| **Title**       | Linear size optimal q-ary constant-weight codes and constant-composition codes |
|-----------------|---------------------------------------------------------------------------------|
| **Author(s)**   | Chee, Yeow Meng; Dau, Son Hoang; Ling, Alan C. H.; Ling, San                     |
| **Citation**    | Chee, Y. M., Dau, S. H., Ling, A. C. H., & Ling, S. (2010). Linear size optimal q-ary constant-weight codes and constant-composition codes. IEEE Transactions on Information Theory, 56 (1), 140-151. |
| **Date**        | 2009                                                                            |
| **URL**         | http://hdl.handle.net/10220/7637                                                |
| **Rights**      | © 2009 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: http://dx.doi.org/10.1109/TIT.2009.2034814. |
Abstract—An optimal constant-composition or constant-weight code of weight \( w \) has linear size if and only if its distance \( d \) is at least \( 2w - 1 \). When \( d \geq 2w \), the determination of the exact size of such a constant-composition or constant-weight code is trivial, but the case of \( d = 2w - 1 \) has been solved previously only for binary and ternary constant-composition and constant-weight codes, and for some sporadic instances.

This paper provides a construction for quasicyclic optimal constant-composition and constant-weight codes of weight \( w \) and distance \( 2w - 1 \) based on a new generalization of difference triangle sets. As a result, the sizes of optimal constant-composition codes and optimal constant-weight codes of weight \( w \) and distance \( 2w - 1 \) are determined for all such codes of sufficiently large lengths. This solves an open problem of Etzion.

The sizes of optimal constant-composition codes of weight \( w \) and distance \( 2w - 1 \) are also determined for all \( w \leq 6 \), except in two cases.

Index Terms—constant-composition codes, constant-weight codes, difference triangle sets, generalized Steiner systems, Golomb rulers, quasicyclic codes

I. INTRODUCTION

There are two generalizations of binary constant-weight codes as we enlarge the alphabet beyond size two. These are the classes of constant-composition codes and \( q \)-ary constant-weight codes. While a vast amount of knowledge exists for binary constant-weight codes \([1]–[4]\), relatively little is known about constant-composition codes and \( q \)-ary constant-weight codes. Recently, these classes of codes have attracted some attention \([5]–[20]\) due to several important applications requiring nonbinary alphabets, such as in determining the zero error decision feedback capacity of discrete memoryless channels \([21]\), multiple access communications \([22]\), spherical codes for modulation \([23]\), DNA codes \([24]–[26]\), powerline communications \([10], [11]\), frequency hopping \([27]\), and coding for bandwidth-limited channels \([28]\).

As in the case of binary constant-weight codes, the determination of the maximum size of a constant-composition code or a \( q \)-ary constant-weight code of length \( n \) given constraints on its distance, weight and/or composition, constitutes a central problem in their investigation.

The ring \( \mathbb{Z}/q\mathbb{Z} \) is denoted by \( \mathbb{Z}_q \). For integers \( m \leq n \), the set of integers \( \{m, m+1, \ldots, n\} \) is denoted \([m,n]\). The set \([1,n]\) is further abbreviated to \([n]\). A partition \( \lambda = [\lambda_1, \ldots, \lambda_N] \) of integers such that \( \lambda_1 \geq \cdots \geq \lambda_N \geq 1 \). The \( \lambda_i \)’s are the parts of the partition. Disjoint set union is denoted by \( \sqcup \).

If \( X \) and \( R \) are sets, \( X \) finite, then \( R^X \) denotes the set of vectors of length \(|X|\), where each component of a vector \( u \in R^X \) has value in \( R \) and is indexed by an element of \( X \), that is, \( u = (u_x)_{x \in X} \). A \( q \)-ary code of length \( n \) is a set \( C \subseteq \mathbb{Z}_q^n \) for some \( X \) of size \( n \). The elements of \( C \) are called codewords. The support of a vector \( u \in \mathbb{Z}_q^n \), denoted \( \text{supp}(u) \), is the set \( \{x \in X : u_x \neq 0\} \). The Hamming norm or weight of \( u \in \mathbb{Z}_q^n \) is defined as \(|u| = |\text{supp}(u)| \). The distance induced by this norm is called the Hamming distance, denoted \( d_H(\cdot, \cdot) \), so that \( d_H(u,v) = |u - v| \), for \( u, v \in \mathbb{Z}_q^n \). A code \( C \) is said to have distance \( d \) if \( d_H(u,v) \geq d \) for all distinct \( u, v \in C \). The composition of a vector \( u \in \mathbb{Z}_q^n \) is the tuple \( \overrightarrow{|u|} = [w_1, \ldots, w_{q-1}] \), where \( w_i = |\{x \in X : u_x = i\}| \), \( i \in \mathbb{Z}_q \setminus \{0\} \). A code \( C \) is said to have constant weight \( w \) if every codeword in \( C \) has weight \( w \), and is said to have constant composition \( \overrightarrow{|u|} \) if every codeword in \( C \) has composition \( \overrightarrow{|u|} \). Hence, every constant-composition code is a constant-weight code. We refer to a \( q \)-ary code of length \( n \), distance \( d \), and constant weight \( w \) as an \( (n,d,w)_{q^{\text{c}}} \)-code.

In addition, the code has constant composition \( \overrightarrow{|u|} \), then it is referred to as an \( (n,d,\overrightarrow{|u|})_{q^{\text{c}}} \)-code. An \( (n,d,w)_{q^{\text{c}}} \)-code and an \( (n,d,\overrightarrow{|w|})_{2^{\text{c}}} \)-code coincide in definition, and are binary constant-weight codes. The maximum size of an \( (n,d,w)_{q^{\text{c}}} \)-code is denoted \( A_q(n,d,w) \) and that of an \( (n,d,\overrightarrow{|w|})_{2^{\text{c}}} \)-code is denoted \( A_q(n,d,\overrightarrow{|w|}) \). Any \( (n,d,w)_{q^{\text{c}}} \)-code or \( (n,d,\overrightarrow{|w|})_{2^{\text{c}}} \)-code attaining the maximum size is called optimal.

The following operations do not affect distance and composition properties of an \( (n,d,\overrightarrow{|w|})_{q^{\text{c}}} \)-code:

1) reordering the components of \( \overrightarrow{|u|} \), and
2) deleting zero components of \( \overrightarrow{|u|} \).

Consequently, throughout this paper, attention is restricted to those compositions \( \overrightarrow{|u|} = [w_1, \ldots, w_{q-1}] \), where \( w_1 \geq \cdots \geq w_{q-1} \geq 1 \), that is, \( \overrightarrow{|u|} \) is a partition. For succinctness, the sum \( \sum_{i=1}^{q-1} w_i \) of all the parts of a partition \( \overrightarrow{|u|} = [w_1, \ldots, w_{q-1}] \) is denoted by \( \sum \overrightarrow{|u|} \).

The focus of this paper is on determining \( A_q(n,d,w) \) and \( A_q(n,d,\overrightarrow{|w|}) \) for those \( d, w \) and \( \overrightarrow{|w|} \) for which \( A_q(n,d,w) = O(n) \) and \( A_q(n,d,\overrightarrow{|w|}) = O(n) \).

The Johnson-type bound of Svanström for ternary constant-composition codes \([5]\) Theorem 1) extends easily to the

Linear Size Optimal \( q \)-ary Constant-Weight Codes and Constant-Composition Codes

Yeow Meng Chee, Senior Member, IEEE, Son Hoang Dau, Alan C. H. Ling, and San Ling
following (see also \cite{27} Proposition 1.3):

**Proposition 1.1 (Johnson Bound):**
\[ A_q(n, d, [w_1, w_2, \ldots, w_{q-1}]) \leq \left\lfloor \frac{n}{w_1} A_q(n - 1, d, [w_1 - 1, w_2, \ldots, w_{q-1}]) \right\rfloor. \]

The following Johnson-type bound for q-ary constant-weight codes was established in \cite{6} Theorem 10.

