On the Minimum Distance of Array Codes as LDPC Codes

Kyeongcheol Yang, *Member, IEEE*, and Tor Helleseth, *Fellow, IEEE*

***Abstract*—For a prime q and an integer $j \leq q$, the code $\mathcal{C}(q,j)$ is a class of low-density parity-check (LDPC) codes from array codes which has a nice algebraic structure. In this correspondence, we investigate the minimum distance $d(q,j)$ of the code in an algebraic way. We first prove that the code is invariant under a doubly transitive group of "affine" permutations. Then, we show that $d(5,4)=8$, $d(7,4)=8$, and $d(q,4) \geq 10$ for any prime $q > 7$. In addition, we also analyze the codewords of weight 6 in the case of $j = 3$ and the codewords of weight 8 in $\mathcal{C}(5,4)$ and $\mathcal{C}(7,4)$.**

***Index Terms*—Array codes, low-density parity-check (LDPC) codes, minimum distance.**

I. Introduction

Low-density parity-check (LDPC) codes first discovered by Gallager [2] achieve a remarkable performance with iterative decoding that is very close to the Shannon limit [5], [7]. In most cases, LDPC codes are generated by a computer search since there are few methods for constructing them algebraically.

Recently, Fan [3] proposed a class of algebraically constructed LDPC codes from a family of array codes in [1]. For high rate and moderate length (say up to about 5000), these codes perform as well as the best comparable randomly constructed regular LDPC codes given in [4]. Mittelholzer derived generator matrices for the codes in a closed form and gave some upper bounds on the minimum Hamming distance of the codes [6].

Let q be a prime and $j \leq q$ an integer. Let $\mathcal{C}(q,j)$ be the binary code of length q^2, whose parity-check matrix is given by

$$H(q,j) = \begin{bmatrix} I & I & I & \dots & I \\ I & P & P^2 & \dots & P^{q-1} \\ I & P^2 & P^4 & \dots & P^{2(q-1)} \\ & \vdots & & & \vdots \\ I & P^{(j-1)} & P^{2(j-1)} & \dots & P^{(j-1)(q-1)} \end{bmatrix}$$

where I is the $q \times q$ identity matrix and P is the permutation matrix defined by

$$P = \begin{bmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ & \vdots & & \vdots & \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}.$$

Since each column of $H(q,j)$ has j ones and each row has q ones, the code $\mathcal{C}(q,j)$ can be regarded as a (j,q) regular LDPC code. It is easily shown that $H(q,j)$ has rank $qj - j + 1$ and, therefore, $\mathcal{C}(q,j)$ has dimension $q^2 - qj + j - 1$.

In general, it is a very interesting problem to find the minimum distance of LDPC codes. Tanner derived some bounds by graph analysis [9], which relate the minimum distance to the eigenvalues of the matrix $H^T H$ as a real matrix, where H is a parity-check matrix and T is the transpose operator.

Using the algebraic structure of the code $\mathcal{C}(q,j)$, it is possible to analyze the minimum distance $d(q,j)$ of $\mathcal{C}(q,j)$. In fact, Mittelholzer gave an upper bound on $d(q,j)$ as follows [6]:

$$d(q,j) \leq \begin{cases} 6, & \text{if } j = 3 \\ 12, & \text{if } j = 4 \\ 20, & \text{if } j = 5 \\ 32, & \text{if } j = 6. \end{cases}$$

In the case of $j = 3$, the upper bound is tight, that is, $d(q,3) = 6$. Note that $d(q,i) \geq d(q,j)$ for any $i \geq j$, since $\mathcal{C}(q,i) \subseteq \mathcal{C}(q,j)$ for any $i \geq j$.

To find $d(q,j)$ in general seems to be a very hard problem. Our main contribution in this correspondence is to develop a method that allows us to improve existing results on $d(q,j)$ for the case $j = 4$. We first prove that the code $\mathcal{C}(q,j)$ is invariant under a doubly transitive group of "affine" permutations. Then we show that $d(5,4) = 8$, $d(7,4) = 8$, and $d(q,4) \geq 10$ for any prime $q > 7$. In addition, we also analyze the codewords of weight 6 in the case of $j = 3$ and the codewords of weight 8 in $\mathcal{C}(5,4)$ and $\mathcal{C}(7,4)$.

