# On q-ary Codes Correcting All Unidirectional Errors of a Limited Magnitude

R. Ahlswede, H. Aydinian, L.H. Khachatrian and L.M.G.M Tolhuizen *

Dedicated to the memory of Rom Varshamov

**Abstract**

We consider codes over the alphabet $Q = \{0, 1, \ldots, q-1\}$ intended for the control of unidirectional errors of level $\ell$. That is, the transmission channel is such that the received word cannot contain both a component larger than the transmitted one and a component smaller than the transmitted one. Moreover, the absolute value of the difference between a transmitted component and its received version is at most $\ell$.

We introduce and study $q$-ary codes capable of correcting all unidirectional errors of level $\ell$. Lower and upper bounds for the maximal size of those codes are presented.

We also study codes for this aim that are defined by a single equation on the codeword coordinates (similar to the Varshamov-Tenengolts codes for correcting binary asymmetric errors). We finally consider the problem of detecting all unidirectional errors of level $\ell$.

**Keywords:** asymmetric channel, unidirectional errors, Varshamov-Tennengolts codes.

**Mathematics Subject Classification:** 94B25, 94B60.

*L.M.G.M. Tolhuizen is with Philips Research Laboratories, Prof. Holstlaan 4, 5656 AA Eindhoven, The Netherlands; ludo.tolhuizen@philips.com

# 1 Introduction

An extensive theory of error control coding has been developed (cf. [26],[20],[19]) under the assumption of symmetric errors in the data bits; i.e. errors of type $0 \rightarrow 1$ and $1 \rightarrow 0$ can occur simultaneously in a codeword.

However in many digital systems such as fiber optical communications and optical disks the ratio between probability of errors of type $1 \rightarrow 0$ and $0 \rightarrow 1$ can be large. Practically we can assume that only one type of errors can occur in those systems. These errors are called asymmetric. Thus the binary asymmetric channel, also called $Z$-channel (shown in Figure. 1),

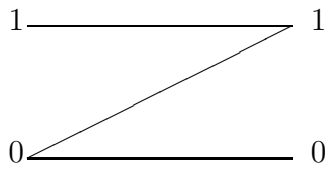


Figure 1: the Z-channel

has the property that a transmitted 1 is always received correctly but a transmitted 0 may be received as a 0 or 1.

Unidirectional errors slightly differ from asymmetric type of errors: both $1 \rightarrow 0$ and $0 \rightarrow 1$ type of errors are possible, but in any particular word all the errors are of the same type. The statistics shows that in some of LSI/VLSI ROM and RAM memories the most likely faults are of the unidirectional type. The problem of protection against unidirectional errors arises also in designing of fault-tolerant sequential machines, in write-once memory system, in asynchronous systems etc.

Clearly any code capable of correcting (detecting) $t$-symmetric errors can be also used to correct (to detect) $t$-unidirectional or $t$-asymmetric errors. Obviously also any $t$-unidirectional error correcting (detecting) code is capable of correcting (detecting) $t$-asymmetric errors. Note that there are $t$-asymmetric error correcting codes with higher information rate than that of $t$-symmetric error correcting codes ([33],[8],[15]). For constructions of codes correcting unidirectional errors see [34] and [12]. It can be shown that the detection problems for asymmetric and unidirectional errors are equivalent (see [5]) i.e. any $t$-error detecting asymmetric code is also a $t$-error detecting unidirectional code.

First results on asymmetric error correcting codes are due to Kim and Freiman [16], and Varshamov [28],[29]. In [28] Varshamov introduced a metric for asymmetric errors and obtained bounds for codes correcting asymmetric errors. In [29] Varshamov ( and later Weber et al. [34]) proved that linear codes capable of correcting $t$-asymmetric errors are also capable of correcting $t$-symmetric errors. Thus only non-linear constructions may go beyond symmetric error correcting codes.

In 1965 Varshamov and Tennengolts gave the first construction of nonlinear codes correcting asymmetric errors [31].

The idea behind these codes (which we call VT-codes) is surprisingly simple. Given $n \in \mathbb{N}$ and an integer $a$ the VT-code $\mathcal{C}(n,a)$ is defined by

$$\mathcal{C}(n,a) = \left\{ (x_1,\ldots,x_n) \in \{0,1\}^n : \sum_{i=1}^{n} i x_i \equiv a \ \ (\mod m) \right\} \tag{1.1}$$

where $m \geq n+1$ is an integer.

Varshamov and Tennengolts showed that the code $\mathcal{C}(n,a)$ is capable of correcting any single asymmetric error. Moreover taking $m = n+1$ there exists an $a \in \{0,\ldots,n\}$ so that

$$|\mathcal{C}(n,a)| \geq \frac{2^n}{n+1}. \tag{1.2}$$

Recall that for the maximum size of binary single symmetric error correcting codes we have

$$A(n,1) \leq \frac{2^n}{n+1}. \tag{1.3}$$

Varshamov [30] showed that $|\mathcal{C}(n,0)| \geq |\mathcal{C}(n,a)|$.

A number theoretical result due to von Sterneck (1902) [10, p. 87] allows to determine the weight distribution of VT-codes. This result and its special cases were rediscovered many times (see [14],[22],[23],[27]). From a practical point of view VT-codes have the advantage of a very simple decoding algorithm. For systematic encoding of VT-codes see [1] and [6].

In general we call a code of length $n$, correcting $t$-asymmetric errors a VT-code if it is given by the set of solutions $(x_1,\ldots,x_n) \in \{0,1\}^n$ of a congruence (or several congruences) of the type

$$\sum_{i=1}^{n} f(i) x_i \equiv a(\mod M) \tag{1.4}$$

where $f : [n] \to \mathbb{Z}$ is an injection, $a$ and $M$ are integers.
We note that there are deep relationships between VT-codes and some difficult problems in Additive Number Theory [33], [11].

The idea of VT-codes was further developed by Constantin and Rao [8], (see also Helleseth and Kløve [15]) by constructing group-theoretical codes based on Abelian Groups.
Levenshtein noticed that VT-codes can also be used to correct single insertion/deletion errors [18].

Modifications of VT-codes where used to construct new codes correcting $t$-asymmetric errors [33], [24], [13], [7] and bursts of errors [25], [32] (see also [6], [9], [12] for other constructions). For an excellent survey on the results in this direction see Kløve [17].
Very few constructions are known for codes correcting unidirectional errors (for more information see [4]). Note that VT-codes (1.1) and its known modifications are not capable of correcting unidirectional errors.

In 1973 Varshamov introduced a $q$-ary asymmetric channel [33].

The inputs and outputs of the channel are $n$-sequences over the $q$-ary alphabet $Q = \{0, 1, \ldots, q-1\}$. If the symbol $i$ is transmitted then the only symbols which the receiver can get are $\{i, i+1, \ldots, q-1\}$. Thus for any transmitted vector $(x_1, \ldots, x_n)$ the received vector is of the form $(x_1 + e_1, \ldots, x_n + e_n)$ where $e_i \in Q$ and

$$x_i + e_i \leq q - 1, \ i = 1, \ldots, n. \tag{1.5}$$

Then it is said that $t$-errors have occurred if $e_1 + \cdots + e_n = t$. Generalizing the idea of VT-codes, Varshamov [33] presented several constructions of $t$-error correcting codes for the defined channel. These codes have been shown in [21] to have larger cardinality than BCH codes correcting $t$ errors for $q \geq 2$ and for large $n$.

We continue here the work started in [2]. We consider **a special type of asymmetric errors in a $q$-ary channel**, where the magnitude of each component of $\mathbf{e}$ satisfies $0 \leq e_i \leq \ell$ for $i = 1, \ldots, n$. We refer to $\ell$ as level.

Correspondingly we say that **an unidirectional error of level $\ell$ has occurred**, if the output is either $\mathbf{x} + \mathbf{e}$ or $\mathbf{x}$ - $\mathbf{e}$ (in the latter case, it is of course required that $x_i \geq e_i$ for all $i$).

If the error vector $\mathbf{e}$ has Hamming weight $d_H(\mathbf{e}) = t$, then we say that $t$ errors of level $\ell$ have occured.

Thus the general problem is the following.

Given $n, \ell, t, q$ construct $q$-ary codes of length $n$ capable of correcting $t$ errors of level $\ell$. Of course we wish the size of a code to be as big as possible.

Note the difference between the channel described above and Varshamov's channel when $q > 2$. This is shown for $q = 3$, $l = 1$, $t \geq 2$ in Figure 2.