**Proposition 1.2 (Johnson Bound):**
\[ A_q(n, d, w) \leq \left\lfloor \frac{n(q - 1)}{w} A_q(n - 1, d, w - 1) \right\rfloor. \]

**Definition 1.1 (Refinement):** A partition \( \overline{\omega} = [w_1, \ldots, w_q] \) is a refinement of \( \overline{\sigma} = [v_1, \ldots, v_p] \) (written \( \overline{\omega} \gg \overline{\sigma} \)) if there exist pairwise disjoint sets \( I_1, \ldots, I_p \subseteq [q] \) satisfying \( \bigcup_{j \in [q]} I_j = [q] \) such that \( \sum_{i \in I_j} w_i = v_j \) for each \( j \in [q] \).

Chu et al. \cite{27} made the following observation.

**Lemma 1.1:** If \( \overline{\omega} \gg \overline{\sigma} \), then \( A_q(n, d, \overline{\omega}) \geq A_q(n, d, \overline{\sigma}) \).

Given \( q \) and \( w \), the condition for \( A_q(n, d, \overline{\omega}) = O(n) \) to hold can be characterized as follows.

**Proposition 1.3:** \( A_q(n, d, \overline{\omega}) = O(n) \) if and only if \( d \geq 2 \sum w - 1 \).

**Proof:** \( A_q(n, d, \overline{\omega}) = O(n) \) when \( d \geq 2 \sum w - 1 \) follows easily from the Johnson bound.

Rödl’s proof \cite{29} of the Erdős-Hanani conjecture \cite{30} implies that \( A_2(n, d, w) = (1 - o(1))(\frac{w}{d+2})^{n/2} \), so that \( A_2(n, d, w) = \Omega(n^2) \) for all \( d \leq 2w - 2 \). Therefore, by Lemma 1.1, \( A_q(n, d, \overline{\omega}) = \Omega(n^2) \) for all \( d \leq 2 \sum w - 2 \).

A similar proof yields:

**Proposition 1.4:** \( A_q(n, d, w) = O(n) \) if and only if \( d \geq 2w - 1 \).

**A. Problem Status and Contribution**

For constant-composition codes, it is trivial to see that

\[ A_q(n, d, \overline{\omega}) = \begin{cases} 1, & \text{if } d \geq 2 \sum w + 1 \\ \lfloor n/\sum w \rfloor, & \text{if } d = 2 \sum w. \end{cases} \]

When \( d = 2 \sum w - 1 \), our knowledge of \( A_q(n, d, \overline{\omega}) \) is limited. We know that \( A_2(n, 2w - 1, w) = A_2(n, 2w, w) = \lfloor n/w \rfloor \), trivially. \( A_q(n, 2 \sum w - 1, \overline{\omega}) \) has also been completely determined by Svanström et al. \cite{7}. In particular, \( A_3(n, 2 \sum w - 1, \overline{\omega}) = \lfloor n/w_1 \rfloor \) holds for all \( n \) sufficiently large. Beyond this (for \( q \geq 4 \)), \( A_q(n, 2 \sum w - 1, \overline{\omega}) \) has not been determined, except in one instance: \( A_q(n, 5, [1, 1, 1, 1]) = n \) for \( n \geq 7 \), established by Chee et al. \cite{13}.

For constant-weight codes, we have

\[ A_q(n, d, w) = \begin{cases} 1, & \text{if } d \geq 2w + 1 \\ \lfloor n/w \rfloor, & \text{if } d = 2w. \end{cases} \]

An explicit formula for \( A_3(n, 2w - 1, w) \) has been obtained by Őstergård and Svanström \cite{6}. When \( q \geq 4 \), the value of \( A_q(n, 2w - 1, w) \) is not known.

The main contribution of this paper is the following two results.

**Main Theorem 1:** Let \( \overline{\omega} = [w_1, \ldots, w_{q-1}] \). Then \( A_q(n, 2 \sum w - 1, \overline{\omega}) = \lfloor n/w \rfloor \) for all sufficiently large \( n \).

**Main Theorem 2:** \( A_q(n, 2w - 1, w) = (q - 1)n/w \) for all sufficiently large \( n \) satisfying \( w|(q - 1)n \).

In particular, Main Theorem 2 solves an open problem of Etiyaz concerning generalized Steiner systems \cite{31} Problem 7.

The optimal constant-weight and constant-composition codes constructed in the proofs of Main Theorem 1 and Main Theorem 2 are quasicyclic, and are obtained from difference triangle sets and their generalization.

**II. QUASICYCLIC CODES**

A code is quasicyclic if there exists an \( \ell \) such that a cyclic shift of a codeword by \( \ell \) places is another codeword. More formally, let \( X = Z_n \) and define on \( Z_n^q \) the cyclic shift operator \( T : (u_x)_{x \in X} \mapsto (u_{x+1})_{x \in X} \). A q-ary code \( C \subset Z_n^q \) of length \( n \) is quasicyclic (or more precisely, \( \ell \)-quasicyclic) if it is invariant under \( T^{\ell} \) for some integer \( \ell \in [n] \). If \( \ell = 1 \), such a code is just a cyclic code.

The following two conditions are necessary and sufficient for a code \( C \) of constant weight \( w \) to have distance \( 2w - 1 \).

(C1) For any distinct \( u, v \in C \), \( |\text{supp}(u) \cap \text{supp}(v)| \leq 1 \).

(C2) For any distinct \( u, v \in C \), if \( x \in \text{supp}(u) \cap \text{supp}(v) \), then \( u_x \neq v_x \).

A. Quasicyclic Constant-Composition Codes

The strategy for proving Main Theorem 1 is to construct optimal \( (n, 2 \sum w - 1, \overline{\omega})_q \)-codes (meeting the Johnson bound) that are \( w_1 \)-quasicyclic when \( n \equiv 0 \pmod{w_1} \). Optimal \( (n, 2 \sum w - 1, \overline{\omega})_q \)-codes, \( n \not\equiv 0 \pmod{w_1} \), can be obtained easily from those with \( n \equiv 0 \pmod{w_1} \) by lengthening, as in the lemma below.

**Lemma 2.1 (Lengthening):** If \( A_q(n, 2 \sum w - 1, \overline{\omega}) = \lfloor n/w_1 \rfloor \) and \( n \equiv 0 \pmod{w_1} \), then \( A_q(n + i, 2 \sum w - 1, \overline{\omega}) = \lfloor n/w_1 \rfloor \) for all \( i, 0 \leq i < w_1 \).

**Proof:** Let \( C \subset Z_n^q \) be an \( (n, 2 \sum w - 1, \overline{\omega})_q \)-code of size \( \lfloor n/w_1 \rfloor \). Let \( X' = X \cup \{x_1, \ldots, x_i\} \), where \( \{x_1, \ldots, x_i\} \not\subset X \), and define \( C' \subset Z_n^{X'} \) such that \( C' = \{(c(u))_{u \in X'} : u \in C\} \), where

\[ c(u)_x = \begin{cases} u_x, & \text{if } x \in X \\ 0, & \text{if } x \in \{x_1, \ldots, x_i\}. \end{cases} \]
Then $C'$ is an \((n + i, 2\sum_1^n - 1, \overline{m})_q\)-code of size \(|n/w_1|\). Since \(\left(\frac{n + i}{w_1}\right) = \left|\frac{n}{w_1}\right|\), $C'$ is optimal by the Johnson bound.

As opposed to lengthening a code, we can also shorten a code by selecting a position \(i\), remove those codewords with a nonzero coordinate \(i\), and deleting the \(i\)th coordinate from every remaining codeword.

