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

***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* is a tuple $\bar{\lambda} = [\![\lambda_1, \ldots, \lambda_N]\!]$ of integers such that $\lambda_1 \geq \cdots \geq \lambda_N \geq 1$. The λ_i's are the *parts* of the partition. Disjoint set union is denoted by $\sqcup$.

If X and R are sets, where X is finite, then R^X denotes the set of vectors of length $|X|$, where each component of a vector $\mathsf{u} \in R^X$ has value in R and is indexed by an element of X, that is, $\mathsf{u} = (\mathsf{u}_x)_{x \in X}$. A q-ary code of length n is a set $\mathcal{C} \subseteq \mathbb{Z}_q^X$, for some X of size n. The elements of $\mathcal{C}$ are called *codewords*. For any $\mathsf{u}, \mathsf{v} \in \mathbb{Z}_q^X$, their *support* is the set $\mathrm{supp}(\mathsf{u}, \mathsf{v}) = \{x \in X : \mathsf{u}_x \neq \mathsf{v}_x\}$. We also abbreviate $\mathrm{supp}(\mathsf{u}, 0)$ to $\mathrm{supp}(\mathsf{u})$. The *Hamming norm* or *weight* of $\mathsf{u} \in \mathbb{Z}_q^X$ is defined as $\|\mathsf{u}\| = |\mathrm{supp}(\mathsf{u})|$. The distance induced by this norm is called the *Hamming distance*, denoted $d_H(\cdot,\cdot)$, so that $d_H(\mathsf{u},\mathsf{v}) = \|\mathsf{u} - \mathsf{v}\|$, for $\mathsf{u}, \mathsf{v} \in \mathbb{Z}_q^X$. A code $\mathcal{C}$ is said to have *distance* d if $d_H(\mathsf{u},\mathsf{v}) \geq d$ for all distinct $\mathsf{u}, \mathsf{v} \in \mathcal{C}$. The *composition* of a vector $\mathsf{u} \in \mathbb{Z}_q^X$ is the tuple $\bar{w} = [\![w_1, \ldots, w_{q-1}]\!]$, where $w_i = |\{x \in X : \mathsf{u}_x = i\}|, i \in \mathbb{Z}_q \setminus \{0\}$. A code $\mathcal{C}$ is said to have *constant weight* w if every codeword in $\mathcal{C}$ has weight w, and is said to have *constant composition* $\bar{w}$ if every codeword in $\mathcal{C}$ has composition $\bar{w}$. 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 $(n,d,w)_q$-code. If in addition the code has constant composition $\bar{w}$, then it is referred to as an $(n,d,\bar{w})_q$-code. An $(n,d,w)_2$-code and an $(n,d,[\![w]\!])_2$-code coincide in definition, and are binary constant-weight codes. The maximum size of an $(n,d,w)_q$-code is denoted $A_q(n,d,w)$ and that of an $(n,d,\bar{w})_q$-code is denoted $A_q(n,d,\bar{w})$. Any $(n,d,w)_q$-code or $(n,d,\bar{w})_q$-code attaining the maximum size is called *optimal*.

The following operations do not affect distance and composition properties of an $(n,d,\bar{w})_q$-code:

1) reordering the components of $\bar{w}$;
2) deleting zero components of $\bar{w}$.

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

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

The Johnson-type bound of Svanström for ternary constant-composition codes [5, Th. 1] extends easily to the following (see also [27, Prop. 1.3]:

Manuscript received March 02, 2009; revised September 07, 2009. Current version published December 23, 2009. The work of Y. M. Chee and S. Ling was supported in part by the National Research Foundation of Singapore under Research Grant NRF-CRP2-2007-03. The work of Y. M. Chee was also supported in part by the Nanyang Technological University under Research Grant M58110040.

Y. M. Chee, S. H. Dau, and S. Ling are with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371, Singapore (e-mail: ymchee@ntu.edu.sg; daus0001@ntu.edu.sg; lingsan@ntu.edu.sg).

A. C. H. Ling is with the Department of Computer Science, University of Vermont, Burlington, VT 05405 USA (e-mail: aling@emba.uvm.edu).

Communicated by T. Etzion, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2009.2034814

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 [6, Th. 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 $\bar{w} = [\![w_1,\ldots,w_q]\!]$ is a *refinement* of $\bar{v} = [\![v_1,\ldots,v_{q'}]\!]$ (written $\bar{w} \succcurlyeq \bar{v}$) if there exist pairwise disjoint sets $I_1,\ldots,I_{q'} \subseteq [q]$ satisfying $\cup_{j\in[q']} I_j = [q]$ such that $\sum_{i\in I_j} w_i = v_j$ for each $j \in [q']$.

Chu *et al.* [27] made the following observation.

Lemma 1.1: If $\bar{w} \succcurlyeq \bar{v}$, then $A_q(n,d,\bar{w}) \geq A_{q'}(n,d,\bar{v})$.

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

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

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

Rödl's proof [29] of the Erdös–Hanani conjecture [30] implies that $A_2(n,d,w) = (1-o(1))\binom{n}{w-d/2+1}/\binom{w}{w-d/2+1}$, so that $A_2(n,d,w) = \Omega(n^2)$ for all $d \leq 2w-2$. Therefore, by Lemma 1.1, $A_q(n,d,\bar{w}) \geq A_2(n,d,\sum\bar{w}) = \Omega(n^2)$ for all $d \leq 2\sum\bar{w} - 2$. □

A similar proof yields the following.

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

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

When $d = 2\sum\bar{w}-1$, our knowledge of $A_q(n,d,\bar{w})$ is limited. We know that $A_2(n,2w-1,w) = A_2(n,2w,w) = \lfloor n/w \rfloor$, trivially. $A_3(n,2\sum\bar{w}-1,\bar{w})$ has also been completely determined by Svanström *et al.* [7]. In particular, $A_3(n,2\sum\bar{w} - 1,\bar{w}) = \lfloor n/w_1 \rfloor$ holds for all n sufficiently large. Beyond this (for $q \geq 4$), $A_q(n,2\sum\bar{w}-1,\bar{w})$ has not been determined, except in one instance: $A_4(n,5,[\![1,1,1]\!]) = n$ for $n \geq 7$, established by Chee *et al.* [18]. 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 Östergård and Svanström [6]. When $q \geq 4$, the value of $A_q(n,2w-1,w)$ is not known.

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

Main Theorem 1: Let $\bar{w} = [\![w_1,\ldots,w_{q-1}]\!]$. Then $A_q(n,2\sum\bar{w}-1,\bar{w}) = \lfloor n/w_1 \rfloor$ 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 Etzion concerning generalized Steiner systems [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 ℓ such that a cyclic shift of a codeword by ℓ places is another codeword. More formally, let $X = \mathbb{Z}_n$ and define on $\mathbb{Z}_q^X$ the *cyclic shift operator* $T : (\mathsf{u}_x)_{x\in X} \mapsto (\mathsf{u}_{x-1})_{x\in X}$. A q-ary code $\mathcal{C} \subseteq \mathbb{Z}_q^X$ of length n is *quasicyclic* (or more precisely, ℓ*-quasicyclic*) if it is invariant under T^ℓ 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 $\mathcal{C}$ of constant weight w to have distance $2w-1$.

- C1) For any distinct $\mathsf{u},\mathsf{v} \in \mathcal{C}$, $|\mathrm{supp}(\mathsf{u}) \cap \mathrm{supp}(\mathsf{v})| \leq 1$.
- C2) For any distinct $\mathsf{u},\mathsf{v} \in \mathcal{C}$, if $x \in \mathrm{supp}(\mathsf{u}) \cap \mathrm{supp}(\mathsf{v})$, then $\mathsf{u}_x \neq \mathsf{v}_x$.