II. Representation of Array Codes

Each column of the parity-check matrix $H(q,j)$ has j blocks and each block is a permutation of $(1\,0\,0 \cdots 0\,0)^T$. This motivates introducing a new representation of $H(q,j)$. For this purpose, let

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \triangleq 0, \quad \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \triangleq 1, \quad \begin{bmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} \triangleq 2, \quad \dots, \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \triangleq q-1.$$

That is, the positions of 1's are associated with the elements of $\mathbb{Z}_q$, where $\mathbb{Z}_q$ is the ring of integers modulo q. Then every column of $H(q,j)$ can be expressed as

$$[x, x+i, x+2i, \dots, x+(j-1)i]^T \pmod{q}$$

for some $x, i \in \mathbb{Z}_q$. In this respect, the matrix $H(q,j)$ is analogous to the parity-check matrix of Reed–Solomon codes. As an example, the parity-check matrix $H(5,3)$ of $\mathcal{C}(5,3)$ can be rewritten as the matrix at the top of the following page by a proper column permutation.

Let $\mathcal{T}$ be the set of column indexes for $H(q,j)$, defined by

$$\mathcal{T} = \left\{ [x, x+i, x+2i, \dots, x+(j-1)i]^T \mid x, i \in \mathbb{Z}_q \right\}$$

where the operations are taken by modulo q. Then the code $\mathcal{C}(q,j)$ is the set of solutions over $\mathbb{Z}_2$ of the linear equation

$$\sum_{\boldsymbol{x} \in \mathcal{T}} c_{\boldsymbol{x}} \boldsymbol{x} = 0$$

in the binary variables $c_{\boldsymbol{x}}$ and $\boldsymbol{x} \in \mathcal{T}$, where the summation is taken over $\mathbb{Z}_2$ and the components of $\boldsymbol{x}$ are regarded as symbols in these computations. It is easily checked that if $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathcal{T}$ have more than

Manuscript received April 16, 2003; revised July 24, 2003. This work was supported in part by the Brain Korea 21 Project, the University IT Research Center Project, the Com^{2}Mac-KOSEF, and by the Norwegian Research Council.

K. Yang is with the Department of Electronic and Electrical Engineering, Pohang University of Science and Technology (POSTECH), Pohang, Kyungbuk 790–784, Korea (e-mail: kcyang@postech.ac.kr).

T. Helleseth is with the Department of Informatics, University of Bergen, Bergen, Norway (e-mail: Tor.Helleseth@ii.uib.no).

Communicated by C. Carlet, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2003.820053

0018-9448/03$17.00 © 2003 IEEE

$$\begin{bmatrix}0&0&0&0&0&1&1&1&1&1&2&2&2&2&2&3&3&3&3&3&4&4&4&4&4\\0&1&2&3&4&1&2&3&4&0&2&3&4&0&1&3&4&0&1&2&4&0&1&2&3\\0&2&4&1&3&1&3&0&2&4&2&4&1&3&0&3&0&2&4&1&4&1&3&0&2\end{bmatrix}$$

two identical components, then $\boldsymbol{x} = \boldsymbol{y}$. The support of a code $\boldsymbol{c}$ is defined by

$$\mathrm{supp}(\boldsymbol{c}) = \{\boldsymbol{x} \in \mathcal{T} \mid c_{\boldsymbol{x}} \neq 0\}.$$

For our convenience, we denote $\mathrm{supp}(\boldsymbol{c})$ by a matrix whose columns correspond to the vectors in $\mathrm{supp}(\boldsymbol{c})$.

Proposition 1: For any prime $q \geq 5$ and $j \geq 3$, the code $\mathcal{C}(q,j)$ has Tanner graph of girth 6.

Proof: If two columns $\boldsymbol{x}$ and $\boldsymbol{y}$ of $H(q,j)$ have two ones in common at the same positions, then $\boldsymbol{x} = \boldsymbol{y}$. This implies that there is no cycle of length 4 in the corresponding Tanner graph [8]. Clearly, there is a cycle of length 6, say, a cycle from the three columns indexed by $[0,0,0,0,\ldots,0]^T$, $[0,1,2,3,\ldots,j-1]^T$, and $[2,1,0,q-1,\ldots,q-j+3]^T$ of $H(q,j)$. □

Lemma 2: The code $\mathcal{C}(q,j)$ is invariant under the doubly transitive group G of "affine" permutations of the form

$$\boldsymbol{x} \longmapsto a\boldsymbol{x} + \boldsymbol{b}$$

where $a \in \mathbb{Z}_q^* = \mathbb{Z}_q \backslash \{0\}$, $\boldsymbol{b} \in \mathcal{T}$, and the operations are taken componentwise modulo q.

