AN ABSTRACT OF THE DISSERTATION OF

Noha Elarief for the degree of Doctor of Philosophy in Computer Science

presented on February 4, 2010

Title: Limited Magnitude Error Control Codes

Abstract approved:

Bella Bose

A relatively new model of error control is the limited magnitude error over high radix channels. In this error model, the error magnitude does not exceed a certain limit known beforehand. In this dissertation, we study systematic error control codes for common channels under the assumption that the maximum error magnitude is known a priori. Optimal codes correcting all asymmetric and symmetric errors are given. Further, as it is often the case that we only need to correct a small number of errors, codes that can correct a single error over asymmetric and symmetric channels are also proposed. The designed codes achieve higher code rates than single error correcting codes previously given in the literature. From the error detection point of view, we study both all and t error detecting codes for asymmetric/unidirectional channels and design close-to-optimal codes. Finally, we show how the all asymmetric error correcting codes proposed in this dissertation can be used to detect all symmetric errors.

Limited Magnitude Error Control Codes

by

Noha Elarief

A DISSERTATION

submitted to

Oregon State University

in partial fulfillment of

the requirements for the

degree of

Doctor of Philosophy

Presented February 4, 2010

Commencement June 2010

Doctor of Philosophy dissertation of Noha Elarief presented on February 4, 2010

APPROVED:

Major Professor, representing Computer Science

Director of the School of Electrical Engineering and Computer Science

---

Dean of the Graduate School

I understand that my dissertation will become part of the permanent collection of Oregon State University libraries. My signature below authorizes release of my dissertation to any reader upon request.

Noha Elarief, Author

ACKNOWLEDGMENTS

All praises and thanks be to Allah (God), Most Gracious, Most Merciful. I would not have been able to attain such an achievement except by the will, ease and mercy of Allah; for He said: "Whatever of good reaches you, is from Allah" (Holy Quran, 4:79).

Yet, prophet Muhammad peace and blessings be upon him said: "He who does not thank people does not thank Allah." (Aboo Daawood, 4177 and at-Tirmidhee, 1877). I would therefore like to express my gratitude to all those who offered their valuable help to me throughout my studies. My deep and sincere thanks to my supervisor, Dr. Bella Bose, from whom I have learned a lot, both on the professional and human levels. This work would not have been possible without his guide, support and inspiration. One interesting skill I have learned from him is to try to solve a smaller version of the problem in hand then attempt to generalize the results on the broader problem. As basic as it may sound, this approach had a great impact on my way of thinking.

I am indebted to Dr. Torleiv Kløve for his results on single error correcting codes (Chapter 4).

It is also my pleasure to convey my thanks to my committee members: Dr. Mary Flahive, Dr. Thinh Nguyen, Dr. Timothy Budd and Dr. Jim Coakley for their assistance in refining the final dissertation. Last but not least, I would like to acknowledge the National Science foundation as my work was supported by the NSF grants CCF-0801452 and CCF-0728810.

On the personal level, I would like to dedicate my small accomplishment to my parents Omayma Khedr and Taha Elarief who always encouraged me to pursue higher degrees. It is hard to find suitable words to thank them for everything they have done for me but say "My Lord, have mercy upon them as they brought me up [when I was] little." (Holy Qur'an: 17:24). I owe my most sincere gratitude to my beloved husband Yosof Wanly for his patience, encouragement and support, but especially for sometimes having to stay up late with me to finish my work on time. Special thanks go to my sisters and friends for their love, care and support throughout my studies.

TABLE OF CONTENTS

	Page
1 Introduction	1
2 Optimal all asymmetric error correcting codes	8
2.1 Preliminaries	8
2.2 A lower bound on the number of check digits	9
2.3 Optimal l-AAEC codes	10
2.4 Concluding remarks	12
3 Optimal all symmetric error correcting codes	16
4 Single asymmetric error correcting codes	19
4.1 The B sequence	21
4.2 Code construction	28
4.3 Single symmetric limited magnitude error correction	33
5 Asymmetric/Unidirectional error detecting codes	36
5.1 All error detecting codes	36
5.2 t error detecting codes	41
6 Symmetric error detecting codes	45
7 Conclusion and future work	46
Bibliography	47

LIST OF FIGURES

Figure Page

1.1 Communication system 2

1.2 BSC vs Z-channel 4

1.3 q-ary asymmetric channel vs q-ary asymmetric channel with level 1 . . . 5

LIST OF TABLES

Table	Page
1 Modular $B_1([0,2])$ found by a greedy algorithm	26
2 Modular $B_1([0,3])$ found by a greedy algorithm	27

LIMITED MAGNITUDE ERROR CONTROL CODES

1. INTRODUCTION

A typical communication system can be modeled as shown in Figure 1.1 [13, 16]:

(1) An information source generating a sequence of symbols (a message) from a source alphabet Z_q, the set of integers modulo q, at a *rate R* (measured in symbols per second).

(2) An encoding process which performs two operations: *source* encoding and *channel* encoding. In source encoding (also referred to as data compression), a stream of symbols is encoded into fewer symbols, making use of the structure in the symbol's stream. Then, channel coding adds redundancy to the compressed block in such a way that, in case some symbols were altered during transmission (due to noise or imperfection), the error can be detected and possibly corrected by the decoding process, resulting in a reliable transmission. The later is referred to as error control coding.

(3) A noisy channel which, in practice, refers to the medium through which information is transmitted. This medium can be a communication channel susceptible to noise or interference or a storage media (e.g, logic circuits and memory systems) in which data deteriorates.

(4) A decoding process which reverses the encoding process to recover the original data.

(5) A sink for the information.

An important parameter that determines the maximum transmission rate over the channel is the *capacity C*, defined as the maximum amount of information that can

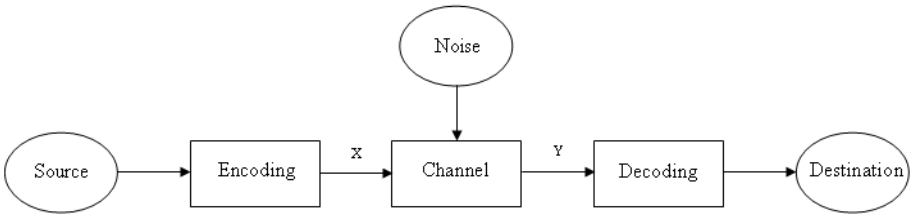

FIGURE 1.1. Communication system

be sent reliably over the channel and is equal to the maximal mutual information of X and Y: $max\ I(X,Y)$, such that X is the channel input and Y is the channel output. In [18] , one of the fundamental theorems of coding theory was introduced: the noisy-channel coding theorem (Shannon's theorem). The theorem states that if a source transmits information at a rate R over a noisy channel of capacity C such that $R < C$, then there exists a coding technique which enables the transmission at an arbitrarily small error probability. While Shannon's theorem points out the existence of error-correction techniques enabling reliable transmission, it does not describe how such codes are constructed.

Error control codes provide the means to detect and/or correct errors. In general, more errors can be detected than corrected. This is because to correct the error it is necessary to identify the position, magnitude and type of error (increasing/decreasing). Moreover, error detecting codes are easier to design than error correcting codes. Yet, the choice of using error detecting over error correcting codes is application specific. In applications where the source and destination can communicate in a two way mode error detecting codes may be sufficient since the destination can request the retransmission of data when error is detected in the received message. This scheme is referred to as automatic repeat request (ARQ). On the other hand, for applications like the paging systems [16] where a mobile user is being sent alphanumerical characters as text messages, it is not possible for the

destination to communicate back with the source requesting retransmission. In such a case, the receiver must be able to employ error correction techniques to recover the original data.

In block coding, the message to be sent is partitioned into blocks of k symbols over Z_q, i.e there are q^k possible blocks. Every group of k symbols (referred to as *information symbols*) is encoded into a longer block of length n, a *codeword*. Thus, there are $r = n - k$ redundant symbols, the *check symbols*. We say that a code is *optimal* if it uses the minimum possible redundancy. The encoding can be done either systematically or non-systematically. In a *systematic code* the encoding process is such that in the resulting codeword the information symbols can be separated from the check symbols . Therefore, data processing and encoding/decoding can be done in parallel which is advantageous in real time applications. However, this is not possible with non-systematic codes. Our main focus in this dissertation is on systematic codes.

In order to design a code for a specific application, we need to first identify a model capturing the channel properties. A *channel model* is a description of the probability to receive a symbol i when a symbol j is sent, for $i, j \in Z_q$. We mainly deal with discrete memoryless channels; i.e the probability that j is received given that i was sent, $P(j|i)$, is independent from other symbols that were/will be sent. Most work in error correcting codes was done under the assumption of binary *symmetric* errors: both $1 \rightarrow 0$ and $0 \rightarrow 1$ errors can occur at the same transmission. The binary symmetric channel (BSC) is a special case of the *q-ary symmetric channel* for the case where $q = 2$. The transition probabilities for a *q-ary symmetric channel* are defined as [15]:

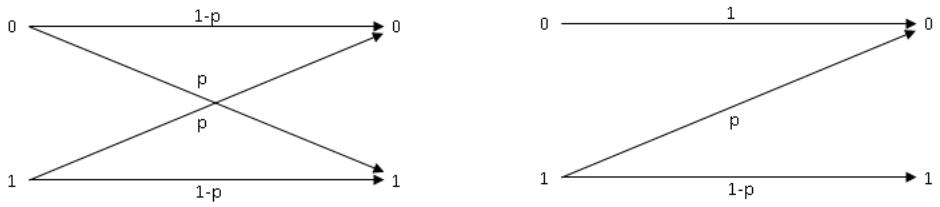

FIGURE 1.2. BSC (left) vs Z-channel (right)

$$P(j|i) = \begin{cases} 1-p, & j=i \\ \frac{p}{q-1}, & j \neq i \end{cases}$$

where p is the symbol error probability. However, it is often the case that only one type of error, known beforehand, is likely to occur. For example, in optical systems photons may decay but new photons cannot be generated. We refer to these errors as *asymmetric* errors giving rise to *q-ary asymmetric channels* with the following transition probabilities (we assume the dominant error type is the decreasing error):

$$P(j|i) = \begin{cases} 1-p, j=i \\ \frac{p}{i}, j<i \\ 0, j>i \end{cases}$$

Figure 1.2 illustrates the difference between the BSC and the binary asymmetric channel (also known as the Z-channel).

