Optimal q-Ary Error Correcting/All Unidirectional Error Detecting Codes

Yeow Meng Chee, *Senior Member, IEEE*, and Xiande Zhang

***Abstract*— Codes that can correct up to t symmetric errors and detect all unidirectional errors, known as t-EC-AUED codes, are studied in this paper. Given positive integers q, a, and t, let $n_q(a, t+1)$ denote the length of the shortest q-ary t-EC-AUED code of size a. We introduce combinatorial constructions for q-ary t-EC-AUED codes via one-factorizations of complete graphs, and concatenation of MDS codes and codes from resolvable set systems. Consequently, we determine the exact values of $n_q(a, t+1)$ for several new infinite families of q, a, and t.**

***Index Terms*— Unidirectional errors, EC-AUED codes, one-factorizations, concatenation.**

I. Introduction

CLASSICAL error control codes have been designed for use on binary *symmetric channels*, i.e., both $1 \to 0$ and $0 \to 1$ errors can occur during transmission. However, errors in some VLSI and optical systems are asymmetric in nature [1], [2], where the error probability from 1 to 0 is significantly higher than that from 0 to 1. Practically we can assume that only one type of errors can occur in those systems. These errors are called *asymmetric errors*.

Different from asymmetric errors, *unidirectional errors* can be caused by certain faults in digital devices, where both $1 \to 0$ and $0 \to 1$ type of errors are possible, but in any particular word all the errors are of the same type. Digital units that produce unidirectional errors as a consequence of internal failure are data transmission systems, magnetic recording mass memories, and LSI/VLSI circuits such as ROM memories [3]. The number of random errors caused by these failures is usually limited, while the number of unidirectional errors can be large. For this reason, it is useful to consider codes that are capable of correcting a relatively small number of random errors and detecting any number of unidirectional errors. Considerable attention has been paid to this problem, see for example [3]–[16].

Manuscript received April 12, 2017; revised November 1, 2017; accepted January 15, 2018. Date of publication January 31, 2018; date of current version July 12, 2018. X. Zhang was supported by NSFC under Grant 11771419 and Grant 11301503. This work was supported by the Fundamental Research Funds for the Central Universities.

Y. M. Chee is with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371 (e-mail: ymchee@ntu.edu.sg).

X. Zhang is with the School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, China (e-mail: drzhangx@ustc.edu.cn).

Communicated by M. Lentmaier, Associate Editor for Coding Theory.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2018.2800055

In 1973, Varshamov introduced a q-ary asymmetric channel [17], where the inputs and outputs of the channel are sequences over the q-ary alphabet $R = \{0, 1, \ldots, q-1\}$. If the symbol i is transmitted then the only symbols which the receiver can get are $i, i+1, \ldots, q-1$. We say that the type of this error is *increasing*. Naturally, we have another type of error which is *decreasing*. The *q-ary unidirectional channel* is the channel on which all errors within a codeword are of the same type (all increasing or all decreasing). Recent work on q-ary unidirectional errors can be found in [5] and [18]–[21] for example.

In this paper, we study constructions for q-ary codes which can correct up to t symmetric errors and detect all unidirectional errors (known as t-EC-AUED codes). We are only interested in codes that are optimal when considering the shortest lengths for given sizes. Let $n_q(a, t+1)$ denote the length of the shortest q-ary t-EC-AUED code of size a. We introduce several combinatorial constructions for t-EC-AUED codes and determine the exact values of $n_q(a, t+1)$ for new infinite families of q, a and t.

Our main results are as follows:

(i) determining values of $n_3(a, t+1)$ for $a \leq 12$ and all t;

(ii) for integers $k \geq 2$, $n_k(a, k-1) = 2k-1$ with $k+1 \leq a \leq 2k-1$; if k is odd, then $n_k(2k, k-1) = 2k-1$;

(iii) for prime powers $q \geq 2$, $n_q(a, q) = 2q+2$ with $2q-1 \leq a \leq q^2$;

(iv) given positive integers s, $\lambda \geq 1$ and $\alpha \geq 2$,

$$n_q(sn, T) = 2\lambda s(n-1)/(\alpha-1)$$

for all sufficiently large n satisfying $sn \equiv 0 \pmod{\alpha}$ and $\lambda s(n-1) \equiv 0 \pmod{\alpha-1}$, where $T = \frac{\lambda s(n-1)}{\alpha-1} - \lambda$ and $q = \frac{sn}{\alpha}$;

(v) given positive integers $\lambda \geq 1$ and $\alpha \geq 2$,

$$n_q(\alpha q, T) = 2\lambda(\alpha q - 1)/(\alpha - 1) - 2$$

for all sufficiently large q satisfying $\lambda(\alpha q - 1) \equiv 0 \pmod{\alpha - 1}$, where $T = \frac{\lambda\alpha(q-1)}{\alpha-1} - 1$.

(vi) values for several other families of $n_q(a, t+1)$ are stated in Table I.

Previously, only values of $n_2(a, t+1)$ for $a \leq 14$ and $n_3(a, t+1)$ for $a \leq 9$ were known by [5].

