

Generalized Bose-Lin Codes, a Class of Codes Detecting Asymmetric Errors of Limited Magnitude

Irina Naydenova

► **To cite this version:**

Irina Naydenova. Generalized Bose-Lin Codes, a Class of Codes Detecting Asymmetric Errors of Limited Magnitude. WCC 2011 - Workshop on coding and cryptography, Apr 2011, Paris, France. pp.341-350, 2011. <inria-00614399>

HAL Id: inria-00614399

<https://hal.inria.fr/inria-00614399>

Submitted on 11 Aug 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Generalized Bose-Lin Codes, a Class of Codes Detecting Asymmetric Errors of Limited Magnitude

Irina Naydenova

Department of Informatics, University of Bergen, Norway
irina@ii.uib.no

Abstract. Bose and Lin introduced a class of systematic codes for detection of binary asymmetric errors. Later, in [4] this class was generalized and the Generalized Bose-Lin (GBL) codes were introduced. In this note, we describe a Generalized Bose-Lin codes of limited magnitude l . For these codes, the possible undetectable errors are characterized, the undetectable errors of minimum weight are determined and the number of undetectable errors of minimal weight is found.

list of keywords: *error detection, q-ary asymmetric channel, Generalized Bose-Lin codes, asymmetric errors of limited magnitude*

1 Introduction

Bose and Lin introduced a class of binary systematic codes for detection of asymmetric errors. This class was generalized for any q and in [4] the Generalized Bose-Lin codes were presented. Using this generalization we consider Generalized Bose-Lin codes of limited magnitude. For these codes the transmission channel is asymmetric. The received word cannot contain a component larger than the transmitted one. Moreover, when the asymmetric error is of limited magnitude, say l , the value of the difference between a transmitted component and its received version is at most l . In this note we characterize the undetectable errors, find the minimum weight of undetectable errors and the number of undetectable errors of minimal weight. The considered codes are systematic, i.e., the information bits are separately identified from the check bits. It is shown how long should be the check sequence such that to have a maximum number of detected errors.

2 Notations and definitions

Let $F = \{0, 1, \dots, q - 1\}$. In a q -ary asymmetric channel (which we denote by q -ASC), the symbols transmitted over the channel are symbols from F , and if a is transmitted only $b \in \{0, 1, \dots, a\}$ can be received. In this note, we consider a

special type of asymmetric errors in a q -ary channel, where the error magnitude ($a - b$) do not exceed a certain threshold l . So, if a is transmitted only $b \in \{a - l, \dots, a\}$ can be received.

The following notations were introduced in [4], we repeat them for completeness. Let F^k be the set of all sequences of length k with symbols from F . For $\mathbf{x} = (x_0, x_1, \dots, x_{k-1}) \in F^k$, let

$$w(\mathbf{x}) = \sum_{i=0}^{k-1} x_i, \text{ the weight of } \mathbf{x},$$

$$u(\mathbf{x}) = \sum_{i=0}^{k-1} (q - 1 - x_i), \text{ the coveight of } \mathbf{x}.$$

Clearly, $w(\mathbf{x}) + u(\mathbf{x}) = k(q - 1)$.

For non-negative integers a and s , where $a < q^s$, let

$$\langle a \rangle_s = (a_{s-1}, a_{s-2}, \dots, a_0) \in F^s$$

where

$$a = \sum_{i=0}^{s-1} a_i q^i, \quad a_i \in F,$$

that is, $\langle a \rangle_s$ is essentially the q -ary expansion of a . Define

$$w(a) = w(\langle a \rangle_s) = \sum_{i=0}^{s-1} a_i.$$

For two sequences \mathbf{x} and \mathbf{y} , $\mathbf{y} \subseteq \mathbf{x}$ denotes that \mathbf{x} covers \mathbf{y} , that is, $y_i \leq x_i$ for all i .

For integers a and n , let $[a]_n$ denote the (least non-negative) residue of a modulo n .

For integers $m \geq 0$ and $n \geq 0$, let $S(m, n)$ denote the number of sequences in F^m of weight n . A discussion of expressions for and computation of $S(m, n)$ is given in [4]. Here we will give the lemmas, which are used later in this note.

