# Error probabilities for bounded distance decoding

Andreas Faldum
Institut für Medizinische Biometrie, Epidemiologie und Informatik
Johannes-Gutenberg-Universität
D-55101 Mainz
Germany
e-mail: faldum@imbei.uni-mainz.de

Julio Lafuente and Gustavo Ochoa*
Departamento de Matemática e Informática
Universidad Pública de Navarra
Campus de Arrosadia
31006 Pamplona
Spain
email: lafuente@unavarra.es
email: ochoa@unavarra.es

Wolfgang Willems†
Institut für Algebra und Geometrie
Otto-von-Guericke-Universität
D-39016 Magdeburg
Germany
e-mail: wolfgang.willems@mathematik.uni-magdeburg.de

**Abstract. Decoding errors can be seen from the point of view of the receiver or the transmitter. This naturally leads to different functions for the decoding error probability. We study their behaviour and the relation between these two functions. Though both functions are equally good when used to compare two codes with respect to decoding errors only one of them reflects in general the properties such a function should have. This is not the function one usually considers in the literature when studying decoding errors. Both functions coincide only if the underlying code is perfect. The investigations in this paper can be seen as a continuation of earlier work of MacWilliams (see chap. 16.1 in [2]).**

*Both authors are supported by MTM2004-08219-C02-01.

†Part of this paper was written during a stay of the author in Pamplona in November 2004. The author would like to thank the Departamento de Matemática e Informática de la Universidad Pública de Navarra for its hospitality and financial support.

**Keywords:** Linear codes, bounded distance decoding, decoding error probabilities.

**Mathematics Subject Classification:** 94B05, 94B70

# 1 Introduction

The quality of an error-correcting code when used for data transmissions heavily depends on the speed of encoding and decoding algorithms and of course on the probability of erronous decoding. In this note we are interested in the latter question, i.e., on the probability that a decoded word is not the transmitted one. Clearly, this probability depends on the channel properties and the decoding strategy. Throughout the paper we assume that the channel is $q$-nary symmetric (qSC). Furthermore with $p \leq \frac{q-1}{q}$ we always denote the symbol error probability. Each symbol is assumed to be changed into another fixed symbol with probability $\frac{p}{q-1}$ when transmitted through the channel. For transmission we only use linear $[n, k, d]$ codes which are defined over finite fields with $q$ elements. In addition, we assume that all codewords are used with the same probability. On the receiver side we can take different decoding strategies. We may decode only up to $t \leq \frac{d-1}{2}$ errors or decode beyond that bound. In the latter case many attempts to understand the decoding error probabilities have been undertaken; see for instance [7], [8], [10] and the references given there. Thus in this paper we mainly focus on decoding errors if we correct only up to $t \leq \frac{d-1}{2}$ errors by choosing the codeword nearest to the received word (bounded distance decoding). Note that such a decoding procedure is incomplete since we do not take into account situations in which no codeword exists within distance $\leq t$ to the received word (decoding failure). The probability of decoding failure was already computed by MacWilliams (see chap. 16.1 of [2]). Furthermore decoding up to bounded distance is the classical situation for which fast algorithms exist. Clearly, we decode erroneously if the transmitter sends $c \in C$ and the receiver gets a word $w$ which has distance $\leq t$ to some codeword $c' \neq c$. Being more precise we may choose two different point of views.
From the side of the transmitter it is natural to ask:
*What is the probability* $\mathrm{P_{ue}}(C, t, p)$ *that a word* $w$ *with* $\mathrm{d}(w, c') \leq t$ *for some codeword* $c' \in C \setminus \{c\}$ *is received conditioned on* $c \in C$ *transmitted?*
More precisely, if

$$\mathrm{B}_t(c) = \{w \mid w \in \mathbb{F}_q^n,\ \mathrm{d}(c, w) \leq t\}$$

denotes the ball of radius $t$ with center $c$ then

$$\mathrm{P}_{ue}(C, t, p) = \mathrm{P}(Y \in \cup_{c \neq c' \in C} \mathrm{B}_t(c') \mid X = c)$$

where $X$ and $Y$ denote, respectively, the random variables "to send a codeword $c \in C$" and "to receive a word $w \in \mathbb{F}_q^n$". Note that this probability does not depend on the transmitted codeword $c$. Thus we may also write

$$\mathrm{P}_{ue}(C, t, p) = \mathrm{P}(Y \in \cup_{0 \neq c \in C} \mathrm{B}_t(c) \mid X = 0).$$

Therefore

$$\begin{aligned}
\mathrm{P}_{ue}(C,t,p) &= \sum_{0\neq c\in C}\ \sum_{v\in \mathrm{B}_t(c)} \mathrm{P}(Y=v \mid X=0)\\
&= \sum_{0\neq c\in C}\ \sum_{v\in \mathrm{B}_t(c)} \mathrm{P}(Y=-c+v \mid X=-c)\\
&= \sum_{0\neq c\in C}\ \sum_{w\in \mathrm{B}_t(0)} \mathrm{P}(Y=w \mid X=-c)\\
&= (|C|-1)\,\mathrm{P}(Y\in \mathrm{B}_t(0) \mid X\in C\setminus\{0\})\,.
\end{aligned}$$