Our paper is organized as follows. In Section II, we introduce necessary notation and briefly describe the problem status. Section III gives a construction of optimal EC-AUED codes from near one-factorizations, where result (ii) is

TABLE I
VALUES OF $n_q(a,T)$ FROM LEMMAS 18 AND 20

k	q	a	T	$n_q(a,T)$	Apply Lemma 18 with
≥ 1	$2k+1$	$[4k+1, 6k+3]$	$3k$	$6k+2$	RBIBD$(6k+3,3,1)$
≥ 3	$2k$	$[4k-1, 6k]$	$3k-2$	$6k-2$	$(3,1)$-RGDD of type 2^{3k}
≥ 1	$3k+1$	$[6k+1, 12k+4]$	$4k$	$8k+2$	RBIBD$(12k+4,4,1)$
≥ 2	$3k$	$[6k-1, 12k]$	$4k-2$	$8k-2$	$(4,1)$-RGDD of type 3^{4k}
≥ 58	$3k+2$	$[6k+3, 12k+8]$	$4k+1$	$8k+4$	$(4,1)$-RGDD of type 2^{6k+4}
k	q	a	T	$n_q(a,T)$	Apply Lemma 20 with
≥ 2	$2k+1$	$[4k+1, 6k+3]$	$3k-1$	$6k+2$	RBIBD$(6k+3,3,1)$
≥ 2	$3k+1$	$[6k+1, 12k+4]$	$4k-1$	$8k+2$	RBIBD$(12k+4,4,1)$

obtained. In Section IV, we apply concatenation method to various codes with good Hamming distance to get results (iii)-(vi). In Section V, we improve results in [5] and determine completely $n_3(a, t+1)$ for $a \leq 12$ and all t, which is our result (i). Finally, a conclusion is given in Section VI.

II. PRELIMINARIES

Necessary and sufficient conditions for correcting and detecting errors of each of the three types, symmetric, asymmetric and unidirectional, are known in [22] and [23]. To state these conditions, we need some necessary notation.

Let X be a finite set, and R^X denote 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, $\mathsf{u} = (\mathsf{u}_x)_{x \in X}$, and $\mathsf{u}_x \in R$ for each $x \in X$. For $\mathsf{x}, \mathsf{y} \in R^X$, let $N(\mathsf{x}, \mathsf{y})$ denote the number of positions i where $\mathsf{x}_i > \mathsf{y}_i$. If $N(\mathsf{y}, \mathsf{x}) = 0$, then the vector x is said to *cover* the vector y and we write $\mathsf{x} \geq \mathsf{y}$. If $\mathsf{x} \geq \mathsf{y}$ or $\mathsf{y} \geq \mathsf{x}$ the vectors x and y are said to be *ordered*, otherwise they are *unordered*.

A *code* is a set $\mathcal{C} \subseteq R^X$ for some X. The elements of $\mathcal{C}$ are called *codewords*. A code is called a *t-EC-AUED code* if it is able to correct up to t symmetric errors and detect all unidirectional errors. Clearly a code is 0-EC-AUED if any pair of codewords are unordered. For general t, a characterization of when a code is a t-EC-AUED code is known as follows.

Theorem 1 [24]: A code $\mathcal{C}$ is a t-EC-AUED code if and only if $N(\mathsf{x}, \mathsf{y}) \geq t+1$ and $N(\mathsf{y}, \mathsf{x}) \geq t+1$, for all distinct $\mathsf{x}, \mathsf{y} \in \mathcal{C}$.

Define the *asymmetric distance* of two vectors x and y as $d_{as}(\mathsf{x}, \mathsf{y}) = \min\{N(\mathsf{x}, \mathsf{y}), N(y, \mathsf{x})\}$. Then codes with minimum asymmetric distance T are $(T-1)$-EC-AUED codes. Let $n_q(a, T)$ denote the length of the shortest q-ary $(T-1)$-EC-AUED code of size a. We say that a q-ary $(T-1)$-EC-AUED code of length $n_q(a, T)$ and size a is *optimal*.

The lower bound derived by Böinck and van Tilborg [4] for the length of binary $(T-1)$-EC-AUED codes is

$$n_2(a, T) \geq \left\lceil (4 - \frac{2}{\lceil a/2 \rceil})T \right\rceil.$$

In the same paper, they show that if $n_2(a, T) = (4 - \frac{2}{\lceil a/2 \rceil})T$ holds, then the code must be a constant weight code; and if further $a \equiv 0 \pmod 4$, then T must be divisible by $a/2$.

For non-binary codes, the lower bound of $n_q(a, T)$ was generalized in [5].

Theorem 2 [5]: $n_q(a, T) \geq GBT_q(a, T)$, where

$$GBT_q(a, T) = \left\lceil \frac{2a(a-1)T}{a(a-\alpha) - (a - \alpha q)(\alpha + 1)} \right\rceil$$

and $\alpha = \lfloor a/q \rfloor$.

The function GBT has a property that for all $\mu \geq 0$, $GBT_q(q\mu + (q-1), T) = GBT_q(q\mu + q, T)$. That is, by deleting one codeword from the optimal code of size $q\mu + q$, we obtain an optimal code of size $q\mu + (q-1)$.

Lemma 3 [5]: If $n_q(q\mu + q, T) = GBT_q(q\mu + q, T)$, then $n_q(q\mu + q - 1, T) = GBT_q(q\mu + q - 1, T)$.

In fact, Lemma 3 can be extended whenever $n_q(a, T) = GBT_q(a, T)$ and $GBT_q(a', T) = GBT_q(a, T)$, for $a' < a$.

Both the Böinck-van Tilborg bound and GBT bound are closely related to Plotkin bound, where the codes achieve the bounds when each symbol occurs almost the same number of times in a fixed position. In such cases, concatenating short codes is a very useful method to construct optimal long codes [25]. As stated in the following lemma, Naydenova and Kløve [5] showed that optimal t-EC-AUED codes could be obtained by concatenating two optimal short codes for fixed q, a and general T.

Lemma 4 [5]: If $n_q(a, T_1) = GBT_q(a, T_1)$, $n_q(a, T_2) = GBT_q(a, T_2)$, and

$$GBT_q(a, T_1) + GBT_q(a, T_2) = GBT_q(a, T_1 + T_2),$$

then

$$n_q(a, T_1 + T_2) = GBT_q(a, T_1 + T_2).$$

By Theorem 2, we have $n_q(a, T) \geq 2T$ if $q \geq a$. In fact, $n_q(a, T) = 2T$ in this case since the $a \times 2T$ array formed by T column vectors $(1, 2, \ldots, a)$ and T column vectors $(a, a-1, \ldots, 1)$ is an optimal code. From now on, we assume that $q < a$.