Furthermore, a closely related model is the *q-ary unidirectional channel* in which the error type is not known a priori, nevertheless within a particular word only one type can occur. In [4], common sources of unidirectional errors in VLSI devices are given: multiple faults in address decoders, open line and line shortening in word lines, failures in power supplies and stuck-at-faults in shift registers.

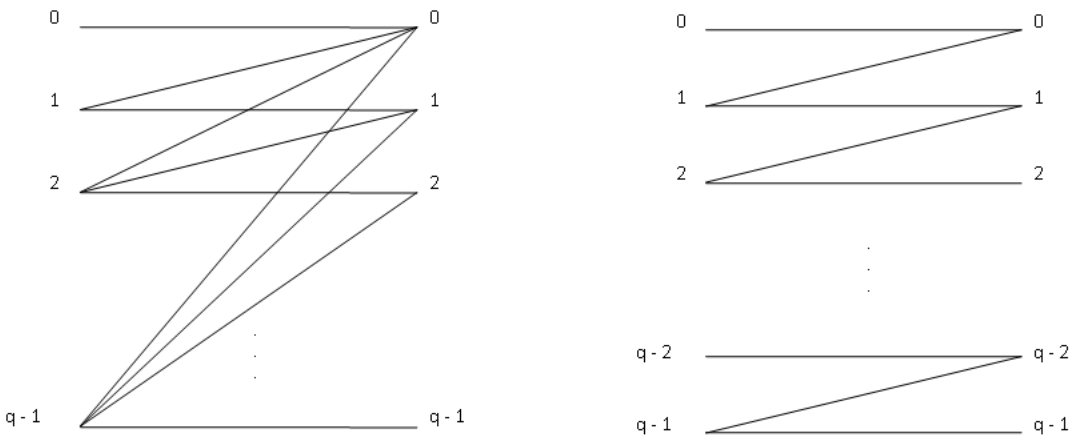

FIGURE 1.3. q-ary asymmetric channel (left) vs q-ary asymmetric channel with level 1 (right)

Not until recently has the notion of *limited magnitude errors* been introduced [2]. For a vector $x = (x_{n-1}, x_{n-2}, \ldots, x_0)$ over Z_q we say that the corresponding channel output $x' = (x'_{n-1}, x'_{n-2}, \ldots, x'_0)$ suffers a *symmetric* error of maximum magnitude l (or l-limited magnitude error) if and only if $x_i - e_i \leq x'_i \leq x_i + e_i$, where $0 \leq e_i \leq l$, $\forall i \in \{0, 1, \ldots, n\}$. On the other hand, we say that x' suffers an *asymmetric* error of maximum magnitude l if and only if $x_i - e_i \leq x'_i \leq x_i$. Figure 1.3 illustrates the difference between the traditional q-ary asymmetric channel and the q-ary asymmetric channel with level $l = 1$. In [9] an interesting application for this special case of q-ary asymmetric channel was pointed out: multi-level flash memories. Unlike traditional single-level flash memories where each cell stores only one bit, multi-level flash memories achieve higher storage capacities and thus lower manufacturing costs by programming the cells into one of $q > 2$ threshold voltages thereby storing $\log_2 q$ bits per cell. Nevertheless, increasing the number of threshold levels imposes an important challenge [11]: the voltage difference between states

is narrowed since - technically - the voltage window is limited. A natural consequence is that reliability issues such as low data retention, program disturbs and programing/erasing endurance become more significant [9]. Errors in such cases are typically in one dominant direction and of limited magnitude.

The question that arises is then: how, if at all, does this additional piece of information (i.e knowing the maximum error magnitude) help in designing more efficient error correcting/detecting codes? In this dissertation, we try to explore that in depth. As the notion of limited magnitude error is a recent one, the only work over channels with limited magnitude errors (to the best of our knowledge) were published by Ahlswede et al. [2, 1] and Cassuto et al. [9, 10]. Ahlswede et al. [2, 1] introduced the limited magnitude error model and studied its properties. They also proposed non-systematic error correcting codes for the unidirectional and asymmetric channels. On the other hand, Cassuto et al. [9, 10] proposed the use of asymmetric limited magnitude channels as an error model for Flash Memories. Moreover, they designed non-systematic and systematic codes that can correct t asymmetric errors and showed how the proposed encoding/decoding algorithms can be implemented for practical use in Flash Memories. In this dissertation we extend the work done in this domain by proposing new families of error control codes. The given codes are advantageous over the ones found in the literature since they are systematic and/or achieve higher code rates. In Chapter 2, we first give a bound on the number of check digits in codes that correct all asymmetric errors of limited magnitude l (l-AAEC codes). Then we present a code that uses the minimum possible number of check symbols and is thus optimal. Properties of the q-ary *symmetric* channel with level l are explored in Chapter 3. We show that the code construction ideas used for l-AAEC codes can be applied to design codes correcting all symmetric errors of

maximum level l (l-ASEC codes). Furthermore, in Chapter 4 we propose systematic codes which correct single limited magnitude asymmetric errors (single l-AEC codes). The proposed code achieves a higher rate than the one given in [10] for the case where $t = 1$. The essence of the code construction is to find a sequence of numbers that can be used as the leading non-zero term in the columns of the parity check matrix. These sequences are special cases of modular $B_h(S)$ sequences which will be defined in Section 4.1. Methods to find those sequences are also given in Section 4.1. In Section 4.2, the code construction and the optimality of the code are considered. In Section 4.3, we show that a similar idea can be used to construct codes correcting single symmetric errors of limited magnitude. In the second part of the dissertation, error detection is studied. In Chapter 5 we design systematic error detecting codes for q-ary symmetric, asymmetric and unidirectional channels with known maximum error magnitude l. We first consider systematic all l-limited magnitude asymmetric error detecting (l-AAED) codes, giving a lower bound on the number of check digits and proposing an l-AAED code that uses minimum possible redundancy when $kl + l(\frac{q^r-1}{q-1}) < q^r$. Then we study the t error detecting problem showing that the systematic t-unidirectional error detecting codes proposed in [6, 17] achieve higher detecting capabilities when the maximum error magnitude is known. In Chapter 6, the error detecting problem for limited magnitude symmetric channels is considered; we show that a code correcting all asymmetric errors of maximum magnitude l (an l-AAEC code) can also be used to detect all symmetric errors of the same maximum magnitude. Finally, concluding remarks and open problems are given in Chapter 7.

2. OPTIMAL ALL ASYMMETRIC ERROR CORRECTING CODES

2.1. Preliminaries.

Knowledge of the maximum error level gives nice properties that can be used in the design of error correcting codes. We start by defining a distance metric capturing these properties as mentioned in [1]:

Definition 2.1. Let $x = (x_{n-1}, x_{n-2}, \ldots, x_0)$ and $y = (y_{n-1}, y_{n-2}, \ldots, y_0)$ be two vectors over Z_q, then the distance between x and y is defined as:

$$d(x,y) \quad = \quad max\{|x_i - y_i| : i \in \{0,1,\ldots,n-1\}\}$$

It is worth noting that, by properties of absolute values, $d(x,y)$ defines a metric. Moreover, $d(x,y) \leq q-1$ by definition.

The following theorem gives necessary and sufficient conditions on the minimum distance of an all l-limited magnitude error correcting (l-AAEC) code.

Theorem 2.2. [1] *A code $C \subseteq Q^n$ is an l-AAEC code if and only if, for all distinct codewords, $x, y \in C$, $d(x,y) \geq l+1$.*

Let $A_a(n,l,q)$ denote the maximum number of codewords in a q-ary l-AAEC code of length n. A bound on $A_a(n,l,q)$ and a non-systematic l-AAEC code achieving this bound are given in [1]:

Theorem 2.3. [1] $\forall n \in \{1,2,3\ldots\}$ *and* $l \in Q$, $A_a(n,l,q) = \left\lceil \frac{q}{l+1} \right\rceil^n$.

Theorem 2.4. [1] *Let C be the code of length n over Z_q defined as*

$$C \quad = \quad \{(x_{n-1}, x_{n-2}, \ldots, x_0) : x_i \equiv 0 \mod (l+1),\ \forall i \in \{0,1,\ldots,n-1\}\}$$

Then, C is an l-AAEC code with $\left\lceil \frac{q}{l+1} \right\rceil^n$ *codewords.*

Finally, for further analysis, $x \pmod a$ denotes the component-wise least non-negative remainder of a vector x when divided by an integer a.

2.2. **A lower bound on the number of check digits.**

In the following theorem, we investigate the minimum number of check digits needed to encode information vectors of a certain length.

Theorem 2.5. *Let C be a systematic q-ary l-AAEC code, such that the number of information digits in a codeword is k. Then, the number of check digits, r, satisfies the following condition*

$$r \geq \frac{k \times \log(l+1)}{\log \left\lceil \frac{q}{l+1} \right\rceil}.$$

Proof. Consider the subset of information vectors, $V = \{(x_{k-1}, x_{k-2}, \ldots, x_0) : 0 \leq x_i \leq l, \forall i \in \{0,1,\ldots,k-1\}\}$. V can be viewed as the set of all vectors of length k over Z_{l+1}. Hence, $\forall x, y \in V$, $d(x,y) \leq l$, and $|V| = (l+1)^k$. Therefore, by Theorem 2.2, the checks assigned to vectors in V must be at least $l+1$ apart for errors to be successfully corrected. Theorem 2.2 and Theorem 2.3 together give a bound on the number of vectors satisfying such criterion and we get:

$$\left\lceil \frac{q}{l+1} \right\rceil^r \geq (l+1)^k$$

Taking the log of both sides of the above inequality we get the desired property. □

One important implication of the above theorem is that it is not possible to design a systematic code correcting all errors of maximum magnitude l when $l = q-1$,

since the expression $\frac{k\times\log(l+1)}{\log\lceil\frac{q}{l+1}\rceil}$ approaches infinity in this case. Therefore, for the rest of the chapter, we assume $l \leq q-2$.

2.3. **Optimal l-AAEC codes.**

Codes which require exactly $r = \left\lceil \frac{k\times\log(l+1)}{\log\lceil\frac{q}{l+1}\rceil} \right\rceil$ check digits are presented.

