REPORTS
IN
INFORMATICS

ISSN 0333-3590

Optimal Binary and Ternary t-EC-AUED Codes

Irina Naydenova, Torleiv Kløve

REPORT NO 377 **November 2008**

Department of Informatics

UNIVERSITY OF BERGEN

Bergen, Norway

This report has URL http://www.ii.uib.no/publikasjoner/texrap/ps/2008-377.ps

Reports in Informatics from Department of Informatics, University of Bergen, Norway, is available at http://www.ii.uib.no/publikasjoner/texrap/.

Requests for paper copies of this report can be sent to:

Department of Informatics, University of Bergen, Høyteknologisenteret,
P.O. Box 7800, N-5020 Bergen, Norway

Optimal Binary and Ternary t-EC-AUED Codes

Irina Naydenova, Torleiv Kløve, Fellow, IEEE
Department of Informatics,
University of Bergen, Norway
irina_gancheva@yahoo.com, Torleiv.Klove@ii.uib.no

Abstract

This paper is devoted to the non-symmetric channels. Here we will present t-EC-AUED codes. Böinck and van Tilborg gave a bound on the length of binary t-EC-AUED codes. A generalization of this bound to arbitrary alphabet size is given. This generalized Böinck - van Tilborg bound, combined with constructions, is used to determine the length of some optimal binary and ternary t-EC-AUED codes. The size of optimal 0-EC-AUED codes is the numver of vectors of length n and weight $\lceil n(q-1)/2 \rceil$. So we will make computations for $t > 0$, but for completeness, we give also the codes for $t = 0$.

1 Introduction

Most classes of codes have been designed for use on *symmetric channels*. However, in certain applications, such as optical communications, the error probability from 1 to 0 is significantly higher than the error probability from 0 to 1. These applications can be modeled by an *asymmetric channel*, on which only $1 \to 0$ transitions can occur (*asymmetric errors*).

Further, some other memory systems behave like an *unidirectional channel*, on which, even though both $1 \to 0$ and $0 \to 1$ errors are possible, all errors within the message are of the same type (increasing or decreasing) when sending a certain message (*unidirectional errors*).

In this paper we construct some optimal codes which can correct up to t errors and detect all unidirectional errors.

2 Some Definitions and Notations

Let $F_q = \{0, 1, 2, ..., q-1\}$ for $q \geq 2$.

Definition 1 *The q-**ary asymmetric channel** is the channel on which the only transitions that can occur are $x \to y$, where $0 \leq y \leq x \leq q-1$.*

If all $y \leq x$ are possible as a received symbol, we call the channel *complete*. As an example of a noncomplete channel is the channel introduced by Ahlswede and Aydinian [1], on which when x is sent only 0 and x can be received. In this work we assume that the channel is complete, when we considering an asymmetric channel.

Definition 2 *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).*

The codes, which are used to encode the message, sent over these channels, are called *q-ary asymmetric codes* and *q-ary unidirectional codes*, respectively.

Let C be a code over F_q^n. Let $\mathbf{x}, \mathbf{y} \in F_q^n$ and let $N(\mathbf{x}, \mathbf{y})$ denote the number of positions i where $x_i > y_i$. If $N(\mathbf{y}, \mathbf{x}) = 0$ the vector $\mathbf{x}$ is said to *cover* the vector $\mathbf{y}$ ($\mathbf{x} > \mathbf{y}$). If $\mathbf{x} \geq \mathbf{y}$ or $\mathbf{y} \geq \mathbf{x}$ the vectors $\mathbf{x}$ and $\mathbf{y}$ are said to be *ordered*, otherwise they are *unordered*. The *Hamming distance* $d_H(\mathbf{x}, \mathbf{y})$ between $\mathbf{x}$ and $\mathbf{y}$ is the sum of $N(\mathbf{x}, \mathbf{y})$ and $N(\mathbf{y}, \mathbf{x})$:

$$d_H(\mathbf{x}, \mathbf{y}) = N(\mathbf{x}, \mathbf{y}) + N(\mathbf{y}, \mathbf{x}) = \#\{i \mid x_i \neq y_i\}.$$

From the error detection point of view, the asymmetric and the unidirectional codes are equivalent, that is, a code capable of detecting up to t asymmetric errors is also capable of detecting t unidirectional errors.

Necessary and sufficient conditions for correcting and detecting errors of each of the three types, symmetric, asymmetric and unidirectional, are known [2]. However, sometimes a combination of correction and detection is required or even correction and/or detection of errors of different type. In this work we will discuss codes which are able to correct up to t symmetric errors and detect all unidirectional errors. Such a code is called a *t-EC-AUED* code.

Binary t-EC-AUED codes, in particular for $t = 1$, have been extensively studied. We construct some optimal binary and ternary t-EC-AUED codes for $t \geq 1$.