Proof: It is easily checked that $a\boldsymbol{x} + \boldsymbol{b} \in \mathcal{T}$ for any $a \in \mathbb{Z}_q^*$ and $\boldsymbol{b} \in \mathcal{T}$. □

From the structure of $H(q,j)$, every codeword of $\mathcal{C}(q,j)$ has even weight. It is also easily checked that $d(q,2) = 4$ for any prime $q \geq 3$. The following theorem is known in [6], but we will prove it here using Lemma 2.

Theorem 3: For any prime $q \geq 5$

$$d(q,3) = 6.$$

Proof: In order to get $d(q,3) \geq 6$, it suffices to show that there are no codewords of weight 4. Suppose that there exists a codeword $\boldsymbol{c}$ of weight 4. By Lemma 2, we can assume without loss of generality that $\boldsymbol{c}$ has the following support:

$$\begin{bmatrix}0 & 0 & x & x\\0 & i & x+k_1 & x+k_2\\0 & 2i & x+2k_1 & x+2k_2\end{bmatrix}$$

where $i \in \mathbb{Z}_q^*$ and $x, k_1, k_2 \in \mathbb{Z}_q$. Since the zeros in the first column should be cancelled out for $\boldsymbol{c}$ to be a codeword, we can assume without loss of generality that $x + k_1 = 0$ and $x + 2k_2 = 0 \pmod{q}$. Then we have $x + k_2 = i$ and $x + 2k_1 = 2i$. This is possible only in the case of $i = 0$, which is a contradiction.

On the other hand, $d(q,3) \leq 6$ comes from the fact that there exists a codeword of weight 6, as will be shown in Theorem 4. □

III. Codewords of Weight 6 in $\mathcal{C}(q,3)$

Let $\boldsymbol{c}$ be a codeword of weight 6 in $\mathcal{C}(q,3)$. By Lemma 2, we can assume without loss of generality that $\boldsymbol{c}$ has the following support:

$$\begin{bmatrix}0 & 0 & y & y & z & z\\0 & i & 0 & y+l & z+k_1 & z+k_2\\0 & 2i & -y & y+2l & z+2k_1 & z+2k_2\end{bmatrix}$$

where $i, y, \in \mathbb{Z}_q^*$ and $z, l, k_1, k_2 \in \mathbb{Z}_q$. Since the third zero in the first column should be canceled out for $\boldsymbol{c}$ to be a codeword, it suffices to consider only two possible cases: $y + 2l = 0$ or $z + 2k_1 = 0 \pmod{q}$.

Case i) $y + 2l = 0 \pmod{q}$: We can assume without loss of generality that $i = z + k_1$ and $y + l = z + k_2 \pmod{q}$, and so $\boldsymbol{c}$ has the following support:

$$\begin{bmatrix}0 & 0 & 2z+2k_2 & 2z+2k_2 & z & z\\0 & z+k_1 & 0 & z+k_2 & z+k_1 & z+k_2\\0 & 2z+2k_1 & -2z-2k_2 & 0 & z+2k_1 & z+2k_2\end{bmatrix}.$$

If $2z + 2k_1 = z + 2k_1$ and $-2z - 2k_2 = z + 2k_2$, then we have $z = 0$ and $k_2 = 0$ and so the sixth column is the same as the first column, which is a contradiction. If $2z + 2k_1 = z + 2k_2$ and $-2z - 2k_2 = z + 2k_1$, then we have $z + k_1 = 0$ and so the second column is the same as the first column, which is a contradiction.

Case ii) $z + 2k_1 = 0 \pmod{q}$: In this case, $\boldsymbol{c}$ has the following support:

$$\begin{bmatrix}0 & 0 & y & y & -2k_1 & -2k_1\\0 & i & 0 & y+l & -k_1 & -2k_1+k_2\\0 & 2i & -y & y+2l & 0 & -2k_1+2k_2\end{bmatrix}.$$

There are two subcases for the second row: $i = -k_1$ and $y + l = -2k_1 + k_2$ or $i = -2k_1 + k_2$ and $y + l = -k_1$.