2.3.1. *Encoding algorithm.*

Input: The information vector: $(x_{k-1}, x_{k-2}, \ldots, x_0)$.

Output: The encoded vector: $x = (x_{k-1}, x_{k-2}, \ldots, x_0, c_{r-1}, c_{r-2}, \ldots, c_0)$.

(1) Compute a, the number with radix $(l+1)$ representing $(x_{k-1}, x_{k-2}, \ldots, x_0) \pmod{(l+1)}$:
$a = y_{k-1}(l+1)^{k-1} + y_{k-2}(l+1)^{k-2} + \ldots + y_0(l+1)^0$,
where $y_i = x_i \pmod{(l+1)}, i \in \{0, 1, \ldots, k-1\}$.

(2) Represent a in radix $\lceil\frac{q}{l+1}\rceil$ number with r digits: $(a_{r-1}, a_{r-2}, \ldots, a_0)$.

(3) Compute the check part: $c = (c_{r-1}, c_{r-2}, \ldots, c_0)$, where $c_i = (l+1)a_i, \forall i \in \{0, 1, \ldots, r-1\}$.

(4) Output the encoded vector $x = (x_{k-1}, x_{k-2}, \ldots, x_0, c_{r-1}, c_{r-2}, \ldots, c_0)$.

Example 2.6. We encode the word $(6,2,8,1)$ over Z_{10}, assuming a maximum error level of 2. The number of check digits needed is $r = \left\lceil \frac{4\log(2+1)}{\log\lceil\frac{10}{2+1}\rceil} \right\rceil = 4$. With notations as above, $a = 0\times 3^3 + 2\times 3^2 + 2\times 3^1 + 1\times 3^0 = 25$ and thus $(0,1,2,1)$ is the representation of a in base 4. Therefore, the encoded codeword is $(6,2,8,1,0,3,6,3)$.

Theorem 2.7. *The above construction yields codewords of minimum distance $l+1$.*

Proof. Given two distinct information vectors: $v_1 = (x_{k-1}, x_{k-2}, \ldots, x_0)$ and $v_2 = (y_{k-1}, y_{k-2}, \ldots, y_0)$, there are two possibilities: $v_1 \pmod{(l+1)} \neq v_2 \pmod{(l+1)}$ in which case each vector is assigned different check digits and, since the check

digits are multiples of $(l+1)$, the distance between the resulting codewords is at least $l+1$. For the second case, $v_1 \pmod{(l+1)} = v_2 \pmod{(l+1)}$, v_1 and v_2 are assigned the same check digits. Nevertheless, by distinctness of v_1 and v_2, $\exists i \in \{0,1,\ldots,k-1\}$ such that $x_i = y_i + m(l+1)$ for some $m \geq 1$. Therefore, $d(v_1,v_2) \geq l+1$, and the resulting codewords satisfy the desired property. □

2.3.2. *Decoding algorithm.*

Input: The channel output: $x' = (x'_{k-1}, x'_{k-2}, \ldots, x'_0, c'_{r-1}, c'_{r-2}, \ldots, c'_0)$.

Output: The recovered codeword: $(x_{k-1}, x_{k-2}, \ldots, x_0, c_{r-1}, c_{r-2}, \ldots, c_0)$.

(1) Recover the check symbols, $(c_{r-1}, c_{r-2}, \ldots, c_0)$, by rounding each received check symbol upwards to the nearest multiple of $(l+1)$.

(2) Compute a, the number with radix $Z_{\lceil \frac{q}{l+1} \rceil}$ representing $(\frac{c_{r-1}}{l+1}, \frac{c_{r-2}}{l+1}, \ldots, \frac{c_0}{l+1})$: $a = (\frac{c_{r-1}}{l+1}) \lceil \frac{q}{l+1} \rceil^{r-1} + (\frac{c_{r-2}}{l+1}) \lceil \frac{q}{l+1} \rceil^{r-2} + \ldots + (\frac{c_0}{l+1}) \lceil \frac{q}{l+1} \rceil^{0}$.

(3) Represent a in radix $(l+1)$ with k digits: $y = (y_{k-1}, y_{k-2}, \ldots, y_0)$.

(4) Let $e_i = (y_i - x'_i) \pmod{(l+1)}$. The information symbols are: $(x_{k-1}, x_{k-2}, \ldots, x_0)$, such that $x_i = x'_i + e_i$, $i = 0,1,\ldots,k-1$.

(5) Output the codeword: $(x_{k-1}, x_{k-2}, \ldots, x_0, c_{r-1}, c_{r-2}, \ldots, c_0)$.

Example 2.8. Let the encoded word be as in example 2.6 and the channel output be $x' = (4,2,7,1,0,3,5,1)$. Rounding the check symbols upwards to the nearest multiple of 3, we get $(0,3,6,3)$. As in Steps 2 and 3 of the algorithm, we compute $a = 0121_4 = 25$, and $y = (0,2,2,1)$. Thus, the correct information symbols are $(6,2,8,1)$.

Theorem 2.9. *Let x be a codeword encoded using the algorithm given in Section 2.3.1, and let x' be the l-asymmetric channel output. Then, the above decoding algorithm successfully recovers x.*

Proof. Let $x = (x_{k-1}, x_{k-2}, \ldots, x_0, c_{r-1}, c_{r-2}, \ldots, c_0)$, then, by the channel properties, $x' = (x'_{k-1}, x'_{k-2}, \ldots, x'_0, c'_{r-1}, c'_{r-2}, \ldots, c'_0)$ is such that $x_i - l \leq x'_i \leq x_i$ and $c_i - l \leq c'_i \leq c_i$. Moreover, the encoding algorithm yields check symbols that are multiples of $l+1$, i.e. c'_i lies between two successive multiples of $l+1$. Therefore, the first step of the decoding algorithm successfully recovers the check symbols. It can also be seen that Steps 2 and 3 of the above algorithm reverse the operations of Steps 1 and 2 of the encoding algorithm. Hence, with notations as above, $y = (y_{k-1}, y_{k-2}, \ldots, y_0) = (x_{k-1}, x_{k-2}, \ldots, x_0) \pmod{(l+1)}$. At Step 4, e_i can be seen as the magnitude of the error at the i^{th} information symbol, such that

$$x_i \;=\; x'_i + e_i \equiv y_i \pmod{(l+1)}.$$

Thus

$$e_i \;\equiv\; (y_i - x'_i) \pmod{(l+1)}.$$

Since the maximum error magnitude is l (i.e. $0 \leq e_i \leq l$) the value of e_i is successfully computed at Step 4 of the decoding algorithm, recovering the information symbols. □

2.4. **Concluding remarks.**

The codes presented in this chapter are advantageous over other l-AAEC codes given in the literature, namely in [10, 1]. The code constructions given in [10] start with t symmetric error correcting codes over $l+1$ to construct codes that can correct t asymmetric errors of maximum magnitude l. It is known that no such code exists when $t = n$ since the minimum distance of any t symmetric error correcting codes is $2t+1$ [14]. Moreover, the codes given in [10] are not optimal

in general which makes the use of the l-AAEC codes presented in this chapter more favorable as t approaches n. As opposed to the l-AAEC codes proposed in [1], our code construction is systematic; information symbols are separable from the check symbols resulting in faster encoding/decoding operations. Fortunately, the cost of having a systematic code is low: we show that the rate of our l-AAEC code is very close to the one given in [1]. The rate R of an error correcting code is given as $R = \frac{k}{n}$ where k is the number of information digits and n is the length of the code. For the code given in [1], the rate, $R_{non-systematic}$, is

$$\begin{aligned} R_{non-systematic} &= \frac{\log_q \lceil \frac{q}{l+1} \rceil^n}{n} \\ &= \log_q \lceil \frac{q}{l+1} \rceil. \end{aligned}$$

The rate of the proposed code, $R_{systematic}$, is

$$\begin{aligned} R_{systematic} &= \frac{k}{k+r} \\ &= \frac{k}{k+k\left\lceil \frac{\log_q(l+1)}{\log_q \lceil \frac{q}{l+1} \rceil} \right\rceil} \\ &= \frac{1}{1+\left\lceil \frac{\log_q(l+1)}{\log_q \lceil \frac{q}{l+1} \rceil} \right\rceil}, \end{aligned}$$

which can be approximated to

$$\begin{aligned} R_{systematic} &\approx \frac{1}{1+\frac{\log_q(l+1)}{\log_q \frac{q}{l+1}}} \\ &= \frac{\log_q \frac{q}{l+1}}{\log_q \frac{q}{l+1} + \log_q(l+1)} \\ &= \frac{\log_q \frac{q}{l+1}}{\log_q q - \log_q(l+1) + \log_q(l+1)} \\ &= \log_q \frac{q}{l+1}. \end{aligned}$$

The table below illustrates the closeness of the values of $R_{systematic}$ and $R_{non-systematic}$ for $q = 8$ and $q = 16$:

q	l	$R_{non-systematic}$	$R_{systematic}$
8	1	0.66	0.5
	2	0.52	0.5
	3	0.33	0.33
	4	0.33	0.25
	5	0.33	0.25
	6	0.33	0.25
16	1	0.75	0.5
	2	0.64	0.5
	3	0.5	0.5
	4	0.5	0.33
	5	0.39	0.33
	6	0.39	0.33
	7	0.25	0.25
	8	0.25	0.25
	9	0.25	0.25
	10	0.25	0.25
	11	0.25	0.25
	12	0.25	0.25
	13	0.25	0.25
	14	0.25	0.25

3. OPTIMAL ALL SYMMETRIC ERROR CORRECTING CODES

We begin by exploring some of the properties of l limited magnitude all symmetric error correcting codes. For a vector $x = (x_{n-1}, x_{n-2}, \ldots, x_0)$ over Z_q we say that the corresponding channel output $x' = (x'_{n-1}, x'_{n-2}, \ldots, x'_0)$ suffers a symmetric error of maximum magnitude l if and only if $x_i - e_i \leq x'_i \leq x_i + e_i$, where $0 \leq e_i \leq l$, $\forall i \in \{0, 1, \ldots, n\}$. As shown below, the similarity between the properties of l-ASEC (all l-limited magnitude symmetric error correcting) codes and l-AAEC codes allows us to extend the code construction idea we presented in the previous section to design a family of l-SEC codes.