In [5], the values of $n_2(a, T)$ for $a \leq 14$ and all T have been determined by direct constructions and the Böinck-van Tilborg bound. For ternary case, they constructed some optimal codes up to size 9. We summarize their results for ternary codes as below.

Lemma 5 [5]: For $T \geq 1$, we have

(i) $n_3(a, T) = GBT_3(a, T)$ for $a \in \{4, 5, 6\}$;
(ii) $\lceil 21T/8 \rceil \leq n_3(7, T) \leq \lceil 8T/3 \rceil$;
(iii) $n_3(a, T) = \lceil 8T/3 \rceil = GBT_3(a, T)$ for $a \in \{8, 9\}$ and $T \not\equiv 1 \pmod 3$.

III. A Construction from One-Factorizations

In this section, we give a construction of optimal q-ary t-EC-AUED codes based on one-factorizations, which yield our main result (ii) by the extension of Lemma 3. For integers $m \leq n$, the set of integers $\{m, m+1, \ldots, n\}$ is denoted by $[m, n]$. When $m = 1$, the set $[1, n]$ is further abbreviated to $[n]$.

Let $a = 2k-1$. The ring $\mathbb{Z}/a\mathbb{Z}$ is denoted by $\mathbb{Z}_a$. Let K_a be a complete graph with vertex set $\mathbb{Z}_a$. For each $j \in \mathbb{Z}_a$, take

$$T_j = \{\{t+j, -t+j\} : 1 \leq t \leq k-1\}, \tag{1}$$

where the addition is in $\mathbb{Z}_a$. Then $\{T_j : j \in \mathbb{Z}_a\}$ is a *near one-factorization of* K_a. Each T_j is a *near one-factor* which misses the vertex j.

Construction 6: For each $k \geq 2$, construct a $(2k-1) \times (2k-1)$ array A over $[0, k-1]$, where rows and columns are indexed by $\mathbb{Z}_{2k-1}$. For a cell in the ith row and the jth column, let $A_{i,j} = 0$ if $i = j$ and $A_{i,j} = x$ if $i \in \{x+j, -x+j\}$. Let $\mathcal{A}$ be the collection of rows of A.

Theorem 7: $n_k(2k-1, k-1) = 2k-1$ for all integers $k \geq 2$.

Proof: By Theorem 2, we have $n_k(2k-1, k-1) \geq 2k-1$. It suffices to prove that the code $\mathcal{A}$ constructed in Construction 6 has minimum asymmetric distance $k-1$.

For any two rows x and y of A indexed by i_1 and i_2 respectively, we claim that $N(\mathsf{x}, \mathsf{y}) \geq k-1$. In fact, by the definition of near one-factorization, there exists a column indexed by j_0 and an element $x_0 \in [k-1]$ such that $\{i_1, i_2\} = \{x_0 + j_0, -x_0 + j_0\} \in T_{j_0}$, i.e., $A_{i_1,j_0} = A_{i_2,j_0} = x_0$. Without loss of generality, assume that $i_1 = x_0 + j_0$ and $i_2 = -x_0 + j_0$. Thus for each $y \in [k-1]$, we have

$$i_1 = -y + j_0 + (x_0 + y)$$

and

$$i_2 = y + j_0 + (-x_0 - y)$$

in $\mathbb{Z}_{2k-1}$. By the construction of A, we have $A_{i_1,j_0-y} = A_{i_2,j_0+y}$ which equals $x_0 + y$ or $-(x_0+y)$ whoever falls in $[k-1]$. So for each $y \in [k-1]$, if $A_{i_1,j_0-y} > A_{i_2,j_0-y}$, we must have $A_{i_1,j_0+y} < A_{i_2,j_0+y}$. Thus $N(\mathsf{x}, \mathsf{y}) = N(\mathsf{y}, \mathsf{x}) = k-1$. ∎

Example 8: Let $k = 2$ and $k = 3$. Then applying Construction 6 and Theorem 7 gives an optimal binary 0-EC AUED codes of size three, and an optimal ternary 1-EC AUED codes of size five.

$$\begin{array}{c} 0\,1\,1 \\ 1\,0\,1 \\ 1\,1\,0 \end{array} \qquad \begin{array}{c} 0\,1\,2\,2\,1 \\ 1\,0\,1\,2\,2 \\ 2\,1\,0\,1\,2 \\ 2\,2\,1\,0\,1 \\ 1\,2\,2\,1\,0 \end{array}$$

Remark 1: The array A from Construction 6 has extra property that in each row, each nonzero element occurs twice and the zero element occurs exactly once.

Construction 9: For odd integers $k \geq 3$, let B be a $(2k-1) \times (2k-1)$ array with the entry $B_{i,j} \equiv A_{i,j} + (k-1)/2 \pmod{k}$, where A is the array from Construction 6. Let u be a vector of length $2k-1$ with all entries being $(k-1)/2$. Denote $\mathcal{B}$ the collection of rows of B and let $\mathcal{B}' = \mathcal{B} \cup \{\mathsf{u}\}$.

Theorem 10: $n_k(2k, k-1) = 2k-1$ for all odd integers $k \geq 3$.