3 Generalized Bose-Lin codes

The Generalized Bose-Lin codes are systematic codes determined by four (integral) parameters, $q \geq 2$ (symbol alphabet size), k (number of information symbols), r (number of check symbols), and ω where $0 \leq \omega \leq r$.

A codeword is a sequence in F^{k+r} . It consists of an information sequence \mathbf{x} with k information symbols concatenated by a check sequence $c(\mathbf{x})$ with r check symbols. We use the notations $\rho = r - \omega$, $\sigma = S(\omega, \lfloor (q-1)\omega/2 \rfloor)$, where σ is the number of all sequences in F^ω of weight $\lfloor (q-1)\omega/2 \rfloor$ and let

$$\{\mathbf{b}_{\omega,0}, \mathbf{b}_{\omega,1}, \dots, \mathbf{b}_{\omega,\sigma-1}\},$$

be the listing of all these sequences. We denote by $\theta = q^\rho$, the number of sequences in F^ρ . Finally, $\mu = \sigma\theta$ will be the number of all possible check sequences.

Let $u = u(\mathbf{x})$, the coweight of \mathbf{x} . The check sequence, which depends only on u modulo μ , that is, the integer $[u]_\mu$, is determined as

$$[u]_\mu = \alpha\theta + [u]_\theta$$

where $0 \leq [u]_\theta < \theta$ and $0 \leq \alpha < \sigma$. The *check sequence* is defined by $c(\mathbf{x}) = c_1(\mathbf{x})|c_2(\mathbf{x})$ where $|$ denotes concatenation,

$$c_1(\mathbf{x}) = \mathbf{b}_{\omega, \alpha}$$

(a sequence of length ω and weight $\lfloor (q-1)\omega/2 \rfloor$), and

$$c_2(\mathbf{x}) = \langle [u]_\theta \rangle_\rho$$

(the q -ary expansion of the residue of u modulo θ).

In [4], the following results are proven.

Theorem 1. *Let C be the GBL-code with parameters q, k, r, ω . A codeword $\mathbf{x}|c(\mathbf{x}) \in C$ can be transformed to the codeword $\mathbf{y}|c(\mathbf{y}) \neq \mathbf{x}|c(\mathbf{x})$ by transmission over a complete q -ASC if and only if*

$$\mathbf{y} \subset \mathbf{x} \text{ and } \langle \lambda \rangle_\rho \subseteq \langle [u(\mathbf{x})]_\theta \rangle_\rho,$$

where $\lambda = [u(\mathbf{x}) - u(\mathbf{y})]_\mu$.

Theorem 2. *Let C be the GBL-code with parameters q, k, r, ω , and assume that the transmission is over a complete q -ASC. The code C detects all errors of weight up to*

$$(\sigma - 1)\theta + (q - 1)\rho,$$

but there are undetectable errors of weight

$$(\sigma - 1)\theta + (q - 1)\rho + 1.$$

4 Generalized Bose-Lin Codes of Limited Magnitude

Generalized Bose-Lin codes of limited magnitude l are systematic. First we will characterize the possible undetectable errors and then we will determine the minimum weight of the undetectable errors for these codes. The number of the undetectable errors of the minimal weight is found too. We will consider the check sequence such that to have maximum number of detected errors.

The first result is.

Theorem 3. *Let C be the GBL-code of limited magnitude l with parameters q, k, r and ω . A codeword $\mathbf{x}|c(\mathbf{x}) \in C$ can be transformed to the codeword $\mathbf{y}|c(\mathbf{y}) \neq \mathbf{x}|c(\mathbf{x})$ by transmission over a q -ASC if and only if*

$$\mathbf{x} - \mathbf{1} \subseteq \mathbf{y} \subset \mathbf{x} \text{ and } \langle \lambda \rangle_\rho \subseteq \langle L \rangle_\rho,$$

where $\mathbf{1} = (l, l, \dots, l)$ of length k , $\lambda = [u(\mathbf{x}) - u(\mathbf{y})]_\mu$ and $L = l(\theta - 1)/(q - 1)$.