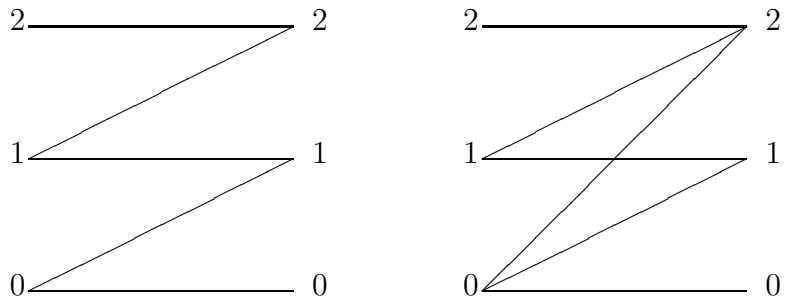


Figure 2:

Asymmetric errors with level 1 Varshamov's channel

In this paper we consider $q$-ary codes correcting all asymmetric errors of given level $\ell$, (that is $t = n$) for which we use the abbreviation $\ell$-AEC code, and $\ell$-UEC codes that correct all unidirectional errors of level $\ell$. As above our alphabet is $Q \triangleq \{0, 1, \ldots, q-1\}$.

In Section 2 we define distances that capture the capabilities of a code to correct all asym-

metric or unidirectional errors of level $\ell$.

For given $\ell$, let $A_a(n,\ell)_q$ and $A_u(n,\ell)_q$ denote the maximum number of words in a q-ary AEC code, or UEC code respectively, of length $n$. Clearly $A_u(n,\ell)_q \leq A_a(n,\ell)_q$.

In Section 3 we determine $A_a(n,\ell)_q$ exactly for all $n, \ell$ and $q$.

In Section 4 we give upper and lower bounds on $A_u(n,\ell)_q$, which imply that for fixed $q$ and $\ell$ the asymptotic growth rate for $A_u(n,\ell)_q$ equals that of $A_a(n,\ell)$.

In Section 5 we study $\ell$-AEC and $\ell$-UEC codes of VT-type. It is shown that any $\ell$-AEC code of VT-type can be transformed into an $\ell$-UEC code of VT-type of equal length and cardinality. Upper and lower bounds on the maximum number of codewords in a $q$-ary $\ell$-UEC code of length $n$ of VT-type are derived. For certain pairs $(\ell, q)$ we give a construction of optimal $\ell$-UEC codes.

In Section 6 we consider the problem of detecting all errors of level $\ell$.

# 2 Distances and error-correcting capabilities

In this section we introduce two distances that capture the capabilities of a code for correcting all symmetrical and unidirectional errors of a certain level. Throughout this section we write $L$ for $[0,\ell]$ (where for integers $a < b$ we use the abbreviation $[a,b] \triangleq \{a, a+1, \ldots, b\}$).

**Definition 1** *For* $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in Q^n$ *and* $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in Q^n$,

$$\begin{aligned} d_{\max}(\mathbf{x},\mathbf{y}) &= \max\{|x_i - y_i| : i = 1,2,\ldots,n\} \\ d_u(\mathbf{x},\mathbf{y}) &= \begin{cases} d_{\max}(\mathbf{x},\mathbf{y}) & \text{if } \mathbf{x} \geq \mathbf{y} \text{ or } \mathbf{y} \geq \mathbf{x}, \\ 2d_{\max}(\mathbf{x},\mathbf{y}) & \text{if } \mathbf{x} \text{ and } \mathbf{y} \text{ are incomparable}, \end{cases} \end{aligned}$$

*where* $\mathbf{x} \geq \mathbf{y}$ *means that* $x_i \geq y_i$ *for all* $i$.

Later on for short we will write $d(\mathbf{x},\mathbf{y})$ for $d_{\max}(\mathbf{x},\mathbf{y})$.

Note that $d_u$ does not define a metric: take $\mathbf{x}$=(0,2), $\mathbf{y}$=(1,0) and $\mathbf{z}$=(1,2). Then $d_u(\mathbf{x},\mathbf{y}) = 4 > 1 + 2 = d_u(\mathbf{x},\mathbf{z}) + d_u(\mathbf{z},\mathbf{y})$.

**Lemma 1** *Let* $\mathbf{x}, \mathbf{y} \in Q^n$. *The two following assertions are equivalent:*
*(i)* $d(\mathbf{x},\mathbf{y}) \leq \ell$
*(ii) there exist* $\mathbf{e} \in L^n$, $\mathbf{f} \in L^n$ *such that* $\mathbf{x} + \mathbf{e} = \mathbf{y} + \mathbf{f} \in Q^n$.

**Proof.** Suppose that $(i)$ holds. We define $\mathbf{e}$ and $\mathbf{f}$ as

$$e_i = \max(0, y_i - x_i) \text{ and } f_i = \max(0, x_i - y_i), \quad i = 1,2,\ldots,n.$$

As $d(\mathbf{x},\mathbf{y}) \leq \ell$, the vectors $\mathbf{e}$ and $\mathbf{f}$ are in $L^n$, and for each $i$, we have that $x_i + e_i = y_i + f_i = \max(x_i, y_i) \in Q$. That is $(ii)$ holds.

Conversely, suppose that $(ii)$ holds, then for each $i$ we have that $|x_i - y_i| = |f_i - e_i| \leq \max(f_i, e_i) \leq \ell$, where the first inequality holds since $e_i$ and $f_i$ both are non-negative. $\square$

The following proposition readily follows from Lemma 1.

**Proposition 1** *A code $\mathcal{C} \subset Q^n$ is an $\ell$-AEC code if and only if $d(\mathbf{x}, \mathbf{y}) \geq \ell + 1$ for all distinct $\mathbf{x}$,$\mathbf{y}$ in $\mathcal{C}$.*

Note that Proposition 1 and the definition of $d(\mathbf{x}, \mathbf{y})$ imply that for $\ell \geq q-1$, an $\ell$-AEC code (and therefore also an $\ell$-UEC code) contains at most a single codeword. **For this reason, we assume in the remainder of the paper that $\ell \leq q - 2$.**

**Lemma 2** *Let $\mathbf{x}, \mathbf{y} \in Q^n$. The two following assertions are equivalent.*
*$(i)$ $\mathbf{y} \geq \mathbf{x}$ and $d(\mathbf{x}, \mathbf{y}) \leq 2\ell$,*
*$(ii)$ there exist $\mathbf{e} \in L^n, \mathbf{f} \in L^n$ such that $\mathbf{x} + \mathbf{e} = \mathbf{y} - \mathbf{f} \in Q^n$.*

**Proof.** Suppose that $(i)$ holds. We define $\mathbf{e}$ and $\mathbf{f}$ as

$$e_i = \lceil \frac{1}{2}(y_i - x_i) \rceil \text{ and } f_i = \lfloor \frac{1}{2}(y_i - x_i) \rfloor, \;\; i = 1, 2, \ldots, n.$$

As $\mathbf{y} \geq \mathbf{x}$, both $\mathbf{e}$ and $\mathbf{f}$ have only non-negative components and for each $i$, we have that $f_i \leq e_i \leq \lceil \frac{1}{2}(2l) \rceil = \ell$; moreover, we obviously have that $\mathbf{e} + \mathbf{f} = \mathbf{y} - \mathbf{x}$. Finally, for each $i$ we have that $x_i + e_i = y_i - f_i \leq y_i \leq q - 1$, so $\mathbf{x} + \mathbf{e} = \mathbf{y} - \mathbf{f} \in Q^n$. We conclude that $(ii)$ holds. Conversely suppose that $(ii)$ holds. Then $\mathbf{y} - \mathbf{x} = \mathbf{e} + \mathbf{f}$ and so $\mathbf{y} \geq \mathbf{x}$, and for each $i$ we have that $|y_i - x_i| = y_i - x_i = e_i + f_i \leq \ell + \ell = 2\ell$. That is $(i)$ holds. $\square$

Combination of Lemma 1 and Lemma 2 yields the following

**Proposition 2** *A code $\mathcal{C} \subset Q^n$ is an $\ell$-UEC code if and only if $d_u(\mathbf{x}, \mathbf{y}) \geq 2\ell + 1$ for all distinct $\mathbf{x}$, $\mathbf{y}$ in $\mathcal{C}$.*

# 3 $\ell$-AEC codes

It turns out that $A_a(n, \ell)_q$ can be determined exactly for all integers $n$ and each $\ell \in Q$.