A characterization when a code is a t-EC-AUED code is known, [3]:

Theorem 1 *A code C is a t-EC-AUED code if and only if $N(\mathbf{x}, \mathbf{y}) \geq t + 1$ and $N(\mathbf{y}, \mathbf{x}) \geq t + 1$, for all distinct $\mathbf{x}, \mathbf{y} \in C$.*

Let $n_q(a, t+1)$ denote the length of the shortest t-EC-AUED code of size a over F_q^n. We call a t-EC-AUED code of length $n_q(a, t + 1)$ and size a *optimal*.

Böinck and van Tilborg gave a Plotkin type lower bound for the length of a binary t-EC-AUED code [6]:

$$n_2(a, t + 1) \geq \left\lceil \left(4 - \frac{2}{\lceil a/2 \rceil}\right)(t + 1) \right\rceil.$$

In the next section we make a generalization of this bound and using it and some lemmas, which we will present, we construct some optimal binary and ternary t-EC-AUED codes.

We remark that for $t = 0$ it has been shown by de Bruijn et al. [5] that for given n the largest 0-EC-AUED code of length n is the code of all codewords of weight $\lceil n(q-1)/2 \rceil$. There is no simple formula for this number in general, for $q = 2$ it is $\binom{n}{\lceil n/2 \rceil}$. For larger q the size of the codes is discused in the last section.

3 A generalized Böinck-van Tilborg bound

In this paper the expression $t + 1$ occurs on many places, so we find it convenient to use the notation $T \overset{\text{def}}{=} t + 1$.

The lower bound which was derived by Böinck and van Tilborg for the length of a binary t-EC-AUED codes, rewritten in our notations is:

$$n_2(a, T) \geq \left\lceil \left(4 - \frac{2}{\lceil a/2 \rceil}\right) T \right\rceil. \tag{1}$$

In this section we generalize Böinck - van Tilborg bound to non-binary codes. Let

$$f(m_0, m_1, \ldots, m_{q-1}) = \sum_{0 \leq i < j \leq (q-1)} m_i m_j,$$

$$\begin{aligned} S_1 &= m_0 + m_1 + ... + m_{q-1} = \sum_{i=0}^{q-1} m_i, \\ S_2 &= m_0^2 + m_1^2 + ... + m_{q-1}^2 = \sum_{i=0}^{q-1} m_i^2. \end{aligned}$$

Then $S_1^2 = S_2 + 2f(m_0, m_1, \ldots, m_{q-1})$ and so

$$f(m_0, m_1, .., m_{q-1}) = \frac{1}{2}(S_1^2 - S_2).$$

Let $\lambda(a)$ be the maximum of $f(m_0, m_1, .., m_{q-1})$ over $(m_0, m_1, \ldots, m_{q-1})$, where $m_0, m_1, ..., m_{q-1}$ are non-negative integers such that $S_1 = a$.

Lemma 1 *If C is an $(T-1)$-EC-AUED code of length n and size a, then*

$$n \geq \frac{a(a-1)T}{\lambda(a)}.$$

Proof: Consider $\sum_{\substack{\mathbf{x},\mathbf{y}\in C\\ \mathbf{x}\neq\mathbf{y}}} N(\mathbf{x}, \mathbf{y})$. Since C is a $(T-1)$-EC-AUED code, $N(\mathbf{x}, \mathbf{y}) \geq T$ for all distinct $\mathbf{x}, \mathbf{y} \in C$, and so

$$\sum_{\substack{\mathbf{x},\mathbf{y}\in C\\ \mathbf{x}\neq\mathbf{y}}} N(\mathbf{x}, \mathbf{y}) \geq a(a-1)T. \quad (2)$$

Let $m_{l,i}$ be the number of codewords $\mathbf{x}$ such that $x_l = i$. Then,

$$\begin{aligned} \sum_{\substack{\mathbf{x},\mathbf{y}\in C\\ \mathbf{x}\neq\mathbf{y}}} N(\mathbf{x}, \mathbf{y}) &= \sum_{l=1}^{n} \sum_{0\leq i<j\leq q-1} m_{l,i}\, m_{l,j} \\ &= \sum_{l=1}^{n} f(m_{0,l}, m_{1,l}, \ldots, m_{q-1,l}) \\ &\leq n\lambda(a). \end{aligned}$$