Proof: The sent codeword is $\mathbf{x}|c_1(\mathbf{x})|c_2(\mathbf{x})$ and the received codeword is $\mathbf{y}|c_1(\mathbf{y})|c_2(\mathbf{y})$, where $\mathbf{x} \neq \mathbf{y}$. According to the construction of GBL codes, we see that this is possible if and only if

$$\mathbf{x} - \mathbf{l} \subseteq \mathbf{y} \subseteq \mathbf{x}, \text{ where } \mathbf{l} = (l, l, \dots, l) \text{ of length } k, \quad (1)$$

$$c_1(\mathbf{y}) = c_1(\mathbf{x}), \text{ since } w(c_1(\mathbf{y})) = w(c_1(\mathbf{x})) = \lfloor (q-1)\omega/2 \rfloor \quad (2)$$

and

$$c_2(\mathbf{x}) - \langle L \rangle_\rho \subseteq c_2(\mathbf{y}) \subseteq c_2(\mathbf{x}). \quad (3)$$

Further, by definition, $c_2(\mathbf{x})$ is the q -ary expansion of $u(\mathbf{x})$ modulo θ and $c_2(\mathbf{y})$ is the q -ary expansion of $u(\mathbf{y})$ modulo θ . Also, we note that if $\mathbf{y} \subseteq \mathbf{x}$, then $u(\mathbf{y}) > u(\mathbf{x})$. Hence, suppose that (1), (2), and (3) are satisfied, and let

$$u = u(\mathbf{x})$$

and

$$j\mu - \lambda = u(\mathbf{y}) - u(\mathbf{x}),$$

where $0 \leq \lambda < \mu$ and $1 \leq j \leq \lfloor \frac{k\mu}{\mu} \rfloor$, since $0 \leq u(\mathbf{y}) - u(\mathbf{x}) \leq kl$. Note that $\lambda = [u(\mathbf{x}) - u(\mathbf{y})]_\mu$. Let

$$[u]_\mu = \alpha\theta + [u]_\theta \text{ and } [u + j\mu - \lambda]_\mu = \beta\theta + [u + j\mu - \lambda]_\theta.$$

Since $[u + (j\mu - \lambda)]_\mu = [u - \lambda]_\mu$ and $[u + (j\mu - \lambda)]_\theta = [u - \lambda]_\theta$, we get from the definition of the code that

$$\begin{aligned} c_1(\mathbf{x}) &= \mathbf{b}_{\omega, \alpha} c_2(\mathbf{x}) = \langle [u]_\theta \rangle_\rho, \\ c_1(\mathbf{y}) &= \mathbf{b}_{\omega, \beta} c_2(\mathbf{y}) = \langle [u - \lambda]_\theta \rangle_\rho. \end{aligned}$$

Hence, (2) is satisfied if and only if $\mathbf{b}_{\omega, \alpha} = \mathbf{b}_{\omega, \beta}$, that is, if and only if

$$\beta = \alpha,$$

and (3) is satisfied if and only if

$$\langle [u]_\theta - L \rangle_\rho \subseteq \langle [u - \lambda]_\theta \rangle_\rho \subseteq \langle [u]_\theta \rangle_\rho.$$

$\langle [u - \lambda]_\theta \rangle_\rho \subseteq \langle [u]_\theta \rangle_\rho$ was considered in more details in [4] and it was shown that we must have $\lambda < \theta$ and in particular, we must have $\lambda \leq [u]_\theta$.

Now we consider $\langle [u]_\theta - L \rangle_\rho \subseteq \langle [u - \lambda]_\theta \rangle_\rho$. Using the conclusions above we have $\langle [u]_\theta - L \rangle_\rho \subseteq \langle [u - \lambda]_\theta \rangle_\rho$ is equivalent to $\langle [u]_\theta \rangle_\rho - \langle L \rangle_\rho \subseteq \langle [u]_\theta \rangle_\rho - \langle \lambda \rangle_\rho$, which is $\langle \lambda \rangle_\rho \subseteq \langle L \rangle_\rho$. Since $\langle L \rangle_\rho \subseteq \langle [u]_\theta \rangle_\rho$, $\langle \lambda \rangle_\rho \subseteq \langle L \rangle_\rho$ is stronger condition and this completes the proof of the theorem.

Our next result is.

