

# REPORTS IN INFORMATICS

ISSN 0333-3590

Necessary conditions for codes to be good  
for error detection

Irina Naydenova, Torleiv Kløve

REPORT NO 342

January 2007



*Department of Informatics*  
**UNIVERSITY OF BERGEN**  
*Bergen, Norway*

This report has URL <http://www.ii.uib.no/publikasjoner/texrap/ps/2007-342.ps>  
Reports in Informatics from Department of Informatics, University of Bergen, Norway, is  
available at <http://www.ii.uib.no/publikasjoner/texrap/>.

Requests for paper copies of this report can be sent to:  
Department of Informatics, University of Bergen, Høyteknologisenteret,  
P.O. Box 7800, N-5020 Bergen, Norway

# Necessary conditions for codes to be good for error detection

Irina Naydenova, Torleiv Kløve  
Department of Informatics  
University of Bergen, Norway  
Irina.Gancheva@ii.uib.no, Torleiv.Klove@ii.uib.no

## Abstract

Codes for error detection on a  $q$ -ary symmetric channel are studied. It is shown that for given  $M$ ,  $d$ , and  $A$ , there exists a value  $\mu(d, \kappa)$ , where  $\kappa = \ln M - \ln A$ , such that if  $C$  is an  $(n, M, d)$  code with  $A_d \geq A$  and  $n \geq \mu(d, \kappa)$ , then  $C$  is not good for error detection. Explicit approximations for  $\mu(d, \kappa)$  are given.

## 1 Introduction

The  $q$ -ary symmetric channel with symbol probability  $p$ , where  $0 \leq p \leq \frac{q-1}{q}$ , is defined as follows: symbols from  $GF(q)$  are transmitted over the channel, and

$$P(b \text{ received} \mid a \text{ sent}) = \begin{cases} 1 - p & b = a \\ \frac{p}{q-1} & b \neq a \end{cases}$$

An  $(n, M)_q$  code is a subset of  $GF(q)^n$  of size  $M$ . The vectors of the code are called codewords. The minimum distance  $d$  of a code is the smallest (Hamming) distance between any two distinct codewords. Sometimes  $d$  is included in the notation of the code:  $(n, M, d)_q$ . The distance distribution of a code  $C$  is  $A_i$ ,  $i = 0, 1, \dots, n$  where

$$A_i = \frac{1}{M} \#\{(c, c') \in C \times C \mid d(c, c') = i\}.$$

Note that  $A_0 = 1$ ,  $A_i = 0$  for  $0 < i < d$ , and  $A_d > 0$ .

Suppose that an  $(n, M, d)_q$  code  $C$  is used for error detection for transmission over the  $q$ -ary symmetric channel with symbol error probability  $p$ . The probability of undetected error for  $C$  is denoted by  $P_{\text{ue}}(C, p)$ . For most codes we are not able to determine the value of  $P_{\text{ue}}(C, p)$  exactly. Therefore, it is useful to have estimates.  $C$  is called *good* (for error detection) if

$$P_{\text{ue}}(C, p) \leq P_{\text{ue}}(C, (q-1)/q) = \frac{M-1}{q^n} \quad (1)$$

for all  $p \in (0, (q-1)/q)$ . Only some codes have this property. The purpose of this paper is to show that, for given  $\kappa$  and  $d$ , there exists a value  $\mu(d, \kappa)$  such that if  $n \geq \mu(d, \kappa)$  and  $C$  is an  $(n, M, d)_q$  code such that  $A_d \geq A$ , where  $\ln A = \ln M - \kappa$ , then  $C$  is not good for error detection. Further, we give approximations of  $\mu(d, \kappa)$ .

## 2 Existence of $\mu(d, \kappa)$

The probability of undetected error for  $C$  on a symmetric channel with symbol error probability  $p$  is given by (see e.g. [1])

$$P_{\text{ue}}(C, p) = \sum_{i=1}^n A_i \left( \frac{p}{q-1} \right)^i (1-p)^{n-i}. \quad (2)$$

Define

$$P_{\text{ue}}^\perp(C, p) = \frac{1}{M} \sum_{i=0}^n A_i (1-Qp)^i - (1-p)^n, \quad (3)$$

where  $Q = q/(q-1)$ . If  $C$  is linear,

$$P_{\text{ue}}(C^\perp, p) = P_{\text{ue}}^\perp(C, p). \quad (4)$$

Recall that  $C$  is good if  $P_{\text{ue}}(C, p) \leq (M-1)q^{-n}$  for all  $p \in (0, (q-1)/q)$ . We call  $C$  *bad* (for error detection) if  $P_{\text{ue}}(C, p) > (M-1)q^{-n}$  for some  $p \in (0, (q-1)/q)$  and  $C$  is *ugly* if  $P_{\text{ue}}(C, p) \geq Mq^{-n}$  for some  $p \in (0, (q-1)/q)$ . Clearly, being ugly is a stronger condition than not bad. We note that most codes are either good or ugly, but a code may be neither.

