On the properness of some optimal binary linear codes and their dual codes

R. Dodunekova, M.Xiaolei Hu

Chalmers University of Technology and the University of Gothenburg

ACCT 2008, June 16-22, Pamporovo

Contents

Introduction

• The error detecting performance of a linear code depends on the probability that it fails to detect transmission errors.

• The code is proper if this probability is an increasing function of the channel symbol error probability.

• Codes optimal in different ways or close to optimal turn out to be proper.

• Are properness and optimality closely related? How?

Linear codes.

• C - a linear $[n, k, d]_q$ code over the finite field of q elements $GF(q)$.

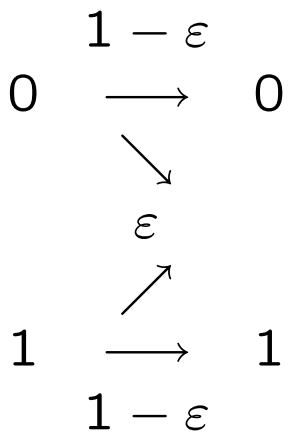
(C is a k-dimensional subspace of the n-dimensional vector space $GF(q)^n$, with Hamming code distance d. The code distance is just the minimum Hamming weight in C. The Hamming weight of a vector equals the number of non-zero positions in it.)

• C is used to detect transmission errors on a q-ary discrete memoryless channel with symbol error probability ε.

Binary symmetric memoryless channel: mathematical model

Natural restriction: $0 \leq \varepsilon \leq \frac{q-1}{q}$ **It is more likely for a symbol to remain unchanged**

Binary symmetric channel:



$0 \leq \varepsilon \leq 1/2$

The channel is memoryless when the separate uses of it are independent.

Error detection with a linear code

- Let $\mathrm{x} \in \mathrm{C}$ denote the code word transmitted and $\mathrm{y} \in \mathrm{GF(q)^n}$ be the vector received.

- When y is not a codeword the decoder makes the correct decision that a transmission error has occurred.

- When y is a codeword, the decoder decides that y was sent. Such a decision is incorrect when y and x are different.

Transmission error remains undetected $\Leftrightarrow$ $y - x \in C$, $y - x \neq 0$.

The probability of undetected error

- **The weight distribution** of an $[n, k, d]_q$ code C is

$$\{A_i,\ A_i = \#\ \text{ of codewords in } C \text{ of weight } i, \quad 0 \le i \le n\}.$$

- **The probability of undetected error**

$$P_{ue}(C, \varepsilon) = \sum_{i=d}^{n} A_i \left(\frac{\varepsilon}{q-1}\right)^i (1-\varepsilon)^{n-i}, \quad 0 \le \varepsilon \le \frac{q-1}{q}.$$

To find a code which is best for error detection...

- In error detection over a particular channel, codes with the smallest probability of undetected error would be best.

- One has to use exhaustive search in order to find such a code

- Even if we had an efficient method for finding the optimal code, this does not solve the problem, since most often ε is not known exactly.

- For this reason the concept of a proper code has been introduced.

Proper error detecting codes

Cheong, Barnes, Friedman 1979, Kasami-Lin 1984, Kløve, V. Korzhik 1995

A linear code is proper, if its undetected error probability is an increasing function of ε.

Thus a proper code performs better on better channels (with smaller symbol error probability), which makes the code appropriate for use in error detection over channels where ε is not known exactly.

Another view to properness

- In the set of $[n,k]_q$ systematic codes, the averaging procedure gives an increasing function (Massey 1978, Wolf and Michelson 1982)

$$P_{ue}(\varepsilon) = q^{-(n-k)}[1-(1-\varepsilon)^k],$$

- In the set of binary $[n,k]$ codes the average undetected error probability is also an increasing function (Cheong and Hellman 1976)

$$P_{ue}(\varepsilon) = \frac{2^k-1}{2^n-1}[1-(1-\varepsilon)^n].$$

Hence a hypothetical "average" code in the class would be proper. In this sense a proper code is similar to an "average" code, which makes the code a reasonable choice in situations where we can't do better.

Keep close to the average if you can't do better!

The question of interest

• **Codes, optimal in some sense, or close to optimal, are prevailing in the list of proper codes** (See Dodunekova, Dodunekov, Nikolova, 2008).

We want to address the question, whether properness and optimality are closely related and how.