Theorem 4. Let C be the GBL-code of limited magnitude l with parameters q, k, r and ω and assume that the transmission is over a q -ASC. The code C detects all errors of weight up to

$$\mu - l \frac{\theta - 1}{q - 1} + l\rho - 1$$

but there are undetectable errors of weight

$$\mu - l \frac{\theta - 1}{q - 1} + l\rho.$$

Proof: The weight of the undetectable error is

$$\begin{aligned} & w(\mathbf{x}|c(\mathbf{x})) - w(\mathbf{y}|c(\mathbf{y})) \\ &= w(\mathbf{x}) - w(\mathbf{y}) + w(c_2(\mathbf{x})) - w(c_2(\mathbf{y})) \\ &= w(\mathbf{x}) - w(\mathbf{y}) + w(\langle [u]_{\theta} \rangle_{\rho}) - w(\langle [u - \lambda]_{\theta} \rangle_{\rho}) \\ &= u(\mathbf{y}) - u(\mathbf{x}) + w(\langle [u]_{\theta} \rangle_{\rho}) - w(\langle [u - \lambda]_{\theta} \rangle_{\rho}) \\ &= j\mu - \lambda + w(\langle \lambda \rangle_{\rho}) \\ &= j\mu - \lambda + w(\lambda). \end{aligned}$$

Suppose that

$$\lambda = \sum_{i=0}^{\rho-1} a_i q^i, \text{ and } \lambda' = \sum_{i=0}^{\rho-1} a'_i q^i,$$

where $a_i, a'_i \in F$ and $\langle \lambda \rangle_{\rho} \subseteq \langle \lambda' \rangle_{\rho}$, that is, $a_i \leq a'_i$ for all i . Then

$$(\lambda' - w(\lambda')) - (\lambda - w(\lambda)) = \sum_{i=0}^{\rho-1} (a'_i - a_i)(q^i - 1) \geq 0. \quad (4)$$

We note that $\langle L \rangle_{\rho} = (l, l, \dots, l)$. Hence $w(\langle L \rangle_{\rho}) = l\rho$. By (4), if also $\langle \lambda \rangle_{\rho} \subseteq \langle L \rangle_{\rho}$, then

$$\lambda - w(\lambda) \leq L - l\rho = l \frac{(\theta - 1)}{q - 1} - l\rho.$$

Therefore, the weight of an undetectable error is lower bounded as follows:

$$j\mu - (\lambda - w(\lambda)) \geq \mu - l \frac{\theta - 1}{q - 1} + l\rho,$$

which proves the theorem.

Next, we will determine the exact number of undetectable errors of minimal weight.

Theorem 5. For a GBL-code of limited magnitude l with parameters q, k, r and ω the number of all undetectable errors of minimal weight $\mu - l \frac{\theta - 1}{q - 1} + l\rho$ is

$$\sum_{t \geq 0} \sum_{\delta=0}^{q-1-l} \left\{ S(k, k(q-1) - t\theta - L - \delta) \sum_{\epsilon=0}^l S(k, \mu - L + \epsilon) S(\rho, l\rho - \epsilon) \right\}.$$

Proof: The weight of the undetectable error is

$$w(\mathbf{x}|c(\mathbf{x})) - w(\mathbf{y}|c(\mathbf{y})) = j\mu - \lambda + w(\lambda),$$

where

$$0 \leq j \leq \left\lfloor \frac{kl}{\mu} \right\rfloor, \\ \lambda = [u(\mathbf{x}) - u(\mathbf{y})]_{\mu}, \quad 0 \leq \lambda \leq [u(\mathbf{x})]_{\theta} \leq \theta - 1, \quad \langle \lambda \rangle_{\rho} \subseteq \langle L \rangle_{\rho} \subseteq \langle [u(\mathbf{x})]_{\theta} \rangle_{\rho}.$$

We have that

$$\lambda - w(\lambda) \leq L - l\rho \leq [u]_{\theta} - w([u]_{\theta}), \quad \text{since } \langle \lambda \rangle_{\rho} \subseteq \langle L \rangle_{\rho} \subseteq \langle [u]_{\theta} \rangle_{\rho}.$$

Consider the undetectable error of minimal weight we should have equality in both places. So, we have undetectable error of minimal weight in the cases when

$$j = 1, \quad \lambda = L - \epsilon, \quad 0 \leq \epsilon \leq l \quad \text{and} \quad [u]_{\theta} = L + \delta, \quad 0 \leq \delta \leq q - 1 - l.$$

We note that $[u]_{\theta} = L + \delta$ if and only if $u = t\theta + L + \delta$ for some $t \geq 0$, since $L + \delta < \theta$.