If we write $A_i$ for the number of codewords which have weight $i$ and we specialize to $t=0$ we get

$$(*)\qquad \begin{aligned}
\mathrm{P}_{\mathrm{ue}}(C,0,p) &= \mathrm{P}(Y\in C\setminus\{0\} \mid X=0)\\
&= \sum_{i=1}^{n} A_i \left(\frac{p}{q-1}\right)^{i} (1-p)^{n-i}\\
&= (1-p)^n \sum_{i=1}^{n} A_i \left(\frac{p}{(q-1)(1-p)}\right)^{i}
\end{aligned}$$

Observe that this probability is often called the probability of undetected error. It has been studied in several papers (in case of a binary field see for instance [6]).
In contrast, from the side of the receiver it is natural to ask:
*What is the probability* $\mathrm{P}_{\mathrm{fd}}(C,t,p)$ *that* $c'\in C\setminus\{c\}$ *has been transmitted conditioned on some* $w$ *with* $\mathrm{d}(w,c)\le t\le \frac{d-1}{2}$ *received?*
Again, more precisely

$$\mathrm{P}_{\mathrm{fd}}(C,t,p) = \mathrm{P}(X\in C\setminus\{c\} \mid Y\in \mathrm{B}_t(c))\,,$$

or, under our assumptions on equiprobability

$$\mathrm{P}_{\mathrm{fd}}(C,t,p) = \mathrm{P}(X\in C\setminus\{0\} \mid Y\in \mathrm{B}_t(0))\,.$$

Then

$$\begin{aligned}
\mathrm{P}(Y\in \mathrm{B}_t(0))\cdot \mathrm{P}_{\mathrm{fd}}(C,t,p) &=\\
&= \mathrm{P}(X\in C\setminus\{0\}\,,\, Y\in \mathrm{B}_t(0))\\
&= \sum_{0\neq c\in C}\ \sum_{w\in \mathrm{B}_t(0)} \mathrm{P}(X=c\,,\, Y=w)\\
&= \sum_{0\neq c\in C}\ \sum_{w\in \mathrm{B}_t(0)} \mathrm{P}(Y=w \mid X=c)\cdot \mathrm{P}(X=c)\\
&= \frac{1}{|C|}\mathrm{P}_{\mathrm{ue}}(C,t,p)
\end{aligned}$$

Both probabilities have been studied in the literature; for the first see for instance [9], for the second [5]. Though they are different they have many properties in common as we will see. In particular they are equally good if we use them to find an optimal $[n, k, d]$ code ($n$ and $k$ fixed) with respect to decoding errors. In either case it turns out that for sufficiently small symbol error probability $p$ the quality of a code is only a question on the weight distribution as long as we decode only up to $t \leq \frac{d-1}{2}$ errors.

In chapter 16.1 of [2] Berlekamp deduces a formula for

$$\mathrm{P}(Y \in \cup_{c\in C} \mathrm{B}_t(c)),$$

i.e., for the probability of decoding (either correct or incorrect). The formula involves the coefficients of some Taylor series and was first observed by MacWilliams. In contrast we give closed formulas for the probability of incorrect decoding and investigate these functions. In particular we study the behaviour of the probability of incorrect decoding as a function of $p$ and $t$.

# 2 Comparing $\mathrm{P}_{\mathrm{fd}}(C, t, p)$ and $\mathrm{P}_{\mathrm{ue}}(C, t, p)$

Although the values $\mathrm{P}_{\mathrm{fd}}(C, t, p)$ and $\mathrm{P}_{\mathrm{ue}}(C, t, p)$ may differ the next result shows that minimizing $\mathrm{P}_{\mathrm{fd}}$ in the class of $[n, k]$ codes equals the problem of minimizing $\mathrm{P}_{\mathrm{ue}}$ in the same class of codes. Actually, $\mathrm{P}_{\mathrm{fd}}$ and $\mathrm{P}_{\mathrm{ue}}$ differ only in terms independent of the code.

**Theorem 2.1** *Let $C$ be an $[n, k, d]$ code and let $t \leq \frac{d-1}{2}$. Then*

$$\begin{aligned} \mathrm{P}_{\mathrm{fd}}(C, t, p) &= \frac{\mathrm{P}_{\mathrm{ue}}(C, t, p)}{\mathrm{P}_{\mathrm{ue}}(C, t, p) + \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}} \\ &= 1 - \frac{\sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}}{\mathrm{P}_{\mathrm{ue}}(C, t, p) + \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}}\,. \end{aligned}$$

Proof: According to the discussions in the first section we have

$$\begin{aligned} \frac{\mathrm{P}_{\mathrm{ue}}(C, t, p)}{\mathrm{P}_{\mathrm{fd}}(C, t, p)} &= |C| \cdot \mathrm{P}(Y \in \mathrm{B}_t(0)) \\ &= |C| \sum_{c\in C} \mathrm{P}(Y \in \mathrm{B}_t(0) \mid X = c) \mathrm{P}(X = c) \\ &= \mathrm{P}(Y \in \mathrm{B}_t(0) \mid X = 0) + \sum_{0\neq c\in C} \mathrm{P}(Y \in \mathrm{B}_t(0) \mid X = c) \\ &= \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i} + \mathrm{P}_{\mathrm{ue}}(C, t, p)\,, \end{aligned}$$

and the assertion of the theorem follows.

Observe that

$$|C| \cdot \mathrm{P}(Y \in \mathrm{B}_t(0)) = \sum_{c \in C} \mathrm{P}(Y \in \mathrm{B}_t(c))$$

is the probability of decoding up to $t$ errors. As a consequence we have

**Corollary 2.2** *Let $C$ be an $[n,k,d]$ code and let $t \leq \frac{d-1}{2}$. Then*

*a)* $\mathrm{P}_{\mathrm{ue}}(C,t,p) \leq \mathrm{P}_{\mathrm{fd}}(C,t,p)$.