Proof: The lower bound can be checked by Theorem 2. For the upper bound, we only need to show that $\mathcal{B}$ in Construction 9 is a $(k-2)$-EC-AUED code by Remark 1. This follows from the fact that $B_{i_1,j_0-y} = B_{i_2,j_0+y}$ for each $y \in [1, k-1]$ as in the proof of Theorem 7. ∎

Example 11: Applying Construction 9 and Theorem 10 with $k = 3$ gives an optimal ternary 1-EC AUED codes of size six.

$$\begin{array}{c} 1\,1\,1\,1\,1 \\ 1\,2\,0\,0\,2 \\ 2\,1\,2\,0\,0 \\ 0\,2\,1\,2\,0 \\ 0\,0\,2\,1\,2 \\ 2\,0\,0\,2\,1 \end{array}$$

IV. A Construction by Concatenation

We first give a simple but very useful construction of EC-AUED codes by concatenation. As mentioned in Section II, this method has been widely used to construct codes achieving Plotkin type bounds. For any q-ary word $c = (c_1, c_2, \ldots, c_n)$, let $q-1-c := (q-1-c_1, q-1-c_2, \ldots, q-1-c_n)$ and $c|(q-1-c) = (c_1, \ldots, c_n, q-1-c_1, \ldots, q-1-c_n)$. For any two words x and y, the Hamming distance of x and y, denoted by $d_H(\mathsf{x}, \mathsf{y})$, is the number of positions i such that $\mathsf{x}_i = \mathsf{y}_i$. It is obvious that $d_H(\mathsf{x}, \mathsf{y}) = N(\mathsf{x}, \mathsf{y}) + N(\mathsf{y}, \mathsf{x})$.

Lemma 12: Let C be a q-ary code of length n with minimum Hamming distance d. Then $\{c|(q-1-c) : c \in C\}$ is a q-ary $(d-1)$-EC-AUED code of length $2n$ with $|C|$ words.

Proof: For any two words $\mathsf{x} = c|(q-1-c)$ and $\mathsf{y} = c'|(q-1-c')$, since $N(q-1-c, q-1-c') = N(c', c)$, we have $N(\mathsf{x}, \mathsf{y}) = N(c, c') + N(q-1-c, q-1-c') = N(c, c') + N(c', c) = d_H(c, c') \geq d$. It's similar that $N(\mathsf{y}, \mathsf{x}) \geq d$. ∎

By Lemma 12, we can construct good EC-AUED codes from codes with large Hamming distance.

Theorem 13: $n_q(q^2, q) = 2q+2$ for all prime powers q.

Proof: The lower bound is checked by Theorem 2. The upper bound is obtained by applying Lemma 12 to q-ary MDS codes of length $q+1$ and size q^2 with minimum Hamming distance q [26, Ch. 5]. ∎

A. Constructions from Set Systems

A *set system* is a pair $\mathfrak{S} = (X, \mathcal{A})$, where X is a finite set of *points* and $\mathcal{A} \subseteq 2^X$. Elements of $\mathcal{A}$ are called *blocks*. The *order* of $\mathfrak{S}$ is the number of points in X, and the *size* of $\mathfrak{S}$ is the number of blocks in $\mathcal{A}$. Let K be a set of positive integers. A set system $(X, \mathcal{A})$ is *K-uniform* if $|A| \in K$ for all $A \in \mathcal{A}$. A *parallel class* of a set system $(X, \mathcal{A})$ is a set $\mathcal{P} \subseteq \mathcal{A}$ that partitions X. A *resolvable set system* is a set system whose set of blocks can be partitioned into parallel classes. We refer

the readers to [27] for other related concepts in combinatorial design theory.

Definition 14: Let $(X, \mathcal{A})$ be a $\{k\}$-uniform set system of order n. Then it is an (n, k, λ)-*packing* if each pair of X occurs in at most λ blocks of $\mathcal{A}$.

Given a resolvable (qk, k, λ)-packing of n parallel classes, arbitrarily order the q blocks in each parallel class by elements in $[0, q-1]$. Define a $qk \times n$ q-ary matrix A by indexing each column by a parallel class and each row by a point of the packing. For each parallel class, the corresponding column has the symbol i in the rows indexed by the points in the ith block. Since each pair of points occurs in at most λ blocks, the rows of A form a q-ary code of Hamming distance at least $n-\lambda$. Note that this correspondence is the one used by Semakov and Zinoviev [28] to show the equivalence between *equidistant codes* and RBIBDs. Recently, this method is used again to construct optimal *equitable symbol weight codes*, see for example [29], [30]. By applying Lemma 12 to this equivalence, we have the following result.

Lemma 15: Suppose that there exists a resolvable (a, k, λ)-packing, which has n parallel classes each consisting of q blocks, $q = a/k$. Then there exists a q-ary t-EC-AUED code of size a and length $2n$ with $t = n - \lambda - 1$.

Next, we apply Lemma 15 to some concrete combinatorial objects to determine the values of $n_q(a, T)$.

Definition 16: Let $(X, \mathcal{A})$ be a $\{k\}$-uniform set system and let $\mathcal{G}$ be a partition of X into subsets, called *groups*. The triple $(X, \mathcal{G}, \mathcal{A})$ is a *group divisible design* (GDD) when every 2-subset of X not contained in a group is contained in exactly λ block, and $|A \cap G| \leq 1$ for all $A \in \mathcal{A}$ and $G \in \mathcal{G}$.

We denote such a GDD $(X, \mathcal{G}, \mathcal{A})$ by (k, λ)-GDD. It is obvious that a (k, λ)-GDD $(X, \mathcal{G}, \mathcal{A})$ is an (n, k, λ)-packing with $n = |X|$. The *type* of a GDD $(X, \mathcal{G}, \mathcal{A})$ is the multiset $\langle |G| : G \in \mathcal{G} \rangle$. When more convenient, the exponential notation is used to describe the type of a GDD: a GDD of type $g_1^{t_1} g_2^{t_2} \cdots g_s^{t_s}$ is a GDD where there are exactly t_i groups of size g_i, $i \in [s]$. When a GDD is resolvable, we denote it by RGDD. A (k, λ)-GDD of type 1^n is called a *balanced incomplete block design*, denoted by BIBD(n, k, λ) and RBIBD(n, k, λ) when it is resolvable.