We have to find the number of sequences which have co-weight exactly $u = t\theta + L + \delta$, which is equivalent to have weight exactly $k(q - 1) - u = k(q - 1) - t\theta - L - \delta$. All these sequences have the same length k . So, the number is $S(k, k(q - 1) - t\theta - L - \delta)$.

For every such sequence we have undetectable error of minimal weight $\mu - L + l\rho$. From the definition of λ and using that $j = 1$ we have that $u(\mathbf{y}) - u(\mathbf{x}) = \mu - L + \epsilon$. So, the weight of the error sequence to the information part is $\mu - L + \epsilon$. Then, the weight of the error sequence of the last ρ bits will be $l\rho - \epsilon$. Hence, the number of all error sequences is $S(k, \mu - L + \epsilon)S(\rho, l\rho - \epsilon)$, for $0 \leq \epsilon \leq l$.

The number of undetectable errors of minimal weight when $u = t\theta + L + \delta$ is therefore

$$\sum_{\delta=0}^{q-1-l} \left\{ S(k, k(q-1) - t\theta - L - \delta) \sum_{\epsilon=0}^l S(k, \mu - L + \epsilon) S(\rho, l\rho - \epsilon) \right\}.$$

Then summing over all $t \geq 0$ we receive that the number of undetectable errors of minimal weight for GBL codes of a limited magnitude l is

$$\sum_{t \geq 0} \sum_{\delta=0}^{q-1-l} \left\{ S(k, k(q-1) - t\theta - L - \delta) \sum_{\epsilon=0}^l S(k, \mu - L + \epsilon) S(\rho, l\rho - \epsilon) \right\}.$$

Undetectable errors of minimal weight occur exactly for codewords of co-weight $t\theta + L + \delta$, $0 \leq \delta \leq q - 1 - l$. For these codewords, an error is undetectable if the last ρ symbols of the check part, namely

$$(l, l, \dots, l, l + \delta)$$

are changed to

$$(0, 0, \dots, 0, \delta + \epsilon)$$

and the weight of the error sequence to the information part is $\mu - L + \epsilon$, $0 \leq \epsilon \leq l$.

A natural question is: given q , l and r , which value of ω maximizes

$$A(q, l, r, \omega) = \mu - l \frac{\theta - 1}{q - 1} + l\rho - 1.$$

For $q = 2$ and $l = q - 1$ it was shown by a simple proof in [3] that the maximum is obtained for $\omega = 4$ when $r \geq 5$.

For $q \geq 3$ the maximum is obtained for $\omega = 2$. The result is stated in the following theorem.

Theorem 6. *Let $q \geq 3$. We have $A(q, l, r, 2) > A(q, l, r, 1)$ for $r \geq 3$. For $\omega \geq 3$ we have $A(q, l, r, \omega - 1) > A(q, l, r, \omega)$ for $r \geq \omega$.*

Proof: When $\omega = 1$ we have

$$A(q, l, r, 1) = q^{r-1} \left(1 - \frac{l}{q-1} \right) + (r-1)l + \frac{l}{q-1} - 1$$

and when $\omega = 2$, then

$$A(q, l, r, 2) = q^{r-2} \left(q - \frac{l}{q-1} \right) + (r-2)l + \frac{l}{q-1} - 1$$

Then

$$A(q, l, r, 2) - A(q, l, r, 1) = q^{r-2}l - l \geq 0, \text{ for } r \geq 2.$$

So, $A(q, l, r, 2) > A(q, l, r, 1)$ for $r \geq 3$.

Next, we want to prove that:

$$\begin{aligned} & A(q, l, r, \omega - 1) > A(q, l, r, \omega), \text{ for } \omega \geq 3 \Leftrightarrow \\ & \left\{ S \left(\omega - 1, \left\lfloor \frac{(q-1)(\omega-1)}{2} \right\rfloor \right) - \frac{l}{q-1} \right\} q^{r-(\omega-1)} \\ & \quad + l(r - (\omega - 1)) + \frac{l}{q-1} - 1 > \\ & \left\{ S \left(\omega, \left\lfloor \frac{(q-1)\omega}{2} \right\rfloor \right) - \frac{l}{q-1} \right\} q^{r-\omega} + l(r - \omega) + \frac{l}{q-1} - 1 \Leftrightarrow \\ & \Leftrightarrow q \left\{ S \left(\omega - 1, \left\lfloor \frac{(q-1)(\omega-1)}{2} \right\rfloor \right) - \frac{l}{q-1} \right\} > S \left(\omega, \left\lfloor \frac{(q-1)\omega}{2} \right\rfloor \right) - \frac{l}{q-1}. \end{aligned}$$

We will prove the last inequality.