Theorem 3.1. *A code C is capable of correcting all symmetric errors of maximum magnitude l if and only if C has minimum distance $2l+1$.*

Proof. Let S_x be the set of all words obtained from a codeword $x \in C$, where $|x| = n$, due to n or less symmetric errors of maximum magnitude l, i.e. $S_x = \{(x'_{n-1}, x'_{n-2}, \ldots, x'_0) : x'_i = x_i \pm e_i, e_i \in \{0, 1 \ldots, l\}\}$. Then, it is easy to see that, if C has minimum distance $2l+1$, then $\forall x, y \in C$, $S_x \cap S_y = \emptyset$. Therefore, C is an l-ASEC code.

Conversely, if $\exists x, y \in C$ such that $d(x, y) \leq 2l$, then it is possible to obtain a word, say z, from both x and y due to symmetric errors of magnitude l or less. Hence, a decoder for C cannot correct z. Therefore, the minimum distance should be no less than $2l+1$ for C to be capable of correcting all symmetric errors of maximum magnitude l. □

The above theorem implies that, when $l > \frac{q-2}{2}$, any l-ASEC code can have at most one codeword. Thus, we assume $l \leq \frac{q-2}{2}$.

Theorem 3.2. *Let $A_s(n,l,q)$ denote the maximum number of words in a q-ary l-ASEC code of length n. Then*

$$A_s(n,l,q) \;=\; \left\lceil \frac{q}{2l+1} \right\rceil^n.$$

Proof. Similar to the proof of Theorem 2.3 □

Theorem 3.3. *Let C be a code of length n over Z_q defined as:*

$$C \;=\; \{(x_{n-1},x_{n-2},\ldots,x_0) : x_i \equiv 0 \pmod{(2l+1)},\ \forall i \in \{0,1,\ldots,n-1\}\}.$$

Then, C is an l-ASEC with $A_s(n,l,q)$ codewords.

Proof. Similar to the proof of Theorem 2.4. Digits of the channel output can be decoded in this case by rounding downwards or upwards (whichever is closer) to the nearest multiple of $2l+1$. □

Theorem 3.4. *Let C be a systematic q-ary l-ASEC code, such that the number of information digits in a codeword is k. Then, the number of check digits, r, satisfies the following condition*

$$r \;\geq\; \frac{k \times \log(2l+1)}{\log\left\lceil \frac{q}{2l+1} \right\rceil}.$$

Proof. Similar to the proof of Theorem 2.5 □

Now that we have identified the similarities between l-ASEC and l-AAEC codes, it can be seen that the proposed encoding/decoding algorithms for l-AAEC codes (Section 2.3.1 and 2.3.2 respectively) can be modified in the following way to construct an l-ASEC code. In both algorithms, simply replace all computations including the value $l+1$ with $2l+1$. Moreover, in Step 1 of the decoding algorithm, the

check digits are recovered by rounding the received check digits either upwards or downwards to the nearest multiple of $2l+1$, whichever is closer. Finally, at Step 4 of the decoding algorithm, the information digits are recovered as $x_i = x_i' \pm e_i$, $\forall i \in \{0,1,\ldots,k-1\}$, where $0 \leq e_i \leq l$ such that $x_i \equiv y_i \pmod{(2l+1)}$.

4. SINGLE ASYMMETRIC ERROR CORRECTING CODES

In Chapter 2 and 3, optimal codes that correct *all* errors were proposed. However, in some situations only a few errors are expected to occur. It is therefore beneficial to design codes correcting t errors of limited magnitude to achieve substantial savings (in terms of the check digits) over codes correcting all errors. An interesting special case of t error correcting codes are those that correct a single error. In this chapter, we propose systematic codes which correct single limited magnitude asymmetric errors (single l-AEC codes). The proposed codes achieve higher rates than the ones given in [10] for the case where $t = 1$. We illustrate the main construction by the following examples:

Example 4.1. Suppose we want to construct a single 1-AEC code over $q = 4$. Consider the following parity check matrix for a code C:

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 \\ 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \end{bmatrix},$$

Then C has length 15 and uses 2 check digits. Let $c \in C$ and e be a vector of length 15 with i^{th} component equal to 1 for some $1 \leq i \leq n$ and all other components equal to 0, then

$$(c+e).H^T = c.H^T + e.H^T = e.H^T$$

where $c+e$ is a vector suffering a single asymmetric error of magnitude 1. It is easy to see that the multiplication $e.H^T$ gives the transpose of the i^{th}column of H. Since the columns of H are all distinct, the error location can be determined and the error is corrected.

In general, when $l = 1$, the columns of the parity check matrix are all combinations of r column vectors over q (except the all-zero combination). Therefore the length of the code is $n = q^r - 1$. In theorem 4.10 we will show that this construction is optimal. For higher values of l the construction is less straightforward.

Example 4.2. Let $q = 5$, $l = 2$ and $r = 2$ check digits. We want the column vectors and two times the column vectors of H to be all distinct $\pmod 5$. This is because the error vector can either be e as in the previous example or $2e$ (up to le in general). We note that 2 is a primitive root modulo 5 since $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 3, 2^4 = 1 \pmod 5$. Hence if the leading non-zero elements of the columns of H are taken as the alternating powers of 2 (i.e 1 and 4 or 2 and 3) the desired condition will be satisfied. That is,

$$H = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 4 & 4 & 4 & 4 & 4 \\ 1 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 \end{bmatrix}$$

is a parity check matrix for a single 2-AEC code.

In theorem 4.10, we will show that the above construction is also optimal. The essence of the code construction is to find a sequence of numbers that can be used as the leading non-zero term in the columns of the parity check matrix as illustrated in the above examples. These sequences are special cases of *modular* $B_h(S)$ *sequences* [3] which will be defined in Section 4.1. Methods to find those sequences are also given in Section 4.1. In Section 4.2, the code construction and the optimality of the code are considered. In Section 4.3, we show that a similar idea can be used to construct codes correcting single symmetric errors of limited magnitude.

4.1. **The B sequence.**

4.1.1. *The B_h sequence.*

For integers a, b, where $a \leq b$, we let

$$[a,b] = \{a, a+1, a+2, \ldots, b\}.$$

For a set S of integers, a $B_h(S)$ sequence of length m is a sequence of m distinct positive integers $b_0, b_1, \ldots, b_{m-1}$ such that all sums

$$\sum_{j=1}^{h} a_j b_{i_j},$$

where $0 \leq i_1 < i_2 < \cdots < i_h \leq m-1$ and $a_j \in S$, are distinct.

A modular $B_h(S)$ sequence of length m and modulus v is a sequence of m distinct positive integers such that all sums

$$\Big(\sum_{j=1}^{h} a_j b_{i_j}\Big) \pmod{v}$$

where $0 \leq i_1 < i_2 < \cdots < i_h \leq m-1$ and $a_j \in S$, are distinct. Note that any $B_h(S)$ sequence is a modular sequence modulo v for sufficiently large v. Most known results relate to $B_h([0,1])$ sequences, also known as "B_h sequences" and "distinct sum sets". B_2 sequences are known as "Sidon sequences" and also "distinct difference sets" since

$$c_{i_1} + c_{i_2} \neq c_{j_1} + c_{j_2}$$

then

$$c_{i_1} - c_{j_1} \neq c_{j_2} - c_{i_2}.$$

Therefore all sums of two elements are distinct if and only if all differences of two elements are distinct. Similar results are also valid modulo v. Other names for such distinct difference sets are "difference triangle sets" and "Golomb rulers". Famous modular distinct difference sets are the Singer and the Bose-Chowla sets. For extensive literature on such sets refer to [3] pp. 419-437.

It can be shown that a modular $B_t([0,l])$ sequence can be used to construct l-AEC codes correcting t errors. In this dissertation, we are interested in modular $B_1([0,l])$ sequences.

4.1.2. *General construction of modular $B_1([0,l])$ sequences.*

Given m and l, a modular $B_1([0,l])$ sequence $(b_0, b_1, \ldots, b_{m-1})$ modulo q must have $q \geq ml$. We give a construction where q is not much larger than this.

Theorem 4.3. *Let p be a prime, $p \geq m$ and $p \geq l+1$. Let $q = p(l+1)$ then the sequence $b_i = i(l+1)+1$ for $0 \leq i \leq m-1$ is a modular $B_1([0,l])$ modulus q.*

Proof. We prove the theorem by contradiction. Suppose that $0 < x_i \leq l, 0 \leq x_j \leq l$, and $b_i x_i \equiv b_j x_j \pmod{q}$ that is

$$(i(l+1)+1)x_i \equiv (j(l+1)+1)x_j \pmod{p(l+1)}.$$

In particular, this implies that

$$x_i \equiv x_j \pmod{l+1}.$$

Therefore

$$x_j = x_i > 0.$$

And hence

$$i(l+1)x_i \equiv j(l+1)x_i \pmod{p(l+1)},$$

and so

$$ix_i \equiv jx_i \pmod{p}.$$

But since $0 < x_i \leq l < p$, then $i \equiv j \pmod{p}$. Finally, since $p \geq m$, this implies that $i = j$. □

4.1.3. *Special cases.*

We can make use of the special properties of l and q to construct maximal-length $B_1([0,l])$ sequences. Let q be a prime such that the order α of 2 modulo q is even. Then $B = \{b_i = 2^{2i} \pmod{q} \mid 0 \leq i \leq \alpha/2 - 1\}$ is a $B([0,2])$ modulo q since $2b_i = 2^{2i+1} \pmod{q} \notin B$. In particular, the construction is best possible if $l = 2$ is a primitive root of q (that is $\alpha = q-1$). The corresponding result for $l = 3$:

Theorem 4.4. *Let q be prime such that $q \equiv 1 \pmod{3}$, 3 is a primitive root modulo q and $2 \equiv 3^{\beta} \pmod{q}$ where $\beta \equiv 2 \pmod{3}$, then*

$$B = \{3^{3i} \pmod{q} \mid 1 \leq i \leq (q-1)/3\}$$

is a $B_1([0,3]) \pmod{q}$.