*b)* $\mathrm{P}_{\mathrm{ue}}(C,t,p) = \mathrm{P}_{\mathrm{fd}}(C,t,p)$ *if and only if $C$ is perfect and* $t = \frac{d-1}{2}$.

The following two corollaries are immediate consequences of the above theorem.

**Corollary 2.3** *If $C$ is a code of length $n$ then*

$$\begin{aligned}
\mathrm{P}_{\mathrm{fd}}(C,0,p) &= 1 - \frac{(1-p)^n}{\mathrm{P}_{ue}(C,0,p) + (1-p)^n} \\
&= 1 - \frac{(1-p)^n}{\sum_{i=0}^n A_i \left(\frac{p}{q-1}\right)^i (1-p)^{n-i}} \qquad \text{(by (*), Introduction)} \\
&= 1 - \frac{1}{\sum_{i=0}^n A_i \left(\frac{p}{(q-1)(1-p)}\right)^i}.
\end{aligned}$$

**Corollary 2.4** *Let $C$ and $C'$ be $[n,k,d]$ respectively $[n,k,d']$ codes. For any symbol error probability $0 < p < \frac{q-1}{q}$ and any $t \leq \min\{\frac{d-1}{2}, \frac{d'-1}{2}\}$ fixed the following conditions are equivalent.*

*a)* $\mathrm{P}_{\mathrm{fd}}(C,t,p) < \mathrm{P}_{\mathrm{fd}}(C',t,p)$.

*b)* $\mathrm{P}_{\mathrm{ue}}(C,t,p) < \mathrm{P}_{\mathrm{ue}}(C',t,p)$.

The last corollary shows that both probabilities are equally good if we want to compare two $[n,k]$ codes with respect to decoding error probabilities.

# 3 The probability $\mathrm{P}_{\mathrm{ue}}(C,t,p)$

Let $C$ be an $[n,k,d]$ code over $\mathbb{F}_q$ with weight distribution $A(x) = \sum_{i=0}^n A_i x^i$. Furthermore, let $t \in \mathbb{N}_0$ with $t \leq \frac{d-1}{2}$.

**Theorem 3.1** *We have*

$$\mathrm{P}_{\mathrm{ue}}(C,t,p) = \sum_{i=1}^n A_i \sum_{j=0}^t \sum_{s=0}^j \left[ \binom{i}{s} \left(\frac{p}{q-1}\right)^{i-s} (1 - \tfrac{p}{q-1})^s \binom{n-i}{j-s} p^{j-s} (1-p)^{n-i-j+s} \right].$$

Proof: Remember that

$$\mathrm{P}_{\mathrm{ue}}(C,t,p) = \mathrm{P}(Y \in \cup_{0\neq c\in C}\mathrm{B}_t(c) \mid X=0).$$

Now choose $c \in \mathbb{F}_q^n$ with $\mathrm{wt}(c) = i > 0$. Suppose that 0 is transmitted, receiving a $w \in \mathrm{B}_t(c)$ occurs exactly with probability

$$\sum_{j=0}^{t}\sum_{s=0}^{j}\left[\binom{i}{s}\left(\frac{p}{q-1}\right)^{i-s}\left(1-\frac{p}{q-1}\right)^{s}\binom{n-i}{j-s}p^{j-s}(1-p)^{n-i-j+s}\right]$$

Observe that $\binom{n-i}{j-s} = 0$ when $j-s > n-i$. Also, $i \geq d > t \geq s$. Note that this probability takes the same value for all the $A_i$ codewords of weight $i$. Summing up over all $i = 1,\ldots,n$ yields the assertion of the theorem.

**Corollary 3.2** *For a 1-error correcting code $C$ we have*

$$\begin{aligned}&\mathrm{P}_{\mathrm{ue}}(C,1,p) = \\ &\sum_{i=1}^{n-1}A_i\left(\tfrac{1}{q-1}\right)^{i}p^{i-1}(1-p)^{n-i-1}[i(q-1)+(1-qi)p+(n-1)p^2] \\ &\quad +A_n\left(\tfrac{1}{q-1}\right)^{n}p^{n-1}[n(q-1)-p(n-1)].\end{aligned}$$

Proof: This follows immediately from 3.1. Note that the coefficient by $A_n$ has to be computed differently from the coefficients of the other $A_i$ since the factor $\binom{n-i}{j-s}$ in the formula of 3.1 equals 0 for $i = n, j = 1$ and $s = 0$.

In order to compare $\mathrm{P}_{\mathrm{ue}}$ for two $[n,k]$ codes, say $C$ and $C'$, one may compute the values of the formula in 3.1. However, for symbol error probability $p$ small enough, there is an easier way which we describe next.

**Definition 3.3** Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $f'(x) = \sum_{i=0}^{n} a_i' x^i$ be polynomials with non-negative coefficients $a_i, a_i' \in \mathbb{R}$. We write

$$f(x) \prec f'(x)$$

iff $(a_0,\ldots,a_n) \prec (a_0',\ldots a_n')$ in lexicographical order, i.e., there exists an $s \in \{0,1,\ldots,n\}$ such that $a_i = a_i'$ for all $i < s$ but $a_s < a_s'$.
Clearly, $f(x) \preceq f'(x)$ means $f(x) \prec f'(x)$ or $f(x) = f'(x)$.