Combining this with (2), the lemma follows. □

Next we find an explicit expression for $\lambda(a)$. We note that if the m_i were real numbers, then the maximum of $f(m_0, m_1, \ldots, m_{q-1})$ would be obtained for $m_i = a/(q-1)$ for all i. For non-negative integers m_i let the maximum be obtained for

$$(m_0, m_1, \ldots, m_{q-1}) = (\mu_0, \mu_1, \ldots, \mu_{q-1}).$$

Because of the symmetry we may assume that

$$\mu_0 \leq \mu_1 \leq \cdots \leq \mu_{q-1}.$$

Further, by assumption,

$$\sum_{i=0}^{q-1} \mu_i = a.$$

In particular, $\mu_{q-1} \geq 1$. Let

$$\begin{aligned} m_0 &= \mu_0 + 1, \\ m_{q-1} &= \mu_{q-1} - 1, \\ m_i &= \mu_i \text{ for } 1 \leq i \leq q-2. \end{aligned}$$

Then

$$\begin{aligned}
0 &\leq 2f(\mu_0, \mu_1, \ldots, \mu_{q-1}) - 2f(m_0, m_1, \ldots, m_{q-1}) \\
&= (a^2 - \mu_0^2 - \mu_1^2 - \cdots - \mu_{q-1}^2) - (a^2 - m_0^2 - m_1^2 - \cdots - m_{q-1}^2) \\
&= -\mu_0^2 - \mu_{q-1}^2 + (\mu_0 + 1)^2 + (\mu_{q-1} + 1)^2 \\
&= 2\mu_0 - 2\mu_{q-1} + 2.
\end{aligned}$$

Hence, $\mu_{q-1} \leq \mu_0 + 1$. This implies that if $a = \alpha q + \beta$, where $0 \leq \beta \leq q - 1$, then

$$\begin{array}{ll}
\mu_i = \alpha & \text{for } 0 \leq i < q - \beta, \\
\mu_i = \alpha + 1 & \text{for } q - \beta \leq i < q - 1.
\end{array}$$

Hence

$$\begin{aligned}
\lambda(a) &= \frac{1}{2}\Big\{a^2 - (q-\beta)\alpha^2 - \beta(\alpha+1)^2\Big\} \\
&= \frac{a(a-\alpha) - (a - \alpha q)(1+\alpha)}{2}.
\end{aligned}$$

Combining this with Lemma 1, we get the following bound.

Theorem 2 *For $a \geq 2$ and $T \geq 1$ we have*

$$n_q(a, T) \geq GBT_q(a, T),$$

where

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

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

For $q = 2$, this is exactly the bound (1).
Since

$$GBT_q(q\mu + (q-1), T) = GBT_q(q\mu + q, T),$$

an immediate corollary of the theorem is:

Corollary 1 *A q-ary $(T-1)$-EC-AUED code of length*

$$n < GBT_q(q\mu + q, T)$$

has size $a \leq q\mu + (q-2)$.

4 A method to determine or estimate $n_q(a, T)$

It appears that in many cases, the Böinck - van Tilborg bound and also its generalization is best possible, that is, we have equality in Theorem 2. In [8], we developed a method to prove this in the binary case and in [7] in the ternary case, using an efficient construction method. For a given a, the construction is recursive and requires a computer search for some small values of T to start the recursion. The validity of the recursion is based on two lemmas involving the generalized Böinck - van Tilborg bound. We state and prove them next.

Lemma 2 *For all $a > 0$, $T_1 \geq 0$, and $T_2 \geq 0$, we have*

$$n_q(a, T_1 + T_2) \leq n_q(a, T_1) + n_q(a, T_2).$$

Proof: We represent a code of size a and length n by an $(a \times n)$ matrix with the codewords as the rows. Let C_1 be a $(T_1 - 1)$-EC-AUED code of size a and length $n_q(a, T_1)$ and C_2 a $(T_2 - 1)$-EC-AUED code of size a and length $n_q(a, T_2)$. Let $C = C_1|C_2$ (matrix concatenation). This is an asymmetric code of size a and length

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

Let $(\mathbf{x}|\mathbf{x}')$ and $(\mathbf{y}|\mathbf{y}')$ be distinct codewords of C, where $\mathbf{x}, \mathbf{x}' \in C_1$ and $\mathbf{y}, \mathbf{y}' \in C_2$. Then

$$N((\mathbf{x}|\mathbf{x}'), (\mathbf{y}|\mathbf{y}')) = N(\mathbf{x}, \mathbf{y}) + N(\mathbf{x}', \mathbf{y}') \geq T_1 + T_2.$$

Hence, C is an $(T_1 + T_2 - 1)$-EC-AUED code of length $n_q(a, T_1) + n_q(a, T_2)$. This proves the lemma. □

Lemma 3 *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

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

Proof: Let C_1, C_2 and C be defined as in the proof of the previous lemma. Then, by Theorem 2, Lemma 2, and the given conditions, we get

$$\begin{aligned} GBT_q(a, T_1 + T_2) &\leq n_q(a, T_1 + T_2) \\ &\leq n_q(a, T_1) + n_q(a, T_2) \\ &= GBT_q(a, T_1) + GBT_q(a, T_2) \\ &= GBT_q(a, T_1 + T_2). \end{aligned}$$

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

5 Optimal binary $(T - 1)$-EC-AUED codes

To determine $n_2(a, T)$ we only need to consider a even (by Corollary 1).