**Lemma 1** *Let  $C$  be an  $(n, M)_q$  code and suppose that  $P_{\text{ue}}^\perp(C, p) \geq 1/M$  for some  $p \in (0, (q-1)/q)$ . Define  $\pi$  by*

$$1 - Qp = \frac{\pi}{(q-1)(1-\pi)}.$$

*Then  $P_{\text{ue}}(C, \pi) \geq Mq^{-n}$ .*

*Proof.* We have

$$1 - p = \frac{1}{q(1-\pi)}$$

and so

$$\begin{aligned} 0 &\leq MP_{\text{ue}}^\perp(C, p) - 1 \\ &= \sum_{i=1}^n A_i (1-Qp)^i - M(1-p)^n \\ &= (1-\pi)^{-n} \left\{ \sum_{i=1}^n A_i \left( \frac{\pi}{q-1} \right)^i (1-\pi)^{n-i} - Mq^{-n} \right\} \\ &= (1-\pi)^{-n} \{P_{\text{ue}}(C, \pi) - Mq^{-n}\}. \end{aligned}$$

Hence  $P_{\text{ue}}(C, \pi) \geq Mq^{-n}$ . □

Since  $\pi \in (0, (q-1)/q)$ , we immediately get the following corollary.

**Corollary 1** *If  $C$  is an  $(n, M)_q$  code and  $P_{\text{ue}}^\perp(C, p) \geq 1/M$  for some  $p \in (0, (q-1)/q)$ , then  $C$  is ugly.*

**Corollary 2** *If  $C$  is linear, then  $C$  is ugly if and only if  $C^\perp$  is ugly.*

*Proof.* The if part follows directly from (4) and Corollary 1. Since  $C^{\perp\perp} = C$  we get the if and only if. □

**Remark 1.** For  $q = 2$ , Corollary 2 is Theorem 3.4.2, part 1 in [1]. The proof for general  $q$  given above is a generalization of the proof for  $q = 2$  given in [1].

Remark 2. It is not the case, for linear codes, that  $C$  bad implies that  $C^\perp$  is bad.

We want to find sufficient conditions for a code to be ugly. For a linear code, a general lower bound on  $A_d$  is  $q-1$ , and for a non-linear code a general lower bound on  $A_d$  is  $2/M$ . Now, let  $A$  be some positive number. We will consider  $(n, M, d)_q$  codes for which  $A_d \geq A$ . In the rest of the paper we also use the notation

$$\kappa = \ln(M/A) = \ln M - \ln A.$$

By definition,

$$P_{\text{ue}}^\perp(C, p) \geq \frac{1}{M} + \frac{A}{M}(1 - Qp)^d - (1 - p)^n.$$

Hence, if

$$\frac{A}{M}(1 - Qp)^d \geq (1 - p)^n, \quad (5)$$

then  $P_{\text{ue}}^\perp(C, p) \geq \frac{1}{M}$ . Taking logarithms in (5), we get the equivalent condition

$$-\kappa + d \ln(1 - Qp) \geq n \ln(1 - p).$$

Combining this with Corollary 1, we get the following lemma.

**Lemma 2** *If  $C$  is an  $(n, M, d)_q$  code and*

$$n \geq h(p) = \frac{d \ln(1 - Qp) - \kappa}{\ln(1 - p)},$$

*then  $C$  is ugly.*

Any choice of  $p$ ,  $0 < p < (q-1)/q$  now gives a proof of the existence of a  $\mu(d, \kappa)$  such that if  $n \geq \mu(d, \kappa)$  and  $C$  is an  $(n, M, d)$  code with  $A_d \geq A$ , then  $C$  is ugly for error detection. To get the strongest result from the lemma, we want to find the  $p$  that minimizes  $h(p)$ . We can not find a closed formula for this, but consider approximations.

We will use the notations

$$f(p) = \frac{\ln(1 - Qp)}{\ln(1 - p)}, \text{ and } g(p) = \frac{-1}{\ln(1 - p)}.$$

Then

$$h(p) = d f(p) + \kappa g(p). \quad (6)$$

The function  $f(p)$  is increasing on  $(0, (q-1)/q)$ , it approaches the value  $Q$  when  $p \rightarrow 0+$ , and it approaches infinity when  $p \rightarrow (q-1)/q-$ . Moreover,

$$f'(p) = \frac{-Q(1-p)\ln(1-p) + (1-Qp)\ln(1-Qp)}{(1-p)(1-Qp)\ln(1-p)^2},$$

and

$$f''(p) = \frac{f_1(p)}{-(1-p)^2(1-Qp)^2(\ln(1-p))^3},$$

where

$$\begin{aligned} f_1(p) &= Q^2(1-p)^2(\ln(1-p))^2 \\ &\quad + 2Q(1-p)(1-Qp)\ln(1-p) \\ &\quad - 2(1-Qp)^2\ln(1-Qp) \\ &\quad - (1-Qp)^2\ln(1-p)\ln(1-Qp) \\ &> 0 \end{aligned}$$

for all  $p \in (0, (q-1)/q)$ . Hence  $f$  is convex on  $(0, (q-1)/q)$ . Similarly, the function  $g(p)$  is decreasing on  $(0, (q-1)/q)$ , it approaches infinity when  $p \rightarrow 0+$ , and it takes the value  $-1/\ln q$  for  $p = (q-1)/q$ . Moreover,

$$g'(p) = \frac{-1}{(1-p)\ln(1-p)^2} = \frac{-(1-Qp)}{(1-p)(1-Qp)\ln(1-p)^2},$$

$$g''(p) = \frac{-(2+\ln(1-p))}{(1-p)^2(\ln(1-p))^3} > 0$$

for all  $p \in (0, (q-1)/q)$ , and so  $g(p)$  is also convex on  $(0, (q-1)/q)$ . This implies that the combined function  $h(p)$  is also convex on  $(0, (q-1)/q)$  since  $\kappa > 0$ , and it takes its minimum somewhere in  $(0, (q-1)/q)$ . We denote this minimum by  $\mu(d, \kappa)$ .