**Theorem 3.4** *Let $C$ and $C'$ be $[n,k,d]$ and $[n,k,d']$ codes with weight polynomials $A(x)$ and $A'(x)$ respectively. Suppose that $t \leq \min\{\frac{d-1}{2},\frac{d'-1}{2}\}$. If $p$ is small enough then the following conditions are equivalent.*

*a)* $\mathrm{P}_{\mathrm{fd}}(C,t,p) \leq \mathrm{P}_{\mathrm{fd}}(C',t,p)$.

*b)* $\mathrm{P}_{\mathrm{ue}}(C,t,p) \leq \mathrm{P}_{\mathrm{ue}}(C',t,p)$.

*c)* $A(x) \preceq A'(x)$.

Proof: The equivalence of a) and b) is Corollary 2.4. Thus it remains to prove that b) and c) are equivalent. We may assume that $A(x) \neq A'(x)$ and that $l$ is the smallest position in which the weight distributions of $C$ and $C'$ differ. Now consider the function

$$f(p) = \mathrm{P}_{\mathrm{ue}}(C', t, p) - \mathrm{P}_{\mathrm{ue}}(C, t, p) = \sum_{i=l}^{n} (A'_i - A_i) f_i(p).$$

By 3.1, we know that

$$f_i(p) = \sum_{j=0}^{t} \sum_{s=0}^{j} \left[ \binom{i}{s} \left( \frac{p}{q-1} \right)^{i-s} (1 - \frac{p}{q-1})^s \binom{n-i}{j-s} p^{j-s} (1-p)^{n-i-j+s} \right].$$

We have $0 \leq j \leq t < l$ since $l \geq \min(d, d') > t$. One easily sees that for $i \geq l$ the function $f_i(p)$ is a polynomial of the form

$$f_i(p) = \binom{i}{t} \left( \frac{1}{q-1} \right)^{i-t} p^{i-t} + \text{ terms in } p^r \text{ with } r > i - t.$$

Thus

$$f(p) = (A'_l - A_l) \binom{l}{t} \left( \frac{1}{q-1} \right)^{l-t} p^{l-t} + \text{ terms in } p^r \text{ with } r > l - t.$$

In particular, for $p$ small enough we have $f(p) > 0$ if and only if $A_l < A'_l$. So, whenever $p$ is small enough, then $\mathrm{P}_{\mathrm{ue}}(C, t, p) < \mathrm{P}_{\mathrm{ue}}(C', t, p)$ if and only if $A(x) \prec A'(x)$.

$\square$

We would like to mention that the equivalence of a) and c) can also be found in ([5], Theorem 3). In addition there is an explicit bound up to which the equivalence of a) and c) holds true. For the equivalence of b) and c) we have

**Theorem 3.5** *Let $C$ and $C'$ be $[n, k, d]$ respectively $[n, k, d']$ codes with weight polynomials $A(x)$ respectively $A'(x)$ and let $t \leq \min\{\frac{d-1}{2}, \frac{d'-1}{2}\}$. Suppose that $A(x) \neq A'(x)$ and that $l$ is the smallest position in which the weight distributions of $C$ and $C'$ differ. If $A(x) \preceq A'(x)$ then*

$$\mathrm{P}_{\mathrm{ue}}(C, t, p) \leq \mathrm{P}_{\mathrm{ue}}(C', t, p)$$

*for all $p$ with*

$$p \leq \gamma = \frac{(A'_l - A_l)\binom{l}{t}(q-1)}{(\sum_{i=l}^{n} A_i)(\sum_{j=0}^{t} \binom{n}{j}(q-1)^j) + (A'_l - A_l)\binom{l}{t}(q-1)}.$$

Proof: We put

$$n_r = |\{v \in \cup_{c \in C,\ \mathrm{wt}(c) \geq l}\, B_t(c) \mid \mathrm{wt}(v) = r\}|$$

and

$$n'_r = |\{v' \in \cup_{c' \in C',\ \mathrm{wt}(c') \geq l}\ B_t(c') \mid \mathrm{wt}(v') = r\}|.$$

If we take $m = l - t$ then $n_r = n'_r$ for any $r < m$ and $n'_m - n_m = (A'_l - A_l)\binom{l}{t}$. Hence

$$\begin{aligned}
f(p) &= \mathrm{P}_{\mathrm{ue}}(C', t, p) - \mathrm{P}_{\mathrm{ue}}(C, t, p) \\
&= \sum_{r=m}^{n} (n'_r - n_r) \left(\frac{p}{q-1}\right)^r (1-p)^{n-r} \\
&= (1-p)^n \sum_{r=m}^{n} (n'_r - n_r) \left(\frac{p}{(q-1)(1-p)}\right)^r \\
&= (1-p)^n \sum_{r=m}^{n} (n'_r - n_r) x^r
\end{aligned}$$

where $x = \frac{p}{(q-1)(1-p)}$. Note that $x \in [0, 1]$. Therefore,

$$\begin{aligned}
g(x) = f(p) &= (1-p)^n \Big( (A'_l - A_l)\binom{l}{t} x^m + \sum_{r=m+1}^{n} (n'_r - n_r) x^r \Big) \\
&\geq (1-p)^n \Big( (A'_l - A_l)\binom{l}{t} x^m - \sum_{r=m+1}^{n} n_r x^r \Big) \\
&\geq (1-p)^n x^m \Big( (A'_l - A_l)\binom{l}{t} - x \sum_{r=m+1}^{n} n_r \Big).
\end{aligned}$$