In [4] optimal codes of size $a = 2\mu$ are constructed for $\mu = 1, 2, 3$ by a more direct, but less efficient, method. The size of the codes and the bounds on n are the following:

$$a = 2 \text{ for } 2T \leq n < 3T,$$
$$a = 4 \text{ for } 3T < n < \frac{10}{3}T,$$
$$a = 6 \text{ for } \frac{10}{3}T \leq n < \frac{7}{2}T.$$

We construct optimal codes for $\mu = 4, 5, 6, 7$ by a combination of a computer search and the use of Lemmas 2, 3, and Corollary 1 (for $q = 2$).

When we are considering binary codes we will use the notation

$$BT(2\mu, T) = \left\lceil \left(4 - \frac{2}{\mu}\right) T \right\rceil$$

for the Böinck-van Tilborg bound.

Theorem 3 *For $T \equiv 2 \pmod 4$, we have*

$$\left\lceil \frac{7}{2}T \right\rceil \leq n_2(8,T) \leq \left\lceil \frac{7}{2}T \right\rceil + 1$$

and

$$n_2(8,T) = \left\lceil \frac{7}{2}T \right\rceil,$$

otherwise.

Proof: For $a = 8$ we have $BT(8,T) = \lceil \frac{7}{2}T \rceil$, hence $n_2(8,T) \geq \left\lceil \frac{7}{2}T \right\rceil$.

For $T = 1$, $BT(8,1) = 4$. According to de Bruijn et al., [5], the size of an optimal 1-EC-AUED code of length 4 is $\binom{4}{2} = 6$. So there is no 1-EC-AUED code of length 4 and size 8. A computer search shows that $n_1(8,1) = 5$, which is 1 above the bound.

A computer search shows that for $T = 2$ there is no code meeting the bound $BT(8,2)$ and the length of the best code is 1 above the bound, so $n_2(8,2) = 8$.

Matrices showing this are:

$$C_1 = \begin{bmatrix} 00011 \\ 00101 \\ 00110 \\ 01001 \\ 01010 \\ 01100 \\ 10001 \\ 10010 \end{bmatrix}, \quad C_2 = \begin{bmatrix} 00000111 \\ 00011001 \\ 00101010 \\ 01001100 \\ 01110000 \\ 10010010 \\ 10100100 \\ 11000001 \end{bmatrix}.$$

For $T = 3, 4, 5$, there are codes with length $n_2(8,T) = \lceil \frac{7}{2}T \rceil$. Matrices showing this are:

$$C_3 = \begin{bmatrix} 00000011111 \\ 00011100011 \\ 00101101100 \\ 01010110100 \\ 01101010001 \\ 01110001010 \\ 10011011000 \\ 10100110010 \end{bmatrix}, \quad C_4 = \begin{bmatrix} 00000001111111 \\ 00011110000111 \\ 00101110111000 \\ 01110011001001 \\ 10110101010010 \\ 11000111100100 \\ 11011000011100 \\ 11101000100011 \end{bmatrix},$$

$$C_5 = \begin{bmatrix} 000000000111111111 \\ 000011111000001111 \\ 000101111011110000 \\ 011010011100110001 \\ 011011100111000010 \\ 101100011101000110 \\ 101101100100011001 \\ 110110001010011010 \end{bmatrix}.$$

A computer search shows that there is no codes meeting the bound for $T = 6$. The best code is with length 1 above the bound. So $n_2(8,6) = 22$ and one of the possibilities to obtain C_6 is a concatenation of C_1 and C_5.

Using $BT(8,T) + BT(8,4) = BT(8,T+4)$ for all T and Lemma 3 it follows that the recursion which we will use to obtained codes for all T is $C_T = C_4 | C_{T-4}$.

For all $T \not\equiv 2 \pmod 4$ the length of the codes is exactly $BT(8,T)$ and for $T \equiv 2 \pmod 4$ the length is bounded by $BT(8,T)$ and $BT(8,T)+1$.

