Unidirectional Error Control Codes and Related Combinatorial Problems

R. Ahlswede, H. Aydinian, and L.H. Khachatrian

University of Bielefeld, Dept. of Mathematics, POB 100131, D–33501 Bielefeld
E–mail:ayd@mathematik.uni-bielefeld.de

Abstract

q–ary codes capable of correcting all unidirectional errors of certain level $1 \leq \ell \leq q-2$ are considered. We also discuss some related extremal combinatorial problems.

1 Introduction

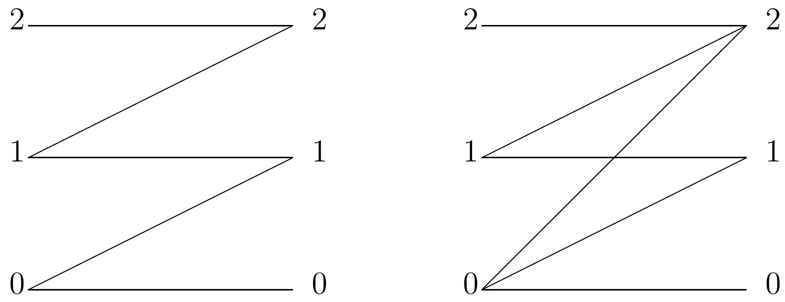
An extensive theory of error control coding has been developed under the assumption of symmetric errors in the data bits; i.e. errors of type $0 \to 1$ and $1 \to 0$ can occur in a codeword.However in many digital systems such as fiber optical communications and optical disks the ratio between probability of errors of type $1 \to 0$ and $0 \to 1$ can be large. Practically we can assume that only one type of errors can occur in those systems. These errors are called asymmetric. The statistics also shows that in some of the recently developed LSI/VLSI ROM and RAM memories the most likely faults are of the unidirectional type. The unidirectional errors slightly differ from asymmetric type of errors: both $1 \to 0$ and $0 \to 1$ type of errors are possible, but in any particular word all the errors are of the same type.The problem of protection against unidirectional errors arises also in designing fault–tolerant sequential machines, in write–once memory systems, in asynchronous systems et al.Codes correcting asymmetric/unidirectional errors are not well studied since they encounter more complicated structures than those for symmetric errors. (for more information see a good collection of papers in [2]). The first construction of nonlinear codes correcting asymmetric single errors was given by Varshamov and Tennengolts [5]. Modifications of VT–codes where used to construct new codes correcting t–asymmetric errors and burst of errors [2]. Very few constructions are known for codes correcting unidirectional errors (see [2]). We call a code of length n, correcting t–asymmetric errors a generalized VT–code if it is given by the set of solutions $(x_1, \dots, x_n) \in \{0,1\}^n$ of a linear congruence of the type

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

where $f(i)$ $(i = 1, \ldots, n)$ is an integer valued function, a and M are integers. There are deep relationships between VT–codes and some difficult problems in Additive Number Theory [6], [3]. In [6] Varshamov introduced a q–ary asymmetric channel. The inputs and outputs of the channel are n–sequences over a q–ary alphabet labelled with integers $\{0, 1, \ldots, q-1\}$. 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 $e_i \in \{0, \ldots, q-1\}$ and $x_i + e_i \leq q-1, \ i = 1, \ldots, n$. Then Varshamov says that t–errors have occured if $e_1 + \cdots + e_n = t$. Generalizing the idea of VT–codes Varshamov presented [6] several ingenious constructions of t–error correcting codes for the defined channel. These codes has been shown to be superior to BCH codes correcting t errors for $q \geq 2$ and for large n.

2 ℓ–AUEC–codes and related problems

The number of symmetric errors in real systems is usually limited, while the number of unidirectional/asymmetric errors can be fairly large. This motivated several authors to consider codes that correct a few symmetrical errors and detect/correct all/many unidirectional (asymmetric) errors.We introduce now a special type of asymmetric errors in a q–ary channel. As above the alphabet Q is labelled with integers $\{0, 1, \ldots, q-1\}$ and for every transmitted vector $x = (x_1, \ldots, x_n)$ the output is of the form $(x_1 + e_1, \ldots, x_n + e_n)$, where "+" denotes real addition, and $x_i + e_i \leq q-1$; $i = 1, \ldots, n$.We say that an asymmetric error $e = (e_1, \ldots, e_n)$ is of level $1 \leq \ell \leq q-1$ if $0 \leq e_i \leq \ell$. We also say that t asymmetric errors have occured if for the Hamming weight $wt_H(e) = t$. Correspondingly we say that t unidirectional errors have occured, if the output is either $x + e$ or $x - e$. The difference between the channel described above and Varshamov's channel for $q > 2$, $l = 1$ is seen in the figure below.



Here we concentrate on the case $t = n$. That is we consider q–ary codes correcting all asymmetric or unidirectional errors of given level ℓ. For those we use the abreviations ℓ–AAEC– and ℓ–AUEC–codes, respectively.For given $1 \leq \ell \leq q-2$ let $A_a(n, \ell)_q$ and $A_u(n, \ell)_q$ denote the maximum number of codewords in a q–ary code of length n, correcting all asymmetric and unidirectional errors, respectively. Clearly $A_u(n, \ell)_q \leq A_a(n, \ell)_q$. Define two distances between $x=(x_1,\dots,x_n)$, $y=(y_1,\dots,y_n)\in Q^n=\{0,1,\dots,q-1\}^n$.

$$d_a(x,y)=\max\{|x_i-y_i| : i=1,\dots,n\}$$
$$d_u(x,y)=\begin{cases} d_a(x,y), & \text{if } x\ge y \text{ or } x\le y\\ 2d_a(x,y), & \text{if } x \text{ and } y \text{ are incomparable}\end{cases}$$

where $x\ge y$ means that $x_i-y_i\ge 0$, for $i=1,\dots,n$.