Next we put $a(C, l) = \sum_{i=l}^{n} A_i$ and $b(q, t) = |B_t(0)| = \sum_{j=0}^{t} \binom{n}{j}(q-1)^j$. Since $p \leq \gamma$ it is easy to see that

$$x \leq \frac{(A'_l - A_l)\binom{l}{t}}{a(C, l) b(q, t)}.$$

Moreover

$$\sum_{r=m+1}^{n} n_r \leq a(C, l) b(q, t).$$

Thus

$$g(x) \quad \geq \quad (1-p)^n x^m \Big( (A'_l - A_l)\tbinom{l}{t} - x a(C, l) b(q, t) \Big)$$

where the right hand side is $\geq 0$ by definition of $\gamma$.

**Remark 3.6** The factor $\gamma$ in the previous Theorem increases if $(A'_l - A_l)\binom{l}{t}$ increases. Furthermore, note that $A'_l - A_l \geq q - 1$. Thus we may replace $\gamma$ in 3.5 by

$$\bar{\gamma} = \frac{\binom{d}{t}(q-1)^2}{(q^k - 1)(\sum_{j=0}^{t} \binom{n}{j}(q-1)^j) + \binom{d}{t}(q-1)^2}$$

which only depends on the parameters $[n,k,d]_q$ and $t$.

**Corollary 3.7** *With the notation as above we have*

*a)* $\mathrm{P}_{\mathrm{ue}}(C,t,p) \geq A_d \binom{d}{t} \left( \frac{p}{(q-1)(1-p)} \right)^{d-t} (1-p)^n.$

*b)* $\lim_{p\to 0} \frac{\mathrm{P}_{\mathrm{ue}}(C,t,p)}{p^{d-t}} = A_d \binom{d}{t} \left( \frac{1}{q-1} \right)^{d-t}.$

Proof: a) By 3.1, we have

$$\mathrm{P}_{ue}(C,t,p) =$$
$$\sum_{i=1}^{n} A_i \sum_{j=0}^{t} \sum_{s=0}^{j} \left[ \binom{i}{s} \left( \frac{p}{q-1} \right)^{i-s} \left( 1 - \frac{p}{q-1} \right)^{s} \binom{n-i}{j-s} p^{j-s} (1-p)^{n-i-j+s} \right]$$

where each summand is non-negative. Taking $i=d$ and $j=s=t$ we get

$$\begin{aligned} \mathrm{P}_{\mathrm{ue}}(C,t,p) &\geq A_d \binom{d}{t} \left( \frac{p}{q-1} \right)^{d-t} \left( 1 - \frac{p}{q-1} \right)^{t} (1-p)^{n-d} \\ &\geq A_d \binom{d}{t} \left( \frac{p}{q-1} \right)^{d-t} (1-p)^{n-d+t}. \end{aligned}$$

b) By 3.1 we obviously have

$$\mathrm{P}_{\mathrm{ue}}(C,t,p) = A_d \binom{d}{t} \left( \frac{1}{q-1} \right)^{d-t} p^{d-t} + \text{ terms in } p^r \text{ with } r > d-t.$$

Thus the assertion follows.

**Example 3.8** Consider the following binary $[15,6,4]$ codes $C$ and $C'$ generated by $(I_6\ A)$ resp. $(I_6\ A')$ where $I_6$ denotes the identity matrix of order 6 and

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix},$$

$$A' = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

By [4], $C$ has weight polynomial

$$A(x) = 1 + 8x^4 + 16x^6 + 21y^8 + 16x^{10} + 2x^{12}$$

and the weight polynomial of $C'$ is

$$A'(x) = 1 + 9x^4 + 51x^8 + 3x^{12}.$$

a) Clearly, $\mathrm{P}_{\mathrm{ue}}(C, 0, p) < \mathrm{P}_{\mathrm{ue}}(C', 0, p)$ if and only if $A\left(\frac{p}{1-p}\right) < A'\left(\frac{p}{1-p}\right)$. Now we consider the function

$$f(p) = \sum_{i=4}^{15}(A'_i - A_i)\left(\frac{p}{1-p}\right)^i =$$
$$\left(\frac{p}{1-p}\right)^4 - 16\left(\frac{p}{1-p}\right)^6 + 30\left(\frac{p}{1-p}\right)^8 - 16\left(\frac{p}{1-p}\right)^{10} + \left(\frac{p}{1-p}\right)^{12}.$$

Note that $f(p) > 0$ for $p$ small enough, for instance if $p \leq \gamma = \frac{1}{64} \sim 0.0156$ by Theorem 3.5. Actually $f(p) > 0$ for $0 < p \leq 0.2113...$ but $f(p) < 0$ in the rest of the interval $(0, \frac{1}{2})$. Thus, only for small symbol error probability $p$ the code $C$ has the smaller detecting error probability $\mathrm{P}_{\mathrm{ue}}$.
b) If we use $C$ and $C'$ for 1-error correction, i.e. $t = 1$ then, by 3.2, we obtain

$$\mathrm{P}_{\mathrm{ue}}(C, 1, p) < \mathrm{P}_{\mathrm{ue}}(C', 1, p)$$

exactly for $0 < p \leq 0.1383....$ The bound $\gamma$ given in 3.5 turns out to be equal to $\frac{4}{1012} = 0.0039525$ which means that $\gamma$ stays far away from the actual bound. Finally note that for symbol error probability $p$ with

$$0.1383... \leq p \leq 0.2113...$$

the code $C$ is the better choice for error detection but $C'$ is better for error correction.