Note that the fact $n_2(8,T) = n_2(7,T)$ follows from Corollary 1. □

Theorem 4 *For $T \geq 2$ we have*

$$n_2(10,T) = \left\lceil \frac{18}{5} T \right\rceil.$$

Proof: For size 10 we use the same method. We have $BT(10,T) = \lceil \frac{18}{5} T \rceil$, hence $n_2(10,T) \geq \lceil \frac{18}{5} T \rceil$. We use that

$$BT(10,T) + BT(10,5) = BT(10,T+5).$$

The recursion which we will use to obtain codes for all T is $C_T = C_5 | C_{T-5}$. We have to note that according to de Bruijn et al., [5], the size of the optimal 1-EC-AUED code of length 4, (since $BT(10,1) = 4$), is 6. So there is no code meeting the bound for $T = 1$. A computer search shows that the length of the best code is 1 above the bound, so $n_2(10,1) = 5$ and the code is presented with the following matrix :

$$C_1 = \begin{bmatrix} 00011 \\ 00101 \\ 00110 \\ 01001 \\ 01010 \\ 01100 \\ 10001 \\ 10010 \\ 10100 \\ 11000 \end{bmatrix}.$$

For all other $T \geq 2$ there are codes meeting the bound. The codes C_T for $T = 2,3,4,5$, needed to start the recursion, are:

$$C_2 = \begin{bmatrix} 00001111 \\ 00110011 \\ 00111100 \\ 01010101 \\ 01011010 \\ 01100110 \\ 01101001 \\ 10010110 \\ 10011001 \\ 10100101 \end{bmatrix}, \quad C_3 = \begin{bmatrix} 00000011111 \\ 00011100011 \\ 00101101100 \\ 01010110100 \\ 01101010001 \\ 01110001010 \\ 10011011000 \\ 10100110010 \\ 10110000101 \\ 11000101001 \end{bmatrix},$$

$$C_4 = \begin{bmatrix} 000000001111111 \\ 000011110000111 \\ 000101110111000 \\ 001110011001001 \\ 010110101010010 \\ 011000111100100 \\ 011011000011100 \\ 011101000100011 \\ 100111001100100 \\ 101001011010010 \end{bmatrix}, \quad C_5 = \begin{bmatrix} 000000000111111111 \\ 000011111000001111 \\ 000101111011110000 \\ 011010011100110001 \\ 011011100111000010 \\ 101100011101000110 \\ 101101100100011001 \\ 110110001010011010 \\ 110110100001100101 \\ 111001010010101100 \end{bmatrix}.$$

If we use the recursion to obtain $C_6 = C_1|C_5$ the code is with length 1 above the bound, since the length of C_1 is 1 above the bound. However there is code meeting exactly the bound, namely $C_6 = C_3|C_3$.

This proves the theorem. The fact $n_2(10, T) = n_2(9, T)$ follows from Corollary 1. □

Theorem 5 *For* $T \equiv 3 \pmod 6$, *we have*

$$\left\lceil \frac{11}{3}T \right\rceil \leq n_2(12, T) \leq \left\lceil \frac{11}{3}T \right\rceil + 1$$

and

$$n_2(12, T) = \left\lceil \frac{11}{3}T \right\rceil,$$

otherwise.

Proof: For size 12 we have $BT(12, T) = \lceil \frac{11}{3}T \rceil$, hence $n_2(12, T) \geq \lceil \frac{11}{3}T \rceil$.

For $T = 1$, $BT(12, 1) = 4$. According to de Bruijn et al., [5], the optimal 1-EC-AUED code of length 4 has size 6. So there is no 1-EC-AUED codes of size 12 and length 4. A computer search shows that the best code is with length $n_2(12, 1) = 6$. The matrix showing this is:

$$C_1 = \begin{bmatrix} 000011 \\ 000101 \\ 000110 \\ 001001 \\ 001010 \\ 001100 \\ 010001 \\ 010010 \\ 010100 \\ 011000 \\ 100001 \\ 100010 \end{bmatrix}.$$

Computations have shown that $n_2(12, 2) = \lceil \frac{11}{3}T \rceil$ but for $T = 3$ there are no codes which meeting this bound. The length is 1 above the bound. For $T = 4, 5, 6, 7, 8$ we have codes meeting exactly the bound. Matrices showing this for $T = 2, 3, 4, 5, 6, 7, 8$ are:

$$C_2 = \begin{bmatrix} 00001111 \\ 00110011 \\ 00111100 \\ 01010101 \\ 01011010 \\ 01100110 \\ 01101001 \\ 10010110 \\ 10011001 \\ 10100101 \\ 10101010 \\ 11000011 \end{bmatrix}, \quad C_3 = \begin{bmatrix} 000000011111 \\ 001111100000 \\ 010001100011 \\ 010010101100 \\ 010101010100 \\ 011010010001 \\ 011100001010 \\ 100011000101 \\ 100100100110 \\ 100110011000 \\ 101000101001 \\ 101001010010 \end{bmatrix},$$