In the case that $i = -k_1$ and $y + l = -2k_1 + k_2$, we have two subcases for the third row. If $2i = -y$ and $y + 2l = -2k_1 + 2k_2$, then $k_1 = 0$ and so column 1 is the same as column 5, which is a contradiction. If $2i = y + 2l$ and $-y = -2k_1 + 2k_2$, then $k_1 = k_2$ and so column 5 is the same as column 6, which is a contradiction.

In the case that $i = -2k_1 + k_2$ and $y + l = -k_1$, we have two subcases for the third row. If $2i = -y$ and $y + 2l = -2k_1 + 2k_2$, then $k_1 = 0$ and so column 1 is the same as column 5, which is a contradiction. If $2i = y + 2l$ and $-y = -2k_1 + 2k_2$, then we have a solution: $i = -2k_1 + k_2$, $l = -3k_1 + 2k_2$, and $y = 2k_1 - 2k_2$, where $k_1, k_2 \in \mathbb{Z}_q$.

Summarizing the above results, we have the following theorem on the support of codewords of weight 6 in the code $\mathcal{C}(q,3)$.

Theorem 4: For any prime $q \geq 5$, all codewords of weight 6 in the code $\mathcal{C}(q,3)$ have as their supports the following set or its image under the group G:

$$\begin{bmatrix}0 & 0 & 2i-2k & 2i-2k & -2i & -2i\\0 & -2i+k & 0 & -i & -i & -2i+k\\0 & -4i+2k & -2i+2k & -4i+2k & 0 & -2i+2k\end{bmatrix}$$

where $i \in \mathbb{Z}_q^*$ and $k \in \mathbb{Z}_q$ with $k \neq i, 2i$.

IV. Minimum Distance of $\mathcal{C}(q,j)$ for $j = 4$

For a prime q, note that $\mathcal{C}(q,i) \subseteq \mathcal{C}(q,j)$ for any $i \geq j$. This implies that $d(q,i) \geq d(q,j)$ for any $i \geq j$ and, therefore, $d(q,4) \geq 6$. A lower bound on the minimum distance $d(q,4)$ of $\mathcal{C}(q,4)$ can be improved as follows.

Lemma 5: For $q \geq 5$, we have $d(q,4) \geq 8$.

Proof: Since $d(q,4) \geq d(q,3) = 6$, it suffices to show that there are no codewords of weight 6 in $\mathcal{C}(q,4)$. Suppose there exists a codeword of weight 6 in $\mathcal{C}(q,4)$. By Theorem 4, we can assume without loss of generality that ***c*** has the following support:

$$\begin{bmatrix} 0 & 0 & 2i-2k & 2i-2k & -2i & -2i \\ 0 & -2i+k & 0 & -i & -i & -2i+k \\ 0 & -4i+2k & -2i+2k & -4i+2k & 0 & -2i+2k \\ 0 & -6i+3k & -4i+4k & -7i+4k & i & -2i+3k \end{bmatrix}$$

where $i \in \mathbb{Z}_q^*$ and $k \in \mathbb{Z}_q$ with $k \neq i, 2i$. Since the fourth zero in the first column should be canceled out for ***c*** to be a codeword, we have only two possible cases: $-7i+4k=0$ or $-2i+3k=0 \pmod{q}$. In each case, there are two identical columns, which is a contradiction. □

Theorem 6: For $q=5$ or 7, $d(q,4)=8$. For any prime $q>7$, we have

$$d(q,4) \geq 10.$$

Proof: By Lemma 5, it suffices to show that there are no codewords of weight 8 in $\mathcal{C}(q,4)$. See the Appendix for more details. □

As in Section III, we also analyze the codewords of weight 8 in $\mathcal{C}(5,4)$ and $\mathcal{C}(7,4)$ in the following two theorems.

Theorem 7: All codewords of weight 8 in the code $\mathcal{C}(5,4)$ have as their supports the following set or its image under the group G:

$$\begin{bmatrix} 0 & 0 & 3z{+}3k & 3z{+}3k & 4z{+}2k & 4z{+}2k & 2z & 2z \\ 0 & 4z{+}k & 0 & 3z & 2z{+}k & 4z{+}k & 3z & 2z{+}k \\ 0 & 3z{+}2k & 2z{+}2k & 3z{+}2k & 0 & 4z & 4z & 2z{+}2k \\ 0 & 2z{+}3k & 4z{+}4k & 3z{+}4k & 3z{+}4k & 4z{+}4k & 0 & 2z{+}3k \end{bmatrix}$$

where $z \in \mathbb{Z}_5^*$ and $k \in \{0, 2z\}$.