We would like to mention here that the actual bound for $p$ *small enough* in 3.4 seems to be difficult to determine. It depends on the weight distributions. However, assuming some additional conditions we can easily compare the decoding error probabilities $\mathrm{P}_{\mathrm{ue}}$ of two codes for all $0 < p < \frac{q-1}{q}$.

**Proposition 3.9** *Let $C$ and $C'$ be $[n, k, d]_q$ respectively $[n, k, d']_q$ codes with weight distribution $(A_0, \ldots, A_n)$ respectively $(A'_0, \ldots, A'_n)$. Suppose that*

$$\sum_{i=0}^{j} A_i \;\leq\; \sum_{i=0}^{j} A'_i$$

*for all $j = 0, \ldots, n$ with strict inequality for at least one $j$. Then*

$$\mathrm{P}_{\mathrm{ue}}(C, t, p) \;<\; \mathrm{P}_{\mathrm{ue}}(C', t, p)$$

*for all $p$ with $0 < p < \frac{q-1}{q}$ and all $t \leq \min\{\frac{d-1}{2}, \frac{d'-1}{2}\}$ .*

Proof: In order to prove that $\mathrm{P}_{\mathrm{ue}}(C,t,p) \ < \ \mathrm{P}_{\mathrm{ue}}(C',t,p)$ we have to show that

$$\sum_{i=0}^{n} A_i f_i(p) \ < \ \sum_{i=0}^{n} A_i' f_i(p)$$

where

$$f_i(p) = \sum_{j=0}^{t}\sum_{s=0}^{j}\left[\binom{i}{s}\left(\frac{p}{q-1}\right)^{i-s}\left(1-\frac{p}{q-1}\right)^{s}\binom{n-i}{j-s}p^{j-s}(1-p)^{n-i-j+s}\right],$$

as shown in 3.1. Now we apply a trick which we learnt from Helleseth, Kløve and Levenshtein (see [8]). Suppose we had already proved

$$f_{i+1}(p) < f_i(p) \qquad \text{for } i = 0,\dots,n$$

where $f_{n+1}(p) = 0$. Then

$$\begin{aligned} f(p) &= \sum_{i=0}^{n}(A_i' - A_i) f_i(p) \\ &= \sum_{j=0}^{n}(f_j(p) - f_{j+1}(p)) \sum_{i=0}^{j}(A_i' - A_i). \end{aligned}$$

Since $f_j(p) - f_{j+1}(p) > 0$ for all $j$ the assumptions of the theorem imply $f(p) > 0$ for $0 < p < \frac{1}{2}$ and the proof is complete. So it remains to show that $f_{i+1}(p) < f_i(p)$ for all $i$ and any $t$.

Recall that

$$f_i(p) = \mathrm{P}(Y \in B_t(c) \mid X = 0)$$

where $c$ is a word such that $d(c,0) = i$. Note that the probability $f_i(p)$ depends only on the weight of $c$ and not that $c$ is a codeword. Clearly, $f_n(p) > f_{n+1}(p) = 0$. Thus we may assume that $i < n$ and, without lost of generality, we may take $c = 1\dots10\dots0$ and $\tilde{c} = c + e$ with $e = 0\dots01$. Now,

$$f_i(p) = \sum_{w \in B_t(c)} \mathrm{P}(Y = w \mid X = 0)$$

and

$$f_{i+1}(p) = \sum_{v \in B_t(\tilde{c})} \mathrm{P}(Y = v \mid X = 0).$$

Observe that, for any $w \in B_t(c)$, we have

$$d(w,\tilde{c}) \le d(w,c) + d(c,\tilde{c}) \le t + 1.$$

Therefore, if $w \in B_t(c) \setminus B_t(\tilde{c})$ then $d(w,c) = t$ and $d(w,\tilde{c}) = t+1$. This means that the last digit of $w$ is 0. Next we consider the bijection

$$\rho : B_t(c) \longrightarrow B_t(\tilde{c})$$

given by

$\rho(w) = w$ if $w \in B_t(c) \cap B_t(\tilde{c})$,

$\rho(w) = w + e$ if $w \in B_t(c) \setminus B_t(\tilde{c})$.

Now, it is easy to observe that $d(w,0) \leq d(\rho(w),0)$ for any $w \in B_t(c)$. Furthermore, since $p < \frac{q-1}{q}$ we have

$$\mathrm{P}(Y = w \mid X = 0) \geq \mathrm{P}(Y = \rho(w) \mid X = 0)$$

with strict inequality for $w \in B_t(c) \setminus B_t(\tilde{c}) \neq \emptyset$.

Finally,

$$\begin{aligned} f_i(p) &= \sum_{w \in B_t(c)} \mathrm{P}(Y = w \mid X = 0) \\ &> \sum_{w \in B_t(c)} \mathrm{P}(Y = \rho(w) \mid X = 0) \\ &= \sum_{v \in B_t(\tilde{c})} \mathrm{P}(Y = v \mid X = 0) = f_{i+1}(p) \end{aligned}$$

which proves the proposition.