$$C_4 = \begin{bmatrix} 000000001111111 \\ 000011110000111 \\ 000101110111000 \\ 001110011001001 \\ 010110101010010 \\ 011000111100100 \\ 011011000011100 \\ 011101000100011 \\ 100111001100100 \\ 101001011010010 \\ 101010100101010 \\ 101100100010101 \end{bmatrix}, \quad C_5 = \begin{bmatrix} 0000000000111111111 \\ 0000011111000001111 \\ 0000101111011110000 \\ 0011010011100110001 \\ 0011011100111000010 \\ 0101100011101000110 \\ 0101101100100011001 \\ 0110110001010011010 \\ 0110110100001100101 \\ 0111001010010101100 \\ 1001110010011001001 \\ 1001111000000110110 \end{bmatrix},$$

$$C_6 = \begin{bmatrix} 0000000000011111111111 \\ 0000011111100000011111 \\ 0000101111101111100000 \\ 0011110001110001100011 \\ 0011110110010110001100 \\ 0111001001111010010100 \\ 1011011010001001111000 \\ 1100110010111100010001 \\ 1101001100110100101010 \\ 1101100101000011011001 \\ 1110010101001101000110 \\ 1110101010000010100111 \end{bmatrix},$$

$$C_7 = \begin{bmatrix} 00000000000001111111111111 \\ 00000011111111000000011111 \\ 00000101111110111111000000 \\ 00111010001111000111000011 \\ 00111010110011111000001100 \\ 01011100011101001001110100 \\ 01011111000010010110111000 \\ 01101101100101110000010011 \\ 10101111001000101001101001 \\ 10110101110001000110100101 \\ 11010110100100100011001110 \\ 11101000111000001110011010 \end{bmatrix}, \quad C_8 = C_2|C_6.$$

Since $BT(12,T) + BT(12,6) = BT(12,T+6)$, the recursion which we will use to obtain codes for all T is $C_T = C_6|C_{T-6}$.

The best code for $T = 9$ is $C_9 = C_3|C_6$, which has length 1 above the bound. So for all $T \equiv 3 \pmod 6$ the length of the codes is bounded by $BT(12,T)$ and $BT(12,T)+1$. For the rest $T \not\equiv 3 \pmod 6$, the length of the codes is exactly $BT(12,T)$. This proves the theorem.

Again from Corollary 1 it follows that $BT(12,T) = BT(11,T)$. □

Theorem 6 *For $T \geq 2$ we have*

$$n_2(14,T) = \left\lceil \frac{26}{7} T \right\rceil.$$

Proof: For size 14 we have $BT(14,T) = \lceil \frac{26}{7}T \rceil$, hence $n_2(14,T) \geq \lceil \frac{26}{7}T \rceil$.

For $T = 1$, $BT(14,1) = 4$. According again to de Bruijn et al., [5], the size of the optimal 1-EC-AUED code of length 4 is 6, so there is no 1-EC-AUED code of length 4 and size 14. A computer search shows that the best code is with length $n_2(14,1)=6$ and the matrix showing this is:

$$C_1 = \begin{bmatrix} 000011 \\ 000101 \\ 000110 \\ 001001 \\ 001010 \\ 001100 \\ 010001 \\ 010010 \\ 010100 \\ 011000 \\ 100001 \\ 100010 \\ 100100 \\ 101000 \end{bmatrix}.$$

Since $BT(14,T)+BT(14,7)=BT(14,T+7)$, we need codes for T from 2 to 8 to start the recursion, which is $C_T = C_7|C_{T-7}$. The codes for $T = 2,3,4,5,6,7,8$ are presented below:

$$C_2 = \begin{bmatrix} 00001111 \\ 00110011 \\ 00111100 \\ 01010101 \\ 01011010 \\ 01100110 \\ 01101001 \\ 10010110 \\ 10011001 \\ 10100101 \\ 10101010 \\ 11000011 \\ 11001100 \\ 11110000 \end{bmatrix}, \quad C_3 = \begin{bmatrix} 000000111111 \\ 001111000011 \\ 010011001101 \\ 010011110010 \\ 011101010100 \\ 011110101000 \\ 100111011000 \\ 101011100100 \\ 101100001101 \\ 101100110010 \\ 110101100001 \\ 110110000110 \\ 111001001010 \\ 111010010001 \end{bmatrix},$$

$$C_4 = \begin{bmatrix} 000000001111111 \\ 000011110000111 \\ 000101110111000 \\ 001110011001001 \\ 010110101010010 \\ 011000111100100 \\ 011011000011100 \\ 011101000100011 \\ 100111001100100 \\ 101001011010010 \\ 101010100101010 \\ 101100100010101 \\ 110001101001001 \\ 110010010110001 \end{bmatrix}, \quad C_5 = \begin{bmatrix} 000000000111111111 \\ 000001111000001111 \\ 000010111011110000 \\ 0011010011100110001 \\ 0011011100111000010 \\ 0101100011101000110 \\ 0101101100100011001 \\ 0110110001010011010 \\ 0110110100001100101 \\ 0111001010010101100 \\ 1001110010011001001 \\ 1001111000000110110 \\ 1010100110100101010 \\ 1010101001110000101 \end{bmatrix},$$