A. Quasicyclic Constant-Composition Codes

The strategy for proving Main Theorem 1 is to construct optimal $(n,2\sum\bar{w}-1,\bar{w})_q$-codes (meeting the Johnson bound) that are w_1-quasicyclic when $n \equiv 0 \pmod{w_1}$. Optimal $(n,2\sum\bar{w}-1,\bar{w})_q$-codes for $n \not\equiv 0 \pmod{w_1}$ 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 $A_q(n,2\sum\bar{w}-1,\bar{w}) = \lfloor n/w_1 \rfloor$ and $n \equiv 0 \pmod{w_1}$, then $A_q(n+i,2\sum\bar{w}-1,\bar{w}) = \lfloor n/w_1 \rfloor$ for all i, $0 \leq i < w_1$.

Proof: Let $\mathcal{C} \subseteq \mathbb{Z}_q^X$ be an $(n,2\sum\bar{w}-1,\bar{w})_q$-code of size $\lfloor n/w_1 \rfloor$. Let $X' = X \cup \{\infty_1,\ldots,\infty_i\}$, where $\infty_1,\ldots,\infty_i \notin X$, and define $\mathcal{C}' \subseteq \mathbb{Z}_q^{X'}$ such that $\mathcal{C}' = \{(c(\mathsf{u})_x)_{x\in X'} : \mathsf{u} \in \mathcal{C}\}$, where

$$c(\mathsf{u})_x = \begin{cases} \mathsf{u}_x, & \text{if } x \in X \\ 0, & \text{if } x \in \{\infty_1,\ldots,\infty_i\}. \end{cases}$$

Then $\mathcal{C}'$ is an $(n+i,2\sum\bar{w}-1,\bar{w})_q$-code of size $\lfloor n/w_1 \rfloor$. Since $\lfloor (n+i)/w_1 \rfloor = \lfloor n/w_1 \rfloor$, $\mathcal{C}'$ is optimal by the Johnson bound. □

As opposed to lengthening a code, we can also *shorten* a code by selecting a position i, removing those codewords with a nonzero coordinate i, and deleting the ith coordinate from every remaining codeword.

Let $n \equiv 0 \pmod{w_1}$. A w_1-quasicyclic $(n,2\sum\bar{w} - 1,\bar{w})_q$-code $\mathcal{C}$ of size n/w_1 can be obtained by *developing* a particular vector $\mathsf{g} \in \mathbb{Z}_q^X$

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

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

Conditions C1) and C2) may be stated in terms of the base codeword g as follows.

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

C4) If $\mathrm{g}_x = \mathrm{g}_y \neq 0$, 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 α, β, ℓ, 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. □

Suppose that $w|(q-1)n$. By Lemma 2.2, there exist positive integers α, β, ℓ, and m such that $n = \alpha\ell, w = \beta\ell$, and $q - 1 = m\beta$. Our strategy is to construct ℓ-quasicyclic optimal $(n, 2w - 1, w)_q$-codes of size $(q-1)n/w = mn/\ell$ (meeting the Johnson bound). In other words, we want to find m vectors, $\mathrm{g}^{(1)}, \ldots, \mathrm{g}^{(m)} \in \mathbb{Z}_q^X$, each of weight w, such that

$$\mathcal{C} = \{T^{\ell i}(\mathrm{g}^{(j)}) : i \in [0, n/\ell - 1] \text{ and } j \in [m]\}$$

is an $(n, 2w-1, w)_q$-code of size mn/ℓ. The vectors $\mathrm{g}^{(1)}, \ldots, \mathrm{g}^{(m)}$ are referred to as *base codewords* of $\mathcal{C}$.

Conditions C1) and C2) can be stated in terms of the base codewords $\mathrm{g}^{(1)}, \ldots, \mathrm{g}^{(m)}$ as follows.

C5) Let $w, x \in \mathrm{supp}(\mathrm{g}^{(i)})$ and $y, z \in \mathrm{supp}(\mathrm{g}^{(j)})$ such that $w \neq x, y \neq z$, and $\{w, x\} \neq \{y, z\}$ if $j = i$. Then, we have the following:
- if $x - w \equiv 0 \pmod{\ell}$, then $2(x - w) \not\equiv 0 \pmod{n}$;
- if $y - w \equiv 0 \pmod{\ell}$, then $x - w \not\equiv z - y \pmod{n}$.

C6) If $\mathrm{g}_z^{(j)} = \mathrm{g}_y^{(j)} \neq 0$ and $z \neq y$, then $z - y \not\equiv 0 \pmod{\ell}$, for all $j \in [m]$.

C7) If $\mathrm{g}_z^{(i)} = \mathrm{g}_y^{(j)} \neq 0$ (z and y are not necessarily distinct), then $z - y \not\equiv 0 \pmod{\ell}$, for all $i, j \in [m], i \neq j$.

III. A New Combinatorial Array

Conditions C3) and C4) [respectively, C5)–C7)] suggest organizing the elements of $\mathrm{supp}(\mathrm{g})$ [respectively, $\mathrm{supp}(\mathrm{g}^{(1)}), \ldots, \mathrm{supp}(\mathrm{g}^{(m)})$] of those quasicyclic constant-composition codes (respectively, constant-weight codes) into a two-dimensional array, with respect to their congruence class modulo w_1 (respectively, ℓ) and the value of their corresponding components in g [respectively, $\mathrm{g}^{(1)}, \ldots, \mathrm{g}^{(m)}$].

Definition 3.1: Let $\bar{\lambda} = [\![\lambda_1, \ldots, \lambda_N]\!]$ be a partition. A $\bar{\lambda}$-*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 λ_1;

P2) the number of nonempty cells in column j is λ_j;

P3) if $B_i = \{b_{i,1}, \ldots, b_{i,N_i}\}$ 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

$$\sigma(\mathsf{B}) = \max_{1 \leq i \leq \lambda_1} (\{b_{i,j} - b_{i,j'} : 1 \leq j' \neq j \leq N_i\} \cup \{\lceil b_{i,j}/2 \rceil : j \in [N_i]\}).$$

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

Example 3.1: A $[\![3, 2, 2]\!]$-array of scope 15

1	7	16
2		14
0	3	

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

19	23	35	61
0	6	20	30

Proposition 3.1: Let $\bar{w} = [\![w_1, \ldots, w_{q-1}]\!]$. If there exists a $\bar{w}$-array B, then there exists a w_1-quasicyclic optimal $(n, 2\sum \bar{w} - 1, \bar{w})_q$-code for all $n \equiv 0 \pmod{w_1}, n \geq 2\sigma(\mathsf{B}) + 1$.

Proof: Let B be a $\bar{w}$-array and let C_j denote the set of entries in column j of B, $j \in [q-1]$. Define a vector $\mathrm{g} \in \mathbb{Z}_q^{\mathbb{Z}_n}, n \geq 2\sigma(\mathsf{B}) + 1$, as follows:

$$\mathrm{g}_x = \begin{cases} j, & \text{if } x \in C_j \\ 0, & \text{otherwise.} \end{cases}$$

Then, g has composition $\bar{w}$ and satisfies conditions C3) and C4). Therefore, g is a base codeword of a w_1-quasicyclic optimal $(n, 2\sum \bar{w} - 1, \bar{w})_q$-code. □

Example 3.3: The $[\![3, 2, 2]\!]$-array in Example 3.1 gives the base codeword

$$\mathrm{g} = 11120002000000303 0^{n-17}$$

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 ℓ-quasicyclic optimal $(n, 2w-1, w)_q$-code of size $(q-1)n/w = mn/\ell$, provided that $\ell | n$ and $n \geq 2\sigma(\mathsf{B}) + 1$.