**Example 3.10** Let $C$ denote the binary $[n = 2^k - 1, k, 2^{k-1}]$ Simplex code. Clearly, $C$ has weight distribution

$$A_0 = 1,\ A_{2^{k-1}} = 2^k - 1 = n,\ \text{and all other} A_i = 0.$$

Let $C'$ be the $[n,k]$ code generated by $e + c$ where $c$ runs through a basis of $C$ and $e = (1,\ldots,1)$ denotes the all one vector. One easily sees that $C'$ has weight distribution

$$A'_0 = 1,\ A'_{2^{k-1}-1} = 2^{k-1},\ A'_{2^{k-1}} = 2^{k-1} - 1,\ \text{and all other } A_i = 0.$$

Thus we may apply 3.9 a) which shows that

$$\mathrm{P}_{\mathrm{ue}}(C,p,t) < \mathrm{P}_{\mathrm{ue}}(C',p,t)$$

for all $0 < p < \frac{1}{2}$. Note that $C'$ is a $[2^k - 2, k, 2^{k-1} - 1]$ code. This is not surprising as we will see in 3.11.

In order to state the next theorem we define the support of a code $C$ of length $n$ as

$$\mathrm{supp}(C) = \{i \mid \text{there exists } (x_1,\ldots,x_n) \in C,\ x_i \neq 0\}.$$

**Theorem 3.11** *Let $C$ and $C'$ be $[n,k]$ codes over the same field $\mathbb{F}_q$ with weight distributions $(A_0,\ldots,A_n)$ resp. $(A'_0,\ldots,A'_n)$. Suppose that*

$$\sum_{i=0}^{j} A_i \leq \sum_{i=0}^{j} A'_i \quad \textit{for all } j = 0,\ldots,n.$$

*If $|\mathrm{supp}(C)| = |\mathrm{supp}(C')|$ then $A_i = A'_i$ for all $i = 0,\ldots,n$, i.e. $C$ and $C'$ are formally equivalent.*

Proof: We put $r_i = A'_i - A_i$ for $i = 0, \dots, n$. By ([11], 4.5.1), we have

$$\sum_{c \in C} \mathrm{wt}(c) = |\mathrm{supp}(C)|(q-1)q^{k-1}.$$

In particular,

$$\begin{aligned} \textstyle\sum_{i=0}^{n} iA_i = \sum_{c\in C} \mathrm{wt}(c) &= |\mathrm{supp}(C)|(q-1)q^{k-1} \\ &= |\mathrm{supp}(C')|(q-1)q^{k-1} \\ &= \textstyle\sum_{c'\in C'} \mathrm{wt}(c') \\ &= \textstyle\sum_{i=0}^{n} iA'_i, \end{aligned}$$

hence $\sum_{i=0}^{n} ir_i = 0 = \sum_{i=1}^{n} ir_i$. Note that $r_1 + r_2 + \dots + r_n = 0$ as $|C| = |C'|$. It follows

$$\begin{aligned} 0 &= \textstyle\sum_{i=1}^{n} ir_i = r_1 + 2r_2 + \dots + nr_n \\ &= (r_1 + \dots r_n) + (r_2 + \dots r_n) + \dots + (r_{n-1} + r_n) + r_n \\ &= n(r_1 + \dots r_n) - [r_1 + (r_1 + r_2) + \dots + (r_1 + \dots + r_{n-1})] \\ &= -[r_1 + (r_1 + r_2) + \dots + (r_1 + \dots r_{n-1})]. \end{aligned}$$

Since by assumption $\sum_{i=0}^{j} r_i = \sum_{i=1}^{j} r_i \geq 0$ we obtain $\sum_{i=1}^{j} r_i = 0$ for all $j = 1, \dots, n$. This shows $r_i = 0$ for all $i = 1, \dots, n$. Hence $A_i = A'_i$ for $i = 1, \dots, n$ and the proof is complete since obviously $A_0 = A'_0$.

By MacWilliams' duality the weight distribution of a dual code $C^\perp$ is uniquely determined by that of $C$. Thus, according to $\mathrm{P_{ue}}$ or $\mathrm{P_{fd}}$ a code $C$ and its dual are related since both probabilities depend only on the weight distribution. However, the connection seems to be quite complicated as the next examples show.

**Examples 3.12** a) By [1], the two best binary $[15, 3, 7]$ codes have weight polynomials

$$A(x) = 1 + x^7 + 2x^8 + 3x^9 + x^{10}$$

and

$$A'(x) = 1 + x^7 + 3x^8 + 2x^9 + x^{11}.$$

By MacWilliams' duality one easily computes for the dual codes that

$$\begin{aligned} A^\perp(x) &= 1 + 10x^2 + 66x^3 + 173x^4 + 358x^5 + 630x^6 + 820x^7 + 795x^8 + \\ &\quad 620x^9 + 382x^{10} + 170x^{11} + 55x^{12} + 14x^{13} + 2x^{14} \end{aligned}$$

and

$$\begin{aligned} A'^\perp(x) &= 1 + 11x^2 + 62x^3 + 175x^4 + 370x^5 + 613x^6 + 812x^7 + 823x^8 + \\ &\quad 612x^9 + 365x^{10} + 182x^{11} + 57x^{12} + 10x^{13} + 3x^{14}. \end{aligned}$$

In particular, $A(x) \prec A'(x)$ and $A^{\perp}(x) \prec A'^{\perp}(x)$.
b) Let $C$ be the binary code with generator matrix

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

One easily checks that $C$ is a $[6,3,2]$ code with weight polynomial

$$A(x) = 1 + x^2 + 4x^3 + x^4 + x^6.$$

The dual $C' = C^{\perp}$ of $C$ is generated by the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

$C^{\perp}$ is also a $[6,3,2]$ code but with weight polynomial

$$A'(x) = 1 + 2x^2 + 5x^4.$$

Now $A(x) \prec A'(x)$ but $A'^{\perp}(x) = A(x) \prec A'(x) = A^{\perp}(x)$.