$$C_6 = \begin{bmatrix} 00000000000011111111111 \\ 00000011111100000011111 \\ 00000101111101111100000 \\ 00011110001110001100011 \\ 00011110110010110001100 \\ 00111001001111010010100 \\ 01011011010001001111000 \\ 01100110010111100010001 \\ 01101001100110100101010 \\ 01101100101000011011001 \\ 01110010101001101000110 \\ 01110101010000010100111 \\ 10011101100001100010011 \\ 10100111100010001110100 \end{bmatrix},$$

$$C_7 = \begin{bmatrix} 00000000000001111111111111 \\ 00000011111110000000111111 \\ 00000101111110111111000000 \\ 00111010001111000111000011 \\ 00111010110011111000001100 \\ 01011100011101001001110100 \\ 01011111000010010110111000 \\ 10011101100101110000010011 \\ 10101111001000101001101001 \\ 11001110110000001110000111 \\ 11100011100101010011100100 \\ 11100100010111100100101010 \\ 11110000111000010101011001 \\ 11110001001010101010010110 \end{bmatrix}, \quad C_8 = C_4|C_4.$$

This proves the theorem for all $T > 1$.
From Corollary 1 we have $BT(14, T) = BT(13, T)$. □

6 Optimal ternary $(T - 1)$-EC-AUED codes

In this section we use the method described above for $q = 3$.

Theorem 7 *For* $T \geq 1$ *we have*

$$n_3(3, T) = 2T,$$
$$n_3(4, T) = \left\lceil \tfrac{12}{5} T \right\rceil,$$
$$n_3(5, T) = n_3(6, T) = \left\lceil \tfrac{5}{2} T \right\rceil.$$

Proof: We first give the proof and the construction of the codes for $a = 6$. We have $GBT_3(6, T) = \left\lceil \frac{5}{2} T \right\rceil$. Hence, $GBT_3(6, T) + GBT_3(6, 2) = GBT_3(6, T + 2)$. Codes showing the stated result for $T = 1$ and $T = 2$ are

$$C_1 = \begin{bmatrix} 200 \\ 020 \\ 002 \\ 100 \\ 010 \\ 001 \end{bmatrix}, \quad C_2 = \begin{bmatrix} 12200 \\ 21020 \\ 20102 \\ 02012 \\ 00221 \\ 11111 \end{bmatrix}.$$

As shown in the proofs of Lemmas 2 and 3, codes C_T that prove the result for general T are obtained by the recursion $C_T = C_2|C_{T-2}$.

Note that the fact $n_3(5,T) = n_3(6,T)$ follows from Corollary 1.

For $a = 3$, we only need one matrix to start the recursion $C_T = C_1|C_{T-1}$:

$$C_1 = \begin{bmatrix} 02 \\ 11 \\ 20 \end{bmatrix}.$$

For $a = 4$, we need 5 matrices to start the recursion $C_T = C_5|C_{T-5}$:

$$C_1 = \begin{bmatrix} 001 \\ 020 \\ 110 \\ 200 \end{bmatrix}, \quad C_2 = \begin{bmatrix} 00022 \\ 01101 \\ 10110 \\ 22000 \end{bmatrix},$$

$$C_3 = \begin{bmatrix} 00000122 \\ 00111011 \\ 02022000 \\ 11200001 \end{bmatrix}, \quad C_5 = \begin{bmatrix} 000000022222 \\ 001111101111 \\ 120012210001 \\ 212220000010 \end{bmatrix},$$

$$C_4 = C_2|C_2.$$

□

We finally consider $a = 7, 8, 9$.

Theorem 8 *We have*

$$\left\lceil \frac{21}{8} T \right\rceil \leq n_3(7,T) \leq \left\lceil \frac{8}{3} T \right\rceil$$

for all $T \geq 1$.