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 $\mathsf{g}^{(1)}, \ldots, \mathsf{g}^{(m)}$ as follows: for $j \in [m]$ and $0 \le z \le n-1$

$$\mathsf{g}_z^{(j)} = \begin{cases} r, & \text{if } z \in C_r \text{ for some } r \in [(j-1)\beta+1, j\beta] \\ 0, & \text{otherwise.} \end{cases} \quad (1)$$

Since the entries of B are distinct, $\mathsf{g}^{(j)}$ is well defined. Moreover, the set of nonzero entries of $\mathsf{g}^{(j)}$ is precisely $[(j-1)\beta+1, j\beta]$, and by property P2), each symbol in $[(j-1)\beta+1, j\beta]$ occurs exactly ℓ times in $\mathsf{g}^{(j)}$. Therefore, $\mathsf{g}^{(j)} \in \mathbb{Z}_q^{\mathbb{Z}_n}$ and has weight $w = \beta\ell$.

We claim that the m vectors $\mathsf{g}^{(1)}, \ldots, \mathsf{g}^{(m)}$ satisfy conditions C5)–C7), and hence form the base codewords for an ℓ-quasicyclic optimal $(n, 2w-1, w)_q$-code. The following establishes this claim.

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

Next, suppose that $z \neq y$ and $\mathsf{g}_z^{(j)} = \mathsf{g}_y^{(j)} = r \neq 0$. By (1), $z, y \in C_r$. Since $z \neq y, z$, and y must belong to different rows of B. Therefore, $z \not\equiv y \pmod{\ell}$ by P1). Thus, $\mathsf{g}^{(1)}, \ldots, \mathsf{g}^{(m)}$ satisfy C6).

Now suppose that $w, x \in \text{supp}(\mathsf{g}^{(i)}), w \neq x$. 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

$$0 < |x - w| \le \sigma(\mathsf{B})$$

and, hence

$$0 < 2|x - w| \le 2\sigma(\mathsf{B}) < 1 + 2\sigma(\mathsf{B}) \le n.$$

It follows that $2(x - w) \not\equiv 0 \pmod{n}$.

Let $w, x \in \text{supp}(\mathsf{g}^{(i)})$ and $y, z \in \text{supp}(\mathsf{g}^{(j)})$, 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

$$x - w \not\equiv z - y \pmod{n}$$

or, equivalently

$$y - w \not\equiv z - x \pmod{n}. \quad (2)$$

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 $0 < |y - w| \le \sigma(\mathsf{B}) < n$, we have $y - w \not\equiv 0 \pmod{n}$. 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 $n \ge 2\sigma(\mathsf{B}) + 1$. If x and z are in different rows, then by P1), $z - x \not\equiv 0 \pmod{\ell}$. 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, $\mathsf{g}^{(1)}, \ldots, \mathsf{g}^{(m)}$ satisfy C5). □

Example 3.4: The $(2, 4)$-array of scope 42 in Example 3.2 gives $\mathsf{g}^{(1)}$ and $\mathsf{g}^{(2)}$, where

$$\mathsf{g}_z^{(1)} = \begin{cases} 1, & \text{if } z \in \{0, 19\} \\ 2, & \text{if } z \in \{6, 23\} \\ 0, & \text{otherwise} \end{cases}$$

$$\mathsf{g}_z^{(2)} = \begin{cases} 3, & \text{if } z \in \{20, 35\} \\ 4, & \text{if } z \in \{30, 61\} \\ 0, & \text{otherwise.} \end{cases}$$

In this case, $q = 5, w = 4, \beta = 2, \ell = 2$, and $m = 2$. The vectors $\mathsf{g}^{(1)}$ and $\mathsf{g}^{(2)}$ form the base codewords of a 2-quasicyclic optimal $(n, 7, 4)_5$-code when n is even and $n \ge 85 = 2 \times 42 + 1$.

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

IV. Generalized Difference Triangle Sets

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

Definition 4.1: An (I, J)-*difference triangle set* (DΔS) is a set $\mathcal{A} = \{A_1, \ldots, A_I\}$, 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 $a_{i,j} - a_{i,j'}, i \in [I], 1 \le j' \neq j \le J$, are all distinct.

Example 4.1: A $(3, 4)$-DΔS is

$$\{\{0, 1, 10, 18\}, \{0, 2, 7, 13\}, \{0, 3, 15, 19\}\}.$$

The corresponding differences are displayed in triangular arrays

$$\begin{array}{ccc} 1 & 10 & 18 \\ & 9 & 17 \\ & & 8 \end{array} \quad \begin{array}{ccc} 2 & 7 & 13 \\ & 5 & 11 \\ & & 6 \end{array} \quad \begin{array}{ccc} 3 & 15 & 19 \\ & 12 & 16 \\ & & 4. \end{array}$$

The *scope* of an (I, J)-DΔS $\mathcal{A} = \{A_1, \ldots, A_I\}$ is

$$m(\mathcal{A}) = \max_{A \in \mathcal{A}} \{a \in A\}.$$

Difference triangle sets with scope as small as possible are often required for applications. Define

$$M(I, J) = \min\{m(\mathcal{A}) : \mathcal{A} \text{ is an } (I, J) - \text{D}\Delta\text{S}\}.$$

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

We generalize difference triangle sets as follows.

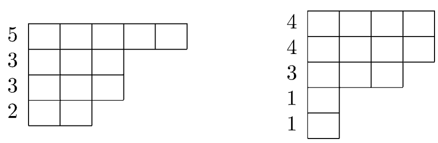
Definition 4.2: Let $\bar{J} = [\![J_1, \ldots, J_I]\!]$ be a partition. A set $\mathcal{A} = \{A_1, \ldots, A_I\}$ with $A_i = \{a_{i,1}, \ldots, a_{i,J_i}\}, 0 = a_{i,1} < \cdots < a_{i,J_i}$, is a $\bar{J}$-*generalized difference triangle set* (GDΔS) if the differences $a_{i,j} - a_{i,j'}, i \in [I], 1 \le j' \neq j \le J_i$, are all distinct.

Thus, a GDΔS is similar to a DΔS, but allowing the sets to be of different sizes. In particular, if $J_1 = \cdots = J_I = J$, then a $\bar{J}$-GDΔS is an (I, J)-DΔS. The scope of a GDΔS $\mathcal{A} = \{A_1, \ldots, A_I\}$ is defined similarly as for a DΔS

$$m(\mathcal{A}) = \max_{A \in \mathcal{A}} \{a \in A\}.$$

We now relate $\bar{J}$-GDΔS to $\bar{\lambda}$-arrays. Let $\bar{\lambda} = [\![\lambda_1, \ldots, \lambda_N]\!]$ be a partition. The *Ferrers diagram* of $\bar{\lambda}$ is an array of cells with N left-justified rows and λ_i cells in row i. The *conjugate* of $\bar{\lambda}$ is the partition $\overline{\lambda^*} = [\![\lambda_1^*, \ldots, \lambda_{\lambda_1}^*]\!]$, where λ_j^* is the number of parts of $\bar{\lambda}$ that are at least j. $\overline{\lambda^*}$ can also be obtained by reflecting the Ferrers diagram of $\bar{\lambda}$ 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, as follows:



Proposition 4.1: Let $\bar{\lambda} = [\![\lambda_1, \ldots, \lambda_N]\!]$ be a partition. If there exists a $\overline{\lambda^*}$-GDΔS of scope s, then there exists a $\bar{\lambda}$-array of scope at most $s\lambda_1$.