In the Appendix in [4] the following Lemma is proven

Lemma 1.

$$S(0, 0) = 1 \text{ and } S(0, n) = 0 \text{ for } n > 0.$$

Further, for $m \geq 1$ we have

$$S(m, n) = \sum_{j=0}^{q-1} S(m-1, n-j).$$

Using it, it follows that:

$$\begin{aligned} S\left(\omega, \left\lfloor \frac{(q-1)\omega}{2} \right\rfloor\right) &= \sum_{j=0}^{q-1} S\left(\omega-1, \left\lfloor \frac{(q-1)\omega}{2} \right\rfloor - j\right) \\ &= S\left(\omega-1, \left\lfloor \frac{(q-1)\omega}{2} \right\rfloor\right) \\ &\quad + \dots\dots\dots \\ &\quad + S\left(\omega-1, \left\lfloor \frac{(q-1)\omega}{2} \right\rfloor - (q-1)\right). \end{aligned}$$

Another lemma from the Appendix in [4] says:

Lemma 2. *If $m \geq 2$ and $0 \leq n_1 < n_2 \leq (q-1)m/2$, then $S(m, n_1) < S(m, n_2)$.*

Using it, for $m = \omega - 1 \geq 2$ (which is $\omega \geq 3$), we have that for $\lfloor \frac{q-1}{2} \rfloor < j \leq q-1$,

$$\begin{aligned} S\left(\omega-1, \left\lfloor \frac{(q-1)\omega}{2} \right\rfloor - j\right) &< S\left(\omega-1, \left\lfloor \frac{(q-1)\omega}{2} \right\rfloor - \left\lfloor \frac{q-1}{2} \right\rfloor\right) \\ &= S\left(\omega-1, \left\lfloor \frac{(q-1)(\omega-1)}{2} \right\rfloor\right), \text{ since:} \end{aligned}$$

If $(q-1)$ is even we have

$$\left\lfloor \frac{(q-1)\omega}{2} \right\rfloor - \left\lfloor \frac{q-1}{2} \right\rfloor = \frac{(q-1)(\omega-1)}{2} = \left\lfloor \frac{(q-1)(\omega-1)}{2} \right\rfloor.$$

If $(q-1)$ is odd and ω is odd, then

$$\left\lfloor \frac{(q-1)(\omega-1)}{2} \right\rfloor = \frac{(q-1)\omega-1}{2} - \frac{q-2}{2} = \left\lfloor \frac{(q-1)\omega}{2} \right\rfloor - \left\lfloor \frac{q-1}{2} \right\rfloor.$$

If $(q-1)$ is odd and ω is even, then

$$\begin{aligned} \left\lfloor \frac{(q-1)(\omega-1)}{2} \right\rfloor &= \frac{(q-1)(\omega-1)-1}{2} = \frac{(q-1)\omega}{2} - \frac{q-2}{2} \\ &= \left\lfloor \frac{(q-1)\omega}{2} \right\rfloor - \left\lfloor \frac{q-1}{2} \right\rfloor. \end{aligned}$$

The function $S(m, n)$ has symmetry, stated in [4], which is.

Lemma 3. *If $m \geq 0$ and $0 \leq n \leq (q-1)m$, then*

$$S(m, n) = S(m, (q-1)m - n).$$

For $0 \leq j < \lfloor \frac{q-1}{2} \rfloor$ we have:

$$\begin{aligned} S\left(\omega - 1, \left\lfloor \frac{(q-1)\omega}{2} \right\rfloor - j\right) &= S\left(\omega - 1, (q-1)(\omega - 1) - \left\lfloor \frac{(q-1)\omega}{2} \right\rfloor + j\right) \\ &= S\left(\omega - 1, \left\lfloor \frac{(q-1)(\omega - 2)}{2} \right\rfloor + j\right). \end{aligned}$$