Proof. Let $b_i = 3^{3i} \in B$ then

$$\begin{aligned} 2b_i &\equiv 3^{3i+\beta} \pmod{q} \\ &\equiv 3^{3j+2} \pmod{q} \end{aligned}$$

for some j. Moreover,

$$3b_i \equiv 3^{3i+1} \pmod{q}$$

and therefore both $2b_i$ and $3b_i \notin B$. It can also be seen that, since q is prime, the multiplicative inverse of b_i exists and thus $2b_i \not\equiv 3b_i$. □

Examples of q and β meeting the criteria in Theorem 4.4 with $q < 1000$:

q	7	139	163	379	571	607	631	751	859
β	2	101	77	149	545	584	98	416	137

When $l \geq 4$, we get the following:

Theorem 4.5. *Let q be a prime such that the order α of l modulo q is a multiple of l. Let*

$$B = \{c_i = l^{li} \pmod{q} \mid 0 \leq i \leq \frac{\alpha}{l} - 1\}.$$

If $ab^{-1} \pmod{q} \notin B$ for $1 \leq a < b \leq l$, then B is a $B_1([0,l]) \pmod{q}$

Proof. Suppose that $ac_i \equiv bc_j \pmod{q}$ for some $a,b \in [1,l-1]$ where, without loss of generality, $j \geq i$. Then

$$ab^{-1} \equiv c_j/c_i \equiv c_{j-i} \pmod{q} \in B.$$

By assumption, this implies that $a = b$ and so $i = j$. □

Example 4.6. For $5 \leq l \leq 12$ there are primes $q \equiv 1 \pmod{l}$ such that the order of l modulo q is $\alpha = (q-1)/2$. Among those there are some for which the conditions

of Theorem 4.5 are satisfied. The smallest primes are:

l	smallest primes
5	$281, 421, 701, 1051, 1231, 1301, 1471, 1571, 1951$
6	$73, 673, 769$
7	$3557, 3613, 4481$
8	$929, 1697, 2081$
9	$487, 1063, 2539$
10	$4441, 11681, 15881$
11	$8009, 16633$
12	$6217, 6673, 7873$

In this table, the smallest prime, for $l = 6$, is 73, and we give a detailed description as an illustration. The order of 6 modulo 73 is $(73-1)/2 = 36$. We have $6^6 \equiv 9 \pmod{73}$,

$$\begin{aligned} B &\equiv \{6^0, 6^6, 6^{12}, 6^{18}, 6^{24}, 6^{30}\} \pmod{73} \\ &= \{1, 9, 8, 72, 64, 65\}, \end{aligned}$$

and

i	0	1	2	3	4	5
$1 \cdot 6^{6i}$	1	9	8	72	64	65
$2 \cdot 6^{6i}$	2	18	16	71	55	57
$3 \cdot 6^{6i}$	3	27	24	70	46	49
$4 \cdot 6^{6i}$	4	36	32	69	37	41
$5 \cdot 6^{6i}$	5	45	40	68	28	33
$6 \cdot 6^{6i}$	6	54	48	67	19	25

q	r	$[c_i]$	$2c_i \pmod q$
2	1	$[1]$	$[0]$
5	2	$[1,4]$	$[2,3]$
6	3	$[1,3,5]$	$[2,0,4]$
9	4	$[1,3,4,7]$	$[2,6,8,5]$
11	5	$[1,3,4,5,9]$	$[2,6,8,10,7]$
14	6	$[1,3,4,5,7,13]$	$[2,6,8,10,0,12]$
15	7	$[1,3,4,5,7,12,13]$	$[2,6,8,10,14,9,11]$
18	8	$[1,3,4,5,7,9,15,17]$	$[2,6,8,10,14,0,12,16]$
21	9	$[1,3,4,5,7,9,16,17,20]$	$[2,6,8,10,14,18,11,13,19]$
22	10	$[1,3,4,5,7,9,11,17,19,21]$	$[2,6,8,10,14,18,0,12,16,20]$
25	11	$[1,3,4,5,7,9,11,12,19,20,21]$	$[2,6,8,10,14,18,22,24,13,15,17]$
29	12	$[1,3,4,5,7,9,11,12,13,23,25,28]$	$[2,6,8,10,14,18,22,24,26,17,21,27]$
30	13	$[1,3,4,5,7,9,11,12,13,15,23,25,29]$	$[2,6,8,10,14,18,22,24,26,0,16,20,28]$

TABLE 1. Modular $B_1([0,2])$ found by a greedy algorithm

4.1.4. *Examples of modular $B_1([0,2])$ found by a greedy algorithm.*

We want a sequence of positive integers $S = c_0, c_1, \ldots, c_{m-1}$ and a modulus q such that $|\{c_i \mid 0 \le i \le m-1\} \cup \{2c_i \pmod q \mid 0 \le i \le m-1\}| = 2m$. Clearly we must have $q \ge 2m$. We designed a greedy algorithm that constructs a modular $B_1([0,2])$ sequence S as follows. The sequence is initialized to $S = \{1\}$. Then at step i, where $2 \le i \le q-1$, the integer i is added to the sequence if and only if $2i \pmod q \notin S$ and $\nexists c_j \in S$ such that $i \equiv 2c_j \pmod q$. Some examples found by the algorithm are listed in Table 1. For each length, we give the sequence with smallest modulus found.

For any prime p and integer a, let $v_p(a)$ be the exact power of p dividing a (this is known as the p-adic valuation of a). A general construction for $l = 2$ is then: given q, consider the sequence of integers c such that $1 \le c \le q/2$ and $v_2(c)$ is even (that is, $c = 4^\alpha \gamma$ where γ is odd). This gives the elements less than or equal to $q/2$ in the greedy construction above. For example, for $q = 35$, we get the following

sequence:

$$1,3,4,5,7,9,11,12,13,15,16,17.$$

The greedy algorithm gives

$$1,3,4,5,7,9,11,12,13,15,16,17,27,28,29,33.$$

The length of the sequence is

$$m = \left\lfloor \frac{q}{4} \right\rfloor + \left\lfloor \frac{q}{4^2} \right\rfloor + \left\lfloor \frac{q}{4^3} \right\rfloor + \cdots .$$

We see that

$$m < \frac{q}{4} + \frac{q}{4^2} + \frac{q}{4^3} + \cdots = \frac{q}{3}.$$

On the other hand, if $4^i \le q < 4^{i+1}$ for some positive integer i, then

$$m \ge \frac{q}{4} + \frac{q}{4^2} + \cdots + \frac{q}{4^k} - i = \frac{q}{3}\left(1 - \frac{1}{4^{i-1}}\right) - i.$$

For example, for $q = 100$, the bounds are $28.25 < m < 33.3$, that is $29 \le m \le 33$. Direct computation shows that $m = 32$.

q	n	$[c_i]$
3	1	[1]
7	2	[1, 6]
8	3	[1, 4, 7]
15	5	[1, 4, 5, 7, 13]
20	6	[1, 4, 5, 9, 13, 17]
26	7	[1, 4, 5, 7, 13, 16, 23]
28	9	[1, 4, 5, 7, 9, 13, 17, 24, 25]
34	10	[1, 4, 5, 7, 9, 11, 17, 20, 29, 31]
40	13	[1, 4, 5, 7, 9, 11, 13, 19, 20, 23, 32, 35, 37]
50	14	[1, 4, 5, 7, 9, 11, 13, 16, 23, 25, 28, 40, 43, 47]

TABLE 2. Modular $B_1([0,3])$ found by a greedy algorithm

4.1.5. *Examples of modular $B_1([0,3])$ sequences found by a greedy algorithm.* Similar to Section 4.1.4, a greedy algorithm is used to find modular $B_1([0,3])$ sequences modulo q. Examples of such sequences are given in Table 4.1.5. A general construction for $l = 3$ is: consider the sequence of integers $c \leq q/3$ such that both $v_2(c)$ and $v_3(c)$ are even, that is, $c = 4^{\alpha}9^{\beta}\gamma$ where $\gcd(\gamma,6) = 1$. The length of the sequence will be approximately $q/6$ (approximately half of the length of the sequence in Section 4.1.4). For example, for $q = 50$ we get the sequence

$$1,4,5,7,9,11,13,16.$$

4.2. **Code construction.**

Using the modular $B_1[0,l]$ sequence $B = (b_0, b_1, \ldots, b_{m-1})$ modulo q, we can construct the following linear single l-AEC code. Let H be the $r \times n$ parity check matrix whose columns are all possible vectors in Z_q^r whose first non-zero element belongs to B. Let C be the null space of H^T. Then C has the following properties:

Theorem 4.7. *C can correct a single asymmetric error of limited magnitude l, where $gcd(q, l!) = 1$.*

Proof. Let $x \in C$ be the sent codeword and x' be the received word such that $x' = x + e$ where $e = (e_1, e_2, \ldots, e_n)$, $\exists i$, $1 \leq i \leq n$, such that $0 < e_i \leq l$ and $\forall j \neq i$, $e_j = 0$. Then, we compute the syndrome

$$\begin{aligned} s = x'H^T &= xH^T + eH^T \\ &= eH^T \\ &= e_i h_i^T \end{aligned}$$

where h_i^T is the transpose of the i^{th} column of H. Let z be the first non-zero element in h_i, then, by construction, we know that

$$z \equiv e_i b \pmod{q}$$

where $b \in B$. By properties of B, both e_i(the error magnitude) and b can be identified. Furthermore, since $gcd(q, e_i) = 1$, then e_i has a multiplicative inverse modulo q, say e_i^{-1}. Hence, the error location can also be determined by computing $e_i^{-1} s = h_i^T$. □

Note that the $B_1[0,l]$ modulo q sequences (for prime q) given in Section 4.1 can be used to construct single l-AEC codes. This is because $gcd(q,e) = 1$ where $1 \leq e \leq l < q$ and thus $gcd(q, l!) = 1$. For the B sequence generated in Theorem 4.3, $q = p(l+1)$ where p is prime, $p \geq l+1$ and $(l+1)$ is prime (if $(l+1)$ is not prime then choose the next integer $l' > l$ such that $(l'+1)$ is prime) and thus $gcd(p(l+1), l!) = 1$. The following example illustrates the code construction using the general modular B sequence as given in Section 4.1.