Let \(n \equiv 0 \pmod{w_1}\). A \(w_1\)-quasicyclic \((n, 2\sum_1^n - 1, \overline{m})_q\)-code $C$ of size \(n/w_1\) can be obtained by developing a particular vector $g \in \mathbb{Z}^X_q$:

\[
C = \{T^i w_1^j(g) : i \in [0, n/w_1 - 1]\}.
\]

Such a vector $g$ is called a base codeword of the quasicyclic code $C$. The remainder of this section develops criteria for a vector $g \in \mathbb{Z}^X_q$ of composition $\overline{w}$ to be a base codeword of a $w_1$-quasicyclic \((n, 2\sum_1^n - 1, \overline{m})_q\)-code, \(n \equiv 0 \pmod{w_1}\).

The conditions (C1) and (C2) may be stated in terms of the base codeword $g$ as follows.

(C3) For $w, x, y, z \in \text{supp}(g)$ such that $w \neq x, y \neq z,$ and \(\{w, x\} \neq \{y, z\}\), we have:
- if $w - x \equiv 0 \pmod{w_1}$, then $2(x - w) \not\equiv 0 \pmod{n}$;
- if $y - z \equiv 0 \pmod{w_1}$, then $w - x \not\equiv z - y \pmod{n}$.

(C4) If $g_x = g_y \neq 0$, then $x - y \not\equiv 0 \pmod{w_1}$.

B. Quasicyclic Constant-Weight Codes

**Lemma 2.2:** Let $n \geq w > 0$ and $q \geq 2$. Then $w | (q - 1)n$ if and only if there exist positive integers $\alpha, \beta, \ell$ and $m$ such that $n = \alpha \ell, w = \beta \ell$, and $q - 1 = m \beta$.

**Proof:** Assume that $w | (q - 1)n$. Let $\ell = \gcd(w, n)$, and let $\alpha = n/\ell, \beta = w/\ell$. Then $\gcd(\alpha, \beta) = 1$. Since $w | (q - 1)n$, we have $\beta \ell | (q - 1)\alpha \ell$. Hence, $\beta | (q - 1)$. Now let $m = (q - 1)/\beta$.

The converse is obvious.

**Proposition 3.1:** Let $X = [\lambda_1, \ldots, \lambda_N]$ be a partition. A $X$-array is a $\lambda_1 \times N$ array $B$ with rows indexed by $i \in [\lambda_1]$ and columns indexed by $j \in [N]$, such that

- (P1) each cell is either empty or contains a nonnegative integer congruent to its row index modulo $\lambda_1$;
- (P2) the number of nonempty cells in column $j$ is $\lambda_j$;
- (P3) if $B_i = \{b_{i,1}, \ldots, b_{i,N}\}$ is the set of entries in row $i$ of $B$, then the differences $b_{i,j} - b_{i,j'}$, $i \in [N], 1 \leq j' \neq j \leq N_i$, are all nonzero and distinct.

The scope of $B$ is

$$\sigma(B) = \max_{1 \leq i \leq \lambda_1} \{\{b_{i,j} - b_{i,j'} : 1 \leq j' \neq j \leq N_i\} \cup \{[b_{i,j}/\ell] : j \in [N_i]\}\}.$$  

In particular, if $\lambda_1 = \cdots = \lambda_N = \lambda$, then a $X$-array $B$ has all cells nonempty, and is referred to as a $(\lambda, N)$-array. From the definition, it is easy to see that the entries of a $X$-array are all distinct.

**Example 3.1:** A $(3, 2, 2)$-array of scope 15:

$$
\begin{array}{ccc}
1 & 7 & 16 \\
2 & 14 \\
0 & 3
\end{array}
$$

**Example 3.2:** A $(2, 4)$-array of scope 42:

$$
\begin{array}{cccc}
19 & 23 & 35 & 61 \\
0 & 6 & 20 & 30
\end{array}
$$

**Proposition 3.1:** Let $\overline{w} = [w_1, \ldots, w_q - 1]$. If there exists a $\overline{w}$-array $B$, then there exists a $w_1$-quasicyclic optimal \((n, 2\sum_1^n - 1, \overline{m})_q\)-code for all $n \equiv 0 \pmod{w_1}, n \geq 2\sigma(B) + 1$.

**Proof:** Let $B$ be a $\overline{w}$-array and let $C_j$ denote the set of entries in column $j$ of $B$, $j \in [q - 1]$. Define a vector $g \in \mathbb{Z}_{\overline{w}}^N$.

Then $g$ has composition $\overline{w}$ and satisfies conditions (C3) and (C4). Therefore $g$ is a base codeword of a $w_1$-quasicyclic optimal \((n, 2\sum_1^n - 1, \overline{m})_q\)-code.
Example 3.3: The $[3, 2, 2]$-array in Example 3.1 gives the base codeword
\[ g = 11120002000003030n^{n-17} \]
for a 3-quasicyclic optimal $(n, 13, [3, 2, 2])_4$-code when $n \equiv 0 \pmod{3}$, $n \geq 33$.

Proposition 3.2: Suppose that $w = \beta \ell$ and $q - 1 = m \beta$. If there exists an $(\ell, q - 1)$-array B, then there exists an $\ell$-quasicyclic optimal $(n, 2w - 1, w)_{\ell}$-code of size $(q - 1)n/w = mn/\ell$, provided that $\ell | n$ and $n \geq 2\sigma(B) + 1$.

Proof: Let $B$ be an $(\ell, q - 1)$-array and let $C_i$ denote the set of entries in column $i$ of $B$, $i \in [q - 1]$. We define the $m$ vectors $g^{(1)}, \ldots, g^{(m)}$ as follows: for $j \in [m]$ and $0 \leq z \leq n - 1$,
\[ g_z^{(j)} = \begin{cases} r, & \text{if } z \in C_r \text{ for some } r \in [(j - 1)\beta + 1, j\beta] \\ 0, & \text{otherwise.} \end{cases} \tag{1} \]
Since the entries of B are distinct, $g_z^{(j)}$ is well-defined. Moreover, the set of nonzero entries of $g^{(j)}$ is precisely $[(j - 1)\beta + 1, j\beta]$, and by property (P2), each symbol in $[(j - 1)\beta + 1, j\beta]$ occurs exactly $\ell$ times in $g^{(j)}$. Therefore, $g_z^{(j)} \in \mathbb{Z}_{\ell}^n$ and has weight $w = \beta \ell$. We claim that the $m$ vectors $g^{(1)}, \ldots, g^{(m)}$ satisfy conditions (C5)–(C7), and hence form the base codewords for an $\ell$-quasicyclic optimal $(n, 2w - 1, w)_{\ell}$-code. The following establishes this claim.

First, suppose that $i \neq j$. If $g_z^{(i)}$ and $g_z^{(j)}$ are nonzero, then $g_z^{(i)} \in [(i - 1)\beta + 1, i\beta]$ and $g_z^{(j)} \in [(j - 1)\beta + 1, j\beta]$. Since $i \neq j$, we have $g_z^{(i)} \neq g_z^{(j)}$. Therefore (C7) is satisfied.

Next, suppose that $z \neq y$ and $g_z^{(j)} = g_y^{(j)} = r \neq 0$. By (1), $z, y \in C_r$. Since $z \neq y$, $z$ and $y$ must belong to different rows of $B$. Therefore, $z \neq y \pmod{\ell}$ by (P1). Thus, $g_z^{(1)}, \ldots, g_z^{(m)}$ satisfy (C6).

Now suppose that $w, x \in \text{supp}(g_z^{(i)}), w \neq x$. By (1), there exist $r_w$ and $r_x$ such that $w \in C_{r_w}$ and $x \in C_{r_x}$. If $x - w \equiv 0 \pmod{\ell}$, then by (P1), $x$ and $w$ are in the same row of $B$. Therefore,
\[ 0 < |x - w| \leq \sigma(B), \]
and hence,
\[ 0 < 2|x - w| \leq 2\sigma(B) < 1 + 2\sigma(B) \leq n. \]
It follows that $2|x - w| \neq 0 \pmod{n}$.