From Corollary 1 and Lemma 2 we get the following necessary condition for a code to be good.

**Corollary 3** *If  $C$  is good for error detection, then  $n < \mu(d, \kappa)$ .*

We next consider  $d \geq \kappa$  and  $\kappa \geq d$  separately. In particular, we find approximations for  $\mu(d, \kappa)$  when  $d \gg \kappa$  or  $\kappa \gg d$ . We denote by  $p_m$  the value of  $p$  where  $h(p)$  has its minimum; this minimum is by definition  $\mu(d, \kappa)$ .

### 3 On $\mu(d, \kappa)$ when $d \geq \kappa$

In this section, we let  $\kappa = \alpha d$ , where  $\alpha$  is a parameter,  $0 \leq \alpha \leq 1$ . Then

$$h(p) = d \frac{\ln(1-Qp) - \alpha}{\ln(1-p)}$$

and

$$\frac{h'(p)}{d} = \frac{-Q(1-p)\ln(1-p) + (1-Qp)\ln(1-Qp)}{(1-p)(1-Qp)\ln(1-p)^2} - \frac{\alpha}{(1-p)\ln(1-p)^2}.$$

In particular  $h'(p) = 0$  if (and only if)

$$\alpha = \frac{-Q(1-p)\ln(1-p) + (1-Qp)\ln(1-Qp)}{1-Qp}. \quad (7)$$

We want to solve this for  $p$  in terms of  $\alpha$ . There is no closed form of this solution. However, we can find good approximations. For  $\alpha \rightarrow 0+$ , we see that  $p \rightarrow 0$  and  $h(p) \rightarrow Q$ . We will first study this important case in more details. We note that  $\alpha \rightarrow 0+$  implies that  $d \rightarrow \infty$ . The parameter  $\kappa$  may also grow, but then at a slower rate (since  $d/\kappa \rightarrow 0$ ).

**Theorem 1** *Let*

$$y = \sqrt{\frac{\alpha}{2Q(Q-1)}}.$$

*There exist numbers  $a_i$  and  $b_i$  for  $i = 1, 2, \dots$  such that, for any  $r \geq 0$ ,*

$$p_m = \sum_{i=1}^r a_i y^i + O(y^{r+1}),$$

*and*

$$\mu(d, \alpha d) = dQ \left\{ 1 + 2(Q-1) \sum_{i=1}^r b_i y^i + O(y^{r+1}) \right\}$$

when  $y \rightarrow 0$  (that is  $\alpha \rightarrow 0$ ). The first few  $a_i$  and  $b_i$  are given by the following table:

$$\begin{aligned}
a_1 &= 2, \\
a_2 &= -(8Q + 2)/3, \\
a_3 &= (26Q^2 + 22Q - 1)/9, \\
a_4 &= -(368Q^3 + 708Q^2 - 12Q + 8)/135, \\
b_1 &= 1, \\
b_2 &= (2Q - 1)/3, \\
b_3 &= (2Q^2 - 2Q - 1)/18, \\
b_4 &= -2(Q - 2)(2Q - 1)(Q + 1)/135.
\end{aligned}$$

Proof: First we note that  $\alpha = 2Q(Q - 1)y^2$  and so

$$h(p) = d \frac{\ln(1 - Qp) - 2Q(Q - 1)y^2}{\ln(1 - p)},$$

and

$$h'(p) = d \frac{H(p, y)}{(1 - p)(1 - Qp)(\ln(1 - p))^2},$$

where

$$\begin{aligned}
H(p, y) &= -Q(1 - p) \ln(1 - p) + (1 - Qp) \ln(1 - Qp) \\
&\quad - 2Q(Q - 1)y^2(1 - Qp).
\end{aligned}$$

Hence  $h'(p) = 0$  if  $H(p, y) = 0$ . Taking the Taylor expansion of  $H(\sum a_i y^i, y)$  we get

$$\begin{aligned}
H\left(\sum a_i y^i, y\right) &= \frac{a_1^2 - 4}{4} y^2 \\
&\quad + \frac{a_1}{6} (Qa_1^2 + a_1^2 + 6a_2 + 12Q) y^3 + \dots
\end{aligned}$$

All coefficients for  $i \leq r$  should be zero. In particular, the coefficient of  $y^2$  shows that  $a_1^2 = 4$ . Since  $a_1 y^2$  is the dominating term in the expression for  $p$  when  $y$  is small and  $p > 0$ , we must have  $a_1 > 0$  and so  $a_1 = 2$ . Next the coefficient of  $y^3$  shows that  $a_2 = -(16Q + 4)/6$ . In general, we get equations in the  $a_i$  which can be used to determine the  $a_i$  recursively. The recursions seems to be quite complicated in general and we have not found an explicit general expression for  $a_i$ . Substituting the expression for  $p$  into  $h(p)$  and taking Taylor expansion, we get the expression for  $\mu(d, \kappa)$ .  $\square$

Remark. We do not know when the infinite series  $\sum_{i=1}^{\infty} a_i y^i$  and  $\sum_{i=1}^{\infty} b_i y^i$  converge (we believe that they do, but it may depend on  $q$ ).