Example 4.8. Suppose $l = 2$ and $p = 5$. Thus $q = p(l+1) = 5 \times 3 = 15$. Using Theorem 4.3 we get the sequence $B = \{1,4,7,10,13\}$. For $r = 2$, the H matrix will be

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & \cdots & 1 & 4 & \cdots & 4 & 7 & \cdots & 7 & 10 & \cdots & 10 & 13 & \cdots & 13 \\ 1 & 4 & 7 & 10 & 13 & 0 & 1 & \cdots & 14 & 0 & \cdots & 14 & 0 & \cdots & 14 & 0 & \cdots & 14 & 0 & \cdots & 14 \end{bmatrix}$$

This code has length $n = 5 + 5 \times 15 = 80$, with 2 check digits capable of correcting single $l = 2$ limited magnitude errors. Let $2B = \{2,8,14,5,11\}$ be the set which consists of the double of the elements in B. Suppose the syndrome is $s = (2,4)$. Since the first non-zero element in s is $2 \in 2B$ then the error magnitude

is $e_i = 2$. Now $2^{-1} \equiv 8 \pmod{15}$, $8s = (1,2)$ which is the 7^{th} column of H and thus, subtracting 2 from the 7^{th} digit of the received word, the correct word can be obtained.

Theorem 4.9. *The length of the code, n, is* $m\frac{q^r-1}{q-1}$.

Proof. By construction n is the number of all possible vectors over Z_q^r whose first element belongs to B and thus

$$\begin{aligned} n &= \sum_{j=1}^{r} |B| q^{r-j} \\ &= m\frac{q^r-1}{q-1}. \end{aligned}$$

□

Theorem 4.10. *The* $B_1([0,1])$ *sequence* $1,2,\ldots,q-1$ *can be used to construct an optimal single* 1*-AEC code. Moreover, the* $B_1([0,2])$ *and* $B_1([0,3])$ *sequences given in Section 4.1.3 yield optimal codes for* $l = 2$ *and* $l = 3$ *respectively.*

Proof. The bound on the size of any single l-AEC code, C', is given in Theorem 8 in [10]:

$$|C'| \sum_{i=0}^{1} \binom{n}{i} l^i \leq q^n$$

hence, when $l = 1$

$$|C'|(1+n) \leq q^n.$$

Furthermore, the sequence $1,2,\ldots,q-1$ has length $q-1$. Therefore, by Theorem 4.9 the length of the designed code C is

$$\begin{aligned} n &= (q-1)(\frac{q^r-1}{q-1}) \\ &= q^r-1 \end{aligned}$$

and thus

$$\begin{aligned} |C|(1+n) &= |C|(1+q^r-1) \\ &= |C|(q^r) \\ &= q^{n-r}(q^r) \\ &= q^n. \end{aligned}$$

Therefore the code is optimal. Similarly it can be seen that the code constructions for $l=2$ and $l=3$ with the B sequence defined in Section 4.1.3 are also optimal by observing that the length of the sequences are $q/2$ and $q/3$ respectively and that single 2-AEC and 3-AEC codes C' and C'' are such that

$$|C'|(1+2n) \leq q^n,$$

and

$$|C''|(1+3n) \leq q^n.$$

□

Now, we compare our codes with the ones given in [10]. For $l=1$, it is shown in Theorem 4.10 that our construction is optimal. On the other hand, the construction

given in [10] is not optimal in general. For example, starting with a $(7,4)$ Hamming code, the given construction over $q=4$ has length at most 6 when 2 check digits are used whereas the optimal length is $q^2-1=15$. For $l>1$, according to Theorem 4.9 we have that

$$\begin{aligned} n &\geq m\frac{q^r-1}{q-1} \\ &\geq \frac{q^r-1}{q-1}. \end{aligned}$$

In [10], the code given has length n' where

$$n' \leq \frac{(l+1)^{rs}-1}{l}$$

such that

$$s = \log_{l+1}\frac{q}{2}.$$

Hence

$$n' \leq \frac{(\frac{q}{2})^r-1}{l}.$$

Therefore, for large enough q

$$n \geq n',$$

and thus, using the same number of check digits, our construction can be used to encode more information digits than the construction given in [10].

4.3. **Single symmetric limited magnitude error correction.**

In this section, we give codes correcting a single symmetric error of maximum magnitude l (single l-SEC). In this error model, a symbol $a \in Z_q$ can be changed into $a \pm e$ where $0 \leq e \leq l$.

For $l = 1$, single 1-SEC codes are equivalent to single symmetric error correcting codes in the Lee metric. Optimal such codes are known [3]: Let H be the parity check matrix whose columns are all vectors in Z_q^r whose first non-zero elements are in $\{1, 2, \ldots, \frac{q-1}{2}\}$(for odd q). Then the corresponding code can correct any symmetric error of limited magnitude 1. Moreover, in the general symmetric case where $l = q-1$, Hamming codes can be used in order to correct a single error. However, when $2 \leq l \leq q-2$, using a $B_1([-l,l])$ sequence, we can apply the same construction given in the previous section in order to design single l-SEC codes achieving higher rate than the Hamming code. We want a set $c_0, c_1, \ldots, c_{m-1}$ and a modulus q such that all $c_i x_i \pmod q$ for $-l \leq x_i \leq l$ are distinct. We give a general construction for a modular $B_1([-l,l])$ similar to one in Section 4.3. Let p be a prime, $p \geq m$ and $p \geq 2l+1$. Let $q = p(2l+1)$ and let $c_i = i(2l+1)+1$ for $0 \leq i \leq m-1$. Similar to the proof for the $B_1([0,l])$ sequence in Section 4.1.2, we show that this is indeed a modular $B_1([-l,l])$. Suppose that $c_i x_i \equiv c_j x_j \pmod q$, where $x_i \neq 0$, that is

$$(i(2l+1)+1)x_i \equiv (j(2l+1)+1)x_j \pmod{p(2l+1)}.$$

In particular, this implies that

$$x_i \equiv x_j \pmod{2l+1}.$$

But since $x_i, x_j \in \{-l, -l+1, \ldots, l-1, l\}$ and $x_i \neq 0$, this implies that $x_j = x_i \neq 0$. Hence

$$i(2l+1)x_i \equiv j(2l+1)x_i \pmod{p(2l+1)}$$

and so

$$ix_i \equiv jx_i \pmod{p}.$$

Since $x_i \neq 0$, we have $\gcd(x_i, p) = 1$ and so $i \equiv j \pmod{p}$. Finally, since $p \geq m$, then $i = j$.

Now, similar to the assumption in Theorem 4.7, we need to enforce that $gcd(q, e) = 1$,where $e \in [-l, -1] \cup [1, l]$. Therefore, in the above construction we assume that $(2l+1)$ is prime (otherwise, take a higher maximum-magnitude, say l' such that $(2l'+1)$ is prime).

Again, using modular $B_1[-l, l]$ sequences we can construct single l-SEC codes. Let H be the $r \times n$ parity check matrix whose columns are all possible vectors over Z_q^r with the first non-zero element in B and let C be the null space of H^T. Then it can be proved that this code is indeed a single l-SEC code. The proof is similar to that of Theorem 4.7 above. We illustrate this idea with the following example.

Example 4.11. Let $l = 2$ and $p = 5$. Thus $q = p(2l+1) = 25$. The modular $B_1[-2, 2]$ modulo 25 in this case is $B = \{1, 6, 11, 16, 21\}$, $2B = \{2, 12, 22, 7, 17\}$, $-B = \{24, 19, 14, 9, 4\}$ and $-2B = \{23, 13, 3, 18, 8\}$. With $r = 2$, we can construct the following single l-SEC code. The code has length $n = 130$ out of which $k = 128$ digits are information digits. Thus the H matrix has 130 columns from Z_{25}^2. The first nonzero element of

each column belongs to B. Suppose the syndrome is $s = (3,21)$. Since the first nonzero element of s is $3 \in -2B$, the error magnitude is $e_i = -2$. We then find the inverse of e_i modulo q :$(-2)^{-1} = 12 \pmod{25}$. This implies that the i^{th} digit such that $h_i^T = 12s = (11,2)$ is in error. Hence, the error location i and its magnitude e_i are determined.

5. ASYMMETRIC/UNIDIRECTIONAL ERROR DETECTING CODES

As shown in [7, 5, 6], an asymmetric error detecting code can detect the same number of unidirectional errors. This is because the necessary and sufficient conditions for both codes are the same: a code C is capable of detecting t asymmetric/unidirectional errors if and only if for distinct codewords $X,Y \in C$ either $D_H(X,Y) \geq t+1$ (where D_H is the Hamming distance [14]) or X and Y are *unordered* (see Definition 5.1). Similarly, for the limited magnitude case, asymmetric and unidirectional error detecting codes have the same detection capabilities. This is further explained in Theorem 5.3.

Codes detecting limited magnitude asymmetric/unidirectional errors were considered in [1]. Nevertheless, the proposed codes are non-systematic and are shown not to be optimal in general. In this chapter we study both t and *all* error detecting codes. A code is t-error detecting, if and only if t or less errors cannot change one codeword into another codeword and is all error detecting when $t = n$, where n is the length of the code.

5.1. All error detecting codes.

We derive a lower bound on the number of check digits needed to encode systematic codes able to detect all asymmetric errors of maximum magnitude l (l-AAED codes). Moreover, we design an l-AAED code reaching the lower bound when $kl + l(\frac{q^r-1}{q-1}) < q^r$.

Definition 5.1. Let $x = (x_{n-1}, x_{n-2}, \ldots, x_0)$ and $y = (y_{n-1}, y_{n-2}, \ldots, y_0)$ be two vectors over Z_q. We say that x and y are *unordered* if both $N(x,y) \geq 1$ and $N(y,x) \geq 1$, such that $N(x,y) \triangleq |\{i : x_i > y_i\}|$.

Definition 5.2. With notations as above, define the distance metric, d_{max} [1], as

$$d_{max}(x,y) \quad = \quad max\{|x_i - y_i| : i \in \{0,1,\ldots,n-1\}\}$$

Theorem 5.3. *A code C is an l-AAED code if and only if , for all distinct codewords* $x, y \in C$, *either x and y are unordered or* $d_{max}(x,y) \geq l+1$.