Theorem 17 [31]: Fix integers $g, \lambda \geq 1$ and $k \geq 2$. There exists an integer $u_0(g, k)$ such that for all $u \geq u_0$, a (k, λ)-RGDD of type g^u exists if and only if $\lambda g(u-1) \equiv 0 \pmod{k-1}$ and $gu \equiv 0 \pmod{k}$.

Lemma 18: Suppose that there exists an (α, λ)-RGDD of type s^n, such that $2\lambda(s-1) < sn - \alpha$. Then $n_q(sn, T) = 2\lambda s(n-1)/(\alpha - 1)$, where $T = \frac{\lambda s(n-1)}{\alpha - 1} - \lambda$ and $q = \frac{sn}{\alpha}$.

Proof: It is easy to check that when $2\lambda(s-1) < sn - \alpha$, we have $n_q(sn, T) \geq 2\lambda s(n-1)/(\alpha - 1)$ by Theorem 2. The equality could be obtained by Lemma 15 and the fact that the given GDD is a resolvable (sn, α, λ)-packing. ∎

Theorem 19: Given positive integers s, $\lambda \geq 1$ and $\alpha \geq 2$, $n_q(sn, T) = 2\lambda s(n-1)/(\alpha - 1)$ for all sufficiently large n satisfying $sn \equiv 0 \pmod{\alpha}$ and $\lambda s(n-1) \equiv 0 \pmod{\alpha - 1}$, where $T = \frac{\lambda s(n-1)}{\alpha - 1} - \lambda$ and $q = \frac{sn}{\alpha}$.

Proof: For fixed s, α and λ, we have $2\lambda(s-1) < sn - \alpha$ for sufficiently large n. Hence the conclusion follows by Lemma 18 and the asymptotic existence of (α, λ)-RGDD of type s^n in Theorem 17. ∎

Lemma 20: If there exists an RBIBD$(\alpha q, \alpha, \lambda)$ with $q \geq 3$, then $n_q(\alpha q, T) = 2\lambda(\alpha q - 1)/(\alpha - 1) - 2$, where $T = \frac{\lambda \alpha(q-1)}{\alpha - 1} - 1$.

Proof: Delete one parallel class from the RBIBD$(\alpha q, \alpha, \lambda)$ to get a resolvable $(\alpha q, \alpha, \lambda)$-packing. Then apply Lemma 15. ∎

Theorem 21: Given positive integers $\lambda \geq 1$ and $\alpha \geq 2$, $n_q(\alpha q, T) = 2\lambda(\alpha q - 1)/(\alpha - 1) - 2$ for all sufficiently large q satisfying $\lambda(\alpha q - 1) \equiv 0 \pmod{\alpha - 1}$, where $T = \frac{\lambda \alpha(q-1)}{\alpha - 1} - 1$.

Proof: By the asymptotic existence RBIBD$(\alpha q, \alpha, \lambda)$ in Theorem 17. ∎

In Table I, we give some examples of exact values of $n_q(a, T)$ determined by Lemmas 18, 20 and the extension of Lemma 3. The existence of combinatorial objects used in this table can be found in [27].

Before closing this section, we note that for two binary vectors x and y of equal number of 1's, we have that $N(\mathsf{x}, \mathsf{y}) = N(\mathsf{y}, \mathsf{x}) = \frac{1}{2} d_H(\mathsf{x}, \mathsf{y})$. So a binary constant weight code with minimum Hamming distance d is a $(\frac{d}{2} - 1)$-EC AUED code. It's well known that the rows of the incidence matrix of a BIBD form a binary constant weight code. In Table II, we give two examples of equivalent objects for optimal binary EC AUED codes. However, the existence of corresponding BIBDs used in Table II is very rare by referring to [32].

V. Optimal Ternary t-EC-AUED Codes

In this section, we give some direct constructions of optimal ternary t-EC-AUED codes up to size 12. For some of the codes we search directly by computer, but when the length becomes big, the search space will be huge. In this case, we map each ternary code to be a resolvable set system as in Section IV. Suppose there is a ternary t-EC-AUED code of size a and length n. Let the rows be indexed by X of size a, then for each column, we obtain three blocks by collecting all the indices of rows with same entries. Thus we get a resolvable set system of order a and size $3n$, where each parallel class has three blocks. Conversely, we can get the corresponding ternary code from such a resolvable set system. However, to ensure that the code is a t-EC-AUED code, the set system must satisfy extra conditions, which are not easy to be characterized.

In the following constructions, if we construct a resolvable set system instead of the ternary code, we list the three blocks in each parallel class in order, for which the entries in the corresponding rows will be assigned to 0, 1 and 2 respectively. If we list the optimal code itself, we usually denote C_T the optimal $(T-1)$-EC-AUED code.

Further, in design theory, people usually equip the desired designs with some group structures to reduce the search space. What they do is try to find a partial result, which can be developed to the complete desired design by using the group structure. For example, if a block B is developed by $\mathbb{Z}_n$, then B_i, $i \in \mathbb{Z}_n$ are obtained such that $B_i = \{b + i : b \in B\}$. We will apply this idea to some of our constructions.

Lemma 22: $n_3(7, 8) = 21$.