Assuming that  $\kappa\alpha \rightarrow 0$  and taking the first three terms of approximation, we get

$$\mu(d, \kappa) \approx dQ + \sqrt{2d\kappa Q(Q - 1)} + \frac{2Q - 1}{3} \kappa, \quad (8)$$

(the other terms goes to zero with  $y$ ).

Because of the big  $O$  term in Theorem 1, we do not know if the approximation is smaller or larger than the exact value. Only for approximations larger than  $\mu(d, \kappa)$  we can be sure that the corresponding code is ugly. We will call such approximations *upper* approximations.

By definition,  $h(p)$  is an upper approximation for any  $p$ . One way to get a good upper approximation is to choose for  $p$  a good approximation for  $p_m$ . For example,

taking the first term in the approximation for  $p_m$ , that is,  $p = \sqrt{2\alpha/(Q(Q-1))}$ , we get

$$\mu(d, \kappa) \leq h\left(\sqrt{2\alpha/(Q(Q-1))}\right). \quad (9)$$

**Example 1** Consider  $q = 2$ ,  $A = 1$  (valid for all linear codes),  $d = 1000$  and  $M = 4$ . Then  $\kappa = 2 \ln 2$  and  $\alpha \approx 0.001386$ . Solving  $h'(p) = 0$  numerically, we get  $p \approx 0.0352540$  and  $\mu(1000, 2 \ln 2) \approx 2075.8565430$ . Taking one, two, three, and four terms respectively in the expression for  $\mu(1000, 2 \ln 2)$  in Theorem 1, as well as the bound (9), we get the following approximations:

| no. of terms |          | value        |
|--------------|----------|--------------|
| 1            |          | 2000         |
| 2            |          | 2074.4659482 |
| 3            | = eq.(8) | 2075.8522426 |
| 4            |          | 2075.8565439 |
|              | eq.(9)   | 2075.9808954 |

We have computed the integers  $\lceil \mu(d, \kappa) \rceil$ ,  $\lceil \text{eq.}(8) \rceil$ , and  $\lceil \text{eq.}(9) \rceil$  for a number of different values of  $d$ . When  $d$  is large then these values differ by at most one, and when  $d$  decreases the difference between the values increases slowly.

The approximation (8) is good for  $\alpha \approx 0$ . When  $\alpha > 0$ , the terms after the third term do not go to zero. However, the approximation in Theorem 1 may still be quite good. We have made some numeric computations that illustrate this. We use the following notations:

$$\eta(\alpha) = \frac{\mu(d, \alpha d)}{d} \text{ and } \nu_r(\alpha) = Q + 2Q(Q-1) \sum_{i=1}^r b_i y^i \quad (10)$$

From the table in Theorem 1, we see that  $b_2 > 0$  for all  $Q$  (remember that  $Q = q/(q-1) \in (1, 2]$ ). Further,  $b_3 > 0$  for  $q = 2$  and  $q = 3$ , but  $b_3 < 0$  for  $q \geq 4$ . Finally,  $b_4 = 0$  for  $q = 2$  and  $b_4 > 0$  for  $q > 2$ . Hence, for all  $\alpha > 0$

$$\begin{aligned} \text{for } q = 2, \quad & \nu_2(\alpha) < \nu_3(\alpha) = \nu_4(\alpha), \\ \text{for } q = 3, \quad & \nu_2(\alpha) < \nu_3(\alpha) < \nu_4(\alpha), \\ \text{for } q \geq 4, \quad & \nu_3(\alpha) < \min\{\nu_2(\alpha), \nu_4(\alpha)\}. \end{aligned}$$

A simple calculation shows that for  $q \geq 4$  we have  $\nu_4(\alpha) > \nu_2(\alpha)$  if and only if

$$\alpha > \omega_q \stackrel{\text{def}}{=} \frac{135^2(2Q^2 - 2Q - 1)^2 Q(Q-1)}{2 \cdot 18^2(Q-2)^2(2Q-1)^2(Q+1)^2}.$$

When  $q$  increases, the value of  $\omega_q$  increases from  $\omega_4 \approx 0.023$  to  $\omega_9 \approx 0.378$  and then decreases and approaches zero when  $q \rightarrow \infty$ .

**Example 2** In this example we consider  $q = 2$ . For all values of  $\alpha$  we have computed,  $\nu_2(\alpha) < \eta(\alpha) < \nu_3(\alpha)$ . Some examples are given in the following table.

| $\alpha$  | $\eta(\alpha)$ | $\nu_2(\alpha) - \eta(\alpha)$ | $\nu_3(\alpha) - \eta(\alpha)$ |
|-----------|----------------|--------------------------------|--------------------------------|
| $10^{-6}$ | 2.00200100008  | $-8.33 \cdot 10^{-11}$         | $1.28 \cdot 10^{-17}$          |
| $10^{-3}$ | 2.06424818804  | $-2.63 \cdot 10^{-6}$          | $3.95 \cdot 10^{-10}$          |
| 0.1       | 2.73505913571  | $-2.60 \cdot 10^{-3}$          | $3.16 \cdot 10^{-5}$           |
| 1         | 5.07687209474  | $-7.68 \cdot 10^{-2}$          | $6.46 \cdot 10^{-3}$           |
| 10        | 20.16721044856 | -1.84                          | $7.93 \cdot 10^{-1}$           |

We see that  $\nu_3(\alpha)$  gives a quite good upper approximation to  $\eta(\alpha)$  for all  $\alpha \leq 1$  and even for larger values of  $\alpha$ .