Proof. Let C be a code with the desired properties. Then, $\forall x, y \in C$, no l limited magnitude asymmetric error can convert x to y. Hence, C is an l-AAED code. Conversely, if $\exists\ x, y \in C$ such that x and y are ordered, say x covers y (i.e. $N(x,y) \geq 1$ and $N(y,x) = 0$), and $d_{max}(x,y) \leq l$, then the l-limited magnitude error vector, $e = (e_{n-1}, e_{n-2}, \ldots, e_0)$, where $e_i = x_i - y_i$, can transform x into y. Thus, C is not an l-AAED code. □

Theorem 5.4. *An l-AAED systematic code with k information digits over* Z_q *requires at least* $r = \lceil \log_q(kl+1) \rceil$ *check digits.*

Proof. Consider the following subset of information words

$$\begin{gathered}
(0,0,\ldots,0,0) \\
(0,0,\ldots,0,1) \\
\vdots \\
(0,0,\ldots,0,l) \\
(0,0,\ldots,1,l) \\
\vdots \\
(0,0,\ldots,l,l) \\
\vdots \\
(l,l,\ldots,l,l)
\end{gathered}$$

Any two vectors of the above set must be assigned distinct check vectors, since otherwise the resulting codewords would not satisfy the conditions in Theorem 5.3. Since there are $kl+1$ such information vectors, at least $r = \lceil \log_q(kl+1) \rceil$ check digits are needed. □

For $l = q-1$, optimal systematic AAED codes were proposed by Bose and Pradhan in [8]. The code design is as follows. Suppose $x = (x_{k-1}, x_{k-2}, \ldots, x_0)$ is the given information vector. Let $A = \sum_{i=0}^{k-1}(q-1-x_i)$, then the representation of A in radix-q gives the check vector. This code requires exactly $\lceil \log_q(k(q-1)+1) \rceil$ check digits; thus, the code is optimal.

Theorem 5.5. *The Bose and Pradhan code* [8] *uses at most one more check digit than any l-AAED code.*

Proof. We only need to show $\lceil \log_q(k(q-1)+1) \rceil \leq \lceil \log_q(kl+1) \rceil + 1$. This follows from the following

$$k(q-1)+1 \quad \leq \quad (kl+1)q$$

thus

$$\log_q(k(q-1)+1) \quad \leq \quad \log_q(kl+1)+1$$

□

In the following, we give an l-AAED code that uses the minimum number of check digits as given in Theorem 5.4. We hereby describe the code construction. It is assumed that $\lceil \log_q(kl+1) \rceil = \lceil \log_q(k(q-1)+1) \rceil - 1$, since otherwise $\left(\lceil \log_q(kl+1) \rceil = \lceil \log_q(k(q-1)+1) \rceil\right)$ the Bose and Pradhan code would be optimal. The encoding procedure is as follows. Let $x = (x_{k-1}, x_{k-2}, \ldots, x_0)$ be the given

information vector over Z_q. Compute $A = \sum_{i=0}^{k-1}(q-1-x_i)\ mod\ q^r$, where r is the number of check digits, $r = \lceil \log_q(kl+1) \rceil$. Represent A in radix-q to get the check word $(c_{r-1}, c_{r-2}, \ldots, c_0)$. Now, given the received word, $(x'_{k-1}, x'_{k-2}, \ldots, x'_0, c'_{r-1}, c'_{r-2}, \ldots, c'_0)$, we compute the syndrome $S = (\sum_{i=0}^{k-1}(q-1-x'_i) - v(c'_{r-1}, c'_{r-2}, \ldots, c'_0))\ mod\ q^r$, where $v(y)$ is the decimal value of a vector, y, as a number over radix q. Then, no error is detected if and only if $S = 0$.

Theorem 5.6. *The code construction given above yields an optimal l-AAED code if $kl + l(\frac{q^r-1}{q-1}) < q^r$, where $r = \lceil \log_q(kl+1) \rceil$.*

Proof. We need to show that if $kl + l(\frac{q^r-1}{q-1}) < q^r$, then $S = 0$ if and only if none of the digits of the received word, $(x'_{k-1}, x'_{k-2}, \ldots, x'_0, c'_{r-1}, c'_{r-2}, \ldots, c'_0)$, is in error. It is easy to see that if no error occurred then $S = 0$. Conversely, assume that some digits of the received word suffer an l limited magnitude decreasing error. Then, we have

$$v(c'_{r-1}, c'_{r-2}, \ldots, c'_0) \geq v(c_{r-1}, c_{r-2}, \ldots, c_0) - l\left(\frac{q^r-1}{q-1}\right)$$

and

$$\left(\sum_{i=0}^{k-1}(q-1-x'_i)\right) \leq v(c_{r-1}, c_{r-2}, \ldots, c_0) + kl$$

thus

$$\begin{aligned}\left(\sum_{i=0}^{k-1}(q-1-x'_i)\right) - v(c'_{r-1}, c'_{r-2}, \ldots, c'_0) &\leq kl + l\left(\frac{q^r-1}{q-1}\right) \\ &< q^r\end{aligned}$$

implying that $S \neq 0$. □

Example 5.7. Let $k = 20$, $q = 8$ and $l = 2$ and the information symbols to be encoded be all 0's. Then, $r = \lceil \log_q(kl+1) \rceil = \lceil \log_8(20 \times 2 + 1) \rceil = 2$. Note that the Bose and Pradhan code would use $r = \lceil \log_q(k(q-1)+1) \rceil = 3$ check digits instead. Since we have $kl + l(\frac{q^r-1}{q-1}) = 58 < q^r = 64$, we can use the above construction to encode the information vector. With notations as above, $A = \sum_{i=0}^{k-1}(q - 1 - x_i) \, mod \, q^r = (20 \times 7) mod \, 8^2 = 12$, implying that the check digits are $(1,4)$.

Theorem 5.6 shows the correctness of the code construction when $kl + l(\frac{q^r-1}{q-1}) < q^r$. Nevertheless, when $kl + l(\frac{q^r-1}{q-1}) \geq q^r$, using the same construction, error detection is not guaranteed. Instead, the Bose and Pradhan code should be used in this case. The following example illustrates this idea.

Example 5.8. Let $k = 3, q = 4$ and $l = 1$.Then the above construction would use $r = \lceil \log_4(3 \times 1 + 1) \rceil = 1$. The information vector $(1,1,2)$ is encoded as $(1,1,2,1)$. Now assume that it is received as $(0,0,1,0)$. Computing the syndrome, $S = (((3 - 0) + (3-0) + (3-1)) + 0) \, mod \, 4 = 0$ and no error is detected. We argue below that in this case, since $kl + 1 = 4$ is a power of q, at least one more check digit is needed and therefore the Bose and Pradhan code is optimal.

Conjecture 5.9. *When $kl + l(\frac{q^r-1}{q-1}) \geq q^r$, for $r = \lceil \log_q(kl+1) \rceil$, at least $r' = r+1$ check digits are needed to construct a q-ary l-AAED code and thus the Bose and Pradhan code is optimal.*

The conjecture above can be proved for the special case where $kl+1$ is a power of q (note that $kl + l(\frac{q^r-1}{q-1}) \geq q^r$ in this case). Assume $r = \lceil \log_q(kl+1) \rceil = \log_q(kl + 1)$ check digits are used to encode the information vectors. Thus, there are exactly $kl + 1$ distinct check vectors, say $\{c_1, c_2, \ldots, c_{kl+1}\}$. Consider the set of

$kl+1$ information vectors listed in Theorem 5.4, every vector needs to be assigned a distinct check vector, say vector i in the sequence is assigned c_i. Furthermore, according to Theorem 5.3, the check vector assigned to the information vector $(0,0,\ldots,0)$, c_1, needs to satisfy the following properties: $\forall i \neq 1$, either c_1 covers c_i or $d(c_1,c_i) \geq l+1$. Now consider the next vector in the sequence, $v = (l,l,\ldots,l,l+1)$. Following the same reasoning as in Theorem 5.4, the check vector assigned to v needs to be different from all check vectors assigned to the vectors $(0,0,\ldots,0,1)$ through $(l,l,\ldots,l,l)$, leaving us with only c_1. However, that implies that there exists at least one check vector in $\{c_2,\ldots,c_{kl+1}\}$, say c_i, that is covered by c_1 with $d(c_{1,},c_i) < l+1$ and that resulting codeword $(l,l,\ldots,l,l+1)|c_1$(where $|$ denotes the concatenation of two vectors) will cover the codeword with check vector c_i. Consequently, at least one more check digit is needed and thus the Bose and Pradhan code is optimal. Nonetheless, it is not clear how to prove the above conjecture for the general case.

We now summarize the code design method:

(1) If $\lceil \log_q(kl+1) \rceil = \lceil \log_q(k(q-1)+1) \rceil$, use Bose-Pradhan code (construction is optimal).

(2) If $r = \lceil \log_q(kl+1) \rceil = \lceil \log_q(k(q-1)+1) \rceil - 1$:

- If $kl + l(\frac{q^r-1}{q-1}) < q^r$, use the code design above (construction is optimal)..
- else, use Bose-Pradhan code (conjectured to be optimal).

5.2. t error detecting codes.