Proof: See the Appendix. □

Theorem 8: All codewords of weight 8 in the code $\mathcal{C}(7,4)$ have as their supports the following set or its image under the group G:

$$\begin{bmatrix} 0 & 0 & 5z{+}2k & 5z{+}2k & z{+}2k & z{+}2k & 4z & 4z \\ 0 & 2z{+}k & 0 & 2z{+}k & 4z{+}k & 5z & 5z & 4z{+}k \\ 0 & 4z{+}2k & 2z{+}5k & 6z & 0 & 2z{+}5k & 6z & 4z{+}2k \\ 0 & 6z{+}3k & 4z{+}3k & 3z{+}6k & 3z{+}6k & 6z{+}3k & 0 & 4z{+}3k \end{bmatrix}$$

where $z \in \mathbb{Z}_7^*$ and $k \in \{0, 2z, 4z, 6z\}$.

Proof: See the Appendix . □

V. Concluding Remarks

Our methods can in principle be extended to the cases with larger $j>4$, but will be more awkward to handle since the number of cases that need to have a detailed study will grow. Therefore, a new method seems to be necessary to solve the problem in its full generality.

Appendix
Codewords of Weight 8 in $\mathcal{C}(q,4)$

Assume there is a codeword of weight 8. By Lemma 2, we can assume without loss of generality that it has one of the following supports:

$$\text{Class I: } \begin{bmatrix} 0 & 0 & x & x & y & y & z & z \\ 0 & & 0 & & & & & \\ 0 & & & & 0 & & & \\ 0 & & & & & & 0 & \end{bmatrix}.$$

$$\text{Class II: } \begin{bmatrix} 0 & 0 & x & x & y & y & z & z \\ 0 & & 0 & & & & & \\ 0 & & & 0 & & & & \\ 0 & & & & 0 & & & \end{bmatrix}.$$

$$\text{Class III: } \begin{bmatrix} 0 & 0 & x & x & y & y & z & z \\ 0 & & 0 & & & & & \\ 0 & & & & 0 & & & \\ 0 & & & 0 & & & & \end{bmatrix}.$$

$$\text{Class IV: } \begin{bmatrix} 0 & 0 & x & x & y & y & z & z \\ 0 & & & & 0 & & & \\ 0 & & 0 & & & & & \\ 0 & & & 0 & & & & \end{bmatrix}.$$

A. Class I

Without loss of generality, we can assume that ***c*** has the following support:

$$\begin{bmatrix} 0 & 0 & x & x & -2y & -2y & -3z & -3z \\ 0 & i & 0 & x+j & -y & -2y+l & -2z & -3z+k \\ 0 & 2i & -x & x+2j & 0 & -2y+2l & -z & -3z+2k \\ 0 & 3i & -2x & x+3j & y & -2y+3l & 0 & -3z+3k \end{bmatrix}$$

where $i,x,y,z \in \mathbb{Z}_q^*$ and $j,k,l \in \mathbb{Z}_q$. There are ten cases for the second row:

1) $i=x+j,\quad -y=-2z,\quad -2y+l=-3z+k;$
2) $i=x+j,\quad -y=-3z+k,\quad -2y+l=-2z;$
3) $i=-y,\quad x+j=-2z,\quad -2y+l=-3z+k;$
4) $i=-y,\quad x+j=-3z+k,\quad -2y+l=-2z;$
5) $i=-2y+l,\quad x+j=-2z,\quad -y=-3z+k;$
6) $i=-2y+l,\quad x+j=-3z+k,\quad -y=-2z;$
7) $i=-2z,\quad x+j=-y,\quad -2y+l=-3z+k;$
8) $i=-2z,\quad x+j=-2y+l,\quad -y=-3z+k;$
9) $i=-3z+k,\quad x+j=-y,\quad -2y+l=-2z;$
10) $i=-3z+k,\quad x+j=-2y+l,\quad -y=-2z.$

Considering the requirements for the third and the fourth row, it can be checked by a long and straightforward computation that there is no solution, except for the following two cases:

- $i=-2y+l, x+j=-2z, -y=-3z+k$ (for the second row)
  $2i=x+2j, -x=-3z+2k, -2y+2l=-z$ (for the third row)
  $3i=-3z+3k, -2x=-2y+3l, x+3j=y$ (for the fourth row)
  $q=5;$
- $i=x+j, -y=-3z+k, -2y+l=-2z$ (for the second row)
  $2i=-3z+2k, -x=-2y+2l, x+2j=-z$ (for the third row)
  $3i=-2y+3l, -2x=-3z+3k, x+3j=y$ (for the fourth row)
  $q=7.$

In the first case, we have a solution

$$\begin{bmatrix} 0 & 0 & 3z{+}3k & 3z{+}3k & 4z{+}2k & 4z{+}2k & 2z & 2z \\ 0 & 4z{+}k & 0 & 3z & 2z{+}k & 4z{+}k & 3z & 2z{+}k \\ 0 & 3z{+}2k & 2z{+}2k & 3z{+}2k & 0 & 4z & 4z & 2z{+}2k \\ 0 & 2z{+}3k & 4z{+}4k & 3z{+}4k & 3z{+}4k & 4z{+}4k & 0 & 2z{+}3k \end{bmatrix}$$

where $z \in \mathbb{Z}_5^*$ and $k \in \{0, 2z\}$.

In the second case, we have a solution

$$\begin{bmatrix} 0 & 0 & 5z{+}2k & 5z{+}2k & z{+}2k & z{+}2k & 4z & 4z \\ 0 & 2z{+}k & 0 & 2z{+}k & 4z{+}k & 5z & 5z & 4z{+}k \\ 0 & 4z{+}2k & 2z{+}5k & 6z & 0 & 2z{+}5k & 6z & 4z{+}2k \\ 0 & 6z{+}3k & 4z{+}3k & 3z{+}6k & 3z{+}6k & 6z{+}3k & 0 & 4z{+}3k \end{bmatrix}$$

where $z \in \mathbb{Z}_7^*$ and $k \in \{0, 2z, 4z, 6z\}$.

B. Class II

Without loss of generality, we can assume that $\boldsymbol{c}$ has the following support:

$$\begin{bmatrix} 0 & 0 & 2x & 2x & 3y & 3y & z & z \\ 0 & i & 0 & x & 2y & 3y+j & z+k & z+l \\ 0 & 2i & -2x & 0 & y & 3y+2j & z+2k & z+2l \\ 0 & 3i & -4x & -x & 0 & 3y+3j & z+3k & z+3l \end{bmatrix}$$

where $i, x, y \in \mathbb{Z}_q^*$ and $z, j, k, l \in \mathbb{Z}_q$. There are five cases for the second row.

1) $i = x, \quad 2y = z+k, \quad 3y+j = z+l;$
2) $i = 2y, \quad x = z+k, \quad 3y+j = z+l;$
3) $i = 3y+j, \quad x = z+k, \quad 2y = z+l;$
4) $i = z+k, \quad x = 2y, \quad 3y+j = z+l;$
5) $i = z+k, \quad x = 3y+j, \quad 2y = z+l.$

A long and straightforward check shows that there is no solution.

C. Class III

Without loss of generality, we can assume that $\boldsymbol{c}$ has the following support:

$$\begin{bmatrix} 0 & 0 & -3x & -3x & -2y & -2y & z & z \\ 0 & i & 0 & -2x & -y & -2y+j & z+k & z+l \\ 0 & 2i & 3x & -x & 0 & -2y+2j & z+2k & z+2l \\ 0 & 3i & 6x & 0 & y & -2y+3j & z+3k & z+3l \end{bmatrix}$$

where $i, x, y \in \mathbb{Z}_q^*$ and $z, j, k, l \in \mathbb{Z}_q$. There are five cases for the second row.

1) $i = -2x, \quad -y = z+k, \quad -2y+j = z+l;$
2) $i = -y, \quad -2x = z+k, \quad -2y+j = z+l;$
3) $i = -2y+j, \quad -2x = z+k, \quad -y = z+l;$
4) $i = z+k, \quad -2x = -y, \quad -2y+j = z+l;$
5) $i = z+k, \quad -2x = -2y+j, \quad -y = z+l.$

A long and straightforward check shows that there is no solution.