**Theorem 1** *For all integers $n$ and each $\ell \in Q$, $A_a(n, \ell)_q = \left\lceil \frac{q}{\ell+1} \right\rceil^n$.*

**Proof.** Let $\mathcal{C} \subset Q^n$ be an $\ell$-AEC-code. Let $\varphi : Q \to \left\{0, 1, \ldots \left\lfloor \frac{q-1}{\ell+1} \right\rfloor \right\}$, be defined as

$$\varphi(j) = \left\lfloor \frac{j}{\ell + 1} \right\rfloor, \;\; j = 0, \ldots, q - 1.$$

For any codeword $\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{C}$ define $\varphi^n(\mathbf{x}) = \big(\varphi(x_1), \ldots, \varphi(x_n)\big)$. Clearly $\varphi^n$ is injective: if $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ are such that $\varphi^n(\mathbf{x}) = \varphi^n(\mathbf{y})$, then $|x_i - y_i| \leq \ell$, $(i = 1, \ldots, n)$, that is, $d(\mathbf{x}, \mathbf{y}) \leq \ell$ and so $\mathbf{x} = \mathbf{y}$. This implies that $|\varphi^n(\mathcal{C})| = |\mathcal{C}|$ and since $\left\lfloor \frac{q-1}{\ell+1} \right\rfloor + 1 = \left\lceil \frac{q}{\ell+1} \right\rceil$ we get

$$|\mathcal{C}| \leq \left\lceil \frac{q}{\ell+1} \right\rceil^n. \tag{3.1}$$

The code $\mathcal{C}$ defined as

$$\mathcal{C} = \big\{(x_1, x_2, \ldots, x_n) \in Q^n : x_i \equiv 0 \mod (\ell+1) \text{ for } i = 1, 2, \ldots, n\big\}$$

obviously is an $\ell$-AEC code that achieves equality in (3.1). A received vector can be decoded by component-wise rounding downwards to the nearest multiple of $\ell$+1. □

# 4 $\ell$-UEC codes

In this section, we study $A_u(n, \ell)_q$, the maximum number of words in a $q$-ary $\ell$-UEC code of length $n$. As any $\ell$-UEC code is an $\ell$-AEC code, Theorem 1 implies that

$$A_u(n, \ell)_q \leq A_a(n, \ell)_q = \left\lceil \frac{q}{\ell+1} \right\rceil^n. \tag{4.1}$$

In some special cases the upper bound (4.2) is met with equality.

**Proposition 3** *For all $n$ and $\ell$, $A_u(n, \ell)_{2\ell+2} = 2^n$.*

**Proof.** By Proposition 2 the code $\{0, 2\ell+1\}^n$ meeting $2^n$ has the desired property and $A_u(n, \ell)_{2\ell+2} \leq 2^n$ by (4.1). □

In Section 5 we will construct $q$-ary $\ell$-UEC codes of VT type. For various classes of pairs $(q, \ell)$, (for example, if $\ell+1$ divides $q$), these codes have cardinality $\lceil \frac{q}{\ell+1} \rceil^{n-1}$ and thus they are below the upperbound (4.1) only by a multiplicative factor.

We continue the present section with two constructions for $q$-ary $\ell$-UEC codes valid for all pairs $(q, \ell)$. We denote by $Q_{\ell+1}$ all integers in $Q = [0, q-1]$ that are multiples of $\ell+1$, that is

$$Q_{\ell+1} = \{m \in \{0, 1, \ldots, q-1\} : m \equiv 0 \pmod{\ell+1}\} = \{a(\ell+1) : 0 \leq a \leq b-1\}, \tag{4.2}$$

where

$$b = |Q_{\ell+1}| = \left\lceil \frac{q}{\ell+1} \right\rceil.$$

It is clear that $d(\mathbf{x}, \mathbf{y}) \geq \ell+1$ for any two distinct words $\mathbf{x}, \mathbf{y}$ in $Q^n_{\ell+1}$. In the subsequent two subsections we use $Q^n_{\ell+1}$ to construct a code with minimum asymmetric distance $\ell$+1 for which any two codewords are incomparable. Thus we have created a code with undirectional distance at least $2\ell+2$.

## 4.1 Construction 1: taking a subset of $Q^n_{\ell+1}$

For each $j$ let

$$C(j) = \{(x_1, x_2, \ldots, x_n) \in Q^n_{\ell+1} : \sum_{i=1}^{n} \frac{x_i}{\ell+1} = j\}.$$

Any two distinct words from $C(j)$ clearly are incomparable and so $C(j)$ is an $\ell$-UEC code. It is clear that

$$|C(j)| = |\{(y_1, y_2, \ldots, y_n) \in \{0, 1, \ldots, b-1\}^n : \sum_{i=1}^{n} y_i = j\}|.$$

It is known [3, Thm. 4.1.1] that $|C(j)|$ is maximized for $j = j^* \triangleq \lfloor \frac{1}{2} n(b-1) \rfloor$. Moreover, according to [3, Thm. 4.3.6], the following bounds are valid.

**Proposition 4** *There exist positive constants $c_1$ and $c_2$ (depending on $b = \lceil \frac{q}{\ell+1} \rceil$) such that*

$$c_1 \frac{1}{\sqrt{n}} b^n \leq |C(j^*)| \leq c_2 \frac{1}{\sqrt{n}} b^n.$$

Proposition 4 implies the following theorem.

**Theorem 2** *For each integer $q$ and $\ell \in Q$, there is a constant $c > 0$ such that for each $n$,*

$$A_u(n, \ell)_q \geq c \frac{1}{\sqrt{n}} \lceil \frac{q}{\ell+1} \rceil^n .$$

Clearly, (4.2) and Theorem 2 imply that for fixed $q$ and $\ell$ the asymptotic growth rate of $A_u(n, \ell)_q$ is known.

**Corollary 1** *For each $q$ and each $\ell \in [0, q-1]$* $\lim_{n\to\infty} \sqrt[n]{A_u(n, \ell)_q} = \lceil \frac{q}{\ell+1} \rceil$.

## 4.2 Construction 2: adding tails to words from $Q^n_{\ell+1}$

In order to formulate our second construction clearly, we cast it in the form of a proposition. Later we take appropriate values for certain parameters in this construction to obtain a lower bound on $A_u(n, \ell)_q$.

**Proposition 5** *Let $X \subset Q^n$ be a $\ell$-AEC code. For $\mathbf{x} \in X$, let $S(\mathbf{x})$ denote the sum of its entries, and let $s_1, s_2$ be such that for each $\mathbf{x} \in X$, $s_1 \leq S(x) \leq s_2$. Let $\phi : [s_1, s_2] \to Q^m$ be such that for all $a, b \in [s_1, s_2]$ with $a > b$, there is an $i \in \{1, 2, \ldots, m\}$ such that $(\phi(a))_i < (\phi(b))_i$. Then $\mathcal{C} = \{(\mathbf{x}, \phi(S(x)) : \mathbf{x} \in X\} \subset Q^{n+m}$ is an $\ell$-UEC code.*

**Proof.** Let $\mathbf{u} = (\mathbf{x}, \phi(S(\mathbf{x})))$ and $\mathbf{v} = (\mathbf{y}, \phi(S(\mathbf{y})))$ be two distinct words in $\mathcal{C}$. As $d(\mathbf{x}, \mathbf{y}) \geq \ell + 1$, all we have to show is that $\mathbf{u}$ and $\mathbf{v}$ are incomparable. This is clear if $\mathbf{x}$ and $\mathbf{y}$ are incomparable. Now suppose that $\mathbf{x}$ and $\mathbf{y}$ are comparable, say $\mathbf{x} \geq \mathbf{y}$. Then $S(\mathbf{x}) > S(\mathbf{y})$ and hence, by the property imposed on $\phi$, $u_j < v_j$ for some $j \in [n+1, n+m]$. $\square$

We now apply the construction from Proposition 5. Given $s_1$ and $s_2$, we take $m \triangleq \lceil \log_q(s_2 - s_1 + 1) \rceil$, and define $\phi(s)$ as the $m$-symbols $q$-ary representation of $s_2 - s$. We choose for $X$ a large subset of $Q^n_{\ell+1}$ such that $s_2 - s_1 + 1$ is small, so that $m$ can be small. As shown below we can invoke Chebyshev's inequality to show the existence of a set $X$ such that $|X| > \frac{3}{4} b^n$, while $s_2 - s_1 + 1 < K_1 \sqrt{n}$ for some constant $K_1$. As a consequence, $m$ can be as small as $\frac{1}{2} \log_q n + K_2$ for some constant $K_2$.