Proof: Let $\overline{\lambda^*} = [\![\lambda_1^*, \ldots, \lambda_{\lambda_1}^*]\!]$ and let $\mathcal{A} = \{A_1, \ldots, A_{\lambda_1}\}$ be a $\overline{\lambda^*}$-GDΔS of scope s. Construct a $\lambda_1 \times N$ array B as follows: If $A_i = \{a_{i,1}, \ldots, a_{i,\lambda_i^*}\}$, then the (i, j)th cell of $\mathsf{B}, i \in [\lambda_1], j \in [N]$, contains $b_{i,j} = a_{i,j}\lambda_1 + (i \bmod \lambda_1)$ if $j \in [\lambda_i^*]$, and empty otherwise. Then, the filled cells of B take the shape of the Ferrers diagram of $\overline{\lambda^*}$. Thus, the number of nonempty cells in column j of B is precisely λ_j. It is also easy to see that each entry in row i of B is congruent to $i \bmod \lambda_1$. The differences $b_{i,j} - b_{i,j'}$ are all distinct because the differences $a_{i,j} - a_{i,j'}$ are all distinct in the GDΔS $\mathcal{A}$. Moreover, all of these differences are at most $s\lambda_1$. Finally, for any $i \in [\lambda_1]$ and $j \in [\lambda_i^*]$

$$\left\lceil \frac{b_{i,j}}{2} \right\rceil \leq \left\lceil \frac{s\lambda_1 + (\lambda_1 - 1)}{2} \right\rceil \leqslant \frac{s\lambda_1 + \lambda_1}{2} \leqslant s\lambda_1.$$

Therefore, B is a $\bar{\lambda}$-array of scope at most $s\lambda_1$. □

Corollary 4.1: If there exists a (λ, N)-DΔS of scope s, then there exists a (λ, 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 $[\![4, 4, 2]\!]$-GDΔS via the proof of Proposition 4.1. If the $[\![4, 4, 2]\!]$-GDΔS is $\mathcal{A} = \{\{0, 1, 10, 18\}, \{0, 2, 7, 13\}, \{0, 3\}\}$, the $[\![3, 3, 2, 2]\!]$-array obtained is

1	4	31	55
2	8	23	41
0	9		

This array has scope 54.

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

1	4	31	55
2	8	23	41
0	9	45	57

This array has scope 57.

V. Proofs of the Main Theorems

In this section, we use Golomb rulers to construct GDΔS and provide proofs to Main Theorem 1 and Main Theorem 2.

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

Theorem 5.1: $M(1, J) \leq (J - 1)\wp(J - 1)$

Proposition 5.1: For any partition $\bar{J} = [\![J_1, \ldots, J_I]\!]$, there exists a $\bar{J}$-GDΔS of scope at most $(\sum \bar{J} - 1)\wp(\sum \bar{J} - 1)$.

Proof: By Theorem 5.1, there exists a Golomb ruler $\{R\}$ of $\sum \bar{J}$ marks and scope $m(\{R\}) \leq (\sum \bar{J} - 1)\wp(\sum \bar{J} - 1)$. Partition R into I subsets, $R = R_1 \sqcup \cdots \sqcup R_I$, where $|R_i| = J_i, i \in [I]$. Suppose

$$R_i = \{r_{i,1}, \ldots, r_{i,J_i}\}$$

where $0 \leq r_{i,1} < \cdots < r_{i,J_i}$. For each $i \in [I]$, let

$$A_i = \{a_{i,1}, \ldots, a_{i,J_i}\}$$

where $a_{i,j} = r_{i,j} - r_{i,1}, j \in [J_i]$. Then, the set $\mathcal{A} = \{A_1, \ldots, A_I\}$ forms a $\bar{J}$-GDΔS of scope

$$m(\mathcal{A}) \leq m(\{R\}) \leq \left(\sum \bar{J} - 1\right) \wp \left(\sum \bar{J} - 1\right). \qquad \square$$

The following corollary is immediate.

Corollary 5.1: For any $I > 0$ and $J > 0$, there exists an (I, J)-DΔS of scope at most $(IJ - 1)\wp(IJ - 1)$.

A. Proof of Main Theorem 1

Let $\bar{w} = [\![w_1, \ldots, w_{q-1}]\!]$ be a partition and consider $\overline{w^*} = [\![w_1^*, \ldots, w_{w_1}^*]\!]$. By Proposition 5.1, there exists a $\overline{w^*}$-GDΔS of scope at most $(\sum \bar{w} - 1)\wp(\sum \bar{w} - 1)$. Therefore, by Proposition 4.1, there exists a $\bar{w}$-array of scope at most $w_1(\sum \bar{w} - 1)\wp(\sum \bar{w} - 1)$. Finally, Proposition 3.1 guarantees the existence of a w_1-quasicyclic optimal $(n, 2\sum \bar{w} - 1, \bar{w})_q$-code of size n/w_1 for all $n \equiv 0 \pmod{w_1}, n \geq 2w_1(\sum \bar{w} - 1)\wp(\sum \bar{w} - 1) + 1$. 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 $w = \beta\ell$, where $\beta|(q - 1)$. By Corollary 5.1, there exists an $(\ell, q - 1)$-DΔS of scope at most $(\ell(q - 1) - 1)\wp(\ell(q - 1) - 1)$. Therefore, by Corollary 4.1, there exists an $(\ell, q - 1)$-array of scope at most $\ell(\ell(q-1)-1)\wp(\ell(q-1)-1)$. Finally, Proposition 3.2 guarantees the existence of an ℓ-quasicyclic optimal $(n, 2w - 1, w)_q$-code of size $(q-1)n/w$ for all $n \equiv 0 \pmod{\ell}, n \geq 2\ell(\ell(q-1) - 1)\wp(\ell(q - 1) - 1) + 1$. This proves Main Theorem 2.

In particular, by taking $\beta = 1$ and $\beta = w$, respectively, we have the following results.

i) There exists a w-quasicyclic optimal $(n, 2w - 1, w)_q$-code for all $n \equiv 0 \pmod{w}, n \geq 2w(w(q - 1) - 1)\wp(w(q - 1) - 1) + 1$.

ii) If $w|(q - 1)$, then there exists a cyclic optimal $(n, 2w - 1, w)_q$-code for all $n \geq 2(q - 2)\wp(q - 2) + 1$.

VI. Resolution of an Open Problem of Etzion

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

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

i) B is a transverse of $\mathcal{G}$ for all $B\in\mathcal{B}$;
ii) each t-element transverse of $\mathcal{G}$ is contained in precisely one block of $\mathcal{B}$.

From an $\mathrm{H}(n,q,w,t)$ design $(X,\mathcal{G},\mathcal{B})$, we can form a constant-weight code $\mathcal{C}\subseteq\mathbb{Z}_{q+1}^n$ as follows. Let $G_i=\{\gamma_{1,i},\gamma_{2,i},\dots,\gamma_{q,i}\}$, where $0\notin G_i$. The code $\mathcal{C}$ has a codeword for each block. Assume $B=\{b_1,b_2,\dots,b_w\}$ is a block of $\mathcal{B}$ (this block is denoted by $\{\langle i_1,j_1\rangle,\langle i_2,j_2\rangle,\dots,\langle i_w,j_w\rangle\}$, where $b_s=\gamma_{j_s,i_s}$). We form the codeword $\mathsf{u}\in\mathcal{C}$ corresponding to B as follows: for $i\in[n]$

$$\mathsf{u}_i=\begin{cases} j, & \text{if } b_r=\gamma_{j,i} \text{ for some } r\in[w]\\ 0, & \text{otherwise.}\end{cases}$$

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

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

$$A_{q+1}(n,2(w-t)+1,w)\le q^t\frac{\binom{n}{t}}{\binom{w}{t}}.$$

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

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

The next result establishes the converse when $\binom{w}{t}\,|q^t\binom{n}{t}$.