Proof: Let $X = \mathbb{Z}_7$. The following nine blocks form three parallel classes, where each row is a parallel class. Develop

TABLE II
EQUIVALENT OBJECTS FOR BINARY CODES

a	T	$n_2(a,T)$	Optimal codes equivalent to
$4k+3$	$k+1$	$4k+3$	BIBD$(4k+3, 2k+1, k)$'s
$2k$	k	$4k-2$	BIBD$(2k, k, k-1)$'s

them to 21 parallel classes by $\mathbb{Z}_7$ and keep the order of blocks in each parallel class. Then one can check this resolvable set system gives a ternary 7-EC-AUED code of size 7 and length 21, which is optimal by the fact that $GBT_3(7,8) = 21$. In fact, the codewords are the rows of the 7×21 matrix $M = (A|B|C)$ where A, B and C are circulant matrices with rows indexed by $\mathbb{Z}_7$. The leftmost column of A has zeroes in rows 0, 1, 2, ones in rows 3 and 6, and twos in rows 4 and 5; the leftmost column of B has zeroes in rows 0, 2, 4, ones in rows 5 and 6, and twos in rows 1 and 3; and the leftmost column of C has zeroes in rows 0, 1, 4, ones in rows 3 and 5, and twos in rows 2 and 6.

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

In fact, this resolvable set system can be found in [33, Example 2.3] as a *class-uniformly resolvable design* with partition $2^2 3^1$. ∎

Theorem 23: $n_3(7,T) = \lceil \frac{21}{8} T \rceil$ for all $T \geq 1$.

Proof: For $a = 7$, we have $GBT_3(7,T) = \lceil \frac{21}{8} T \rceil$. When $1 \leq T \leq 7$, $n_3(7,T) = GBT_3(7,T)$ is known by [5]. By Lemma 22, $n_3(7,8) = GBT_3(7,8)$. Hence the construction $C_T = C_8 | C_{T-8}$ gives the optimal code of length $\lceil \frac{21}{8} T \rceil$ for all T by Lemma 4. ∎

Naydenova and Kløve [5], stated that $n_3(9,1) = 4 = GBT_3(9,1) + 1$ and $n_3(9,4) = 12 = GBT_3(9,4) + 1$ by computer search. However, the latter is not true. In fact, we find a 3-EC-AUED code of length 11 and with bigger size 12, which meets the bound in Theorem 2.

Lemma 24: $n_3(a,4) = 11$ for $8 \leq a \leq 12$.

Proof: For $8 \leq a \leq 12$, we have $GBT_3(a,4) = 11$. A 3-EC-AUED code of size 12 and length 11 is constructed below. For $8 \leq a \leq 11$, the optimal codes are obtained by collecting any set of a codewords from C_4.

$$C_4 = \begin{bmatrix} 10022021012 \\ 00202112021 \\ 20100211202 \\ 01020202211 \\ 12001122200 \\ 11111111111 \\ 21221100002 \\ 02112002102 \\ 12210201020 \\ 21012010220 \\ 22200020111 \\ 00121220120 \end{bmatrix}$$

∎

Hence by Lemmas 4 and 5, we determine all values of $n_3(8,T)$ and $n_3(9,T)$.

Theorem 25: $n_3(8,T) = n_3(9,T) = \lceil \frac{8}{3} T \rceil$ for all $T > 1$.

Next, we study values of $n_3(a,T)$ for $a \in \{10, 11, 12\}$. By Lemma 3, it is enough to consider the cases $a = 10, 12$, for which we have $GBT_3(10,T) = \lceil \frac{30T}{11} \rceil$ and $GBT_3(12,T) = \lceil \frac{11T}{4} \rceil$.

Lemma 26: $n_3(a,2) = 6$ for $7 \leq a \leq 16$ and $n_3(a,3) = 9$ for $10 \leq a \leq 25$.

Proof: For $7 \leq a \leq 16$, we have $GBT_3(a,2) = 6$, while for $10 \leq a \leq 25$, we have $GBT_3(a,3) = 9$. An optimal 1-EC-AUED code of size 16 and a 2-EC-AUED code of size 25 are listed below. Optimal codes with smaller sizes can be obtained by deleting some codewords from C_2 and C_3 respectively.

$$C_2 = \begin{bmatrix} 211002 \\ 202011 \\ 201120 \\ 100221 \\ 112020 \\ 120012 \\ 010122 \\ 021021 \\ 022110 \\ 012201 \\ 102102 \\ 111111 \\ 121200 \\ 210210 \\ 220101 \\ 001212 \end{bmatrix}, \quad C_3 = \begin{bmatrix} 010220211 \\ 211200102 \\ 220021101 \\ 102020112 \\ 122100201 \\ 111111111 \\ 110012202 \\ 001102212 \\ 022011210 \\ 012121002 \\ 200211012 \\ 221120010 \\ 202112100 \\ 021212001 \\ 120202110 \\ 100122021 \\ 002201121 \\ 011022120 \\ 020110122 \\ 112210020 \\ 121001022 \\ 201010221 \\ 210101220 \\ 212002011 \\ 101221200 \end{bmatrix}.$$

∎

By now, we have determined $n_3(12,T)$ for $2 \leq T \leq 4$. Since $n_3(9,1) = 4$, we have $n_3(12,1) \geq 4$ which is bigger than $GBT_3(12,1) = 3$. By Lemma 4, we still need to determine $n_3(12,5)$ to construct all optimal codes of size 12.

Lemma 27: $n_3(a,5) = 14$ for $10 \leq a \leq 12$.

Proof: For $10 \leq a \leq 12$, we have $GBT_3(a, 5) = 14$. An optimal code of size 12 is given below.

$$C_5 = \begin{bmatrix} 01212201221000 \\ 22002120022001 \\ 01000222102220 \\ 10201101112211 \\ 11021100201122 \\ 21112010101211 \\ 20022021210110 \\ 22220002000202 \\ 12120111120020 \\ 10110222011012 \\ 02211210010121 \\ 00101012222102 \end{bmatrix}$$

■

Hence by Lemmas 4 and 5, we determine all values of $n_3(12, T)$.