**Theorem 3** *For each $q$ and $\ell$, there exists a positive constant $K$ such that for each $n$,*

$$A_u(n, \ell)_q \geq K b^n n^{-\frac{1}{2} \log_q b}, \text{ where } b = \lceil \frac{q}{\ell + 1} \rceil \ .$$

**Proof.** We start with the well-known Chebyshev inequality.

**Proposition 6** *Let $Y_1, Y_2, \ldots, Y_n$ be independent, identically distributed random variables, each with average $\mu$ and variance $\sigma^2$. For each $\epsilon > 0$, we have that*

$$prob(|\sum_{i=1}^{n} Y_i \ - n\mu| > \epsilon \cdot n) \leq \frac{\sigma^2}{n\epsilon^2} \ .$$

We choose now $\epsilon = \frac{2\sigma}{\sqrt{n}}$ and get

$$\text{Prob}(|\sum_{i=1}^{n} Y_i - n\mu| \leq 2\sigma\sqrt{n}) \geq \frac{3}{4}. \tag{4.3}$$

In the above, we take each $Y_i$ uniformly distributed in $Q_{\ell+1} = \{a(\ell + 1) : 0 \leq a \leq b - 1\}$. It follows from (4.3) that the set $X$ defined as

$$X = \{x \in Q^n_{\ell+1} : n\mu - 2\sigma\sqrt{n} \leq \sum_{i=1}^{n} x_i \leq n\mu + 2\sigma\sqrt{n}\}$$

has cardinality at least $\frac{3}{4} b^n$.
As a consequence of this and Proposition 5, there exists a constant $K_2$ such that for each $n$, there is an $\ell$-AUEC code of length at most $n + \frac{1}{2} \log_q n + K_2$.
Now let $n$ be a positive integer. Choose $n_0$ such that

$$n_0 + \frac{1}{2} \log_q n_0 + K_2 \leq n \text{ and } (n_0 + 1) + \frac{1}{2} \log_q (n_0 + 1) + K_2 \geq n.$$

Our construction shows the existence of an $\ell$-AUEC code of length $n$ with at least $\frac{3}{4}b^{n_0}$ words. The definition of $n_0$ implies that

$$\log_q(n_0+1) \le \log_q(n+1-\frac{1}{2}\log_q n_0 - K_2) \le \log_q(n+1-K_2), \text{ and so}$$

$$n_0 \ge n-1-K_2-\frac{1}{2}\log_q(n_0+1) \ge n-1-K_2-\frac{1}{2}\log_q(n+1-K_2).$$

From the final inequality, it follows that there exists a constant $K_3$ such that $n_0 \ge n - \frac{1}{2}\log_q n - K_3$. We conclude that

$$\frac{3}{4}b^{n_0} \ge \frac{3}{4}b^n n^{-\frac{1}{2}\log_q b} b^{-K_3}.$$

□

# 5 $\ell$-UEC codes of Varshamov-Tennengolts type

In this section we study VT-type $\ell$-UEC codes. Note however that unlike the VT-codes, the codes we introduce here are defined by means of some linear equation (rather than a congruence) over the real field. Namely given $Q = [0, q-1] \subset \mathbb{R}$ and $a_0, \ldots, a_{n-1}, a \in \mathbb{Z}$ let

$$X = \{(x_0, \ldots, x_{n-1}) \in Q^n : \sum_{i=0}^{n-1} a_i x_i = a\}. \tag{5.1}$$

Note that $X$ defines an $\ell$-UEC code if and only if for each distinct $\mathbf{x}, \mathbf{y} \in X$ holds $\mathbf{x}-\mathbf{y} \notin [-\ell, \ell]^n$ and $\mathbf{x}-\mathbf{y} \notin [0, 2\ell]^n$.

Thus an obvious sufficient condition for the set of vectors $X \subset Q^n$ to be an $\ell$-UEC code is that the hyperplane $H$ defined by

$$H = \left\{(x_0, \ldots, x_{n-1}) \in \mathbb{R}^n : \sum_{i=0}^{n-1} a_i x_i = 0\right\}$$

does not contain vectors from $[-\ell, \ell]^n \cup [0, 2\ell]^n$, except for the zero vector.

An $\ell$-UEC code of VT-type may have the advantage of a simple encoding and decoding procedure.

In particular, let $\mathcal{C}$ be a code given by 5.1 where for $i = 0, 1, \ldots, n-1$, $a_i = (\ell+1)^i$. In view of observation above $\mathcal{C}$ is an $\ell$-AEC code. Suppose now for a received vector $\mathbf{y} = (y_0, \ldots, y_{n-1})$ we have

$$\sum_{i=0}^{n-1} (\ell+1)^i y_i = a'$$

with $a' \ge a$. Then the transmitted vector $(x_0, \ldots, x_{n-1}) = (y_0 - e_0, \ldots, y_{n-1} - e_{n-1})$, where the error vector $(e_0, \ldots, e_{n-1})$ is just the $(\ell+1)$-ary representation of the number $a' - a$.

Similarly, if $a' \le a$, then $(x_0, \ldots, x_{n-1}) = (y_0 - e_0, \ldots, y_{n-1} - e_{n-1})$, where $(e_0, e_1, \ldots, e_{n-1})$ is the $(\ell+1)$-ary representation of $a - a'$.

For given $\ell, q$ and $n$, we define $LA_u(n,\ell)_q$ = the maximum size of an $\ell$-UEC code, over the alphabet $[0, q-1]$, defined by a linear equation (5.1).
Correspondingly we use $LA_a(n,\ell)_q$ for $\ell$-AEC codes.

**Theorem 4** *For all $n, q$ and $\ell$, $LA_a(n,\ell)_q = LA_u(n,\ell)_q$.*

**Proof.** Suppose an $\ell$-AEC code $\mathcal{C}$ is defined by (5.1), that is $\mathcal{C} = X$. Suppose also w.l.o.g. that $a_0, \ldots, a_k < 0$ $(k < n-1)$, $a_{k+1}, a_{k+1}, \ldots a_n \ge 0$, and $s \triangleq a_0 + \cdots + a_k$. Let $\mathcal{C}'$ be the code defined by the equation

$$-\sum_{i=0}^{k} a_i y_i + \sum_{j=k+1}^{n-1} a_j y_j = a - s(q-1) \tag{5.2}$$

Note that for each $\mathbf{c} = (c_o, \ldots, c_{n-1}) \in \mathcal{C}$ the vector $\mathbf{c}' = (q-1-c_0, \ldots, q-1-c_k, c_{k+1}, \ldots, c_{n-1}) \in Q^n$ is a solution of (5.2), that is $\mathbf{c}' \in \mathcal{C}'$. The opposite is also true. Hence we have $|\mathcal{C}| = |\mathcal{C}'|$. Note further that the condition $\mathbf{c} - \mathbf{b} \notin [-\ell, \ell]^n$ for each distinct $\mathbf{c}, \mathbf{b} \in \mathcal{C}$ (this we have since $\mathcal{C}$ is an $\ell$-AEC code) implies that for the corresponding $\mathbf{c}', \mathbf{b}' \in \mathcal{C}'$ we also have $\mathbf{c}' - \mathbf{b}' \notin [-\ell, \ell]^n$. Moreover since $-a_0, \ldots, -a_k, a_{k+1}, \ldots, a_{n-1} > 0$ we have $\mathbf{c}' - \mathbf{b}' \notin Q^n$, which implies that $\mathcal{C}'$ is an $\ell$-UEC code. Thus we have

$$LA_a(n,\ell)_q \le LA_u(n,\ell)_q.$$

This completes the proof since we also have the inverse inequality. □

For future reference, we note the obvious fact that for all $n, \ell, q$ and $q'$, we have

$$LA_u(n,\ell)_q \ge LA_u(n,\ell)_{q'} \text{ if } q \ge q'. \tag{5.3}$$

**Remark** Given $\ell$ and $q$ let $a_0, a_1, \ldots, a_n$ be nonzero integers such that the code $\mathcal{C} = X$ defined by (5.1) is an $\ell$-UEC code over the alphabet $Q = [0, q-1]$. Then the following is true.

**Proposition 7** *The code $\mathcal{C}^*$ defined by*

$$\mathcal{C}^* = \left\{ (z_0, \ldots, z_{n-1}) \in Q^n : \sum_{i=0}^{n-1} a_i z_i \equiv a \pmod{2\ell S + 1} \right\},$$

*where $S \triangleq a_0 + \cdots + a_{n-1}$ is an $\ell$-UEC code.*

**Proof.** If for two distinct $\mathbf{z}, \mathbf{z}' \in \mathcal{C}^*$ holds $\sum_{i=0}^{n-1} a_i(z_i - z_i') = 0$ then $\mathbf{z}, \mathbf{z}'$ belong to some translate of code $\mathcal{C}$ and hence $d_u(\mathbf{z}, \mathbf{z}') \ge 2\ell + 1$. Conversely if $\sum_{i=0}^{n-1} a_i(\mathbf{z} - \mathbf{z}'_{\mathbf{i}}) \ne 0$ then there

exists $j$ (by the pigeonhole principle) such that $|z_j - z'_j| \geq 2\ell + 1$. Therefore in both cases $d_u(\mathbf{z}, \mathbf{z}') \geq 2\ell + 1$. $\square$

Thus we have $|\mathcal{C}^*| \geq |\mathcal{C}|$ which shows that in general the codes given by some congruence could have better performance. Note however that by construction given above we cannot have much gain as compared to the code given by (5.1). This is clear since $|\mathcal{C}| \geq c|\mathcal{C}^*|$ for some constant $c \leq \frac{(q-1)S}{2S\ell+1} < \frac{q-1}{2\ell}$.

