) in the statement of the theorem hold for $\mathcal{C}$. Using $a_i = \frac{1}{n}\sum_{k=0}^{n-1}(-1)^{\langle k,i\rangle}A_k$ in (6), it can be brought to the form shown by (15) at the bottom of this page.

If $0 \le j \le 2^{s+1}-1$, then $j_{r-1} = j_{r-2} = \cdots = j_{s+1} = 0$ and (15) becomes (16) also displayed at the bottom of this page. Equation (16) proves that the jth spectral component of the code and its 2^s-cyclic shifted version both either take only the value zero or take all values from F_q, if $0 \le j \le 2^{s+1}-1$.

For $2^{s+1} \le j \le 2^r - 1$, let $A_j \in J(\mu, s, j_{s-1}, \ldots, j_0)$. Then (15) can be written as (17) shown at the bottom of this page.

Now if $A_j = 0$, then $A_k = 0$ for all $A_k \in J(\mu, s, j_{s-1}, \ldots, j_0)$ and from (17) we get $A_j^{(s)} = 0$. It remains to show that if A_j takes all values from F_q then so does $A_j^{(s)}$. Suppose, on the contrary, that $A_j^{(s)}$ takes only the value zero and A_j takes all values from F_q. This is not possible, since then the code and its 2^s-cyclic shifted version will have different dimensions, for all zero spectral components remain zero spectral components whereas a nonzero spectral component becomes a zero spectral component. This completes the proof for the "if part" of the theorem. □

Example 3: Consider the length $n = 4$ ternary codes. Since $r = 2$ the only nontrivial QCD codes are the CD codes. From Theorem 3, the spectral components 0 and 1 are free and $\{2, 3\}$ form a constrained set of spectral components. Hence there are, in total, eight CD codes, of which six are nontrivial. Table II shows all the codewords of these six codes along with their spectra.

Example 4: Among all length–8 dyadic codes over any field of odd characteristic, there are $2^4 = 16$ CD codes corresponding to the following four constrained sets of spectral components:

$$\{0\} \quad \{1\} \quad \{2, 3\} \quad \{4, 5, 6, 7\}$$

and $2^6 = 64$ 2-QCD codes corresponding to the following six constrained sets of spectral components:

$$\{0\} \quad \{1\} \quad \{2\} \quad \{3\} \quad \{4, 6\} \quad \{5, 7\}.$$

Example 5: Among all length–16 dyadic codes over any field of odd characteristic, there are 2^5 CD codes, 2^8 2-QCD codes, and 2^{12} 4-QCD codes corresponding to the constrained sets shown in Table I.

IV. Enumeration of QCD Codes and Dual QCD Codes

In this section, we enumerate the number of 2^s-QCD codes for a specified dimension and also show that the dual code of a QCD code is also QCD and it is easily identified in the transform domain.

A. Enumeration of QCD Codes

For a specified length, say $n = 2^r$, and $0 \le s \le r-1$, the size of the constrained sets and the number of such constrained sets determine the possible dimensions for 2^s-QCD codes. The following theorem provides this information.

$$A_j^{(s)} = \frac{(-1)^{j_s}}{n}\sum_{k=0}^{n-1}\left\{\sum_{i=0}^{n-1}(-1)^{[\oplus_{u=s+1}^{r-1} j_u \prod_{\lambda=s}^{u-1} i_\lambda]\oplus[\oplus_{u=0}^{r-1}(j_u\oplus k_u)i_u]}\right\}A_k. \tag{15}$$

$$A_j^{(s)} = \frac{(-1)^{j_s}}{n}\sum_{k=0}^{n-1}\left\{\sum_{i=0}^{n-1}(-1)^{[\oplus_{u=0}^{r-1}(j_u\oplus k_u)i_u]}\right\}A_k = (-1)^{j_s}A_j. \tag{16}$$

$$\begin{aligned} A_j^{(s)} &= \frac{(-1)^{j_s}}{n}\sum_{k=0}^{n-1}\left\{\sum_{i=0}^{n-1}(-1)^{\{[\oplus_{u=s+1}^{\mu} j_u \prod_{\lambda=s}^{u-1} i_\lambda]\oplus[\oplus_{u=s}^{r-1}(j_u\oplus k_u)i_u]\}\oplus[\oplus_{u=0}^{s-1}(j_u\oplus k_u)i_u]}\right\}A_k \\ &= \frac{(-1)^{j_s}}{n}\sum_{k\,|\,A_k\in J(\mu,s,j_{s-1},\ldots,j_0)}\left\{\sum_{i=0}^{n-1}(-1)^{\{[\oplus_{u=s+1}^{\mu} j_u \prod_{\lambda=s}^{u-1} i_\lambda]\oplus[\oplus_{u=s}^{r-1}(j_u\oplus k_u)i_u]\}}\right\}A_k. \end{aligned} \tag{17}$$