Theorem 28: $n_3(11, T) = n_3(12, T) = \left\lceil \frac{11T}{4} \right\rceil$ for all $T > 1$.

By simple computation, we know that $GBT_3(10, T) = GBT_3(12, T)$ for most integers T. The smallest integer T with $GBT_3(10, T) < GBT_3(12, T)$ is 11.

Lemma 29: $n_3(10, 11) = 30$.

Proof: Let $X = \mathbb{Z}_{10}$. The following nine blocks form three parallel classes in each row. Develop them to 30 parallel classes by $\mathbb{Z}_{10}$ and keep the order of blocks in each parallel class. Then one can check this resolvable set system gives a ternary 10-EC-AUED code of size 10 and length 30, which is optimal by Theorem 2. In fact, the codewords are the rows of the 10×30 matrix $M = (A|B|C)$ where A, B and C are circulant matrices with rows indexed by $\mathbb{Z}_{10}$. The leftmost column of A has zeroes in rows 0, 1, 2, 3, ones in rows 4, 6, 8, and twos in rows 5, 7, 9; the leftmost column of B has zeroes in rows 0, 1, 4, 5, ones in rows 2, 6, 9, and twos in rows 3, 7, 8; and the leftmost column of C has zeroes in rows 0, 2, 3, 7, ones in rows 1, 6, 9, and twos in rows 4, 5, 8.

$$\{0, 1, 2, 3\}, \{4, 6, 8\}, \{5, 7, 9\}$$
$$\{0, 1, 4, 5\}, \{2, 6, 9\}, \{3, 7, 8\}$$
$$\{0, 2, 3, 7\}, \{1, 6, 9\}, \{4, 5, 8\}$$

■

Now we are in a position to determine $n_3(10, T)$ for all $T > 1$.

Theorem 30: $n_3(10, T) = \left\lceil \frac{30T}{11} \right\rceil$ for all $T > 1$.

Proof: For $a = 10$, we have $GBT_3(10, T) = \left\lceil \frac{30T}{11} \right\rceil$. For $T = 2, \ldots, 10, 12$, the bound is met since $GBT_3(10, T) = GBT_3(12, T)$ for these cases. For $T = 11$, the bound is achieved by Lemma 29. The optimal code C_T for all $T \geq 13$ is given by recursion $C_T = C_{11}|C_{T-11}$. ■

Finally, for completeness, when $T = 1$, we note that $n_3(a, 1) = 4 = GBT_3(a, 1) + 1$ for $8 \leq a \leq 19$ since by de Bruijn *et al.* [34],

$$B(n, q) = \left\{ (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n | \sum_{i=1}^{n} x_i = \left\lceil \frac{n(q-1)}{2} \right\rceil \right\}$$

is a 0-EC-AUED code with maximal size for given length n.

VI. Conclusion

We investigated the length of the shortest q-ary t-EC-AUED codes of size a. A direct construction of optimal codes was given via one-factorizations of complete graphs. We further provided a general construction of a $(d-1)$-EC-AUED code of length $2n$ from a code of length n and minimum Hamming distance d. Finally, we would like to suggest the study of codes for which the words are the rows of a concatenation of circulant matrices, similar to those constructed from resolvable packings in Section V.

Acknowledgments

The authors thank the anonymous reviewers and the associate editor for their constructive comments and suggestions that greatly improved the quality of this paper.

References

[1] S. D. Constantin and T. R. N. Rao, "On the theory of binary asymmetric error correcting codes," *Inf. Control*, vol. 40, no. 1, pp. 20–36, Jan. 1979.
[2] J. Pierce, "Optical channels: Practical limits with photon counting," *IEEE Trans. Commun.*, vol. COM-26, no. 12, pp. 1819–1821, Dec. 1978.
[3] M. Blaum and H. Van Tilborg, "On t-error correcting/all unidirectional error detecting codes," *IEEE Trans. Comput.*, vol. 38, no. 11, pp. 1493–1501, Nov. 1989.
[4] F. J. H. Böinck and H. Van Tilborg, "Constructions and bounds for systematic tEC/AUED codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1381–1390, Nov. 1990.
[5] I. Naydenova and T. Kløve, "Some optimal binary and ternary t-EC-AUED codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 4898–4904, 2009.
[6] Y. M. Chee and A. C. H. Ling, "Limit on the addressability of fault-tolerant nanowire decoders," *IEEE Trans. Comput.*, vol. 58, no. 1, pp. 60–68, Jan. 2009.
[7] Z. Zhang and X.-X. Xia, "LYM-type inequalities for tEC/AUED codes," *IEEE Trans. Inf. Theory*, vol. 39, no. 1, pp. 232–238, Jan. 1993.
[8] Z. Zhang and C. Tu, "On the construction of systematic tEC/AUED codes," *IEEE Trans. Inf. Theory*, vol. 39, no. 5, pp. 1662–1669, Sep. 1993.
[9] J. Bruck and M. Blaum, "New techniques for constructing EC/AUED codes," *IEEE Trans. Comput.*, vol. 41, no. 10, pp. 1318–1324, Oct. 1992.
[10] M.-C. Lin, "Constant weight codes for correcting symmetric errors and detecting unidirectional errors," *IEEE Trans. Comput.*, vol. 42, no. 11, pp. 1294–1302, Nov. 1993.
[11] S. Al-Bassam, "Another method for constructing t-EC/AUED codes," *IEEE Trans. Comput.*, vol. 49, no. 9, pp. 964–966, Sep. 2000.
[12] D. Nikolos, N. Gaitanis, and G. Philokyprou, "Systematic t-error correcting/all unidirectional error detecting codes," *IEEE Trans. Comput.*, vol. C-35, no. 5, pp. 394–402, May 1986.
[13] D. K. Pradhan, "A new class of error-correcting/detecting codes for fault-tolerant computer applications," *IEEE Trans. Comput.*, vol. 29, no. 6, pp. 471–481, Jun. 1980.
[14] D. J. Lin and B. Bose, "Theory and design of t-error correcting and $d(d > t)$-unidirectional error detecting (t-EC d-UED) codes," *IEEE Trans. Comput.*, vol. 37, no. 4, pp. 433–439, Apr. 1988.
[15] D. L. Tao, C. R. P. Hartmann, and P. K. Lala, "An efficient class of unidirectional error detecting/correcting codes," *IEEE Trans. Comput.*, vol. C-37, no. 7, pp. 879–882, Jul. 1988.
[16] S. Kundu and S. M. Reddy, "On symmetric error correcting and all unidirectional error detecting codes," *IEEE Trans. Comput.*, vol. 39, no. 6, pp. 752–761, Jun. 1990.
[17] R. R. Varshamov, "A class of codes for asymmetric channels and a problem from the additive theory of numbers," *IEEE Trans. Inf. Theory*, vol. IT-19, no. 1, pp. 92–95, Jan. 1973.
[18] N. Elarief and B. Bose, "Optimal, systematic, q-ary codes correcting all asymmetric and symmetric errors of limited magnitude," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 979–983, Mar. 2010.