## 5.1 Lower and upper bounds for $LA_u(n, \ell)_q$

**Theorem 5** *For all integers $q, n$ and $\ell$ satisfying $q > \ell + 1$ we have*

$$\frac{\ell}{q-1}\left(\frac{q}{\ell+1}\right)^n \leq LA_u(n,\ell)_q \leq \lceil \frac{q}{\ell+1} \rceil^{n-1}.$$

**Proof.** Consider the equation

$$\sum_{i=0}^{n-1} (\ell+1)^i x_i = a, \tag{5.4}$$

and let $X$ be the set of vectors $\mathbf{x} \in Q^n$ satisfying (5.4). As we have seen in the introduction of this section, $X$ is a $q$-ary $\ell$-UEC code.

Note also that $X = \varnothing$ if $a \notin I \triangleq [0, (q-1)\frac{(\ell+1)^n - 1}{\ell}]$. Hence we infer that there exists an $a \in I$ such that

$$|X| \geq \frac{|Q^n|}{|I|} = q^n / \left((q-1)\frac{(\ell+1)^n - 1}{\ell} + 1\right) \geq \left(\frac{q}{\ell+1}\right)^n \cdot \frac{\ell}{q-1}\,.$$

This gives the lower bound for $LA_u(n, \ell)_q$.
Let now $X$ be a $q$-ary $\ell$-UEC code defined by (5.1).

To prove the upper bound we consider the mapping $\psi : Q \to \mathbb{Z}_b$, where $b \triangleq \lceil \frac{q}{\ell+1} \rceil$, defined by

$$\psi(j) \equiv j \pmod{b};\ j = 0, \ldots, q-1.$$

Correspondingly for a codeword $\mathbf{x} = (x_0, \ldots, x_{n-1}) \in X$ we define $\psi^n(\mathbf{x}) = (\psi(x_0), \ldots, \psi(x_{n-1}))$. Let us show that $\psi^n$ is an injection on $X$. Suppose $\psi^n(\mathbf{x}) = \psi^n(\mathbf{x}')$ for two codewords $\mathbf{x}, \mathbf{x}' \in X$. By definition of $\psi$ we have $\mathbf{x} - \mathbf{x}' = b\mathbf{e}$, where $\mathbf{e} \in [-\ell, \ell]^n$. As $\mathbf{x}$ and $\mathbf{x}'$ both are in $X$ we have

$$\sum_{i=0}^{n-1} a_i e_i = 0. \tag{5.5}$$

We define $\mathbf{x}^* = \mathbf{x}' + (b-1)\mathbf{e}$ and claim that $\mathbf{x}^*$ is in $X$. In view of (5.5), it is sufficient to show that $\mathbf{x}^* \in Q^n$. For $1 \leq i \leq n$ let now $e_i \geq 0$. Then $x_i^* = x'_i + (b-1)e_i \geq x'_i \geq 0$ and $x_i^* = x_i - e_i \leq x_i \leq q-1$, so $x_i^* \in Q$. In a similar way it is proved that $x_i^* \in Q$ if $e_i \leq 0$. Since $\mathbf{x} - \mathbf{x}^* = \mathbf{e} = [-\ell, \ell]^n$, and $\mathbf{x}$ and $\mathbf{x}^*$ both are in $X$, we conclude that $\mathbf{e}{=}\mathbf{0}$, so $\mathbf{x} = \mathbf{x}'$. Thus $\psi^n$ is an injection, which implies that $|X| = |\psi^n(X)|$.

Define now

$$H' = \{(y_0, \ldots, y_{n-1}) \in \mathbb{Z}_b^n : \sum_{i=0}^{n-1} a_i y_i \equiv a (\mathrm{mod} b)\}.$$

It is easy to see that $\psi^n(X) \subset H'$. We can assume without loss of generality that $g.c.d.(a_0, \ldots, a_{n-1}) = 1$, so $(a_0(\mod b), \ldots, a_{n-1}(\mod b)) \neq (0, \ldots, 0)$.

Thus $H' \subset \mathbb{Z}_b^n$ is a hyperplane over $\mathbb{Z}_b$ and hence

$$|X| = |\psi^n(X)| \leq |H'| = b^{n-1}.$$

□

## 5.2 Construction of optimal codes

We call a VT-type $\ell$-UEC code VT-type optimal or shortly optimal if it attains the upper bound in Theorem 5. In this section we construct, for various classes of pairs $(\ell, q)$, maximal $q$-ary $\ell$-UEC codes for each length $n$.
Given integers $\ell \in [1, q-1],\ n,\ r$ we define

$$\mathcal{C}_n(r) = \left\{ (x_0, \ldots, x_{n-1}) \in Q^n : \sum_{i=0}^{n-1} (\ell+1)^i x_i = \alpha S_n + r \right\}, \tag{5.6}$$

$$\text{where } S_n \triangleq \sum_{i=0}^{n-1} (\ell+1)^i = \frac{(\ell+1)^n - 1}{\ell}, \quad \text{and } \alpha \triangleq \lfloor \frac{q-1}{2} \rfloor. \tag{5.7}$$

As we have seen before, $\mathcal{C}_n(r)$ is an $\ell$-UEC code for all $n$ and $r$.
For notational convenience, we denote the cardinality of $\mathcal{C}_n(r)$ by $\gamma_n(r)$, that is,

$$\gamma_n(r) = |\mathcal{C}_n(r)| \ . \tag{5.8}$$

**Proposition 8** *For each $n \geq 2$ and each $r$,*

$$\gamma_n(r) = \sum_{x_0} \gamma_{n-1} \left( (\alpha + r - x_0)/(\ell+1) \right) \ ,$$

*where the sum extends over all $x_0 \in Q$ satisfying $x_0 \equiv \alpha + r \pmod{\ell+1}$.*

**Proof.** By definition $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$ is in $\mathcal{C}_n(r)$ if and only if $\sum_{i=0}^{n-1} (\ell+1)^i x_i - \alpha S_n = r$. Using that $S_n = (\ell+1) S_{n-1} + 1$, the latter equality can also be written as $\sum_{i=1}^{n-1} (\ell+1)^i x_i - \alpha S_{n-1} = r - x_0 + \alpha$. In other words $\mathbf{x}$ is in $\mathcal{C}_n(r)$ if and only if $x_0 \equiv r + \alpha \pmod{\ell+1}$ and $(x_1, \ldots, x_{n-1})$ is in $\mathcal{C}_{n-1}(r')$, where $r' = (r - x_0 + \alpha)/(\ell+1)$. □

In the remainder of this section, we use the notation $\langle x \rangle_y$ to denote the integer in $[0, y-1]$ that is equivalent to $x$ modulo $y$. In other words, $\langle x \rangle_y = x - \lfloor \frac{x}{y} \rfloor \cdot y$.

**Lemma 3** *Let $e$ and $f$ be integers such that $0 \le e \le f-1$. We have that*

$$|\{x \in Q : x \equiv e \pmod f\}| = \begin{cases} \lceil \frac{q}{f} \rceil & \text{if } e < \langle q \rangle_f \\ \lfloor \frac{q}{f} \rfloor & \text{if } e \ge \langle q \rangle_f \end{cases}$$

**Proof.** We obviously have that

$$\{x \in Q : x \equiv e \pmod f\} = \{e+f, e+2f, \ldots, e+mf\},$$

where $m$ is such that $e+mf \le q-1$ and $e+(m+1)f \ge q$. In other words $m = \lfloor \frac{q-1-e}{f} \rfloor$. Writing $q = \lambda f + \langle q \rangle_f$, we have $m - \lambda = \lfloor \frac{\langle q \rangle_f - 1 - e}{f} \rfloor$, which equals 0 if $\langle q \rangle_f \ge e+1$, and $-1$ otherwise. This proves the lemma. □

**Theorem 6** *Let $u_1, u_2, \ldots$ and $v_1, v_2, \ldots$ be sequences of integers such that:*
(1) $0 \le u_1 + \alpha \le v_1 + \alpha \le q-1$,
*and for each $n \ge 2$*
(2) $\lceil \frac{1}{\ell+1}(u_n + \alpha - (q-1)) \rceil \ge u_{n-1}$,
(3) $\lfloor \frac{1}{\ell+1}(v_n + \alpha) \rfloor \le v_{n-1}$, *and*
(4) $\ell+1$ *divides $q$, or for each $r \in [u_n, v_n]$, $\langle \alpha + r \rangle_{\ell+1} < \langle q \rangle_{\ell+1}$.*
*Then for each $n \ge 1$ and $r \in [u_n, v_n]$ we have $\gamma_n(r) = \lceil \frac{q}{\ell+1} \rceil^{n-1}$.*

**Proof.** We proceed by induction on $n$.
For $n = 1$ the assertion is true because of condition (1).
Now let $n \ge 2$, and suppose the assertion is true for $n-1$. Let $r \in [u_n, v_n]$. According to Proposition 8, we have that

$$\gamma_n(r) = \sum_{x_0} \gamma_{n-1}\left(\frac{r+\alpha-x_0}{\ell+1}\right) \quad . \tag{5.9}$$