**Example 3** Now, consider  $q = 10$ . We have  $\omega_{10} \approx 0.37435$ . For all values of  $\alpha$  we have computed,  $\nu_3(\alpha) < \eta(\alpha) < \min\{\nu_2(\alpha), \nu_4(\alpha)\}$ . Some examples are given in the following table.

| $\alpha$  | $\eta(\alpha)$ | $\nu_2(\alpha) - \eta(\alpha)$ | $\nu_3(\alpha) - \eta(\alpha)$ | $\nu_4(\alpha) - \eta(\alpha)$ |
|-----------|----------------|--------------------------------|--------------------------------|--------------------------------|
| $10^{-6}$ | 1.11160842243  | $8.41 \cdot 10^{-11}$          | $-1.37 \cdot 10^{-13}$         | $2.21 \cdot 10^{-16}$          |
| $10^{-3}$ | 1.12722947097  | $2.53 \cdot 10^{-6}$           | $-1.31 \cdot 10^{-7}$          | $6.63 \cdot 10^{-9}$           |
| 0.1       | 1.30724978395  | $1.74 \cdot 10^{-3}$           | $-9.26 \cdot 10^{-4}$          | $4.50 \cdot 10^{-4}$           |
| 0.37435   | 1.55839493272  | $9.26 \cdot 10^{-3}$           | $-1.00 \cdot 10^{-2}$          | $9.26 \cdot 10^{-3}$           |
| 1         | 1.98651890138  | $2.89 \cdot 10^{-2}$           | $-5.53 \cdot 10^{-2}$          | $8.23 \cdot 10^{-2}$           |
| 10        | 6.50984287366  | $2.47 \cdot 10^{-1}$           | -2.42                          | 11.345                         |

Also for  $q = 10$ , we get good upper approximations even for  $\alpha = 10$ .

## 4 On $\mu(d, k)$ when $\kappa \geq d$

In this section, we let  $d = \beta\kappa$ , where  $\beta$  is a parameter,  $0 \leq \beta \leq 1$ . Then

$$h(p) = \kappa \frac{\beta \ln(1 - Qp) - 1}{\ln(1 - p)}$$

and

$$\begin{aligned} \frac{h'(p)}{\kappa} &= \beta \frac{(-Q(1-p)\ln(1-p) + (1-Qp)\ln(1-Qp))}{(1-p)(1-Qp)\ln(1-p)^2} \\ &= -\frac{1}{(1-p)\ln(1-p)^2}. \end{aligned}$$

In particular  $h'(p) = 0$  if (and only if)

$$\beta = \frac{1 - Qp}{-Q(1-p)\ln(1-p) + (1-Qp)\ln(1-Qp)}. \quad (11)$$

We want to solve this for  $p$  in terms of  $\beta$ , but again there is no closed form of this solution. We first consider approximations for  $\beta \rightarrow 0+$ . This implies that  $\kappa \rightarrow \infty$ ;  $d$  may also increase, but then at a slower rate. For  $\beta \rightarrow 0+$ , we see that  $p_m \rightarrow 1/Q$  (that is,  $1 - Qp_m \rightarrow 0$ ) and  $h(p_m) \rightarrow \kappa/\ln q$ .

**Theorem 2** Let

$$\lambda = \ln q \quad \text{and} \quad \Lambda = \ln(\beta\lambda/(q-1)).$$

There exist polynomials  $A_i(x)$  and  $B_i(x)$  for  $i = 0, 1, 2, \dots$  such that, for any  $r \geq 0$ ,

$$1 - Qp_m = \frac{\lambda}{q-1} \sum_{i=1}^r A_i(\Lambda)\beta^i + O(\beta^{r+1}(\ln \beta)^{\deg A_{r+1}}),$$

and

$$\mu(\beta\kappa, \kappa) = \frac{\kappa}{\lambda} \left\{ \sum_{i=0}^r B_i(\Lambda)\beta^i + O(\beta^{r+1}(\ln \beta)^{\deg B_{r+1}}) \right\}$$

for  $\beta \rightarrow 0$ . The first few  $A_i(x)$  and  $B_i(x)$  are given by the following table:

$$\begin{aligned} A_1(x) &= x + \lambda - 1, \\ A_2(x) &= (2x^2 + (4\lambda - 2)x + 2\lambda^2 - 3\lambda)/2, \\ A_3(x) &= (6x^3 + 3(6\lambda - 1)x^2 - 3(-6\lambda^2 + 5\lambda + 2)x + 6\lambda^3 - 11\lambda^2 + 3)/6, \\ B_0(x) &= 1, \\ B_1(x) &= -(x - 1), \\ B_2(x) &= -(2x + \lambda - 2)/2, \\ B_3(x) &= -(3x^2 + 3\lambda x + \lambda^2 - 3)/6. \end{aligned}$$

Proof: Let  $\eta = q - 1$  and  $\pi = 1 - Qp$ . Then  $1 - p = (1 + \eta\pi)/q$  and  $Q(1 - p) = (1 + \eta\pi)/\eta$ . Hence

$$h'(p) = \kappa \frac{G(\pi, \beta)}{(1 - p)(1 - Qp) \ln(1 - p)^2},$$

where

$$G(\pi, \beta) = -\beta \frac{1 + \eta\pi}{\eta} \ln\left(\frac{1 + \eta\pi}{q}\right) + \beta\pi \ln \pi - \pi.$$

Therefore,  $h'(p) = 0$  if and only if  $G(\pi, \beta) = 0$ .