Proposition 6.1: Suppose that $\binom{w}{t}\,|q^t\binom{n}{t}$. Then, a $\mathrm{GS}(t,w,n,q)$ exists if

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

Proof: Let $\mathcal{C}$ be an (optimal) $(n,2(w-t)+1,w)_{q+1}$-code of size $q^t\binom{n}{t}/\binom{w}{t}$. Define

$$X=\{(i,j): i\in[n] \text{ and } j\in[q]\}$$
$$\mathcal{G}=\{G_i: i\in[n]\}$$

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

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

Finally, let $\mathcal{B}=\{B^{\mathsf{u}}:\mathsf{u}\in\mathcal{C}\}$.

We claim that $(X,\mathcal{G},\mathcal{B})$ is a $\mathrm{GS}(t,w,n,q)$. Indeed, $|B|=w$ for all $B\in\mathcal{B}$, and $|B\cap G_i|\le 1$ for all $B\in\mathcal{B}$ and $i\in[n]$. Hence, it remains to show that any t-element transverse of $\mathcal{G}$ is contained in exactly one block of $\mathcal{B}$. Suppose B^{u} and B^{v} are two different blocks containing a particular t-element transverse of $\mathcal{G}$. Then, $|\mathrm{supp}(\mathsf{u})\cap\mathrm{supp}(\mathsf{v})|\ge t$, implying $d_H(\mathsf{u},\mathsf{v})\le 2(w-t)<2(w-t)+1$, a contradiction. Therefore, any t-element transverse of $\mathcal{G}$ is contained in at most one block, and hence in exactly one block, since $|\mathcal{B}|=|\mathcal{C}|=q^t\binom{n}{t}/\binom{w}{t}$. □

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

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

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 $n\ge n_0$, where $w|nk$, a $\mathrm{GS}(1,w,n,k)$ 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 $\mathrm{GS}(1,w,n,k)$ 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 $\mathrm{GS}(1,w,n,k)$ 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 $\bar{w}=[\![w_1,\dots,w_{q-1}]\!]$ and a positive integer w, define

$$N_{\mathrm{ccc}}(\bar{w}) = \min\left\{n_0: A_q\left(n,2\sum\bar{w}-1,\bar{w}\right)=\left\lfloor\frac{n}{w_1}\right\rfloor \text{ for all } n\ge n_0\right\}$$

and

$$N_{\mathrm{cwc}}(w) = \min\left\{n_0: A_q(n,2w-1,w)=\frac{(q-1)n}{w} \text{ for all } n\ge n_0 \text{ satisfying } w|(q-1)n\right\}.$$

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

A. Bounds on $N_{\mathrm{ccc}}(\bar{w})$

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

$$N_{\mathrm{ccc}}(\bar{w})\le 2w_1\left(\sum\bar{w}-1\right)\wp\left(\sum\bar{w}-1\right)+1. \quad (3)$$

By Bertrand's postulate, $\wp(x) \leq 2x$ for all $x \geq 1$. For x sufficiently large, better asymptotic bounds on $\wp(x)$ exist (see, for example, [42]), but we are after quantifiable bounds. This implies

$$N_{\rm ccc}(\bar{w}) \leq 4w_1 \left(\sum \bar{w} - 1\right)^2 + 1.$$

We now prove a lower bound on $N_{\rm ccc}(\bar{w})$.

Proposition 7.1: Let $\bar{w} = [\![w_1, \ldots, w_{q-1}]\!]$ be a partition. If $w_1|n$ and there exists an $(n, 2\sum \bar{w} - 1, \bar{w})_q$-code of size n/w_1, then $n \geq w_1^2 k(k-1) + w_1$, where $k = \lfloor \sum \bar{w}/w_1 \rfloor$. 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 $\mathcal{C} = \{\mathsf{u}^{(1)}, \ldots, \mathsf{u}^{(n/w_1)}\}$ be an $(n, 2\sum \bar{w} - 1, \bar{w})_q$-code of size n/w_1. Then, $\mathcal{C}$ can be regarded as an $n/w_1 \times n$ matrix C, whose ith row is $\mathsf{u}^{(i)}, i \in [n/w_1]$. Let N_i be the number of nonzero entries in column i of C. Then, $\sum_{i=1}^n N_i = (n\sum \bar{w})/w_1$. 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 $\mathcal{C}$ 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

$$\sum_{i=1}^n \binom{N_i}{2} \leq \binom{|\mathcal{C}|}{2} = \binom{n/w_1}{2}$$

or, equivalently

$$\sum_{i=1}^n N_i(N_i - 1) \leq \frac{n(n-w_1)}{w_1^2}. \quad (4)$$

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

$$\frac{n\sum \bar{w}}{w_1} = kn + r.$$

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

$$\begin{aligned}\sum_{i=1}^n N_i(N_i - 1) &\geq r(k+1)k + (n-r)k(k-1) \\ &\geq nk(k-1). \quad (5)\end{aligned}$$

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:

$$\begin{aligned}\left(\sum \bar{w}\right)^2 - w_1\left(\sum \bar{w} - 1\right) &\leq N_{\rm ccc}(\bar{w}) \\ &\leq 4w_1\left(\sum \bar{w} - 1\right)^2 + 1.\end{aligned}$$

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

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

The proof of Main Theorem 2 in Section V-B shows that $N_{\rm cwc}(w) \leq 2w(w(q-1)-1)^2 + 1$.

For constant-weight codes, the following result of Etzion [31, Th. 1] gives $N_{\rm cwc}(w) \geq (w-1)(q-1) + 1$.

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 $N_{\rm cwc}(w)$. 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 $\mathsf{g}^{(1)}, \ldots, \mathsf{g}^{(q-1)}$, for which the (n/w)-quasicyclic code

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

is an $(n, 2w-1, w)_q$-code. Let us write $\mathsf{u} \stackrel{\rm T}{\leftarrow} \mathsf{g}^{(i)}$ if $\mathsf{u} = T^{wj}(\mathsf{g}^{(i)})$ for some j. Suppose that $\mathsf{g}^{(i)} \in \{0, i\}^n, i \in [q-1]$. Then, $\mathcal{C}$ is an $(n, 2w-1, w)_q$-code if the following two conditions hold.

C8) $|{\rm supp}(\mathsf{u}, \mathsf{v})| = 0$ if $\mathsf{u} \stackrel{\rm T}{\leftarrow} \mathsf{g}^{(i)}$ and $\mathsf{v} \stackrel{\rm T}{\leftarrow} \mathsf{g}^{(i)}$ for some i.

C9) $|{\rm supp}(\mathsf{u}, \mathsf{v})| \leq 1$ if $\mathsf{u} \stackrel{\rm T}{\leftarrow} \mathsf{g}^{(i)}$ and $\mathsf{v} \stackrel{\rm T}{\leftarrow} \mathsf{g}^{(j)}$ for $i \neq j$.

We observe that C8) holds immediately if for every $i \in [q-1]$, $\mathsf{g}^{(i)}$ is chosen so that ${\rm supp}(\mathsf{g}^{(i)})$ contains w elements which are congruent to $0, 1, \ldots, w-1 \pmod{w}$, respectively.