According to condition (4), either $\ell+1$ divides $q$, or $\langle \alpha + r \rangle_{\ell+1} < \langle q \rangle_{\ell+1}$. In both cases Lemma 3 implies that the sum in (5.9) has $\lceil \frac{q}{\ell+1} \rceil$ terms.
For each $x_0 \in Q$ we have that $r+\alpha-x_0 \le r+\alpha \le v_n+\alpha$ and $r+\alpha-x_0 \ge r+\alpha-(q-1) \ge u_n+\alpha-(q-1)$. That is, for each $x_0 \in Q$

$$u_n + \alpha - (q-1) \le r + \alpha - x_0 \le v_n + \alpha. \tag{5.10}$$

Combining (5.10) with conditions (2) and (3) we find that for each $x_0$ in $Q$, such that $r+\alpha-x_0$ is a multiple of $\ell+1$, we have

$$\frac{r+\alpha-x_0}{\ell+1} \in [u_{n-1}, v_{n-1}].$$

The induction hypothesis implies that each term in the sum in (5.9) equals $\lceil \frac{q}{\ell+1} \rceil^{n-2}$. □

**Theorem 7** *Let $\ell$ and $q$ be such that $\ell+1$ divides $q$. Let $u_1=-\alpha$, $v_1=\alpha$, and for $n\geq 2$, $u_n=(\ell+1)u_{n-1}+\alpha$ and $v_n=(\ell+1)v_{n-1}-\alpha$. In other words, for $n\geq 1, v_n=-u_n=\frac{\alpha}{\ell}\left[(\ell-1)(\ell+1)^{n-1}+1\right]$.*
*Then for each $n\geq 1$ and $r\in[u_n,v_n]$, we have*

$$\gamma_n(r)=LA_u(n,\ell)_q=\left(\frac{q}{\ell+1}\right)^{n-1}.$$

**Proof.** We apply Theorem 6. It is immediately clear that conditions (1), (3) and (4) are satisfied. Moreover, for each $n\geq 2$, $u_n+\alpha-(q-1)=(\ell+1)u_{n-1}+2\alpha-(q-1)\geq(\ell+1)u_{n-1}-1$, so condition (3) is satisfied as well. □

**Theorem 8** *Let $c\in[0,\ell], \delta\in\{0,1\}$, and $m$ be such that*

$$q=2m(\ell+1)+2c+1+\delta \text{ and } 2c+\delta\neq\ell.$$

*We define $\lambda_1=0$, and for $n\geq 2$,*

$$\lambda_n=(\ell+1)\lambda_{n-1}-\eta, \text{ where } \eta=\begin{cases} 0 & \text{if } 2c+\delta\leq\ell-1,\\ \lceil\frac{1}{2}(\ell-\delta)\rceil & \text{if } 2c+\delta\geq\ell+1.\end{cases}$$

*Moreover, for $n\geq 1$, we define*

$$u_n=-c+\lambda_n(\ell+1) \text{ and } v_n=-c+\lambda_n(\ell+1)+\langle q\rangle_{\ell+1}-1.$$

*If $m\leq c-1-\lceil\frac{1}{2}(\ell-\delta)\rceil$ or $2c+\delta\leq\ell$ and $m\leq c$, then for each integer $n$ and $r\in[u_n,v_n]$,*

$$\gamma_n(r)=LA_u(n,\ell)_q=\lceil\frac{q}{\ell+1}\rceil^{n-1}.$$

**Proof.** We apply Theorem 6. Note that

$$\alpha=\lfloor\frac{q-1}{2}\rfloor=m(\ell+1)+c.$$

We first check condition (1): $u_1+\alpha=-c+\alpha=m(\ell+1)\geq 0$ and $u_1+\alpha\leq v_1+\alpha=m(\ell+1)+\langle q\rangle_{\ell+1}-1\leq q-1$.
The definition of $u_n$ and $v_n$ implies that for each $n$ and each $r\in[u_n,v_n]$ we have that

$$r+\alpha\in[u_n+\alpha,v_n+\alpha]=[(\lambda_n+m)(\ell+1),(\lambda_n+m)(\ell+1)+\langle q\rangle_{\ell+1}-1],$$

so condition (4) is satisfied.
For verifying Condition (2), we note that

$$\lceil\frac{1}{\ell+1}(u_n+\alpha-(q-1))\rceil=\lceil\frac{1}{\ell+1}(u_n-\alpha-\delta)\rceil=(\lambda_n-m)+\lceil\frac{-\delta-2c}{\ell+1}\rceil.$$

As $\lambda_n=\lambda_{n-1}(\ell+1)-\eta=u_{n-1}+c-\eta$ condition (2) is satisfied if and only if

$$m\leq c-\eta-\lfloor\frac{\delta+2c}{\ell+1}\rfloor. \tag{5.11}$$

For verifying condition (3) we note that

$$\lfloor \frac{1}{\ell+1}(v_n+\alpha)\rfloor = \lfloor \frac{1}{\ell+1}((\lambda_n+m)(\ell+1)+\langle q\rangle_{\ell+1})\rfloor = \lambda_n + m.$$

As $\lambda_n = (\ell+1)\lambda_{n-1} - \eta = v_{n-1} + c - \langle q\rangle_{\ell+1} + 1 - \eta$, condition (3) is satisfied if and only if

$$m \le \langle q\rangle_{\ell+1} - 1 - c + \eta \tag{5.12}$$

We distinguish between two cases.
**Case 1** $2c+\delta \le \ell - 1$.
Then $\langle q\rangle_{\ell+1} = 2c+\delta+1$, and $\lfloor \frac{\delta+2c}{\ell+1}\rfloor = 0$. That is, (5.11) reduces to the inequality $m \le c - \eta$ and (5.12) reduces to $m \le c + \delta + \eta$. As $\eta = 0$, we see that (5.11) and (5.12) both are satisfied if $m \le c$.
**Case 2** $2c+\delta \ge \ell + 1$.
Then $\langle q\rangle_{\ell+1} = 2c+\delta-\ell$, and $\lfloor \frac{\delta+2c}{\ell+1}\rfloor = 1$. Consequently, (5.11) reduces to the inequality $m \le c - \eta - 1$, and (5.12) reduces to $m \le c+\delta-\ell-1+\eta$. With our choice for $\eta$, we see that (5.11) and (5.12) both are satisfied if $m \le c - \eta - 1 = c - 1 - \lceil \frac{1}{2}(\ell-\delta)\rceil$. □

**Corollary 2** *Let $q = (b-1)(\ell+1)+d$ for integers $1 \le b-1 < d \le \ell$. Then for each $n$*

$$LA_u(n,\ell)_q = b^{n-1} = \left\lceil \frac{q}{\ell+1} \right\rceil^{n-1}.$$

**Proof.** Suppose $b-1$ is even. Then we can write

$$q = 2m(\ell+1)+d = 2m(\ell+1)+2c+1+\delta,$$

where $c = (d-1-\delta)/2$ and $m = (b-1)/2$. The condition $b-1 < d \le \ell$ implies that $2c+\delta \le \ell - 1$ and $m \le c$. Therefore by Theorem 8 we have

$$\gamma_n(r) = b^{n-1}, \text{ where } r \in [-c, c].$$

Suppose now $b-1$ is odd. Then

$$q = (2m+1)(\ell+1)+d = 2m(\ell+1)+d+\ell+1 = 2m(\ell+1)+2c+1+\delta,$$

where $c = (d+\ell-\delta)/2$ and $m = (b-2)/2$.

Now the condition $b-1 < d$ implies $m \le c - 1 - \lceil \frac{1}{2}(\ell-\delta)\rceil$ and hence by Theorem 8 we have

$$\gamma_n(r) = b^{n-1}, \text{ where } r \in [u_n, v_n].$$

□

In conclusion of this section let us note that the determination of $LA_u(n,\ell)_q$ in general seems to be a difficult problem. As was shown above codes defined by (5.6) are best possible for certain parameters $q$ and $\ell$, mentioned in Theorems 6 and 7. However we do not know how good these codes are for other parameters.

An interesting open problem is to decide what is the $\max_r |\mathcal{C}_n(r)|$ for given $\ell$ and $q$. Note that for some cases the code $\mathcal{C}_n(0)$ has the size bigger than the lower bound in Theorem 5. Let for example $\ell = 2,\ q = 7$. Then it is not hard to observe that the number of solutions $c_n$ of (5.6) satisfies the recurrence $c_n = 2c_{n-1} + c_{n-2}$. This gives the bound $|\mathcal{C}_n(r)| \geq K(2,41)^n$, where $2,41 \approx 1 + \sqrt{2}$ is the largest root of the characteristic equation $x^2 - 2x - 1 = 0,\ K$ is a constant. The same recurrence we obtain for any $q = 2\ell + 3$, which implies that for $q = 2\ell + 3$ and $\ell \geq 2$ one has $|\mathcal{C}_n(r)| \geq K(2,41)^n > \frac{\ell}{q-1}\left(\frac{q}{\ell+1}\right)^n$ (the lower bound in Theorem 5). Note however that this is not the case for $\ell = 1,\ q = 5$.