If  $\pi \rightarrow 0+$ , then  $\ln((1 + \eta\pi)/q) \rightarrow -\ln q$  and  $\pi \ln \pi \rightarrow 0$ . Hence, for small  $\pi$ ,

$$0 = \frac{G(\pi, \beta)}{\pi} \approx \frac{\ln q}{\eta} - \frac{\pi}{\beta}.$$

Therefore,  $\pi \approx \beta\lambda/\eta$ . We write  $\pi = \beta\lambda(1 + y)/\eta$  (where  $y$  will depend on  $\beta$ ). Then

$$\ln \pi = \Lambda + \ln(1 + y).$$

Hence, if  $\Gamma(y) = G(\pi, \beta)$  we get

$$\begin{aligned} \Gamma(y) = \frac{\beta}{\eta} \left\{ & -(1 + \beta\lambda(1 + y)) \ln(1 + \beta\lambda(1 + y)) \right. \\ & + (1 + \beta\lambda(1 + y))\lambda \\ & + \beta\lambda(1 + y)(\Lambda + \ln(1 + y)) \\ & \left. - \lambda(1 + y) \right\}. \end{aligned}$$

We now write  $y = \sum_{i=1}^r \alpha_i(\Lambda)\beta^i + O(\beta^{r+1})$ . Formally treating  $\Lambda$  as if it were a constant, we can take the Taylor expansion of  $\Gamma(y)$  in terms of  $\beta$  and we get an expansion of the form  $\sum_{i=1}^{\infty} c_i\beta^i$ , where the  $c_i$  are polynomials of  $\Lambda$ . Since these polynomials  $c_i$  must be identically zero, we get equations to determine the polynomials  $A_i(x)$ . Substituting the series of  $p_m$  into  $h(p)$  and taking the Taylor expansion, we get the series of  $\mu(\beta\kappa, \kappa)$ .  $\square$

Remark 1. To formally justify that we treat  $\Lambda$  as if it were a constant, we should prove that  $\Lambda$  is algebraically independent of the other quantities involved, that is, there is no non-trivial polynomial equation in  $\Lambda$  with coefficients expressed as rational functions of the remaining quantities. We have not done this, but it is highly likely that it is true.

Remark 2. Note that  $\Lambda \rightarrow -\infty$  when  $\beta \rightarrow 0+$ .

As to convergence, the situation is similar to Theorem 1.

Assuming that  $d\beta \ln \beta \rightarrow 0$  and taking the first two terms of the approximation we get

$$\mu(d, \kappa) \approx \frac{\kappa}{\ln q} - \frac{d}{\ln q} \left( \ln \left( \frac{d \ln q}{\kappa(q-1)} \right) - 1 \right), \quad (12)$$

(the other terms go to zero with  $\beta$ ).

Again because of the big  $O$  term in Theorem 2, we do not know if the approximation is smaller or larger than the exact value, but we have shown that the approximation is good when  $\beta \rightarrow 0$ .

Taking a good approximation for  $p_m$  and inserting this into  $h(p)$  we get good upper approximations. For example, taking the first term in the approximation for  $1 - Qp_m$ , that is,  $1 - Qp = \lambda\beta/(q - 1)$ , then we get

$$\mu(\beta\kappa, \kappa) \leq h \left( \frac{q - 1 - \beta \ln q}{q} \right) \quad (13)$$

**Example 4** Consider  $q = 2$ ,  $d = 2$ ,  $A = 1$ , and  $M = 2^{1000}$ . Then  $\kappa = 1000 \ln 2$  and  $\beta \approx 0.002885$ . Solving  $h'(p) = 0$  numerically, we get  $p \approx 0.4990185$  and  $\mu(2, 1000 \ln 2) \approx 1020.8737393$ . Taking one, two, three, and four terms respectively in the expression for  $\mu(2, 1000 \ln 2)$  in Theorem 2, as well as the bound (13), we get the following approximations:

| no. of terms |           | value        |
|--------------|-----------|--------------|
| 1            |           | 1000         |
| 2            | = eq.(12) | 1020.8169587 |
| 3            |           | 1020.8741384 |
| 4            |           | 1020.8737363 |
|              | eq.(13)   | 1021.219184  |

We have made numeric calculations for a number of  $\beta > 0$ . The terms after the second do not go to zero, but we may still get good approximations. We take two, three and four terms of the approximation. Here the notations are the following:

$$\sigma(\beta) = \frac{\mu(\beta\kappa, \kappa)}{\kappa} \text{ and } \xi_r(\beta) = \frac{1}{\ln q} \sum_{i=0}^r B_i(\Lambda) \beta^i \quad (14)$$

Simple calculations (we leave out the details) shows that

$$B_1(\Lambda) \geq 0 \text{ if and only if } \beta \leq \frac{e(q-1)}{\ln(q)},$$

where as usual  $e = \exp(1)$ ,

$$B_2(\Lambda) \geq 0 \text{ if and only if } \beta \leq \frac{e(q-1)}{\sqrt{q} \ln(q)},$$

and  $B_3(\Lambda) \geq 0$  if and only if  $q \leq 31$  and

$$\frac{q-1}{\sqrt{q} \ln(q)} \exp(-\Omega_q) \leq \beta \leq \frac{q-1}{\sqrt{q} \ln(q)} \exp(\Omega_q)$$

where  $\Omega_q = \sqrt{1 - \frac{(\ln(q))^2}{12}}$ .