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 $\mathsf{g}^{(1)}, \ldots, \mathsf{g}^{(q-1)}$ for such a code as follows. For $i \in [q-1]$, $\mathsf{g}^{(i)} \in \{0, i\}^n$ satisfies

$$\begin{aligned}{\rm supp}\left(\mathsf{g}^{(i)}\right) = \{&0, 1 + (i-1)w, 2 + 2(i-1)w, \ldots, \\ &(w-1) + (w-1)(i-1)w\}. \quad (6)\end{aligned}$$

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 $\mathsf{u} = T^{kw}(\mathsf{g}^{(i)})$ and $\mathsf{v} = T^{lw}(\mathsf{g}^{(j)}), i \neq j$, so that $|{\rm supp}(\mathsf{u}, \mathsf{v})| \geq 2$. Suppose that $a, b \in {\rm supp}(\mathsf{u}, \mathsf{v})$ and $a \equiv x \pmod{w}, b \equiv y \pmod{w}$. By (6), we have

$$\begin{aligned}a &= x + x(i-1)w + kw \pmod{n} \\ &= x + x(j-1)w + \ell w \pmod{n}\end{aligned}$$

and

$$\begin{aligned}b &= y + y(i-1)w + kw \pmod{n} \\ &= y + y(j-1)w + \ell w \pmod{n}\end{aligned}$$

where the terms kw and ℓw result from the cyclic shift operations applied on $\mathsf{g}^{(i)}$ and $\mathsf{g}^{(j)}$. These equations imply

$$xw(i-j) + (k-\ell)w \equiv 0 \pmod{n}$$

TABLE I
LINEAR SIZE OPTIMAL $(n, 2\sum\bar{w}-1, \bar{w})_q$-CODES OF WEIGHT AT MOST SIX

Weight	Distance	Composition $\overline{w}$	Base codeword	Condition on length n	Size	Remark
2	3	$[\![1,1]\!]$	12	$n \geq 3$	n	Trivial
3	5	$[\![2,1]\!]$	112	$n \geq 5$	$\lfloor n/2 \rfloor$	Trivial
		$[\![1,1,1]\!]$	1203	$n \geq 7$	n	[18]
4	7	$[\![3,1]\!]$	1112	$n \geq 7$	$\lfloor n/3 \rfloor$	Trivial
		$[\![2,2]\!]$	112002	$n \geq 10$	$\lfloor n/2 \rfloor$	This paper
		$[\![2,1,1]\!]$	112003	$n \geq 10$	$\lfloor n/2 \rfloor$	Refinement of $[\![2,2]\!]$
		$[\![1,1,1,1]\!]$	1200304	$n \geq 13$	n	This paper
5	9	$[\![4,1]\!]$	11112	$n \geq 9$	$\lfloor n/4 \rfloor$	Trivial
		$[\![3,2]\!]$	110200020001	$n \geq 15$	$\lfloor n/3 \rfloor$	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	$n \geq 23$	n	This paper
			1200300000000405	$n = 21$	21	This paper
6	11	$[\![5,1]\!]$	111112	$n \geq 11$	$\lfloor n/5 \rfloor$	Trivial
		$[\![4,2]\!]$	1111200002	$n \geq 20$	$\lfloor n/4 \rfloor$	This paper
		$[\![4,1,1]\!]$	1111200003	$n \geq 20$	$\lfloor n/4 \rfloor$	Refinement of $[\![4,2]\!]$
		$[\![3,3]\!]$	111200020002	$n \geq 21$	$\lfloor n/3 \rfloor$	This paper
		$[\![3,2,1]\!]$	111200020003	$n \geq 21$	$\lfloor n/3 \rfloor$	Refinement of $[\![3,3]\!]$
		$[\![3,1,1,1]\!]$	111200030004	$n \geq 21$	$\lfloor n/3 \rfloor$	This paper
		$[\![2,2,2]\!]$	1120020030000003	$n \geq 30$ or $n = 26$	$\lfloor n/2 \rfloor$	This paper
		$[\![2,2,1,1]\!]$	1120020030000004	$n \geq 30$ or $n = 26$	$\lfloor n/2 \rfloor$	Refinement of $[\![2,2,2]\!]$
		$[\![2,1,1,1,1]\!]$	1120030040000005	$n \geq 30$ or $n = 26$	$\lfloor n/2 \rfloor$	Refinement of $[\![2,2,2]\!]$
		$[\![1,1,1,1,1,1]\!]$	1200300000040500006	$n \geq 35$ or $n = 31$	n	This paper

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 $A_q(n, 2\sum\bar{w}-1, \bar{w})$ with $\sum\bar{w} \leq 6$, 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: $A_q(n, 2\sum\bar{w}-1, \bar{w}) \leq A_2(n, 2\sum\bar{w}-2, \sum\bar{w})$.

Table I 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^{n-4}. In order to construct these base codewords, we use either optimal Golomb rulers or a simple computer search to establish the best $\bar{\lambda}$-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 note that the values of $A_3(n, 2(w_1+w_2)-1, [\![w_1, w_2]\!])$ are included for completeness although they have been determined earlier by Östergård and Svanström [6, Th. 8].

Table III gives the exact value of $N_{\rm ccc}(\bar{w})$ for all $\bar{w}$ such that $\sum\bar{w} \leq 6$, except when $\bar{w} = [\![1,1,1,1,1,1]\!]$. We compare these values with bounds on $N_{\rm ccc}(\bar{w})$ given by (3) 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.

TABLE II
SIZES OF SOME SMALL OPTIMAL CONSTANT-COMPOSITION CODES WITH $d = 2\sum\bar{w} - 1$

$\overline{w}$ \ n	6	7	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
$[\![1,1]\!]$																											
$[\![2,1]\!]$																											
$[\![1,1,1]\!]$	4																										
$[\![3,1]\!]$	1																										
$[\![2,2]\!]$	1	2	2	3																							
$[\![2,1,1]\!]$	1	2	2	3																							
$[\![1,1,1,1]\!]$	1	2	2	3	5	6	9																				
$[\![4,1]\!]$	1	1	1																								
$[\![3,2]\!]$	1	1	1	2	2	2	3	3	4																		
$[\![3,1,1]\!]$	1	1	1	2	2	2	3	3	4																		
$[\![2,2,1]\!]$	1	1	1	2	2	2	3	3	4	6	6	7															
$[\![2,1,1,1]\!]$	1	1	1	2	2	2	3	3	4	6	6	7															
$[\![1,1,1,1,1]\!]$	1	1	1	2	2	2	3	3	4	6	6	7	9	12	16		21										
$[\![5,1]\!]$	1	1	1	1	1																						
$[\![4,2]\!]$	1	1	1	1	1	2	2	2	2	3	3	3	4	4													
$[\![4,1,1]\!]$	1	1	1	1	1	2	2	2	2	3	3	3	4	4													
$[\![3,3]\!]$	1	1	1	1	1	2	2	2	2	3	3	3	4	4	5												
$[\![3,2,1]\!]$	1	1	1	1	1	2	2	2	2	3	3	3	4	4	5												
$[\![3,1,1,1]\!]$	1	1	1	1	1	2	2	2	2	3	3	3	4	4	5												
$[\![2,2,2]\!]$	1	1	1	1	1	2	2	2	2	3	3	3	4	4	5	7	7	8	9	10		13	14	14			
$[\![2,2,1,1]\!]$	1	1	1	1	1	2	2	2	2	3	3	3	4	4	5	7	7	8	9	10		13	14	14			
$[\![2,1,1,1,1]\!]$	1	1	1	1	1	2	2	2	2	3	3	3	4	4	5	7	7	8	9	10		13	14	14			
$[\![1,1,1,1,1,1]\!]$	1	1	1	1	1	2	2	2	2	3	3	3	4	4	5	7	7	8	9	10	13	14	16	20	25		31