One can also observe that for $q = 7,\ \ell = 1$ we have $|\mathcal{C}_n(r)| \geq K(3,51)^n$. Without going into detail we note that this can be derived from the recurrence $c_n = 4c_{n-1} - 2c_{n-2} + c_{n-3}$ for the number of solutions $c_n$ of (5.6) (with $r = 0,\ q = 7,\ \ell = 1$).

One may use a generating functions approach to analize the problem.
Let $f(x)=1+x+x^2+\ldots+x^{q-1}$. We are interested in the largest coefficient of the polynomial $f(x)f(x^{\ell+1})f(x^{(\ell+1)^2})f(x^{(\ell+1)^3})\cdots f(x^{(\ell+1)^{n-1}})$. If, for example, we take $q = 5, \ell = 1$ and $n = 4$, the largest coefficient equals 20 (attained with $x^{24}, x^{28}, x^{32}$ and $x^{36}$), while the coefficient of $x^a$ for $a = \lfloor \frac{q-1}{2} \rfloor \frac{(\ell+1)^n-1}{\ell} = 30$ only equals 17.

## 5.3 Asymptotic growth rate of $\ell$-UEC codes of VT type

In the previous section we explicitly constructed maximal $q$-ary $\ell$-UEC codes of VT type of arbitrary length for some classes of pairs $(\ell, q)$ – but not for all.

In this section we state a less ambitious goal, namely, given $\ell$ and $q$, to determine the asymptotic behaviour of $\sqrt[n]{LA_u(n,\ell)_q}$. We will show that this quantity converges if $n \to \infty$. As a preparation we need the following

**Lemma 4** *Let $a, b, a_0, a_1, \ldots, a_{m-1}, b_0, b_1, \ldots, b_{n-1}$ be integers such that the codes $\mathcal{A}$ and $\mathcal{B}$, defined as*

$$\mathcal{A} = \{(x_0, x_1, \ldots, x_{m-1}) \in Q^m : \sum_{i=0}^{m-1} a_i x_i = a\} \text{ and } \mathcal{B} = \{(y_0, y_1, \ldots, y_{n-1}) \in Q^n : \sum_{j=0}^{n-1} b_j y_j = b\}$$

*both are non-empty $\ell$-UEC codes. Let $\mathcal{A} \times \mathcal{B} \subset Q^{m+n}$ be the direct product of $\mathcal{A}$ and $\mathcal{B}$:*

$$\mathcal{A} \times \mathcal{B} = \{(\mathbf{x}; \mathbf{y}) : \mathbf{x} \in \mathcal{A}, \mathbf{y} \in \mathcal{B}\}.$$

*Let $M$ be an integer such that $\sum_{i=0}^{n-1} |a_i|(q-1) < M$, and define $\mathcal{C}$ as*

$$\mathcal{C} = \{(z_0, z_1, \ldots, z_{n+m-1}) \in Q^{n+m} : \sum_{i=0}^{n-1} a_i z_i \ + \ \sum_{i=n}^{n+m-1} M b_{i-n} z_i = a + Mb\}.$$

*Then $\mathcal{C} = \mathcal{A} \times \mathcal{B}$, and $\mathcal{A} \times \mathcal{B}$ is a $q$-ary $\ell$-AUEC code.*

**Proof.** It is clear that $\mathcal{A} \times \mathcal{B} \subset \mathcal{C}$. Moreover, $\mathcal{A} \times \mathcal{B}$ is an $\ell$-UEC code: a received word can be decoded by decoding its $m$ leftmost and $n$ rightmost symbols to $\mathcal{A}$ and $\mathcal{B}$, respectively. All we are left with to show is that $\mathcal{C} \subset \mathcal{A} \times \mathcal{B}$. Therefore, let $(z_0, z_1, \ldots, z_{n+m-1})$ be in $\mathcal{C}$. By definition, we have that

$$a + Mb = \sum_{i=0}^{m-1} a_i z_i \ + \ M \cdot \sum_{i=m}^{m+n-1} b_{i-m} z_i, \tag{5.13}$$

and so

$$a - \sum_{i=0}^{m-1} a_i z_i \equiv 0 \bmod M. \tag{5.14}$$

As $\mathcal{A} \neq \emptyset$, there is an $\mathbf{x} \in Q^m$ such that $a = \sum_{i=0}^{m-1} a_i x_i$, and whence

$$|a - \sum_{i=0}^{m-1} a_i z_i| = |\sum_{i=0}^{m-1} a_i (x_i - z_i)| \leq \sum_{i=0}^{m-1} |a_i||x_i - z_i| \leq \sum_{i=0}^{m-1} |a_i|(q-1) < M. \tag{5.15}$$

From (5.14) and (5.15) we conclude that $a = \sum_{i=0}^{m-1} a_i z_i$ and so $(z_0, z_1, \ldots, z_{m-1}) \in \mathcal{A}$. Furthermore using (5.13) we find that $(z_m, z_{m+1}, \ldots, z_{m+n-1})$ is in $\mathcal{B}$. □

Lemma 4 immediately implies that

$$LA_u(\ell, m+n)_q \geq LA_u(\ell, m)_q \cdot LA_u(\ell, n)_q. \tag{5.16}$$

As $LA_u(\ell, n)_q \leq \lceil \frac{q}{\ell+1} \rceil^{n-1}$ we can invoke Fekete's lemma to derive the following result from (5.16):

**Proposition 9** *For each $q$ and $\ell \in Q$, there exists a constant $\beta(\ell, q) \leq \lceil \frac{q}{\ell+1} \rceil$ such that*

$$\lim_{n \to \infty} \sqrt[n]{LA_u(n, \ell)_q} = \beta(\ell, q).$$

Theorem 5 implies that for all $\ell$ and $q$,

$$\frac{q}{\ell+1} \leq \beta(\ell, q) \leq \lceil \frac{q}{\ell+1} \rceil.$$

In particular, $\beta(\ell, q) = \frac{q}{\ell+1}$ if $\ell + 1$ divides $q$ (of course, this is also implied by the much stronger Theorem 7). Note also that for pairs $(\ell, q)$ for which the conditions from Theorem 8 applies, we have $\beta(\ell, q) = \lceil \frac{q}{\ell+1} \rceil$.
Inequality (5.16) implies that for each $n$, $\beta(\ell, q) \geq \sqrt[n]{LA_u(n, \ell)_q}$. For example, consider the case that $q = \ell + 2$. The code

$$\{(x_0, x_1, x_2, x_3) \in Q^4 : \sum_{i=0}^{3} (\ell+1)^i x_i = \ell + 1 + (\ell+1)^3\}$$

has five words, *viz.* (1+$\ell$,1+$\ell$,$\ell$,0), (1+$\ell$,0,1+$\ell$,0), (1+$\ell$,0,0,1), (0,1,1+$\ell$,0), and $(0, 1, 0, 1)$. That is, $\beta(\ell, \ell+2) \geq \sqrt[4]{5} \approx 1.495$. Note that Theorem 5 only allows us to deduce that $\beta(\ell, \ell+2) \geq \frac{\ell+2}{\ell+1}$.
Also note that Corollary 2 with $b = 2$ states that for $\ell \geq 2 \quad \beta(\ell, \ell+3) = 2$.

# 6 The error detection problem

We find it interesting to consider also the error detection problem, i.e. codes detecting unconventional errors of a certain level. It is easy to see that codes detecting asymmetric errors of level $\ell$ can be also used to detect unidirectional errors of level $\ell$. For codes detecting all asymmetric (unidirectional) errors of level $\ell$ we use the abbreviation $\ell$-AED codes (or $\ell$-UED codes).
For integers $\ell, q, n$ satisfying $1 \leq \ell < q$ and $n \geq 1$, we define

$$P_i = \{(a_1, \ldots, a_n) \in Q^n : \sum_{j=1}^{n} a_j = i\}.$$

It is clear that $P_i$ detect each unidirectional error pattern. Note that $|P_i|$ is maximal for $i = i^* = \lfloor \frac{1}{2}n(q-1) \rfloor$, see [3, Thm. 4.1.1]. For $a \in [0, \ell n]$, let $\mathcal{C}_a \subset Q^n$ be defined as

$$\mathcal{C}_a = \bigcup_{i: i \equiv a (\bmod\ \ell n+1)} P_i \tag{6.1}$$

**Proposition 10** *$\mathcal{C}_a$ is an $\ell$-UED-code over the alphabet $Q$.*

**Proof.** Clearly $\mathcal{C}_a$ is an $\ell$-UED code iff for each $\mathbf{x}, \mathbf{y} \in \mathcal{C}_a$ either $\mathbf{x}$ and $\mathbf{y}$ are incomparable or $d(\mathbf{x}, \mathbf{y}) \geq \ell + 1$. Suppose that for some $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ we have $\mathbf{x} > \mathbf{y}$. Then clearly by definition of $\mathcal{C}$ there exists a coordinate $i \in [1, n]$ such that $x_i - y_i \geq \ell + 1$, i.e. $d(\mathbf{x}, \mathbf{y}) \geq \ell + 1$. □

This simple construction gives us a lower bound for the maximum size of an $\ell$-UED code over alphabet $Q$. However we don't know whether it is possible to improve this bound, even for the case $\ell = 1$.