Let $w, x \in \text{supp}(g_z^{(i)})$ and $y, z \in \text{supp}(g_z^{(j)})$, where $w \neq x$, $y \neq z$ such that $y - w \equiv 0 \pmod{\ell}$, and if $i = j$ then $\{w, x\} \neq \{y, z\}$. We want to show that
\[ x - w \equiv z - y \pmod{\ell}, \]
or equivalently,
\[ y - w \equiv z - x \pmod{\ell}. \tag{2} \]
Again, by (1), $w, x, y,$ and $z$ are entries of $B$. Moreover, $w$ and $y$ are in the same row. We consider two cases.

Case $w \neq y$ Since $0 < |y - w| \leq \sigma(B) < n$, we have $y - w \equiv 0 \pmod{n}$. Therefore, if $x = z$, then (2) holds. If $x \neq z$ and both $x$ and $z$ are in the same row, then (2) holds by property (P3) of $B$ and the assumption that $y \neq z$ and $n \geq 2\sigma(B) + 1$. If $x$ and $z$ are in different rows, then by (P1), $z - x \equiv 0 \pmod{\ell}$. Since $y - w \equiv 0 \pmod{\ell}$ and $\ell | n$, (2) follows.

Case $w = y$ We claim that $i = j$. Indeed, assume that $y \in C_{r_y}$ and $w \in C_{r_w}$. Then $r_y \in [(j - 1)\beta + 1, j\beta]$ and $r_w \in [(i - 1)\beta + 1, i\beta]$. Hence, if $i \neq j$, then $r_y \neq r_w$. Therefore, there are two entries in different columns of $B$ that have the same value $y$, which is a contradiction. Hence, $i = j$. Since $\{w, x\} \neq \{y, z\}$, we have $x \neq z$. Therefore, (2) holds.

Consequently, $g^{(1)}, \ldots, g^{(m)}$ satisfy (C5).

Example 3.4: The $(2, 4)$-array of scope 42 in Example 3.2 gives $g^{(1)}$ and $g^{(2)}$, where
\[ g^{(1)}_z = \begin{cases} 1, & \text{if } z \in \{0, 19\} \\ 2, & \text{if } z \in \{6, 23\} \\ 0, & \text{otherwise,} \end{cases} \]
\[ g^{(2)}_z = \begin{cases} 3, & \text{if } z \in \{20, 35\} \\ 4, & \text{if } z \in \{30, 61\} \\ 0, & \text{otherwise.} \end{cases} \]
In this case, $q = 5$, $w = 4$, $\beta = 2$, $\ell = 2$, and $m = 2$. The vectors $g^{(1)}$ and $g^{(2)}$ form the base codewords of a 2-quasicyclic optimal $(n, 7, 4)_5$-code when $n$ is even and $n \geq 85 = 2 \times 42 + 1$.

In view of Proposition 3.1 and Proposition 3.2 to prove Main Theorem 1 and Main Theorem 2, it suffices to construct a $\bar{X}$-array for every partition $\bar{X}$.

IV. GENERALIZED DIFFERENCE TRIANGLE SETS

In this section, the concept of difference triangle sets is generalized and used to produce $\bar{X}$-arrays. We begin with the definition of a difference triangle set.

Definition 4.1: An $(I, J)$-difference triangle set $(D\Delta S)$ is a set $A = \{A_1, \ldots, A_I\}$, where $A_i = \{a_{i,1}, \ldots, a_{i,J}\}$, $0 = a_{i,1} < \cdots < a_{i,J}$, are lists of integers such that the differences $a_{i,j} - a_{i,j'}$, $i \in [I]$, $1 \leq j' \neq j \leq J$, are all distinct.

Example 4.1: A $(3, 4)$-D\Delta S:
\[ \{\{0, 1, 10, 18\}, \{0, 2, 7, 13\}, \{0, 3, 15, 19\}\}. \]
The corresponding differences are displayed in triangular arrays below:
\[
\begin{array}{cccccccc}
1 & 10 & 18 & 2 & 7 & 13 & 3 & 15 & 19 \\
9 & 17 & 5 & 11 & 12 & 16 & 8 & 6 & 4
\end{array}
\]
The scope of an $(I, J)$-D\Delta S $A = \{A_1, \ldots, A_I\}$ is
\[ m(A) = \max_{a \in A} \{a \in A\}. \]
Difference triangle sets with scope as small as possible are often required for applications. Define

\[ M(I, J) = \min\{m(A) : A \in \text{an (I, J)-}\Delta S\} \]

Difference triangle sets were introduced by Kløve [32, 33] and have numerous applications [34–40]. A (1, J)-\(\Delta S\) is known as a Golomb ruler with \(J\) marks.

We generalize difference triangle sets as follows.

**Definition 4.2:** Let \(\mathcal{J} = [J_1, \ldots, J_f]\) be a partition. A set \(A = \{A_1, \ldots, A_f\}\) with \(A_i = \{a_{i1}, \ldots, a_{ii}\}\), \(0 = a_{i1} < \cdots < a_{ii}\), is a \(\mathcal{J}\)-generalized difference triangle set (GD\(\Delta S\)) if the differences \(a_{ij} - a_{ij'}\), \(i \in [I]\), \(1 \leq j' \neq j \leq I_i\), are all distinct.

Thus, a GD\(\Delta S\) is similar to a D\(\Delta S\), but allowing the sets to be of different sizes. In particular, if \(J_1 = \cdots = J_k = J\), then a \(\mathcal{J}\)-GD\(\Delta S\) is an \((I, J)\)-D\(\Delta S\). The scope of a GD\(\Delta S\) \(A = \{A_1, \ldots, A_f\}\) is defined similarly as for a D\(\Delta S\):

\[ m(A) = \max_{a \in A} a \]

We now relate \(\mathcal{J}\)-GD\(\Delta S\) to \(\lambda\)-arrays. Let \(\lambda = [\lambda_1, \ldots, \lambda_N]\) be a partition. The Ferrers diagram of \(\lambda\) is an array of cells with \(N\) left-justified rows and \(\lambda_i\) cells in row \(i\). The conjugate of \(\lambda\) is the partition \(\lambda^\prime = [\lambda_1^\prime, \ldots, \lambda_N^\prime]\), where \(\lambda_i^\prime\) is the number of parts of \(\lambda\) that are at least \(j\). \(\lambda^\prime\) can also be obtained by reflecting the Ferrers diagram of \(\lambda\) along its main diagonal. Conjugation of partitions is an involution.

**Example 4.2:** The Ferrers diagrams of the partition \([5, 3, 3, 2]\) and its conjugate \([4, 4, 3, 1, 1]\) are shown respectively below:

![Ferrers diagrams](image)

**Proposition 4.1:** Let \(\lambda = [\lambda_1, \ldots, \lambda_N]\) be a partition. If there exists a \(\lambda^\prime\)-GD\(\Delta S\) of scope \(s\), then there exists a \(\lambda\)-array of scope at most \(s\lambda_1\).

**Proof:** Let \(\lambda^\prime = [\lambda_1^\prime, \ldots, \lambda_N^\prime]\) and let \(A = \{A_1, \ldots, A_f\}\) be a \(\lambda^\prime\)-GD\(\Delta S\) of scope \(s\). Construct a \(\lambda\times N\) array \(B\) as follows: If \(A_i = \{a_{i1}, \ldots, a_{ii}\}\), then the \((i,j)\)th cell of \(B\), \(i \in [\lambda_1], j \in [N]\), contains \(b_{ij} = a_{i1}\lambda_1 + (i \mod \lambda_1)\) if \(j \in [\lambda_i^\prime]\), and empty otherwise. Then the filled cells of \(B\) take the shape of the Ferrers diagram of \(\lambda^\prime\). Thus, the number of nonempty cells in column \(j\) of \(B\) is precisely \(\lambda_j\). It is also easy to see that each entry in row \(i\) of \(B\) is congruent to \(i \mod \lambda_1\). The differences \(b_{ij} - b_{ij'}\) are all distinct because the differences \(a_{ij} - a_{ij'}\) are all distinct in the GD\(\Delta S\) \(A\). Moreover, all of these differences are at most \(s\lambda_1\). Finally, for any \(i \in [\lambda_1]\) and \(j \in [\lambda_i^\prime]\),

\[ \left[ \frac{b_{ij}}{2} \right] \leq \left[ \frac{s\lambda_1 + (\lambda_1 - 1)}{2} \right] \leq \frac{s\lambda_1 + \lambda_1}{2} \leq s\lambda_1. \]

Therefore \(B\) is a \(\lambda\)-array of scope at most \(s\lambda_1\).