TABLE II
THE CODEWORDS OF THE SIX NONTRIVIAL TERNARY CD CODES OF LENGTH 4 WITH THEIR SPECTRUM

	a_0	a_1	a_2	a_3	A_0	A_1	A_2	A_3		a_0	a_1	a_2	a_3	A_0	A_1	A_2	A_3
$\mathcal{C}_1$	0	0	0	0	0	0	0	0	$\mathcal{C}_2$	0	0	0	0	0	0	0	0
	1	2	1	2	0	1	0	0		1	1	1	1	1	0	0	0
	2	1	2	1	0	2	0	0		2	2	2	2	2	0	0	0
$\mathcal{C}_3$	0	0	0	0	0	0	0	0	$\mathcal{C}_4$	0	0	0	0	0	0	0	0
	1	2	2	1	0	0	0	1		1	2	1	2	0	1	0	0
	2	1	1	2	0	0	0	2		2	1	2	1	0	2	0	0
	1	1	2	2	0	0	1	0		1	1	1	1	1	0	0	0
	2	0	1	0	0	0	1	1		2	0	2	0	1	1	0	0
	0	2	0	1	0	0	1	2		0	2	0	2	1	2	0	0
	2	2	1	1	0	0	2	0		2	2	2	2	2	0	0	0
	0	1	0	2	0	0	2	1		0	1	0	1	2	1	0	0
	1	0	2	0	0	0	2	2		1	0	1	0	2	2	0	0
$\mathcal{C}_5$	0	0	0	0	0	0	0	0	$\mathcal{C}_6$	0	0	0	0	0	0	0	0
	1	2	2	1	0	0	0	1		1	2	2	1	0	0	0	1
	2	1	1	2	0	0	0	2		2	1	1	2	0	0	0	2
	1	1	2	2	0	0	1	0		1	1	2	2	0	0	1	0
	2	0	1	0	0	0	1	1		2	0	1	0	0	0	1	1
	0	2	0	1	0	0	1	2		0	2	0	1	0	0	1	2
	2	2	1	1	0	0	2	0		2	2	1	1	0	0	2	0
	0	1	0	2	0	0	2	1		0	1	0	2	0	0	2	1
	1	0	2	0	0	0	2	2		1	0	2	0	0	0	2	2
	1	2	1	2	0	1	0	0		1	1	1	1	1	0	0	0
	2	1	0	0	0	1	0	1		2	0	0	2	1	0	0	1
	0	0	2	1	0	1	0	2		0	2	2	0	1	0	0	2
	2	0	0	1	0	1	1	0		2	2	0	0	1	0	1	0
	0	2	2	2	0	1	1	1		0	1	2	1	1	0	1	1
	1	1	1	0	0	1	1	2		1	0	1	2	1	0	1	2
	0	1	2	0	0	1	2	0		0	0	2	2	1	0	2	0
	1	0	1	1	0	1	2	1		1	2	1	0	1	0	2	1
	2	2	0	2	0	1	2	2		2	1	0	1	1	0	2	2
	2	1	2	1	0	2	0	0		2	2	2	2	2	0	0	0
	0	0	1	2	0	2	0	1		0	1	1	0	2	0	0	1
	1	2	0	0	0	2	0	2		1	0	0	1	2	0	0	2
	0	2	1	0	0	2	1	0		0	0	1	1	2	0	1	0
	1	1	0	1	0	2	1	1		1	2	0	2	2	0	1	1
	2	0	2	2	0	2	1	2		2	1	2	0	2	0	1	2
	1	0	0	2	0	2	2	0		1	1	0	0	2	0	2	0
	2	2	2	0	0	2	2	1		2	0	2	1	2	0	2	1
	0	1	1	1	0	2	2	2		0	2	1	2	2	0	2	2

Theorem 5: For a given r and $0 \leq s \leq r-1$, there are 2^{s+1} constrained sets of size 1 and 2^s constrained sets of size 2^t, for all $1 \leq t \leq r-1-s$. Hence, the total number of constrained sets is $2^s(r-s+1)$.