• **As a first step, we have studied some length-optimal binary codes** (Jaffe and Bouyukliev, 2001)

The extended binomial moments

• **The extended binomial moments** of an $[n, k, d]_q$ linear code C with weight distribution $\{A_0, A_1, \ldots, A_n\}$ are defined as (Dodunekova and Dodunekov, 1997, 2004)

$$A_\ell^* = \sum_{i=d}^{\ell} \frac{\ell(\ell-1)\ldots(\ell-i+1)}{n(n-1)\ldots(n-i+1)} A_i, \quad d \le \ell \le n,$$
$$A_\ell^* = 0, \quad 0 \le \ell \le d-1.$$

• **They are related to the extended binomial moments of the dual code B_ℓ^* in the way**

$$B_\ell^* + 1 = q^{\ell-k}(A_{n-\ell}^* + 1), \quad \ell = 0, \ldots, n.$$

Discrete sufficient conditions for properness.

Let $d^\perp$ be the dual Hamming distance.

Theorem 1.(Dodunekova and Dodunekov,1997) If

$$A^*_\ell \geq qA^*_{\ell-1}, \quad \ell = d+1, \ldots n-d^\perp+1,$$

then C is proper.

Theorem 2. (Dodunekova and Nikolova, 2005) Suppose C is binary. If

$$\max(d, d^\perp) \geq \left\lceil \frac{n}{2} \right\rceil$$

or

$$\left\lceil \frac{n}{3} \right\rceil + 1 \leq d^\perp \leq \left\lfloor \frac{n}{2} \right\rfloor \quad \text{and} \quad n(n+1-2d^\perp) \leq d(n-d^\perp),$$

then C is proper.

Bounds on the extended binomial moments

Theorem 3. (Dodunekova 2005) The extended binomial moment satisfy

$$\max\{0,\ q^{\ell-n+k}-1\} < A^*_\ell < q^{\min(\ell+1-d,\ k+1-d^\perp)}-1, \quad \ell = d,\ldots,n-d^\perp$$
$$A^*_\ell = q^{\ell-n+k}-1, \quad \ell = n-d^\perp+1,\ldots,n.$$

Properness and optimal linear binary codes of dimension at most 7

An $[n, k, d]$ code is **distance-optimal** if no $[n, k, d-1]$ code exists; it is **length-optimal** (**which is stronger**) if no $[n-1, k, d]$ code exists, and **optimal**, if no $[n+1, k+1, d]$ or $[n+1, k, d+1]$ code exists. **An optimal code cannot be obtained by shortening or puncturing other binary linear codes.** (Jaffe and Bouyukliev 2001)

Summary of optimal binary codes with $k \leq 7$, $n \leq 2^k$

$[n,k,d]$	# codes ($form.equiv.$)	$[n,k,d]$	# codes ($form.equiv.$)	$[n,k,d]$	# codes ($form.equiv.$)
$[8,4,4]$	1	$[12,4,6]$	1	$[16,5,8]$	1
$[21,5,10]^*$	2	$[24,5,12]$	1	$[28,5,14]$	1
$[32,6,16]$	1	$[38,6,18]$	1	$[45,6,22]$	1
$[48,6,24]$	1	$[53,6,26]$	2	$[56,6,28]$	1
$[60,6,30]$	1	$[24,7,10]^*$	6(5)	$[27,7,12]$	1
$[40,7,18]$	172(46)	$[43,7,20]$	7(3)	$[56,7,26]^*$	> 19000
$[59,7,28]$	143(38)	$[64,7,32]$	1	$[71,7,34]$	1
$[75,7,36]^*$	3603	$[79,7,38]$	216(22)	$[82,7,40]$	11(7)
$[87,7,42]$	55(36)	$[90,7,44]$	6(6)	$[93,7,46]$	1
$[96,7,48]$	1	$[102,7,50]^*$	3	$[105,7,52]$	1
$[109,7,54]$	1	$[112,7,56]$	1	$[117,7,58]$	2
$[120,7,60]$	1	$[124,7,62]$	1		

Main result

Theorem 4. All codes in the above table and their duals are proper, except those marked by an asterisk.

The proof uses Theorems 1 and 2 mentioned above. We have used Matlab for computing the extended binomial moments of the codes and their duals and for checking the conditions of theorems 1 and 2. Information about weight distributions and dual code distances has been taken from

Jaffe and Bouyukliev 2001, http://www.codetables.de/

http://www.math.unl.edu/∼djaffe2/
codes/webcodes/binary/codes.cgi?n=28k=5

Comments

Some of the above proper codes lie on the Griesmer bound, i.e., $n = \sum_0^{k-1} \lceil \frac{d}{2^i} \rceil$. It has been noticed earlier that Griesmer codes tend to satisfy the conditions of Theorem 2.

The extended binomial moments have shown to be a useful tool in the study of the undetected error probability function.

It turns out that the extended binomial moments of the optimal proper codes almost lie on the lower bound in Theorem 3.

Thank you for your attention