**Corollary 4.1:** If there exists a \((\lambda, N)\)-GD\(\Delta S\) of scope \(s\), then there exists a \((\lambda, N)\)-array of scope at most \(s\lambda\).

**Example 4.3:** Since \([3, 3, 2, 2]^* = [4, 4, 2]\), we can construct a \([3, 3, 2, 2]^*\)-array from a \([4, 4, 2]\)-GD\(\Delta S\) via the proof of Proposition 4.1. If the \([4, 4, 2]\)-GD\(\Delta S\) is \(A = \{0, 1, 10, 18\}, \{0, 2, 7, 13\}, \{0, 3\}\), the \([3, 3, 2, 2]^*\)-array obtained is

|   |   |   |   |
|---|---|---|---|
| 1 | 4 | 31 | 55 |
| 2 | 8 | 23 | 11 |
| 0 | 9 | 45 | 57 |

This array has scope 54.

**Example 4.4:** From the \((3, 4)\)-D\(\Delta S\) \(A = \{0, 1, 10, 18\}, \{0, 2, 7, 13\}, \{0, 3, 15, 19\}\), we can construct the following \((3, 4)\)-array via the proof of Proposition 4.1

|   |   |   |   |
|---|---|---|---|
| 1 | 4 | 31 | 55 |
| 2 | 8 | 23 | 11 |
| 0 | 9 | 45 | 57 |

This array has scope 57.

V. PROOFS OF THE MAIN THEOREMS

In this section, we use Golomb rulers to construct GD\(\Delta S\) and provide proofs to Main Theorem 1 and Main Theorem 2.

Let \(\varphi(x)\) denote the smallest prime power not smaller than \(x\). Atkinson et al. [40] Lemma 2 proved the following.

**Theorem 5.1:** \(M(1, J) \leq (J - 1)\varphi(J - 1)\).

**Proposition 5.1:** For any partition \(\mathcal{J} = [J_1, \ldots, J_f]\), there exists a \(\mathcal{J}\)-GD\(\Delta S\) of scope at most \((\sum \mathcal{J} - 1)\varphi(\sum \mathcal{J} - 1)\).

**Proof:** By Theorem 5.1 there exists a Golomb ruler \(\{R\}\) of \(\sum \mathcal{J}\) marks and scope \(m(\{R\}) \leq (\sum \mathcal{J} - 1)\varphi(\sum \mathcal{J} - 1)\). Partition \(R\) into \(I\) subsets, \(R = R_1 \sqcup \cdots \sqcup R_I\), where \(|R_i| = J_i\), \(i \in [I]\). Suppose \(R_i = \{r_{i1}, \ldots, r_{ij}\}\), where \(0 \leq r_{i1} < \cdots < r_{ij}\). For each \(i \in [I]\), let \(A_i = \{a_{i1}, \ldots, a_{ij}\}\), where \(a_{ij} = r_{ij} - r_{i1}\), \(j \in [J_i]\). Then the set \(A = \{A_1, \ldots, A_I\}\) forms a \(\mathcal{J}\)-GD\(\Delta S\) of scope \( m(A) \leq m(\{R\}) \leq (\sum \mathcal{J} - 1)\varphi(\sum \mathcal{J} - 1) \).

The following corollary is immediate.

**Corollary 5.1:** For any \(I > 0\) and \(J > 0\), there exists an \((I, J)\)-GD\(\Delta S\) of scope at most \((IJ - 1)\varphi(IJ - 1)\).
A. Proof of Main Theorem 1

Let \( \rho = [w_1, \ldots, w_{q-1}] \) be a partition and consider \( w^* = [w_1', \ldots, w_w'] \). By Proposition 4.1, there exists a \( w^* \)-GD\( \Delta S \) of scope at most \( (\sum w_i - 1)\rho(\sum w_i - 1) \). Therefore, by Proposition 4.1, there exists a \( \rho \)-array of scope at most \( w_1(\sum w_i - 1)\rho(\sum w_i - 1) \). Finally, Proposition 5.1 guarantees the existence of a \( \rho \)-quasicyclic optimal \((n, 2 \sum w_i - 1)\rho(\sum w_i - 1) \)-code of size \( n/w_1 \) for all \( n \equiv 0 \) (mod \( w_1 \)). This, together with Lemma 2.1 proves Main Theorem 1.

B. Proof of Main Theorem 2

Suppose \( w|(q-1)n \). Then by Lemma 2.2 let \( \beta = \sqrt{\ell} \), \( \beta \equiv (q-1) \). By Corollary 5.1, there exists an \((\ell, q-1)\)-D\( \Delta S \) of scope at most \( (\ell(q-1)-1)\equiv\ell(q-1)-1 \). Therefore, by Corollary 4.1, there exists an \((\ell, q-1)\)-array of scope at most \( \ell(q-1)-1\equiv\ell(q-1)-1 \). Finally, Proposition 5.1 guarantees the existence of an \( \ell \)-quasicyclic optimal \((n, 2-w_1+1)\)-code of size \( q\ell(\ell(q-1)-1) \) \( (\sum w_i - 1)\rho(\sum w_i - 1) \)-code of size \( n/w_1 \) for all \( n \equiv 0 \) (mod \( \ell(q-1)-1 \)). This proves Main Theorem 2.

VI. Resolution of an Open Problem of Etzion

A set system is a pair \( S = (X, B) \), where \( X \) is a finite set of points, and \( B \subseteq 2^X \). The elements of \( B \) are called blocks. The order of \( S \) is the number of points, \( |X| \). If \( |B| = k \) for all \( B \in B \), then \( S \) is said to be \( k \)-uniform. Let \( A \subseteq 2^X \). A transverse of \( A \) is a set \( T \subseteq X \) such that \( |T \cap A| \leq 1 \) for all \( A \in A \). Hanani [41] introduced the following generalization of t-designs.

**Definition 6.1:** An \( H(n, q, w, t) \) design is a triple \((X, \mathcal{G}, B)\), where \((X, B)\) is a \( w \)-uniform system of order \( nq \), \( \mathcal{G} = \{G_1, \ldots, G_n\} \) is a partition of \( X \) into \( n \) sets, each of cardinality \( q \), such that

(i) \( B \) is a transverse of \( \mathcal{G} \) for all \( B \in B \);

(ii) each \( t \)-element transverse of \( \mathcal{G} \) is contained in precisely one block of \( B \).

From an \( H(n, q, w, t) \) design \((X, \mathcal{G}, B)\), we can form a constant-weight code \( C \subseteq \mathbb{F}_q^{n+1} \) as follows. Let \( G_i = \{g_{i1}, g_{i2}, \ldots, g_{iq_i}\} \), where \( 0 \notin G_i \). The code \( C \) has a codeword for each block. Assume \( B = \{b_1,b_2,\ldots,b_w\} \) is a block of \( B \) (this block is denoted by \( \langle i_1,j_1 \rangle, \langle i_2,j_2 \rangle, \ldots, \langle i_w,j_w \rangle \)), where \( b_s = \gamma_{j_s,i_s} \). We form the codeword \( u \in C \) corresponding to \( B \) as follows: for \( i \in [n] \),

\[
\begin{align*}
    u_i &= \begin{cases} 
    j, & \text{if } b_{r} = \gamma_{j,i} \text{ for some } r \in [w] \\
    0, & \text{otherwise.}
    \end{cases}
\end{align*}
\]

The distance of \( C \) is at least \( w-t+1 \). If \( C \) has distance \( 2(w-t)+1 \), Etzion [31] calls the \( (n, q, w, t) \) design, from which \( C \) is constructed, a generalized Steiner system \( GS(t, w, n, q) \).