Proof: For $a = 7$, we have $GBT_q(7,T) = \lceil \frac{21}{8} T \rceil$. We do not know if this bound can be met in all cases. Computations have shown that it is met for $T \leq 7$. Codes proving this are the following.

$$C_1 = \begin{bmatrix} 012 \\ 021 \\ 102 \\ 111 \\ 120 \\ 201 \\ 210 \end{bmatrix}, \quad C_3 = \begin{bmatrix} 00001222 \\ 00122011 \\ 02110102 \\ 11010211 \\ 12201001 \\ 20210020 \\ 21101110 \end{bmatrix}.$$

Further, let

$$C_2 = C_1|C_1, \ C_T = C_3|C_{T-3} \text{ for } T = 4,5,6,7.$$

For $T = 8$ the best code we have found so far is $C_4|C_4$ whose length is one above the bound. If there exists a code C_8 meeting the bound for $T = 8$, the recursive construction $C_T = C_8|C_{T-8}$ gives codes meeting the bound for all T. However, if this is not the case, we still can use a recursive construction to get estimates. We note that $\lceil \frac{21}{8} T \rceil = \lceil \frac{8}{3} T \rceil$ for $1 \leq T \leq 7$, and the construction $C_T = C_3|C_{T-3}$ gives a code of length $\lceil \frac{8}{3} T \rceil$ for all T. □

Theorem 9 *We have*

$$\left\lceil \frac{8}{3}T \right\rceil \leq n_3(8,T) \leq n_3(9,T) \leq \left\lceil \frac{8}{3}T \right\rceil + 1$$

for $T \equiv 1 \pmod 3$*, and*

$$n_3(8,T) = n_3(9,T) = \left\lceil \frac{8}{3}T \right\rceil$$

otherwise.

Proof: For $a = 9$ the bound is $GBT_3(9,T) = \lceil \frac{8}{3}T \rceil$. There are no codes meeting the bound for $T = 1$, the bound is 3, but the shortest code has length 4:

$$C_1 = \begin{bmatrix} 0002 \\ 0011 \\ 0020 \\ 0101 \\ 0110 \\ 0200 \\ 1001 \\ 1010 \\ 1100 \end{bmatrix}.$$

For $T = 2$ and $T = 3$, there are codes meeting the bound:

$$C_2 = \begin{bmatrix} 000022 \\ 001111 \\ 020201 \\ 022010 \\ 110011 \\ 112200 \\ 200210 \\ 202001 \\ 221100 \end{bmatrix}, \quad C_3 = \begin{bmatrix} 00002222 \\ 01111112 \\ 02220002 \\ 10120121 \\ 11202011 \\ 12011201 \\ 20210210 \\ 21022100 \\ 22101020 \end{bmatrix}.$$

Since $GBT_3(9,T) + GBT_3(9,3) = GBT_3(9,T+3)$, the recursive construction is $C_T = C_3|C_{T-3}$. A computer search shows that there is no code for $T = 4$ which meet the bound. The best code is with length 1 above the bound. One of the possibilities to obtain C_4 is $C_2|C_2$.

So for $T \equiv 1(mod\ 3)$ the length of the codes is bounded by $GBT_3(9,T)$ and $GBT_3(9,T)+1$ and for the rest T, which are not equivalent to $1(mod\ 3)$ the length of the codes is exactly $GBT_3(9,T)$. □

References

[1] A. Ahlswede and H. Aydinian, "Error control codes for parallel asymmetric channels", *Proceedings of the IEEE Symposium on Information Theory*, Seattle, WA, July, 2006, pp. 1768-1772.

[2] J. H. Weber, "Bounds and Constructions for Binary Block Codes Correcting Asymmetric or Unidirectional Errors", *PhD Thesis*, Delft University of Technology, The Netherlands, 1985.

[3] B. Bose and T. R. N. Rao, "Theory of unidirectional error correcting/detecting codes", *IEEE Trans. Comp.*, vol. 31, 1982, pp. 23-32.

[4] B. Bose and T. Kløve, "Sperner's theorem and unidirectional codes", *P. Charpin and Ø. Ytrehus (eds.), Workshop on Coding and Cryptography 2005*, Bergen, Norway", March 14-18, 2005, pp. 169-175.

[5] N. G. de Bruijn and C. van Ebbenhorst Tengbergen and D. Kruyswijk, "On the set of divisors of a number", *Nieuw Archief voor Wiskunde (2)*, vol. 23, 1951, pp. 191-193.

[6] F. J. H. Boinck and H. C. A. van Tilborg, "Constructions and bounds for systematic tEC/AUED codes", *IEEE Trans. Inform. Theory*, vol. 36, 1990, pp. 1381-1390.

[7] I. Naydenova and T. Kløve, "A bound on q-ary t-EC-AUED codes and constructions of some optimal ternary t-EC-AUED codes", *Book of abstracts of the 2006 International Symposium on Information Theory and its Applications*, Seoul, South Korea, October 29 - November 1, 2006, pp. 3.

[8] I. Gancheva and T. Kløve, "Construction of some optimal t-EC-AUED codes", *Proceedings of the Fourth International Workshop on Optimal Codes and Related Topics*, Pamporovo, Bulgaria, June 17-23, 2005, pp. 152-156.