Proof: Consider the constrained set

$$J(\mu, s, j_{s-1}, \ldots, j_0) = (0, 0, \ldots, 0, j_\mu = 1, j_{\mu-1}, \ldots, j_s, j_{s-1}, \ldots, j_0).$$

For every fixed value of μ and s, where $r-1 \leq \mu \leq s+1$, the above constrained set has 2^s elements corresponding to each $j_0, j_1, \ldots j_{s-1}$ taking two values. Since there are 2^{s+1} free spectral components, each one of them is a constrained set of size 1, we have the total number of constrained sets $(r-1-s)2^s + 2^{s+1} = 2^s(r-s+1)$. □

Theorem 6: For $1 \leq k \leq 2^r - 1$, the number of k-dimensional 2^s-QCD codes of length 2^r is the number of ways in which k can be expressed as

$$k = a_{r-s-1}2^{r-s-1} + a_{r-s-2}a^{r-s-2} + \cdots + a_1 2 + a_0 \qquad (18)$$

where $0 \leq a_0 \leq 2^{s+1}$ and $0 \leq a_i \leq 2^s$ for $i = 1, 2, \ldots, r-1-s$.

Proof: This follows from Theorem 5 since, when spectral components of a constrained set take all values from the field, its contribution to the dimension of the code is equal to the size of the constrained set. □

The following is immediate from Theorem 6.

Corollary 2: For every r and $0 \leq s \leq r-1$, QCD codes exist for all dimension k, where $1 \leq k \leq 2^r - 1$.

Corollary 3: There are exactly two CD codes of each dimension $0 \leq k \leq 2^r - 1$.

Proof: Put $s = 0$ in (18). □

B. Dual QCD Codes

Two vectors $\vec{a} = (a_0, a_1, \ldots, a_{n-1})$ and $\vec{b} = (b_0, b_1, \ldots, b_{n-1})$ over F_q are orthogonal if $\sum_{i=0}^{n-1} a_i b_i = 0$. For a linear code $\mathcal{C}$ over F_q, the set of n-tuples over F_q that are orthogonal to all the codewords of $\mathcal{C}$ is called the dual code of $\mathcal{C}$. Theorem 2 of [8], when specialized to dyadic codes, becomes the following.

Theorem 7: For a dyadic code with spectral components A_j taking only the value zero, where $j \in \boldsymbol{Z} \subset \{0, 1, \ldots, n-1\}$, its dual code takes only the value zero in spectral components A_j where $j \notin \boldsymbol{Z}$.

An immediate consequence is the following statement.

Corollary 4: Self-dual dyadic codes do not exist.

The following corollary follows from combining Theorems 4 and 7.

Corollary 5: The dual of a 2^s-QCD code is also a 2^s-QCD code.

V. Conclusion

In this correspondence, we have extended the well-known transform domain characterization of cyclic codes to dyadic codes which are also QC, called QCD codes, in the WHT domain. The class of QCD codes enjoy the advantage that if the codes were only QC and not dyadic then extension of the field is required to characterize them in the transform domain. It will be interesting to investigate decoding algorithms that make use of the presence of both the QC structure and the dyadic structure. Generalizations of WHTs such as Reverse Jacket transforms and Cocyclic transforms have been investigated in [19]–[24]. The approach of this correspondence may be extended to some other classes of codes using these generalized transforms. Extension of QCD codes over finite fields to QCD codes over integer residue class rings is straightforward using the approach followed for the extension of cyclic codes over fields to these rings in [10] and [11].

Acknowledgment

The authors gratefully acknowledge the anonymous reviewers for their suggestions which helped to improve the content as well as the presentation of the correspondence.