It is not hard to verify that a \( GS(t, w, n, q) \) contains exactly \( q^t(n) \) blocks. By the Johnson bound, we have

\[
A_{q+1}(n, 2(w-t) + 1, w) \leq q^t(n) \binom{w}{t}.
\]

It follows from the above construction that if a \( GS(t, w, n, q) \) exists, then

\[
A_{q+1}(n, 2(w-t) + 1, w) = q^t(n) \binom{w}{t}.
\]

The next result establishes the converse when \( q^t(n) \).

**Proposition 6.1:** Suppose that \( q^t(n) \). Then a \( GS(t, w, n, q) \) exists if

\[
A_{q+1}(n, 2(w-t) + 1, w) = q^t(n) \binom{w}{t}.
\]

**Proof:** Let \( C \) be an (optimal) \((n, 2(w-t)+1)\)-(w)\(-\)code of size \( \binom{n}{t} \). Define

\[
\begin{align*}
    X &= \{(i,j) : i \in [n] \text{ and } j \in [q]\} \\
    G &= \{G_i : i \in [n]\},
\end{align*}
\]

where \( G_i = \{(i,j) : j \in [q]\} \). We associate with each codeword \( u \in C \) a block \( B^u \subseteq X \) as follows:

\[
B^u = \{(i,j) : u_i = j, i \in [n], j \in [q]\}.
\]

Finally, let \( B = \{B^u : u \in C\} \).

We claim that \((X, G, B)\) is a \( GS(t, w, n, q) \). Indeed, \( |B| = w \) for all \( B \in B \), and \( |B \cap G_i| \leq 1 \) for all \( B \in B \) and \( i \in [n] \). Hence, it remains to show that any \( t \)-element transverse of \( G \) is contained in exactly one block of \( B \). Suppose \( B^u \) and \( B^{u'} \) are two different blocks containing a particular \( t \)-element transverse of \( G \). Then \( |\text{supp}(u) \cap \text{supp}(u')| \geq t \), implying \( d_H(u, v) \geq 2(w-t) < 2(w-t) + 1 \), a contradiction. Therefore, any \( t \)-element transverse of \( G \) is contained in at most one block, and hence in exactly one block, since \( |B| = |C| = \binom{n}{t} \binom{w}{t} \).}

**Corollary 6.1:** Suppose that \( \binom{w}{t} \). Then there exists a \( GS(t, w, n, q) \) if and only if

\[
A_{q+1}(n, 2(w-t) + 1, w) = q^t(n) \binom{w}{t}.
\]

Etzion [31] Problem 7] raised the following as an open problem for further research.

**Problem 6.1 (Etzion):** Given \( k \) and \( w \), show that there exists an \( n_0 \) such that for all \( n \geq n_0 \), where \( w|nk \), a \( GS(1, w, n, k) \) exists.

The following result, which is a direct consequence of Main Theorem 2 and Corollary 6.1, solves Problem 6.1.
**Theorem 6.1:** There exists a GS(1, w, n, k) for all sufficiently large n satisfying w|nk.

**Proof:** By Main Theorem 2, we have

\[ A_{k+1}(n, 2w - 1, w) = kn/w, \]

for all sufficiently large n satisfying w|kn. It follows immediately from Corollary 6.1 that there also exists a GS(1, w, n, k) for all sufficiently large n satisfying w|kn.

VII. **Explicit Bounds**

Main Theorem 1 and Main Theorem 2 are asymptotic statements: the hypothesis that n is sufficiently large must be satisfied. But how large must n be? More precisely, for a partition \( \overline{w} = [w_1, \ldots, w_{q-1}] \) and a positive integer w, define

\[ N_{ccc}(\overline{w}) = \min \left\{ n_0 : A_q(n, 2 \sum_i \overline{w} - 1, \overline{w}) = \left\lfloor \frac{n}{w} \right\rfloor \text{ for all } n \geq n_0 \right\}, \]

and

\[ N_{cwc}(w) = \min \left\{ n_0 : A_q(n, 2w - 1, w) = \frac{(q-1)n}{w} \text{ for all } n \geq n_0 \right\}, \]

for all n \geq n_0 satisfying \( w|(q-1)n \).

We give explicit bounds on \( N_{ccc}(\overline{w}) \) and \( N_{cwc}(w) \) in this section.

A. **Bounds on \( N_{ccc}(\overline{w}) \)**

The proof of Main Theorem 1 in Section VII-A shows that

\[ N_{ccc}(\overline{w}) \leq 2w_1 \left( \sum w - 1 \right) + 1. \tag{3} \]

By Bertrand’s postulate, \( \varphi(x) \leq 2x \) for all \( x \geq 1 \). For \( x \) sufficiently large, better asymptotic bounds on \( \varphi(x) \) exist (see for example [52]), but we are after quantifiable bounds. This implies

\[ N_{ccc}(\overline{w}) \leq 4w_1 \left( \sum w - 1 \right)^2 + 1. \]

We now prove a lower bound on \( N_{cwc}(w) \).

**Proposition 7.1:** Let \( \overline{w} = [w_1, \ldots, w_{q-1}] \) be a partition. If \( w_1 n \) and there exists an \( (n, 2 \sum_i w - 1, \overline{w})_q \)-code of size \( n/w_1 \), then \( n \geq w_1^2 k(k-1) + w_1 \), where \( k = \left\lfloor \sum w/w_1 \right\rfloor \). In particular, when \( w_1 = w_2 = \cdots = w_{q-1} \), we have \( n \geq w_1 + w_1^2 (q-1)(q-2) \).

**Proof:** Let \( C = \{u^{(i)} : i \in [n/w_1] \} \) be an \( (n, 2 \sum_i w - 1, \overline{w})_q \)-code of size \( n/w_1 \). Then \( C \) can be regarded as an \( n/w_1 \times n \) matrix \( C \), whose ith row is \( u^{(i)} \), \( i \in [n/w_1] \). Let \( N_i \) be the number of nonzero entries in column \( i \) of \( C \). Then \( \sum_{i=1}^n N_i = (n \sum w)/w_1 \). In each column of \( C \), we associate each pair of distinct nonzero entries with the pair of rows that contain these entries. There are \( \binom{N_i}{2} \) such pairs of nonzero entries in column \( i \) of \( C \). Therefore, there are \( \sum_{i=1}^n \binom{N_i}{2} \) such pairs in all the columns of \( C \). Since there are no pairs of distinct codewords in \( C \) whose supports intersect in two elements, the \( \sum_{i=1}^n \binom{N_i}{2} \) pairs of rows associated with the \( \sum_{i=1}^n \binom{N_i}{2} \) pairs of distinct nonzero entries are also all distinct. Hence,

\[ \sum_{i=1}^n \binom{N_i}{2} \leq \binom{|C|}{2} = \binom{n}{2}, \]

or equivalently,

\[ \sum_{i=1}^n N_i(N_i - 1) \leq \frac{n(n - w_1)}{w_1^2}. \tag{4} \]

Since \( k = \left\lfloor \sum w/w_1 \right\rfloor = \left\lfloor \binom{n}{2}/w_1 \right\rfloor/n \), there exists \( r \in [0, n - 1] \) such that

\[ \frac{n \sum w}{w_1} = kn + r. \]

As \( \sum_{i=1}^n N_i = (n \sum w)/w_1 \) we have

\[ \sum_{i=1}^n N_i(N_i - 1) \geq r(k+1) + (n-r)k(k-1) \geq nk(k-1). \tag{5} \]

From (4) and (5), we have

\[ \frac{n(n - w_1)}{w_1^2} \geq nk(k-1), \]

giving \( n \geq w_1^2 k(k-1) + w_1 \).