Proposition 1. Let $\mathcal{C}\subset\{0,\dots,q-1\}^n$. Then

(i) $\mathcal{C}$ is an ℓ–AAEC–code iff for every $x,y\in\mathcal{C}$ holds $d_a(x,y)\ge \ell+1$

(ii) $\mathcal{C}$ is an ℓ–AUEC–code iff for every $x,y\in\mathcal{C}$ holds $d_u(x,y)\ge 2\ell+1$.

It turns out that it is very easy to determine $A_a(n,\ell)_q$ for any given parameters $1\le\ell\le q-2$ and n. However this is not the case for unidirectional codes.

Theorem 1. *For $1\le\ell\le q-2$ one has $A_a(n,\ell)_q=\left\lceil\frac{q}{\ell+1}\right\rceil^n$.*

Theorem 2. *Given integers $\ell\ge 1$, $q>2(\ell+1)$ we have $c\left(\frac{q}{\ell+1}\right)^n\le A_u(n,\ell)_q\le\left\lceil\frac{q}{\ell+1}\right\rceil^n$ for some constant c.*

Write $q=2m+\varepsilon$, where $\varepsilon\in\{0,1\}$, and let $Q=\{-m,\dots,m+\varepsilon-1\}$. Let us define X to be the set of solutions $x\in Q^n$ of the equation

$$\sum_{i=0}^{n-1}(\ell+1)^i x_i=a. \tag{2.1}$$

It is easy to see that X is a l–AUEC–code.In a special case when $\ell+1|q$ we can maximize $|X|$ over all choices of a.

Theorem 3. *For $\ell+1|q$ ($q=|Q|$) $\max_a|X|=\left(\frac{q}{\ell+1}\right)^{n-1}$.* The maximum assumed for any $a\in Q$ in (2.1).

What can we say about $A_u(n,\ell)_q$, when $\ell+2\le q\le 2(\ell+1)$?

The simplest case is $q=2(\ell+1)$.In this case $A_u(n,\ell)_q=2^n$. However, we have no "good" lower bounds for other cases. A simple lower bound is $A_u(n,\ell)_q\ge\binom{n}{\lfloor\frac{n}{2}\rfloor}$.

Case: $\ell=1$

For $q=3$ we have $A_u(n,1)_3\ge\binom{n}{\lfloor\frac{n}{2}\rfloor}$.

For $q=4$ $A_u(n,1)_4=2^n$.

$q=5$. Simple bounds observed above give us $c(2,5)^n\le A_u(n,1)_5\le 3^n$. However the lower bound can be improved. To this end we look for good constructions of 1–AUEC codes given by means of some equation. Let $Q=\{0,\pm1,\pm2\}$. Given integers $a_0,\dots,a_{n-1},\lambda$ let X be the set of all solutions $x=(x_0,\dots,x_{n-1})\in Q^n$ of an equation

$$\sum_{i=0}^{n-1}a_ix_i=\lambda. \tag{2.2}$$

Proposition 2. The set X is a 1–AUEC code if all subset sums of $a_0, \dots, a_{n-1}$ are distinct.

Note that for $\lambda = 0$ this is also a necessary condition. Let $\{a_0, \dots, a_n\} \subset \mathbb{N}$ has distinct subset sums. Denote by $LA_u(n)_5$ the maximum possible number of solutions $x \in Q^n$ of the (2.2) over all choices of $a_0, \dots, a_n$ and integer λ. A slightly modified version of this problem was raised by Bohman (see [1]) in connection with a sum packing problem of Erdős [3].

Theorem 4. *For some constants* c_1, c_2 *one has* $c_1(2,538)^n < LA_u(n)_5 < c_2(2,723)^n$.

Error Detection Problem The detection problems for asymmetric and unidirectional errors are equivalent, i.e. any t–error detecting asymmetric code is also a t–error detecting unidirectional code. In fact the detection problem for unidirectional errors is much easier than the error correction problem. This problem is completely solved for binary channels (see Borden in [2]). That is for any $1 \le t \le n$; $t, n \in \mathbb{N}$; an optimal code of length n that can detect up to t errors is constructed. For $t < n$ observe that a code C detects all patterns of t or fewer unidirectional errors, iff whenever a codeword x covers a codeword y then for the Hamming distance $d(x, y) > t + 1$. In this case as an optimal code one has to take as codewords all vectors with Hamming weight $w = \left\lfloor \frac{n}{2} \right\rfloor \mod (t + 1)$. This follows from a result of Katona [4].The problem is also solved for the Varshamov's channel, however for the channel we described above the problem is open.

References

[1] R. Ahlswede, H. Aydinian and L.H. Khachatrian, On Bohman's conjecture related to a sum packing problem of Erdős, submitted to Proceedings of the Amer. Math. Aoc.

[2] M. Blaum, Codes for detecting and correcting unidirectional errors. Edited by Mario Blaum. IEEE Computer Society Press Reprint Collections. IEEE Computer Society Press, Los Alamitos, CA, 1993.

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

[4] G. Katona, Families of subsets having no subset containing another with small difference, Niew. Arch. Wisk. (3) 20, 54–67, 1972.

[5] P.R. Varshamov and G.M. Tennengolts, A code which corrects single asymmetric errors (Russian) Avtomat. Telemeh. 26, 282–292, 1965.

[6] P.R. Varshamov, A class of codes for asymmetric channels and a problem from the additive theory of numbers, IEEE Trans. Inform. Theory, IT–19, No. 1, 92–95, 1973.