In [6, 17] , the authors proposed two classes of t-unidirectional error detecting codes over Z_q, with $r = 2$ and $r \geq 3$ check digits. With $r = 2$ check digits, the check vector is the representation of b in radix-m system, where

$b = \left(\sum_{i=0}^{k-1}(q-1-x_i)\right) \; mod \; q^2$ and the code is capable of detecting up to $t = 2$ errors. On the other hand, using $r \geq 3$, the r-digit check is $((q-c_{r-2}), c_{r-2}, c_{r-3}, \ldots, c_0)$ where $b = \left(\sum_{i=0}^{k-1}(q-1-x_i)\right) \; mod \; q^{r-1}$ and $(c_{r-2}, c_{r-3}, \ldots, c_0)$ is the representation of b in radix-q system. In the latter case, up to $q^{r-2}+r-2$ errors can be detected. We refine the properties of the t asymmetric error detecting codes given in [6, 17] for the case where the maximum magnitude of the error, l, is known beforehand:

Theorem 5.10. *The code proposed in* [6, 17] *can detect up to* $t = \frac{q^2}{l} - q$ *asymmetric errors of maximum magnitude* l *using* $r = 2$ *check digits.*

Proof. Assume t errors occurred within the received codeword. Then the syndrome, $S = ((\sum_{i=0}^{k-1}(q-1-x_i')) - (qc_1' + c_0')) \; mod \; q^2$, can have the following possible values:

(1) t errors within the information digits:

$$\begin{aligned} S &\leq \left(\left(\sum_{i=0}^{k-1}(q-1-x_i)\right) + tl - ((qc_1 + c_0)) \; mod \; q^2\right. \\ &\leq tl \; mod \; q^2 \end{aligned}$$

(2) Errors within the check digits:

$$\begin{aligned} S &\leq \left(\left(\sum_{i=0}^{k-1}(q-1-x_i)\right) - (qc_1 + c_0) + ql + l)\right) \; mod \; q^2 \\ &\leq l(q+1) \; mod \; q^2 \end{aligned}$$

(3) t errors in both information and check parts. The maximum error magnitude occurs when both check digits are in error and the remaining $t-2$ errors are

within the information digits:

$$\begin{aligned} S &\leq \left((\sum_{i=0}^{k-1} (q-1-x_i) \right) + (t-2)l - (qc_1 + c_0) + ql + l)) \; mod \; q^2 \\ &\leq l(t+q-1) \; mod \; q^2 \end{aligned}$$

It follows that, with $t \leq \frac{q^2}{l} - q$, in all three cases $S \neq 0$ and thus the error can be detected**.** □

Theorem 5.11. *The code proposed in* [6, 17] *can detect up to* $t = \frac{q^{r-1}}{l} - \frac{q^{r-2}-1}{q-1} + r-3$ *asymmetric errors of maximum magnitude* l *using* $r \geq 3$ *check digits.*

Proof. Assume t errors occurred within the received word. As in [6, 17], we assume the most two significant check digits are not in error since otherwise the error can be easily detected. Let $(x_{k-1}, x_{k-2}, \ldots, x_0, c_{r-1}, c_{r-2}, \ldots, c_0)$ be the transmitted vector and $(x'_{k-1}, x'_{k-2}, \ldots, x'_0, c'_{r-1}, c'_{r-2}, \ldots, c'_0)$ be the received vector. The syndrome is thus computed as $S = ((\sum_{i=0}^{k-1}(q-1-x'_i)) - v(c'_{r-1}, c'_{r-2}, \ldots, c'_0)) \; mod \; q^{r-1}$. Depending on the error position, there are three cases for the syndrome value:

(1) t errors within the information digits:

$$\begin{aligned} S &\leq \left((\sum_{i=0}^{k-1} (q-1-x_i) \right) + tl - v(c_{r-1}, c_{r-2}, \ldots, c_0)) \; mod \; q^{r-1} \\ &\leq tl \; mod \; q^{r-1} \end{aligned}$$

(2) Errors within the check digits:

$$\begin{aligned} S &\leq \left((\sum_{i=0}^{k-1} (q-1-x_i) \right) - v(c_{r-1}, c_{r-2}, \ldots, c_0) + l(\frac{q^{r-2}-1}{q-1})) \; mod \; q^{r-1} \\ &\leq l\left(\frac{q^{r-2}-1}{q-1} \right) \; mod \; q^{r-1} \end{aligned}$$

(3) t errors in both information and check parts. Note that, as in [6, 17], the maximum error magnitude occurs when the least significant $r-2$ check digits are in error and the remaining $t-(r-2)$ errors are within the information digits:

$$\begin{aligned} S &\leq \left((\sum_{i=0}^{k-1} (q-1-x_i) \right) + (t-(r-2))l - v(c_{r-1}, c_{r-2}, \ldots, c_0) + l\left(\frac{q^{r-2}-1}{q-1}\right)) \ mod\ q^{r-1} \\ &\leq (t-r+2)l + l\left(\frac{q^{r-2}-1}{q-1}\right) \ mod\ q^{r-1} \end{aligned}$$

It can be seen that, with $t \leq \frac{q^{r-1}}{l} - \frac{q^{r-2}-1}{q-1} + r - 3$, in all three cases $S \neq 0$ and thus the error can be detected. □

6. SYMMETRIC ERROR DETECTING CODES

In [1, 12], optimal non-systematic and systematic codes (respectively) correcting all asymmetric errors of limited magnitude were given. In this chapter, we show that such codes can also be used to detect all symmetric errors of limited magnitude.

Theorem 6.1. *A code C is an l-all symmetric error detecting (l-ASED) code if and only if, for all distinct codewords, $x, y \in C$, $d_{max}(x,y) \geq l+1$.*

Proof. For a code C of length n, if $d_{max}(C) \geq l+1$, then $\nexists e = (e_{n-1}, e_{n-2}, \ldots, e_0) \in L^n$, where $L = \{0, 1, \ldots, l\}$, such that, for $x = (x_{n-1}, x_{n-2}, \ldots, x_0), y = (y_{n-1}, y_{n-2}, \ldots, y_0) \in C$, $y = (x_{n-1} \pm e_{n-1}, x_{n-2} \pm e_{n-2}, \ldots, x_0 \pm e_0)$ and thus C can detect all symmetric errors of maximum magnitude l.
Now, assume $\exists x, y \in C$ such that $d_{max}(x,y) \leq l$; define the error vector, $e = (y_{n-1} - x_{n-1}, y_{n-2} - x_{n-2}, \ldots, y_0 - x_0)$. By definition of d_{max}, the symbols of e lie in the range $[-l, l]$ and hence is a symmetric l- limited magnitude error vector that can transform x to y. Therefore C is not an l-ASED code. □

Theorem 6.2. *An optimal l-AAEC code is an optimal l-ASED code.*

Proof. This follows from the fact that the necessary and sufficient condition for both codes is that the minimum distance (d_{max}) is $l+1$ (Theorem 2.2 and 6.1) □

7. CONCLUSION AND FUTURE WORK

In this dissertation, error control codes for various channels where the magnitude of the error does not exceed a certain limit known beforehand are given. For asymmetric and symmetric channels, all and single error correcting codes are proposed. In addition, t and all error detecting codes for asymmetric/unidirectional channels are given. Similar ideas may be used to construct codes for the unidirectional channel. Moreover, the B sequences defined in Section 4.1 that were used in the construction of single l-AEC and l-SEC codes, can also be used to construct codes correcting higher number of errors. This will be further explored in later work. Overall, the results are promising; knowing the maximum magnitude the error can enable the design of higher rate codes or even codes that are not possible in general (for example all error correcting codes). We believe this opens the door for more research. For instance, although the non-systematic t l-AEC codes given in [9, 10] are - in many cases - close to optimal this is still not clear for the given systematic variant. Moreover, as pointed out in [10], when the reading resolution is larger than the size of the alphabet (as it is the case with readers that give a real number rather than an integer) it might be more efficient to use codes for limited magnitude erasures. Furthermore, computing the capacity of various limited magnitude error channels is also an interesting question as it determines the maximum information rate at which the source can reliably send information.

BIBLIOGRAPHY

[1] R. Ahlswede, H. Aydinian, L. H. Khachatrian, and L. M. G. M. Tolhuizen, "On q-ary codes correcting all unidirectional errors of a limited magnitude", Proceedings of Ninth International Workshop on Algebraic and Combinatorial Coding Theory, Kranevo, Bulgaria, pp. 20-26, Jun. 2004.

[2] R. Ahlswede, H. Aydinian and L. H. Khachatrian, "Unidirectional error control codes and related combinatorial problems", Proceedings of Eight International Workshop on Algebraic and Combinatorial Coding Theory, Russia, pp. 6-9, Sep. 2002.

[3] E.R. Berlekamp, Algebraic Coding Theory, McGraw-Hill Book, 1968.

[4] M. Blaum, "Codes for Detecting and Correcting Unidirectional Errors", IEEE Computer Society Press, Los Alamitos, CA, 1993.

[5] J.M. Borden, Optimal asymmetric error detecting codes, Information and Control, vol. 53, pp. 66-73, Apr. 1982.

[6] B. Bose, Samir Elmougy and Luca G. Tallini, "Systematic t-Unidirectional Error-Detecting Codes over Zm", IEEE Trans. Comput., vol. 56, no. 7, pp. 876-880, Jul. 2007.

[7] B. Bose and D. J. Lin, Systematic Unidirectional Error-Detecting Codes, IEEE Transactions on Computers, vol. 34, no. 11, pp.. 63-69, Nov. 1985.

[8] B. Bose and D. Pradhan, "Optimal unidirectional error correcting/detecting codes", IEEE Trans. Comput., vol. C-31, pp. 564-568, Jun. 1982.

[9] Y. Cassuto, M. Schwartz, V. Bohossian and J. Bruck, "Codes for multi-level flash memories: correcting asymmetric limited-magnitude errors", Proceedings of ISIT2007, Nice, France, Jun. 2007.

[10] Y. Cassuto, M. Schwartz, V. Bohossian, and J. Bruck, "Codes for Asymmetric Limited-Magnitude Errors with Application to Multi-Level Flash Memories", California Institute of Technology, Pasadena (CA), Tech. Rep. CaltechPARADISE:2008.ETR088, 2008.

[11] B. Eitan, R. Kazerounian, A. Roy, G. Crisenza, P. Cappelletti and A. Modelli, "Multilevel flash cells and their trade-offs", International Electron Devices Meeting, pp.169-172, Dec 1996.

[12] N. Elarief and B. Bose, "Optimal, systematic q-ary codes correcting all asymmetric and symmetric errors of limited magnitude", IEEE Trans. on Information Theory, accepted.

[13] R. W. Hamming, “Coding and information theory”, pp. 1-3, Prentice Hall, Second edition, 1986.

[14] R. W. Hamming, “Error detecting and error correcting codes”, Bell System Technical Journal 29 (2): 147–160, 1950.

[15] T. Kløve and V. Korzhik, “Error Detecting Codes: General Theory and Their Application in Feedback Communication Systems”, pp. 1-2, Springer, 1995.

[16] J. C. Moreira and P. G. Farrell, “Essentials of Error-Control Coding”, pp. 1-3, John Wiley and Sons Ltd, 2006.

[17] I. Naydenova and T. Kløve, Generalized Bose-Lin Codes, a Class of Codes Detecting Asymmetric Errors, IEEE Transactions on Information Theory, vol. 53, no. 3, pp. 1188-1193, Mar. 2007.

[18] C. Shannon, “A mathematical theory of communication”, Bell Syst. Tech. J., vol 27, pp. 379-423, 623-656, 1948.