**Corollary 7.1:**

\[ \left( \sum w \right)^2 - w_1 \left( \sum w - 1 \right) \leq N_{ccc}(\overline{w}) \leq 4w_1 \left( \sum w - 1 \right)^2 + 1. \]

The upper and lower bounds on \( N_{ccc}(\overline{w}) \) in Corollary 7.1 differ approximately by a factor of \( 4w_1 \).

B. **Bounds on \( N_{cwc}(w) \)**

The proof of Main Theorem 2 in Section VII-B shows that

\[ N_{cwc}(w) \leq 2w(w(q-1) - 1)^2 + 1. \]

For constant-weight codes, the following result of Etzion [51] shows that \( N_{cwc}(w) \geq (w-1)(q-1) + 1 \).

**Proposition 7.2:** Given \( q \) and \( w \), if there exists an optimal \( (n, 2w-1, w)_q \)-code of size \( (q-1)n/w \), then \( n \geq (w-1)(q-1) + 1 \).

There is a considerable gap between these upper and lower bounds on \( N_{cwc}(w) \). However, when \( w|n \), a better upper bound can be obtained. We describe the construction below.

The idea of the construction is similar to the idea of the previous ones. We determine \( q - 1 \) base codewords, denoted \( g^{(1)}, \ldots, g^{(q-1)} \), for which the \( (n/w) \)-quasicyclic code

\[ C = \{T^{wj}(g^{(i)}) : i \in [q-1], j \in [0, n/w - 1]\}, \]

is an \( (n, 2w-1, w)_q \)-code. Let us write \( u \vdash^T g^{(i)} \) if \( u = T^{wj}(g^{(i)}) \) for some \( j \). Suppose that \( g^{(i)} \in \{0, i\}^n \) for \( i \in [q-1] \). Then \( C \) is an \( (n, 2w-1, w)_q \)-code if the following two conditions hold.
Theorem 7.1: If \( w|n \) and \( n \geq w((w-1)(q-2)+1) \), then \( A_q(n,2w-1,w) = (q-1)n/w \).

Proof: It suffices to show that there exists an \((n,2w-1,w)\_q\)-code of size \((q-1)n/w\) for any \( n \geq w((w-1)(q-2)+1), n \equiv 0 \pmod{w} \). We construct \( q-1 \) base codewords \( g^{(i)}, \ldots, g^{(q-1)} \) for such a code as follows. For \( i \in [q-1] \), \( g^{(i)} \in \{0,i\}^n \) satisfies
\[
\text{supp}(g^{(i)}) = \{0,1+(i-1)w,2+2(i-1)w, \ldots, (w-1)+(w-1)(i-1)w\}.\tag{6}
\]

Condition (C8) is satisfied immediately. It remains to show that these \( q-1 \) base codewords satisfy (C9). We prove this by contradiction. Assume that there exist \( u = T^{\ell}\_w(g^{(i)}) \) and \( v = T^{\ell}\_w(g^{(j)}) \), \( i \neq j \), so that \( |\text{supp}(u,v)| \geq 2 \). Suppose that \( a, b \in \text{supp}(u,v) \) and \( a \equiv x \pmod{w}, b \equiv y \pmod{w} \). By (6) we have
\[
a = x + x(i-1)w + kw \pmod{n},
\]
and
\[
b = y + y(i-1)w + kw \pmod{n},
\]
where the terms \( kw \) and \( \ell w \) result from the cyclic shift operations applied on \( g^{(i)} \) and \( g^{(j)} \). These equations imply
\[
xw(i-j) + (k-\ell)w \equiv 0 \pmod{n},
\]
and
\[
yw(i-j) + (k-\ell)w \equiv 0 \pmod{n},
\]
which together yield
\[
(x-y)(i-j) \equiv 0 \pmod{n/w}.\tag{7}
\]
However, since \( 0 \leq x \neq y \leq w-1 \) and \( 1 \leq i \neq j \leq q-1 \), we have
\[
0 < |(x-y)(i-j)| \leq (w-1)(q-2) < n/w, \tag{8}
\]
as \( n \geq w(1 + (w-1)(q-2)) \). Thus, (7) and (8) lead to a contradiction.

VIII. Tables for Small-Weight Constant-Composition Codes

In this section, we provide two tables of exact values of \( A_q(n,2\sum w-1,\sum w) \) with \( \sum w \leq 6 \), for almost all \( n \). The only undetermined values in this range are \( A_7(n,11,[1,1,1,1,1,1]) \) when \( n \in \{33,34\} \). The following (trivial) upper bound happens to be very useful when we build up the tables, as it is often tight for codes of small lengths.

Lemma 8.1: \( A_q(n,2\sum w-1,\sum w) \leq A_2(n,2\sum w-2,\sum w) \).

Table II provides the base codewords for quasicyclic optimal codes of sufficiently large lengths. For succinctness, we do not indicate trailing zeros at the end of each base codeword. Therefore, the base codeword 1203, say, should be interpreted as 12030\(^{-4} \). In order to construct these base codewords, we use either optimal Golomb rulers or a simple computer search to establish the best \( \lambda \)-array corresponding to the codes. Table II includes the sizes of optimal codes with small length \( n \). These two tables together give an almost complete solution for the sizes of optimal constant-composition codes of weight at most six.

In Table II, if a cell is empty, then it means that the corresponding size is already determined in Table I. The upper bound for the sizes of codes comes from either the Johnson bound or Lemma 8.1, whichever is smaller. The lower bounds come from optimal codes constructed by hand or by a hill-climbing algorithm. We refer the interested reader to the Appendix for a complete description of these optimal codes. We omit the values of \( A_q(n,2(w_1+w_2)-1,|w_1,w_2|) \) for completeness although it has been determined earlier by Östergård and Svanström [6, Theorem 8].

Table III gives the exact value of \( N_{\text{ccc}}(\sum w) \) for all \( \sum w \) such that \( \sum w \leq 6 \), except when \( \sum w = [1,1,1,1,1,1] \). We compare these values with bounds on \( N_{\text{ccc}}(\sum w) \) given by [6] and Proposition 7.1. There is a large gap between these bounds. It would be interesting to close this gap.

IX. Conclusion

The exact sizes of optimal constant-composition and constant-weight codes having linear size are determined for all such codes of sufficiently large lengths. In the course of
establishing these results, we introduced several new concepts, including that of generalized difference triangle sets and showed how they can be constructed from Golomb rulers. The results obtained in this paper solve an open problem of Etzion.

APPENDIX

Only codes of size at least five are listed here. Those optimal codes of size four or less can be constructed easily by hand.