From Lemma 2 and for $0 \leq j < \lfloor \frac{q-1}{2} \rfloor$ it follows that

$$\begin{aligned} S\left(\omega - 1, \left\lfloor \frac{(q-1)(\omega - 2)}{2} \right\rfloor + j\right) &< S\left(\omega - 1, \left\lfloor \frac{(q-1)(\omega - 2)}{2} \right\rfloor + \left\lfloor \frac{q-1}{2} \right\rfloor\right) \\ &= S\left(\omega - 1, \left\lfloor \frac{(q-1)(\omega - 1)}{2} \right\rfloor\right), \text{ since:} \end{aligned}$$

If $(q-1)$ is even, then

$$\begin{aligned} \left\lfloor \frac{(q-1)(\omega - 2)}{2} \right\rfloor + \left\lfloor \frac{q-1}{2} \right\rfloor &= \frac{(q-1)(\omega - 2)}{2} + \frac{q-1}{2} = \frac{(q-1)(\omega - 1)}{2} \\ &= \left\lfloor \frac{(q-1)(\omega - 1)}{2} \right\rfloor. \end{aligned}$$

If $(q-1)$ is odd and ω is even, then

$$\begin{aligned} \left\lfloor \frac{(q-1)(\omega - 2)}{2} \right\rfloor + \left\lfloor \frac{q-1}{2} \right\rfloor &= \frac{(q-1)(\omega - 2)}{2} + \frac{q-2}{2} = \frac{(q-1)(\omega - 1) - 1}{2} \\ &= \left\lfloor \frac{(q-1)(\omega - 1)}{2} \right\rfloor. \end{aligned}$$

If $(q-1)$ is odd and ω is odd, then

$$\begin{aligned} \left\lfloor \frac{(q-1)(\omega - 2)}{2} \right\rfloor + \left\lfloor \frac{q-1}{2} \right\rfloor &= \frac{(q-1)(\omega - 2) + 1}{2} + \frac{q-2}{2} = \frac{(q-1)(\omega - 1)}{2} \\ &= \left\lfloor \frac{(q-1)(\omega - 1)}{2} \right\rfloor. \end{aligned}$$

So, we have

$$\begin{aligned} S\left(\omega, \left\lfloor \frac{(q-1)\omega}{2} \right\rfloor\right) &= \sum_{j=0}^{q-1} S\left(\omega - 1, \left\lfloor \frac{(q-1)\omega}{2} \right\rfloor - j\right) \\ &< qS\left(\omega - 1, \left\lfloor \frac{(q-1)(\omega - 1)}{2} \right\rfloor\right) - (q-1). \end{aligned}$$

We use the fact that $l < q - 1$, so

$$qS\left(\omega - 1, \left\lfloor \frac{(q-1)(\omega-1)}{2} \right\rfloor\right) - (q-1) < qS\left(\omega - 1, \left\lfloor \frac{(q-1)(\omega-1)}{2} \right\rfloor\right) - l$$

$$\Rightarrow q\left\{S\left(\omega - 1, \left\lfloor \frac{(q-1)(\omega-1)}{2} \right\rfloor\right) - \frac{l}{q-1}\right\} > S\left(\omega, \left\lfloor \frac{(q-1)\omega}{2} \right\rfloor\right) - \frac{l}{q-1}.$$

Therefore, $A(q, l, r, \omega)$, which is the number of detected errors, receives its maximum when $\omega = 2$, for $q \geq 3$.

This result is valid also when $l = q - 1$.

References

1. B. Bose, S. Elmougy, L.G. Tallini, "Systematic t -unidirectional error-detecting codes over Z_m ", *IEEE Trans. Comp.*, vol. 56, pp. 876-880, 2007.
2. B. Bose, D. J. Lin, "Systematic unidirectional error-detecting codes", *IEEE Trans. Comp.*, vol. 34, pp. 1026-1032, 1985.
3. T. Kløve, P. Oprisan, B. Bose, "The probability of undetected error for a class of asymmetric error detecting codes", *IEEE Trans. Inform. Theory*, vol. 51, pp. 1202-1205, 2005.
4. I. Naydenova, T. Kløve, "Generalized Bose-Lin codes, a class of codes detecting asymmetric errors", *IEEE Trans. Inform. Theory*, vol. 53, pp. 1188-1193, 2007.