TABLE III
$N\mathrm{ccc}(\bar{w})$ AND BOUNDS ON $N_{\mathrm{ccc}}(\bar{w})$

Weight	Distance	Composition $\overline{w}$	$N_{\mathrm{ccc}}(\overline{w})$	Bounds on $N_{\mathrm{ccc}}(\overline{w})$ from (3) and Proposition 7.1
2	3	$[\![1,1]\!]$	3	$[3,3]$
3	5	$[\![2,1]\!]$	5	$[5,17]$
		$[\![1,1,1]\!]$	7	$[7,9]$
4	7	$[\![3,1]\!]$	7	$[7,55]$
		$[\![2,2]\!]$	10	$[10,37]$
		$[\![2,1,1]\!]$	10	$[10,37]$
		$[\![1,1,1,1]\!]$	13	$[13,19]$
5	9	$[\![4,1]\!]$	9	$[9,129]$
		$[\![3,2]\!]$	14	$[13,97]$
		$[\![3,1,1]\!]$	14	$[13,97]$
		$[\![2,2,1]\!]$	18	$[17,65]$
		$[\![2,1,1,1]\!]$	18	$[17,65]$
		$[\![1,1,1,1,1]\!]$	23	$[21,33]$
6	11	$[\![5,1]\!]$	11	$[11,251]$
		$[\![4,2]\!]$	18	$[16,201]$
		$[\![4,1,1]\!]$	18	$[16,201]$
		$[\![3,3]\!]$	21	$[21,151]$
		$[\![3,2,1]\!]$	21	$[21,151]$
		$[\![3,1,1,1]\!]$	21	$[21,151]$
		$[\![2,2,2]\!]$	30	$[26,101]$
		$[\![2,2,1,1]\!]$	30	$[26,101]$
		$[\![2,1,1,1,1]\!]$	30	$[26,101]$
		$[\![1,1,1,1,1,1]\!]$	$\in [33,35]$	$[31,51]$

A. Weight Four Codes

1) An optimal $(10,7,[\![1,1,1,1]\!])_5$-code:

0004021300 2103000040 0040000132 1000204003
0320140000.

2) An optimal $(11,7,[\![1,1,1,1]\!])_5$-code:

30000200041 00100034020 20014003000 00003040102
01320000004 04000301200.

3) An optimal $(12,7,[\![1,1,1,1]\!])_5$-code:

010020043000 000200301004 120000000403
200040100030 400301020000 002000430100
003014000002 034100000020 000002004310.

B. Weight Five Codes

1) An optimal $(15,9,[\![2,2,1]\!])_4$-code:

002100200000103 201010003200000 000300000122010
000021030010002 010002002001300 120000120000030.

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:

00301002000020010 00003210010000200
10000031000200002 00020100002100030
20000000123010000 00010003200002100
01200020001003000.

4) An optimal $(n,9,[\![2,1,1,1]\!])_5$-code, $n \in [15,17]$:
Refinement of an optimal $(n,9,[\![2,2,1]\!])_4$-code $n \in [15,17]$.

5) An optimal $(n,9,[\![1,1,1,1,1]\!])_6$-code $n \in [15,18]$:
Refinement of an optimal $(n,9,[\![2,1,1,1]\!])_4$-code $n \in [15,18]$.

6) An optimal $(19,9,[\![1,1,1,1,1]\!])_6$-code:

0045203000000000010 5010020040000000003
0000100050034002000 3004000100000205000
0000400000000320501 0100340200500000000
0503000014000000200 0000002301040000005
4000001000205000300 0000010002003500040
0020000005100034000 2300000000010040050.

7) An optimal $(20, 9, [\![1, 1, 1, 1, 1]\!])_6$-code:

00020000500300004010 51000003400002000000
00000005040000000132 00000350000001002400
02100040003000000050 00001034000200050000
00400200100000030005 00000010250040300000
04050000000030010200 10000000025000043000
20003100000050000040 03005000000000201004
30200000000100400500 00000000001524000003
00030502004000100000 00342000010005000000.

8) An optimal $(22, 9, [\![1, 1, 1, 1, 1]\!])_6$-code:
Lengthening of an optimal $(21, 9, [\![1, 1, 1, 1, 1]\!])_6$-code.

C. Weight Six Codes

1) An optimal $(20, 11, [\![3, 3]\!])_3$-code:

10000000020201002010 00101002001020000020
00022120000100000001 00010000202000201100
01000001000002010202.

2) An optimal $(20, 11, [\![3, 2, 1]\!])_4$-code:
Refinement of an optimal $(20, 11, [\![3, 3]\!])_3$-code.
3) An optimal $(20, 11, [\![3, 1, 1, 1]\!])_5$-code:
Refinement of an optimal $(20, 11, [\![3, 3]\!])_3$-code.
4) An optimal $(20, 11, [\![2, 2, 2]\!])_4$-code:
Refinement of an optimal $(20, 11, [\![4, 2]\!])_3$-code.
5) An optimal $(21, 11, [\![2, 2, 2]\!])_4$-code:

010000332000100020000 033000000021020000010
302010200300000000001 000103000210000032000
200001020003000300100 000200001000001000323
000020000000213103000.

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:

10020200000001000033000 20000031200100030000000
00000003020000200110030 00031020000000000000123
00000000013000013002002 01000000300023000200001
00100000001330000020200 02302300000000101000000.

8) An optimal $(24, 11, [\![2, 2, 2]\!])_4$-code:

300000100000200300000012
030200201300000000001000
010020030002000103000000
000010300020030000010200
003000012000100020000300
200000000213003010000000
000100000000020031200003
100001020000000000332000
001332000000001000000020.

9) An optimal $(25, 11, [\![2, 2, 2]\!])_4$-code:

0000000001223100030000000
0000000100002030003002100
0003001000001003000020002
0030000210000200100000003
1000030020000002010000300
0000100000100000200330200
0101000030300000002000020
3012300002000010000000000
0020003000000000020101030
0300212300010000000000000.

10) An optimal $(27, 11, [\![2, 2, 2]\!])_4$-code:
Lengthening of an optimal $(26, 11, [\![2, 2, 2]\!])_4$-code.
11) An optimal $(28, 11, [\![2, 2, 2]\!])_4$-code:

1100000000022000030000000003000
0000001102000000000000030032000
0000110000000300320002000000000
0200000000100103000320000000000
2010200000000000000000300010003
0020020003100100000000000300000
0000302000030020000000110000000
0000000200302000010000000000031
0031003000000000200100000000020
3000000010000000002201300000000
0002030000001000003010000000200
0000000000000301000000200130200
0300000030000000000000000220110
0003000320000210100000000000000.

12) An optimal $(29, 11, [\![2, 2, 2]\!])_4$-code:
Lengthening of an optimal $(28, 11, [\![2, 2, 2]\!])_4$-code.
13) An optimal $(n, 11, [\![2, 2, 1, 1]\!])_5$-code $n \in [20, 29]$:
Refinement of an optimal $(n, 11, [\![2, 2, 2]\!])_4$-code $n \in [20, 29]$.
14) An optimal $(n, 11, [\![2, 1, 1, 1, 1]\!])_6$-code $n \in [20, 29]$:
Refinement of an optimal $(n, 11, [\![2, 2, 2]\!])_4$-code $n \in [20, 29]$.
15) An optimal $(n, 11, [\![1, 1, 1, 1, 1, 1]\!])_7$-code $n \in [20, 26]$:
Refinement of an optimal $(n, 11, [\![2, 1, 1, 1, 1]\!])_6$-code $n \in [20, 26]$.
16) An optimal $(27, 11, [\![1, 1, 1, 1, 1, 1]\!])_7$-code:

010000000002003040506000000
001000000200300004650000000
100000000020030400065000000
020000000300000100000405060
002000000030000010000560004
200000000003000001000056400
000030400000000005001000026
000003040000000500100000602
000300004000000060020000510
000004500000610020000003000
000400050000061002000300000
000040005000106200000030000
345126000000000000000000000
000000123456000000000000000.

17) An optimal $(28, 11, [\![1, 1, 1, 1, 1, 1]\!])_7$-code: Shorten an optimal $(29, 11, [\![1, 1, 1, 1, 1, 1]\!])_7$-code.
18) An optimal $(29, 11, [\![1, 1, 1, 1, 1, 1]\!])_7$-code: Shorten an optimal $(30, 11, [\![1, 1, 1, 1, 1, 1]\!])_7$-code.
19) An optimal $(30, 11, [\![1, 1, 1, 1, 1, 1]\!])_7$-code: Shorten an optimal $(31, 11, [\![1, 1, 1, 1, 1, 1]\!])_7$-code.
20) An optimal $(32, 11, [\![1, 1, 1, 1, 1, 1]\!])_7$-code: Lengthening of an optimal $(31, 11, [\![1, 1, 1, 1, 1, 1]\!])_7$-code.