**Example 5** Consider  $q = 2$ . We have  $B_1(\Lambda) \geq 0$  for  $\beta \leq 3.9217$ ,  $B_2(\Lambda) \geq 0$  for  $\beta \leq 2.7730$ , and  $B_3(\Lambda) \geq 0$  for  $0.3829 \leq \beta \leq 2.7175$ . For all the values of  $\beta$  we have computed,  $\xi_1(\beta) < \sigma(\beta)$ . For  $\beta \lesssim 0.686$  we have  $\xi_2(\beta) > \sigma(\beta)$ . For  $\beta \gtrsim 0.0859$  we have  $\xi_3(\beta) > \sigma(\beta)$ . Some selected values are given in the following table as an illustration.

| $\beta$   | $\sigma(\beta)$ | $\xi_1(\beta) - \sigma(\beta)$ | $\xi_2(\beta) - \sigma(\beta)$ | $\xi_3(\beta) - \sigma(\beta)$ |
|-----------|-----------------|--------------------------------|--------------------------------|--------------------------------|
| $10^{-6}$ | 1.4427169439    | $-2.14 \cdot 10^{-11}$         | $1.37 \cdot 10^{-16}$          | $-1.11 \cdot 10^{-21}$         |
| $10^{-3}$ | 1.4546436900    | $-1.14 \cdot 10^{-5}$          | $3.38 \cdot 10^{-8}$           | $-1.15 \cdot 10^{-10}$         |
| $10^{-1}$ | 2.0167210449    | $-4.47 \cdot 10^{-2}$          | $3.25 \cdot 10^{-3}$           | $4.83 \cdot 10^{-5}$           |
| 0.5       | 3.5174115967    | $-5.89 \cdot 10^{-1}$          | $2.88 \cdot 10^{-2}$           | $6.96 \cdot 10^{-2}$           |
| 1         | 5.0768720947    | -1.66                          | $-1.91 \cdot 10^{-1}$          | $5.01 \cdot 10^{-1}$           |

We note that

$$\eta(\alpha) = \frac{\mu(d, \alpha d)}{d} = \frac{\mu(\kappa/\alpha, \kappa)}{\kappa/\alpha} = \alpha \sigma(1/\alpha).$$

Therefore, we can compare the approximations given for  $\eta(\alpha)$  and  $\sigma(\beta)$ . For example, for  $\alpha = 1$ , the best upper approximation we got for  $\eta(1)$  has an error of  $6.46 \cdot 10^{-3}$  whereas the best upper approximation of  $\sigma(1)$  has an error of  $5.01 \cdot 10^{-1}$ . Even for  $\alpha = 2.5$  we get a better upper approximation using the best upper approximation to  $\eta(2.5)$ . However, for  $\alpha = 3$ , the upper approximation of  $3\sigma(1/3)$  is better.

**Example 6** For  $q = 10$  the situation is similar to  $q = 2$  and we give some select values without further comments.

| $\beta$   | $\sigma(\beta)$ | $\xi_1(\beta) - \sigma(\beta)$ | $\xi_2(\beta) - \sigma(\beta)$ | $\xi_3(\beta) - \sigma(\beta)$ |
|-----------|-----------------|--------------------------------|--------------------------------|--------------------------------|
| $10^{-6}$ | 0.4343015082    | $-6.53 \cdot 10^{-12}$         | $4.26 \cdot 10^{-17}$          | $-3.54 \cdot 10^{-22}$         |
| $10^{-3}$ | 0.4383243187    | $-3.52 \cdot 10^{-6}$          | $1.08 \cdot 10^{-8}$           | $-3.94 \cdot 10^{-11}$         |
| $10^{-1}$ | 0.6509842874    | $-1.41 \cdot 10^{-2}$          | $1.21 \cdot 10^{-3}$           | $-4.61 \cdot 10^{-5}$          |
| 0.5       | 1.2842347128    | $-1.86 \cdot 10^{-1}$          | $2.06 \cdot 10^{-2}$           | $1.35 \cdot 10^{-2}$           |
| 1         | 1.9865189014    | $-5.26 \cdot 10^{-1}$          | $4.18 \cdot 10^{-4}$           | $1.12 \cdot 10^{-1}$           |

## 5 The redundancy of linear codes

For a linear  $[n, k]$  code,  $\rho = n - k$  is its redundancy, and the relation  $n \geq \mu(d, \kappa)$  is of course equivalent to  $\rho \geq \mu(d, \kappa) - k$ . When  $A$  is relatively large, then  $\mu(d, \kappa) - k$  is relatively small. In this section, we consider this situation in some details when  $\beta \rightarrow 0+$ , that is,  $k \gg d$ .