**Remark 1**. Asymptotically, taking the union of several $P_i$'s does not really help as the largest $P_i$ contains $c\frac{1}{\sqrt{n}}q^n$ words, while nearly all words in $Q^n$ are in the union of about $\sqrt{n}$ sets $P_i$ with consecutive $i$'s.

**Remark 2** The construction is not optimal in general. For example take $\ell$=1 and $q$=$n$=3. It can easily be checked that $(|P_0|, |P_1|, \ldots, |P_6|)$ = (1,3,6,7,6,3,1). Therefore for each $a \in [0, \ell n] = [0, 3]$, $|C_a| \leq 7$. The code consisting of (0,0,0), (2,2,2) and the six permutations of (0,1,2) has eight words and is a 1-UED code.
Consider also two other small cases.
For $\ell = 1$, $q = 4$ and $n = 3$ one easily checks that
$(|P_0|, |P_1|, \ldots, |P_9|)$ = (1,3,6,10,12,10,6,3,1) and so $|C_a|$=16 for all $a \in [0, \ell n] = [0, 3]$.
Similarly for $\ell$=1, $q$=5 and $n$=3 one easily checks that
$(|P_0|, |P_1|, \ldots, |P_{12}|)$ = (1,3,6,10,15,18,19,18,15,10,6,3,1). It follows that $|C_0|$ = 32 and $|C_1| = |C_2| = |C_3| = 31$. Note that $C_0$, the largest of the four codes, does not contain $P_6$, the largest $P_i$.

# References


[1] K.A.S. Abdel-Ghaffar and H. Fereira, "Systematic encoding of the Varshamov-Tennengolts codes and the Constantin-Rao codes", *IEEE Trans. Inform. Theory*, 44, No. 1, 340-345, 1998.

[2] R. Ahlswede, H. Aydinian and L.H. Khachatrian, Undirectional error control codes and related combinatorial problems, in Proceedings of Eight International workshop on Algebraic and Combinatorial Coding Theory, 8–14 September, Tsarskoe Selo, Russia, 6–9, 2002.

[3] I. Anderson, *Combinatorics of Finite Sets*, Clarendon Press, Oxford, 1987.

[4] M. Blaum (ed.), *Codes for detecting and correcting unidirectional errors*, IEEE Computer Society Press Reprint Collections, IEEE Computer Society Press, Los Alamitos, CA, 1993.

[5] J.M. Borden, "Optimal asymmetric error detecting codes", *Information and Control*, 53, No. 1-2, 66-73, 1982.

[6] B. Bose and S.A. Al-Bassam, "On systematic single asymmetric error correcting codes", *IEEE Trans. Inform. Theory*, 46, No. 2, 669-672, 2000.

[7] B. Bose and S. Cunningham, "Asymmetric error correcting codes, Sequences", II (Positiano 1991), 24-35, Springer, New York, 1993.

[8] S.D. Constantin and T.N.N. Rao, "On the theory of binary asymmetric error correcting codes", *Information and Control*, 40, No. 1, 20-36, 1979.

[9] Ph. Delsarte and Ph. Piret, "Bounds and constructions for binary asymmetric error correcting codes", *IEEE Trans. Inform. Theory*, 27, No. 1, 125-128, 1981.

[10] L.E. Dickson, *History of the Theory of Numbers*, Vol. 2, New York: Chelsea, 1952.

[11] P. Erdős, "Problems and results from additive number theory", *Colloq. Theoretic des Nombres, Bruxelles, 1955*, Liege&Paris, 1956.

[12] G. Fang and H.C.A. van Tilborg, "Bound and constructions of asymmetric or unidirectional error-correcting codes", *Applicable Algebra in Engineering, Communication and Engineering*, 3, No. 4, 269-300, 1992.

[13] D. Gevorkian and A.G. Mhitarian, "Classes of codes that correct single asymmetric errors" (in Russian), *Dokl. Akad. Nauk Armyan. SSR*, 70, No. 4, 216-218, 1980.

[14] B.D. Ginzburg, A number-theoretic function with an application in the theory of coding, *Probl. Kybern.*, Vol. 19, 249-252, 1967.

[15] T. Helleseth and T. Kløve, "On group-theoretic codes for asymmetric channels", *Information and Control*, 49, No. 1, 1-9, 1981.

[16] W.H. Kim and C.V. Freiman, "Single error-correcting-codes for asymmetric binary channels", *IRE Trans. on Inform. Theory*, IT-5, 62-66, 1959.

[17] T. Kløve, "Error correcting codes for the assymetric channel", Report, Dept. of Math. Univ. of Bergen, 1981 (with updated bibliography in 1995).

[18] V.I. Levenshtein, "Binary codes capable of correcting deletions and insertions, and reversals", *Sov. Phys. Dokl.*, Vol. 10, 707-710, 1966.

[19] S. Lin and D.J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*, Prentice-Hall, Inc. Englewood Cliffs, New Jersey, 1983.

[20] F.J. MacWilliams and N.J. Sloane, *The Theory of Error-Correcting Codes*, New York: North-Holland, 1988.

[21] R.J. McEliece, "Comments on "Class of codes for asymmetric channels and a problem from additive Theory of Numbers"", *IEEE Trans. Inform. Theory*, 19, No. 1, 137, 1973.

[22] S. Martirossian, "Single-error correcting close-packed and perfect codes", in *Proceedings of First INTAS International Seminar on Coding Theory and Combinatorics* (Tsahkadzor Armenia), 90-115, 1996.

[23] L.E. Mazur, "Certain codes that correct non-symmetric errors", *Problems of Information Transmission*, 10, 4, 308-312, 1976.

[24] M.N. Nalbandjan, "A class of codes that correct multiple asymmetric errors" (in Russian), *Doklady Acad. Nauk Georgian SSR*, 77, 405-408, 1975.

[25] O.S. Oganesyan and V.G. Yagdzhyan, "Classes of codes correcting bursts of errors in an asymmetric channel", *Problemy Peredachi Informatsii*, 6, No. 4, 27-34, 1970.

[26] V.S. Pless, W.C. Huffman, and R.A. Brualdi (eds), *Handbook of Coding Theory*, Vol. I, II, North-Holland, Amsterdam, 1998.

[27] R.P. Stanley and M.F. Yoder, "A study of Varshamov codes for assymetric channels", *Jet Prop. Lab. Tech. Rep.*, 32-1526, Vol. 14, 117-122, 1982.

[28] R.R. Varshamov, "Estimates of the number of signals in codes with correction of nonsymmetric errors"(in Russian)*Avtomatika i Telemekhanika* 25, no. 11, 1628-1629, 1964.(transl: Automation and Remote Contr. 25, 1468-1469, 1965).

[29] R.R. Varshamov, "On some features of asymmetric error-correcting linear codes"(in Russian), *Rep. Acad. Sci. USSR*, Vol. 157, No. 3, 546-548, 1964. (transl: Soviet Physics-Doklady 9, 538-540, 1964.

[30] R.R. Varshamov, "On the theory of assymmetric codes"(in Russian), *Doklady Akademii Nauk USSR*, Vol. 164, 757-760, 1965. (transl: Soviet Physics-Doklady 10, 185-187, 1965).

[31] R.R. Varshamov and G.M. Tennengolts, "A code which corrects single asymmetric errors" (in Russian) *Avtomat. Telemeh.*, 26, 282-292, 1965. (transl: Automation and Remote Contr., 286-290, 1965).

[32] R.R. Varshamov and E.P. Zograbian,"Codes correcting packets of non-symmetricerrors"(in Russian) *Proc. 4'th Symposium on Problems in Inform. Systems*, vol. 1, 87-96, 1970. (Review in RZM no.2, V448, 1970).

[33] R.R. Varshamov, "A class of codes for asymmetric channels and a problem from the additive theory of numbers", *IEEE Trans. Inform. Theory*, 19, No. 1, 92-95, 1973.

[34] J.H. Weber, C. de Vroedt, and D.E. Boekee, "Bounds and constructions for codes correcting unidirectional errors", *IEEE Trans. Inform. Theory*, 35, No. 4, 797-810, 1989.