References

[1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[2] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, "A new table of constant weight codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1334–1380, Nov. 1990.

[3] E. Agrell, A. Vardy, and K. Zeger, "Upper bounds for constant-weight codes," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2373–2395, Nov. 2000.

[4] D. H. Smith, L. A. Hughes, and S. Perkins, "A new table of constant weight codes of length greater than 28," *Electron. J. Combin.*, vol. 13, no. 1, pp. 18–0, 2006, Article #A2 (electronic).

[5] M. Svanström, "Constructions of ternary constant-composition codes with weight three," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2644–2647, Nov. 2000.

[6] P. R. J. Östergård and M. Svanström, "Ternary constant weight codes," *Electron. J. Combin.*, vol. 9, no. 1, 2002, Research Paper 41 (electronic).

[7] M. Svanström, P. R. J. Östergård, and G. T. Bogdanova, "Bounds and constructions for ternary constant-composition codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 1, pp. 101–111, Jan. 2002.

[8] G. T. Bogdanova and S. N. Kapralov, "Enumeration of optimal ternary codes with a given composition," *Problemy Peredachi Informatsii*, vol. 39, no. 4, pp. 35–40, 2003.

[9] Y. Luo, F.-W. Fu, A. J. H. Vinck, and W. Chen, "On constant-composition codes over Z_q," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 3010–3016, Nov. 2003.

[10] W. Chu, C. J. Colbourn, and P. Dukes, "Constructions for permutation codes in powerline communications," *Des. Codes Cryptogr.*, vol. 32, no. 1–3, pp. 51–64, 2004.

[11] C. J. Colbourn, T. Kløve, and A. C. H. Ling, "Permutation arrays for powerline communication and mutually orthogonal Latin squares," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1289–1291, Jun. 2004.

[12] W. Chu, C. J. Colbourn, and P. Dukes, "Tables for constant composition codes," *J. Combin. Math. Combin. Comput.*, vol. 54, pp. 57–65, 2005.

[13] C. Ding and J. Yin, "Algebraic constructions of constant composition codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1585–1589, Apr. 2005.

[14] C. Ding and J. Yin, "Combinatorial constructions of optimal constant-composition codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3671–3674, Oct. 2005.

[15] C. Ding and J. Yuan, "A family of optimal constant-composition codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3668–3671, oct. 2005.

[16] C. Ding and J. Yin, "A construction of optimal constant composition codes," *Des. Codes Cryptogr.*, vol. 40, no. 2, pp. 157–165, 2006.

[17] Y. M. Chee and S. Ling, "Constructions for q-ary constant-weight codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 135–146, Jan. 2007.

[18] Y. M. Chee, A. C. H. Ling, S. Ling, and H. Shen, "The PBD-closure of constant-composition codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2685–2692, Aug. 2007.

[19] Y. M. Chee, S. H. Dau, A. C. H. Ling, and S. Ling, "The sizes of optimal q-ary codes of weight three and distance four: A complete solution," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 1291–1295, Mar. 2008.

[20] Y. M. Chee, G. Ge, and A. C. H. Ling, "Group divisible codes and their application in the construction of optimal constant-composition codes of weight three," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3552–3564, Aug. 2008.

[21] I. E. Telatar and R. G. Gallager, "Zero error decision feedback capacity of discrete memoryless channels," in *Proc. Bilkent Int. Conf. New Trends Commun. Control Signal Process.*, E. Arikan, Ed., 1990, pp. 228–233, Elsevier.

[22] A. G. D'yachkov, "Random constant composition codes for multiple access channels," *Problems Control Inf. Theory/Problemy Upravlen. Teor. Inf.*, vol. 13, no. 6, pp. 357–369, 1984.

[23] T. Ericson and V. Zinoviev, "Spherical codes generated by binary partitions of symmetric pointsets," *IEEE Trans. Inf. Theory*, vol. 41, no. 1, pp. 107–129, Jan. 1995.

[24] O. D. King, "Bounds for DNA codes with constant GC-content," *Electron. J. Combin.*, vol. 10, no. 1, 2003, Research Paper 33 (electronic).

[25] O. Milenkovic and N. Kashyap, *On the Design of Codes for DNA Computing*, ser. Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 2006, vol. 3969, pp. 100–119.

[26] Y. M. Chee and S. Ling, "Improved lower bounds for constant GC-content DNA codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 391–394, Jan. 2008.

[27] W. Chu, C. J. Colbourn, and P. Dukes, "On constant composition codes," *Discrete Appl. Math.*, vol. 154, no. 6, pp. 912–929, 2006.

[28] D. J. Costello and G. D. Forney, "Channel coding: The road to channel capacity," *Proc. IEEE*, vol. 95, no. 6, pp. 1150–1177, Jun. 2007.

[29] V. Rödl, "On a packing and covering problem," *Eur. J. Combin.*, vol. 5, pp. 69–78, 1985.

[30] P. Erdös and H. Hanani, "On a limit theorem in combinatorial analysis," *Publ. Math. Debrecen*, vol. 10, pp. 10–13, 1963.

[31] T. Etzion, "Optimal constant weight codes over Z_k and generalized designs," *Discrete Math.*, vol. 169, no. 1–3, pp. 55–82, 1997.

[32] T. Kløve, "Bounds on the size of optimal difference triangle sets," *IEEE Trans. Inf. Theory*, vol. IT-34, no. 2, pp. 355–361, Mar. 1988.

[33] T. Kløve, "Bounds and construction for difference triangle sets," *IEEE Trans. Inf. Theory*, vol. 35, no. 4, pp. 879–886, Jul. 1989.

[34] W. C. Babcock, "Intermodulation interference in radio systems," *Bell System Tech. J.*, vol. 31, pp. 63–73, 1953.

[35] A. R. Eckler, "The construction of missile guidance codes resistant to random interference," *Bell System Tech. J.*, vol. 38, pp. 973–994, 1960.

[36] J. Robinson and A. Bernstein, "A class of binary recurrent codes with limited error propagation," *IEEE Trans. Inf. Theory*, vol. IT-13, no. 1, pp. 106–113, Jan. 1967.

[37] F. Biraud, E. J. Blum, and J. C. Ribes, "On optimal synthetic linear arrays with applications to radioastronomy," *IEEE Trans. Antennas Propag.*, vol. AP-22, no. 1, pp. 108–109, Jan. 1974.

[38] E. J. Blum, J. C. Ribes, and F. Biraud, "Some new possibilities of optimal synthetic linear arrays for radioastronomy," *Astronom. Astrophys.*, vol. 41, pp. 409–411, 1975.

[39] R. J. F. Fang and W. A. Sandrin, "Carrier frequency assignment for nonlinear repeaters," *COMSAT Tech. Rev.*, vol. 7, pp. 227–245, 1977.

[40] M. D. Atkinson, N. Santoro, and J. Urrutia, "Integer sets with distinct sums and differences and carrier frequency assignment for nonlinear repeaters," *IEEE Trans. Commun.*, vol. COMM-34, no. 6, pp. 614–617, Jun. 1986.

[41] H. Hanani, "On some tactical configurations," *Can. J. Math.*, vol. 15, pp. 702–722, 1963.

[42] R. C. Baker, G. Harman, and J. Pintz, "The difference between consecutive primes. II," *Proc. London Math. Soc. (3)*, vol. 83, no. 3, pp. 532–562, 2001.

Yeow Meng Chee (SM'08) received the B.Math. degree in computer science and combinatorics and optimization and the M.Math. and Ph.D. degrees in computer science from the 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 B.S. 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 and 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.