We assume that  $d$  is fixed,  $n = \mu = \mu(d, \kappa)$  and  $A = \gamma n^\delta$  for some fixed positive  $\gamma$  and  $\delta \leq d$ . Then

$$\kappa = k \ln q - \ln \gamma - \delta \ln \mu < k\lambda. \quad (15)$$

Combining (15) and Theorem 2 (for  $r = 1$ ) we get

$$\mu = k - \frac{\delta \ln \mu}{\lambda} - \frac{\ln \gamma}{\lambda} + (1 - \Lambda) \frac{d}{\lambda} + O(\beta \ln \beta), \quad (16)$$

since  $\kappa \beta^2 \ln \beta = d \beta \ln \beta$  and  $d$  is fixed. In equation (16),  $\mu$  appears both on the left hand side and on the right hand side (both explicit and implicit in  $\Lambda$ ). However, the right hand side only contains  $\ln \mu$  so by bootstrapping we can show that  $\mu \approx k$  and  $\kappa \rightarrow \infty$ . We get  $\beta \ln \beta = \frac{d}{\kappa} (\ln d - \ln \kappa)$  and so  $O(\beta \ln \beta) = O(\frac{d}{\kappa} \ln \kappa) = O(\ln k/k)$ . We note that  $1 - \Lambda > 0$  for  $\kappa > \frac{\lambda d}{\epsilon(q-1)}$  and

$$1 - \Lambda = \ln \kappa + O(1)$$

and so

$$1 < \frac{\mu}{k} < 1 + \frac{d \ln \kappa}{\lambda k} + O\left(\frac{\ln k}{k^2}\right)$$

and

$$0 \leq \ln \mu - \ln k \leq O\left(\frac{\ln k}{k}\right),$$

that is,  $\ln \mu = \ln k + O\left(\frac{\ln k}{k}\right)$ . Substituting this in (15) and (16) and simplifying, we get the following theorem.

**Theorem 3** Let  $C$  be a linear  $[n, k]$  code with minimum distance  $d$ . Assume that  $A_d \geq \gamma n^\delta$ , where  $\delta \leq d$  and  $\gamma$  is some fixed positive number. If the redundancy  $\rho = n - k$  of the code satisfies

$$\rho \geq \frac{d - \delta}{\ln q} \ln k + \frac{1}{\ln q} (d + d \ln(q - 1) - \ln \gamma - d \ln d) + O\left(\frac{\ln k}{k}\right), \quad (17)$$

then the code is ugly for error detection.

Remark. When  $\delta = d$ , then the bound on the redundancy is a fixed number (it does not grow with  $k$ ). Note also that  $A_d \leq \binom{n}{d} \leq n^d/d!$ . Hence

$$-\ln \gamma \geq \ln d! \approx d \ln d - d + \frac{1}{2} \ln(2\pi d)$$

(by Stirling's formula) when  $\delta = d$ . Therefore, the right hand side of (17) is lower bounded by

$$\frac{1}{\ln q} \left\{ d \ln(q-1) + \frac{1}{2} \ln(2\pi d) \right\}.$$

**Example 7** Let  $C$  be a  $[\nu, \zeta]$  code with minimum distance  $d_C \geq 2$ . Let  $H$  is a parity-check matrix for  $C$ . Let  $C_t$  be the  $[t\nu, (t-1)\nu + \zeta]$  code with parity-check matrix  $H_t = H|H| \cdots |H$  (repeated  $t > 1$  times). The minimum distance of  $C_t$  is clearly 2, and it is easy to find a lower bound on  $A_2$ : first choose  $j$  such that  $1 \leq j \leq \nu$  (this can be done in  $\nu$  ways); next choose a pair  $(u, v)$  where  $0 \leq u < v < t$  (this can be done in  $t(t-1)/2$  ways); finally choose  $a \in GF(q) \setminus \{0\}$  (this can be done in  $q-1$  ways). In all, there are  $(q-1)\nu t(t-1)/2$  possible choices of  $j, u, v, a$ . Let  $\mathbf{x}_i$ ,  $i = 0, 1 \dots t\nu - 1$  be the columns of  $H_t$ . For each choice of  $j, u, v, a$  we have

$$a\mathbf{x}_{uv+j} + (-a)\mathbf{x}_{v\nu+j} = \mathbf{0}$$

(since  $\mathbf{x}_{uv+j} = \mathbf{x}_{v\nu+j}$ ). Hence

$$A_2 \geq A = (q-1)\nu t(t-1)/2 = \frac{(q-1)(1-1/t)}{2\nu} n^2.$$

The redundancy of  $C_t$  is  $\nu - \zeta$ . We note that

$$-\ln \gamma = \ln 2 + \ln \nu - \ln(q-1) - \ln(1-1/t).$$

By Theorem 3, if  $t \rightarrow \infty$  and

$$\nu - \zeta \geq \frac{1}{\ln q} \left\{ 2 + \ln(q-1) - \ln 2 + \ln \nu - \ln(1-1/t) + O\left(\frac{\ln t}{t}\right) \right\},$$

then  $C_t$  is ugly. Since  $\ln(1-1/t) \approx 1/t = o((\ln t)/t)$  we can conclude that if

$$\nu - \zeta > \frac{1}{\ln q} \{2 + \ln(q-1) - \ln 2 + \ln \nu\}, \quad (18)$$

then  $C_t$  is ugly for  $t$  sufficiently large.

As an example, let  $C$  be the binary extended  $l$  error correcting BCH code of length  $\nu = 2^m$  (where  $l \geq 2$ ). For this code,  $\nu - \zeta \geq 2m$  and the right hand side of (18) simplifies to  $m - 1 + 2/\ln 2 \approx m + 1.9$ . Hence, (18) is satisfied for all  $m \geq 3$  and so  $C_t$  is ugly for  $t$  sufficiently large.

## Acknowledgment

The research was supported by The Norwegian Research Council.

## References

- [1] T. Kløve and V. I. Korzhik, *Error Detecting Codes, General Theory and Their Application in Feedback Communication Systems*, Kluwer Acad. Publ., Boston, 1995.