| Weight | Distance | Composition $\mathcal{T}$ | Base codeword | Condition on length $n$ | Size | Remark |
|--------|----------|---------------------------|---------------|------------------------|------|--------|
| 3      | 5        | $[1, 1]$                  | 112           | $n \geq 3$             | $\lfloor n/2 \rfloor$ | Trivial |
|        |          | $[1, 1, 1]$               | 1203          | $n \geq 7$             | $\lfloor n/2 \rfloor$ | Trivial |
| 4      | 7        | $[3, 1]$                  | 1112          | $n \geq 7$             | $\lfloor n/3 \rfloor$ | This paper |
|        |          | $[2, 2]$                  | 112002        | $n \geq 10$            | $\lfloor n/2 \rfloor$ | Refinement of $[2, 2]$ |
|        |          | $[2, 1, 1]$               | 112003        | $n \geq 10$            | $\lfloor n/2 \rfloor$ | This paper |
|        |          | $[1, 1, 1, 1]$            | 12000304      | $n \geq 13$            | $\lfloor n/2 \rfloor$ | This paper |
| 5      | 9        | $[4, 1]$                  | 11112         | $n \geq 9$             | $\lfloor n/4 \rfloor$ | Trivial |
|        |          | $[3, 2]$                  | 11020002002001| $n \geq 15$           | $\lfloor n/3 \rfloor$ | This paper |
|        |          | $[3, 1, 1]$               | 110200030001  | $n \geq 15$            | $\lfloor n/3 \rfloor$ | Refinement of $[3, 2]$ |
|        |          | $[2, 2, 1]$               | 100120000203  | $n \geq 18$            | $\lfloor n/2 \rfloor$ | This paper |
|        |          | $[2, 1, 1, 1]$            | 100120000304  | $n \geq 18$            | $\lfloor n/2 \rfloor$ | Refinement of $[2, 2, 1]$ |
|        |          | $[1, 1, 1, 1, 1]$         | 120030000405  | $n \geq 23$            | $\lfloor n/2 \rfloor$ | This paper |
|        |          |                            | 12003000000000405| $n \geq 21$       | $\lfloor n/2 \rfloor$ | This paper |

| $\mathcal{T}$ | \(n\) | 6 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
|----------------|------|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| $[1, 1]$       | 4    |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| $[2, 1]$       | 1    | 1 | 2 | 2 | 3 | 6 | 9 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| $[1, 1, 1]$    | 1    | 1 | 2 | 2 | 3 | 5 | 6 | 9 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| $[2, 2]$       | 1    | 1 | 2 | 2 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| $[2, 1, 1]$    | 1    | 1 | 2 | 2 | 3 | 3 | 4 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| $[1, 1, 1, 1]$ | 1    | 1 | 2 | 2 | 3 | 3 | 4 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| $[3, 1]$       | 1    | 1 | 2 | 2 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| $[3, 2]$       | 1    | 1 | 2 | 2 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| $[3, 3]$       | 1    | 1 | 2 | 2 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| $[2, 2, 1]$    | 1    | 1 | 2 | 2 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| $[2, 1, 1, 1]$ | 1    | 1 | 2 | 2 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| $[1, 1, 1, 1, 1]$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

1) An Optimal (10, 7, [1, 1, 1, 1])_{15}-code: 0004021300 2103000040 004000132 100204003 0320140000
2) An Optimal (11, 7, [1, 1, 1, 1])_{15}-code: 300002000041 00100034020 20014003000 00003040102 01320000004 0400301200
3) An Optimal (12, 7, [1, 1, 1, 1])_{15}-code: 010020043000 000200301004 12000000403 200041000030 400301020000 00200430100 003014000002 034100000020 000000204310

A. Weight Four Codes

1) An Optimal (10, 7, [1, 1, 1, 1])_{15}-code

B. Weight Five Codes

1) An Optimal (15, 9, [2, 2, 1])_{14}-code

TABLE I

LINEAR SIZE OPTIMAL \((n, 2 \sum w_i - 1, \mathcal{T})_d\)-CODES OF WEIGHT AT MOST SIX

TABLE II

SIZES OF SOME SMALL OPTIMAL CONSTANT-COMPOSITION CODES WITH \(d = 2 \sum w_i - 1\)
00210020000103 201010003200000 0003000001220100
000021030010002 01000200201300 12000312000000
003000001220100 000310200001000300

2) An Optimal (16, 9, [2, 2, 1])4-code:
Lengthening of an optimal (15, 9, [2, 2, 1])4-code.

3) An Optimal (17, 9, [2, 2, 1])4-code:
003101002000020200 000032010000002000
12000031000020000000 10001000320000002100
012000200000200000

4) An Optimal (n, 9, [2, 1, 1, 1])5-code, n ∈ [15, 17]:
Refinement of an optimal (n, 9, [2, 1, 1, 1])5-code, n ∈ [15, 17].

5) An Optimal (n, 9, [1, 1, 1, 1])6-code, n ∈ [15, 18]:
Refinement of an optimal (n, 9, [2, 1, 1, 1])4-code, n ∈ [15, 18].

6) An Optimal (19, 9, [1, 1, 1, 1])6-code:
0045203000000000000010 5010302004000000000000000000
0001001005034002000 3004000000000002050000
0004000000003205010 0100304020000000000000000000
05030000014000000200 0000002301040000000000000000
40000010002000000 00000010002305000000
0020000005100034000 23000000000100400050

7) An Optimal (20, 9, [1, 1, 1, 1])6-code:
000020000503000002040105 1000003400000200000000
00000050400000001132 00000350000001002400
0210004000300000000050 00001034000020050000
04000201000003000050 00000010250004030000
04050000000030010200 100000000250000430000
2000310000005000000040 03050950000002010004
30200000001004000500 00000000015240000000
000030502000400010000 00342000010005000000

8) An Optimal (22, 9, [1, 1, 1, 1])6-code:
Lengthening of an optimal (21, 9, [1, 1, 1, 1])6-code.

C. Weight Six Codes

1) An Optimal (20, 11, [3, 3])3-code:
100000000020010200000020 002212000010000001 0001000202000201100
0100001000020201202

2) An Optimal (20, 11, [3, 2, 1])3-code:
Lengthening of an optimal (20, 11, [3, 3])3-code.

3) An Optimal (20, 11, [3, 1, 1, 1])5-code:
Lengthening of an optimal (20, 11, [3, 3])3-code.

4) An Optimal (20, 11, [2, 2, 2])3-code:
Lengthening of an optimal (20, 11, [4, 2])3-code.

5) An Optimal (21, 11, [2, 2, 2])4-code:
01000033200010020000 03300000002102000010
30201200300000000001 00010300021000032000
20000102000300030100 0020000100001000323
0000200000000213103000

6) An Optimal (22, 11, [2, 2, 2])4-code:
Lengthening of an optimal (21, 11, [2, 2, 2])4-code.

7) An Optimal (23, 11, [2, 2, 2])4-code:
1002020000000100000033000 20000031200010000030000000
000000003200020000010300 000310200000000000000123
0000000013000130200020001 001000003000230020001
00100000013300002000 0230230000000101000000

8) An Optimal (24, 11, [2, 2, 2])4-code:
University of Waterloo, Waterloo, ON, Canada, in 1988, 1989, and 1996, respectively.

Currently, he is an Associate Professor at the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. Prior to this, he was Program Director of Interactive Digital Media R&D in the Media Development Authority of Singapore, Postdoctoral Fellow at the University of Waterloo and IBM’s Zürich Research Laboratory, General Manager of the Singapore Computer Emergency Response Team, and Deputy Director of Strategic Programs at the Infocomm Development Authority, Singapore. His research interest lies in the interplay between combinatorics and computer science/engineering, particularly combinatorial design theory, coding theory, extremal set systems, and electronic design automation.

Son Hoang Dau received the Bachelors degree in Applied Mathematics and Informatics from the College of Science, Vietnam National University, Hanoi, Vietnam, in 2006 and the M.S. degree in mathematical sciences from the Division of Mathematical Sciences, Nanyang Technological University, Singapore, where he is currently working towards the Ph.D. degree.

His research interests are coding theory and combinatorics.

Alan C. H. Ling was born in Hong Kong in 1973. He received the B.Math., M.Math., and Ph.D. degrees in combinatorics & optimization from the University of Waterloo, Waterloo, ON, Canada, in 1994, 1995, and 1996, respectively. He worked at the Bank of Montreal, Montreal, QC, Canada, and Michigan Technological University, Houghton, prior to his present position as Associate Professor of Computer Science at the University of Vermont, Burlington. His research interests concern combinatorial designs, codes, and applications in computer science.

San Ling received the B.A. degree in mathematics from the University of Cambridge, Cambridge, U.K., in 1985 and the Ph.D. degree in mathematics from the University of California, Berkeley, in 1990.

Since April 2005, he has been a Professor with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. Prior to that, he was with the Department of Mathematics, National University of Singapore. His research fields include arithmetic of modular curves and application of number theory to combinatorial designs, coding theory, cryptography and sequences.