D. Class IV

Without loss of generality, we can assume that $\boldsymbol{c}$ has the following support:

$$\begin{bmatrix} 0 & 0 & -6x & -6x & y & y & z & z \\ 0 & i & -3x & -4x & 0 & y+j & z+k & z+l \\ 0 & 2i & 0 & -2x & -y & y+2j & z+2k & z+2l \\ 0 & 3i & 3x & 0 & -2y & y+3j & z+3k & z+3l \end{bmatrix}$$

where $i, x, y \in \mathbb{Z}_q^*$ and $z, j, k, l \in \mathbb{Z}_q$. There are five cases for the second row.

1) $i = -3x, \quad -4x = z+k, \quad y+j = z+l;$
2) $i = -4x, \quad -3x = z+k, \quad y+j = z+l;$
3) $i = y+j, \quad -3x = z+k, \quad -4x = z+l;$
4) $i = z+k, \quad -3x = y+j, \quad -4x = z+l;$
5) $i = z+k, \quad y+j = -4x, \quad -3x = z+l.$

A long and straightforward check shows that there is no solution.

REFERENCES

[1] M. Blaum and R. M. Roth, "New array codes for multiple phased burst correction," *IEEE Trans. Inform. Theory*, vol. 39, pp. 66–77, Jan. 1993.

[2] R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 21–28, Jan. 1962.

[3] J. L. Fan, "Array codes as low-desity parity-check codes," in *Proc. 2nd Int. Symp. Turbo Codes*, Brest, France, Sept. 4–7, 2000, pp. 543–546.

[4] D. J. C. MacKay. Encyclopedia of Sparse Graph Codes. [Online]. Available: http://wol.ra.phy.cam.ac.uk/mackay/codes/data.html

[5] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *Electron. Lett.*, vol. 32, pp. 1645–1646, Aug. 1996.

[6] T. Mittelholzer, "Efficient encoding and minimum distance bounds of Reed-Solomon-type array codes," in *Proc. 2002 IEEE Int. Symp. Information Theory (ISIT 2002)*, Lausanne, Switzerland, June/July 2002, p. 282.

[7] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity check codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 619–637, Feb. 2001.

[8] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 533–547, Sept. 1981.

[9] ——, "Minimum-distance bounds by graph analysis," *IEEE Trans. Inform. Theory*, vol. 47, pp. 808–821, Feb. 2001.

Binary and Quadriphase Sequences With Optimal Autocorrelation Properties: A Survey

H. Dieter Lüke, *Senior Member, IEEE*,
Hans D. Schotten, *Member, IEEE*, and Hafez Hadinejad-Mahram

***Abstract*—Time-discrete signals with good autocorrelation properties are used in various applications in communications engineering. From an implementation point of view, usually sequences with a small phase alphabet and a maximal energy efficiency, i.e., a uniform envelope, are most favorable. For this reason, known methods as well as several new construction techniques of binary and quadriphase sequences with optimal or best known autocorrelation properties are discussed in this correspondence. In many cases, the achievable correlation properties can be improved significantly if a single zero element per sequence is accepted. These "almost" binary and "almost" quadriphase sequences are considered as well.**

The optimality criteria used include the maximum absolute sidelobe and the merit factor of the periodic and the odd-periodic autocorrelation function, respectively. For sequence lengths of up to 44 in the binary case and up to 32 in the quadriphase case, the best known parameters obtained by computer search are compared with the constructed results.

***Index Terms*—Binary sequences, optimal correlation properties, quadriphase sequences, sequence tables.**

I. INTRODUCTION

For many applications in measurement, digital communications, and continuous-wave (CW) radar where the desired information is extracted from the received signal using the periodic autocorrelation, it is desirable to use binary sequences whose periodic autocorrelation function (PACF) sidelobes are all zero [1], [2]. However, since such binary sequences with perfect PACF are not known (except for a sequence of length 4) it is necessary to find sequences whose PACF is "as perfect as possible." Additionally, depending on the application, other types of sequences such as polyphase and multivalued sequences and other autocorrelation functions such as the odd-periodic

Manuscript received November 7, 2000; revised July 2, 2003.

H. D. Lüke and H. Hadinejad-Mahram are with the Institute of Communications Engineering of the Aachen University of Technology, 52074 Aachen, Germany (e-mail: lueke@ient.rwth-aachen.de; hafez@ient.rwth-aachen.de).

H. D. Schotten is with Qualcomm CDMA Technologies GmbH, 90411 Nuremberg, Germany (e-mail: hschotte@qualcomm.com).

Communicated by A. M. Klapper, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2003.820035

0018-9448/03$17.00 © 2003 IEEE