[19] F.-W. Fu, S. Ling, and C. Xing, "Constructions of nonbinary codes correcting t-symmetric errors and detecting all unidirectional errors: Magnitude error criterion," in *Coding, Cryptography Combinatorics*, K. Feng, H. Niederreiter, and C. Xing, Eds. Basel, Switzerland: Birkhäuser, 2004, pp. 139–152.
[20] R. Ahlswede, H. Aydinian, L. H. Khachatrian, and L. M. Tolhuizen, "On q-ary codes correcting all unidirectional errors of a limited magnitude," in *Proc. Int. Workshop Algebraic Combinat. Coding Theory (ACCT)*, Kranevo, Bulgaria, Jun. 2004, pp. 19–25.
[21] R. Ahlswede, H. Aydinian, and L. Khachatrian, "Unidirectional error control codes and related combinatorial problems," in *Proc. 8th Int. Workshop Algebraic Combinat. Coding Theory*, Tsarskoe Selo, Russia, Sep. 2002, pp. 6–9.
[22] J. H. Weber, "Bounds and constructions for binary block codes correcting asymmetric or unidirectional errors," Ph.D. dissertation, Dept. Softw. Eng., Delft Univ. Technol., Delft, The Netherlands, 1989.
[23] J. H. Weber, C. de Vroedt, and D. E. Boekee, "Necessary and sufficient conditions on block codes correcting/detecting errors of various types," *IEEE Trans. Comput.*, vol. 41, no. 9, pp. 1189–1193, Sep. 1992.
[24] B. Bose and T. Rao, "Theory of unidirectional error correcting/detecting codes," *IEEE Trans. Comput.*, vol. C-31, no. 6, pp. 521–530, Jun. 1982.
[25] C. Mackenzie and J. Seberry, "Maximal ternary codes and Plotkin's bound," *ARS Combinat.*, vol. 17A, pp. 251–270, 1984.
[26] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2010.
[27] G. Ge and Y. Miao, "PBDs, frames, and resolvability," in *Handbook of Combinatorial Designs*, 2nd ed. C. J. Colbourn and J. H. Dinitz, Eds. Boca Raton, FL, USA: CRC Press, 2007, pp. 261–265.
[28] N. V. Semakov and V. A. Zinoviev, "Equidistant q-ary codes with maximal distance and resolvable balanced incomplete block designs," *Problemi Peredatchi Inf.*, vol. 4, pp. 3–10, Jan. 1968.
[29] Y. M. Chee, H. M. Kiah, A. C. Ling, and C. Wang, "Optimal equitable symbol weight codes for power line communications," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2012, pp. 666–670.
[30] P. Dai, J. Wang, and J. Yin, "Two series of equitable symbol weight codes meeting the plotkin bound," *Designs, Codes Cryptogr.*, vol. 74, no. 1, pp. 15–29, 2015.
[31] J. H. Chan, P. J. Dukes, E. R. Lamken, and A. C. H. Ling, "The asymptotic existence of resolvable group divisible designs," *J. Combinat. Des.*, vol. 21, no. 3, pp. 112–126, 2013.
[32] Y. J. Ionin and T. van Trung, "Symmetric designs," in *Handbook of Combinatorial Designs*, 2nd ed. C. J. Colbourn and J. H. Dinitz, Eds. Boca Raton, FL, USA: CRC Press, 2007, pp. 110–124.
[33] P. Danziger and B. Stevens, "Class-uniformly resolvable designs," *J. Combinat. Des.*, vol. 9, no. 2, pp. 79–99, 2001.
[34] N. G. de Bruijn, C. van E. Tengbergen, and D. Kruyswijk, "On the set of divisors of a number," *Nieuw Arch. Wiskunde*, vol. 23, no. 2, pp. 191–193, 1951.

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 a 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.

Xiande Zhang received the Ph.D. degree in mathematics from Zhejiang University, Hangzhou, Zhejiang, P. R. China in 2009. From 2009 to 2015, she held postdoctoral positions in Nanyang Technological University and Monash University. Currently, she is a Research Professor at school of Mathematical Sciences, University of Science and Technology of China. Her research interests include combinatorial design theory, coding theory, cryptography, and their interactions. She received the 2012 Kirkman Medal from the Institute of Combinatorics and its Applications.