References

[1] T. Kasami, "Gilbert–Varshamov bound for quasicyclic codes of rate 1/2," *IEEE Trans. Inform. Theory*, vol. IT-20, p. 679, Sept. 1974.
[2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1988.
[3] N. Ahmed and K. R. Rao, *Orthogonal Transforms for Digital Signal Processing*. New York: Springer-Verlag, 1975.
[4] K. G. Beauchamp, *Walsh Functions and Their Applications*. New York: Academic, 1975.
[5] S. D. Berman, "Semi-simple cyclic and abelian codes," *Kibernetika*, vol. 3, pp. 21–30, 1967.
[6] P. Camion, "Abelian codes," Math. Res. Ctr, Univ. Wisconsin, Madison, Tech. Rep. 1059, 1971.
[7] F. J. MacWilliams, "Binary codes which are ideals in the group algebra of an abelian group," *Bell Syst. Tech. J.*, vol. 49, pp. 987–1011, 1970.
[8] B. S. Rajan and M. U. Siddiqi, "Transform domain characterization of abelian codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1817–1821, Nov. 1992.
[9] R. E. Blahut, *Theory and Practice of Error Control Codes*. Reading, MA: Addison-Wesley, 1982.
[10] B. S. Rajan and M. U. Siddiqi, "Transform domain characterization of cyclic codes over z_m," *Applicable Alg. Eng., Commun. Comput.*, vol. 5, pp. 261–276, 1994.
[11] ——, "A generalized DFT for abelian codes over z_m," *IEEE Trans. Inform. Theory*, vol. 40, pp. 2082–2090, Nov. 1994.
[12] ——, "Transform decoding of BCH codes over z_m," *Int. J. Electron.*, vol. 75, pp. 1043–1054, 1993.
[13] G. Gunther, "A finite field Fourier transform for vectors of arbitrary length," in *Communications and Cryptography: Two Sides of One Tapestry*, R. E. Blahut, D. J. Costello, U. Maurer, and T. Mittelholzer, Eds. Norwell, MA: Kluwer, 1994.
[14] J. H. van Lint, "Repeated-root cyclic codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 343–345, Mar. 1991.
[15] G. Castagnoli, J. L. Massey, P. A. Schoeller, and V. Seemann, "On repeated-root cyclic codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 337–342, Mar. 1991.
[16] P. Mathys, "Frequency domain description of repeated-root cyclic codes," in *Proc. 1994 IEEE Int. Symp. Information Theory*, Trondheim, Norway, 1994, p. 47.
[17] R. M. Tanner, "A transform theory for a class of group-invariant codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 752–775, July 1988.
[18] B. K. Dey and B. S. Rajan, "F_q-linear cyclic codes over F_{q^m}: DFT characterization," in *Applied Algebra, Algebraic Algorithms and Error Correcting Codes (Lecture Notes in Computer Science)*. New York: Springer-Verlag, 2001, vol. LNCS 2227, pp. 67–76.
[19] M. H. Lee, "Fast complex reverse jacket transform," *IEEE Trans. Circuits Syst.*, submitted for publication.
[20] M. H. Lee, "New reverse jacket transform and its fast algorithm," *IEEE Trans. Circuits Syst.—II*, vol. 47, pp. 39–46, Jan. 2000.
[21] K. J. Horadam, D. L. Flannery, and W. Launey, "Cocyclic Hadamard matrices and difference sets," Roy. Melbourne Inst. Technol., Dept. Math., Res. Rep. 2, Mar. 1997.
[22] A. Baliga and K. J. Horadam, "Cocyclic Hadamard matrices over $z_t \times z_2^2$," *Australis J. Combin.* , vol. 11, pp. 123–134, 1995.
[23] M. H. Lee and J. Y. Park, "A simple binary index generation for reverse jacket sequence," *IEEE Trans. Circuit Syst.—II*, submitted for publication.
[24] M. H. Lee, "A new reverse jacket transform based on Hadamard matrix," in *Proc. 2000 IEEE Int. Symp. Information Theory*, Sorrento, Italy, June 2000, p. 471.

Variable-Length Integer Codes Based on the Goldbach Conjecture, and Other Additive Codes

Peter Fenwick, *Member, IEEE*

***Abstract*—This correspondence introduces a new family of variable-length codes for the integers, initially based on the Goldbach conjecture that every even integer is the sum of two primes. For an even integer we decompose the value into its two constituent primes and encode the ordinal numbers of those primes with an Elias γ code. The method is then elaborated to handle odd integers. The correspondence then develops a more general method of encoding any integer as the sum of two integers and developing suitable basis sets of integers. Although the codes which are generated by these methods are characterized by widely varying and unpredictable lengths, they are over some ranges shorter than most other variable-length codes.**

***Index Terms*—Elias gamma codes, Goldbach conjecture, integers, prime numbers, variable-length codes.**

I. Introduction

Many types of information coding and compression involve a transformation which produces a sequence of integers with a highly skewed frequency distribution. For good compression or a compact representation it is then necessary to represent these integers in a "variable-length" form such that each codeword is self-delimiting and small values are represented much more compactly than larger values. Many such codes have been developed, as summarized by Fenwick [1] (though this account has major errors in describing the Golomb code). The present

Manuscript received August 1, 2001; revised March 3, 2002.

The author is with the Department of Computer Science, University of Auckland, Private Bag 92019, Auckland, New Zealand (e-mail: p.fenwick@auckland.ac.nz).

Communicated by G. Battail, Editor At Large.
Publisher Item Identifier 10.1109/TIT.2002.800483.