# 4 Properties of the functions $\mathrm{P}_{\mathrm{fd}}$ and $\mathrm{P}_{\mathrm{ue}}$

In section 2 we proved that $\mathrm{P}_{\mathrm{fd}}$ and $\mathrm{P}_{\mathrm{ue}}$ are equally good when used to find an optimal code with respect to bounded distance decoding error probability. The function $\mathrm{P}_{\mathrm{fd}}$ carries a nice property, namely it increases monotonically if the symbol error probability $p$ increases monotonically. This fails to be true for $\mathrm{P}_{\mathrm{ue}}$ even if we use the code only for error detection, i.e. $t = 0$. Thus in contrast to $\mathrm{P}_{\mathrm{ue}}$ the decoding error probability $\mathrm{P}_{\mathrm{fd}}$ always reflects the fact that a less reliable channel causes more errors in transmissions which consequently should lead to more errors in the decoding process. That $\mathrm{P}_{\mathrm{fd}}$ is an increasing function in $p$ was first noticed by the first author in ([5], Theorem 2). For reader's convenience we give here an independent proof.

**Proposition 4.1** *Let $C$ be an $[n,k,d]$ code and let $t \leq \frac{d-1}{2}$. Then the decoding error probability $\mathrm{P}_{\mathrm{fd}}(C,t,p)$ is a monotonically increasing function in $p$ on the interval $\left[0, \frac{q-1}{q}\right]$.*

Proof: We put

$$n_r = |\{v \in \cup_{c \in C} B_t(c) \mid wt(v) = r\}|.$$

Note that $n_r = \binom{n}{r}(q-1)^r$ for $r \leq t$. With this notation we have

$$\mathrm{P}_{\mathrm{ue}}(C,t,p) = \sum_{r=t+1}^{n} n_r \left(\frac{p}{q-1}\right)^r (1-p)^{n-r} = (1-p)^n \sum_{r=t+1}^{n} n_r \left(\frac{p}{(q-1)(1-p)}\right)^r$$

and

$$\mathrm{P}_{\mathrm{fd}}(C,t,p) = \frac{\mathrm{P}_{\mathrm{ue}}(C,t,p)}{\mathrm{P}_{\mathrm{ue}}(C,t,p) + \sum_{h=0}^{t} n_h \left(\frac{p}{q-1}\right)^h (1-p)^{n-h}} =$$

$$\frac{(1-p)^n \sum_{r=t+1}^{n} n_r \left(\frac{p}{(q-1)(1-p)}\right)^r}{(1-p)^n \sum_{r=t+1}^{n} n_r \left(\frac{p}{(q-1)(1-p)}\right)^r + (1-p)^n \sum_{h=0}^{t} n_h \left(\frac{p}{(q-1)(1-p)}\right)^h}.$$

If we put $x = \frac{p}{(q-1)(1-p)}$ we get

$$\mathrm{P}_{\mathrm{fd}}(C,t,p) = \frac{\sum_{r=t+1}^{n} n_r x^r}{\sum_{r=t+1}^{n} n_r x^r + \sum_{h=0}^{t} n_h x^h} = f(x).$$

Observe that x is a monotonically increasing function in $p$ in the interval $\left[0, \frac{q-1}{q}\right]$. Therefore, by taking the derivative of $f(x)$ it is easy to check that $\mathrm{P}_{\mathrm{fd}}(C,t,p)$ is a monotonically increasing function in p in the interval $\left[0, \frac{q-1}{q}\right]$ if and only if

$$\sum_{r=t+1}^{n} \sum_{h=0}^{t} (r-h) n_r n_h x^{r+h-1} > 0$$

for $x \in (0,1]$. But this holds obviously true since $r > h$ and $n_r,\ n_h \geq 0$.

Increasing the number $t$ of correctable errors should result in an increasing of the decoding error probability. This fact is reflected by both functions. However the proof for $\mathrm{P}_{\mathrm{fd}}$ turns out to be much more complicated. Note that our result extends the asymptotic version given in [5].

**Proposition 4.2** *If $C$ is an $[n,k,d]$ code and $0 \leq t < t' \leq \frac{d-1}{2}$ then*

*a)* $\mathrm{P}_{\mathrm{ue}}(C,t,p) < \mathrm{P}_{\mathrm{ue}}(C,t',p)$

*b)* $\mathrm{P}_{\mathrm{fd}}(C,t,p) < \mathrm{P}_{\mathrm{fd}}(C,t',p)$

*for all* $p \in (0, \frac{q-1}{q})$.

Proof: a) According to 3.1 we have

$$\mathrm{P}_{\mathrm{ue}}(C,t',p) = \mathrm{P}_{\mathrm{ue}}(C,t,p) +$$

$$+ \sum_{i=1}^{n} A_i \sum_{j=t+1}^{t'} \sum_{s=0}^{j} \left[ \binom{i}{s} \left(\frac{p}{q-1}\right)^{i-s} (1 - \frac{p}{q-1})^s \binom{n-i}{j-s} p^{j-s} (1-p)^{n-i-j+s} \right]$$

where the last triple sum is positive for $p \neq 0$.
b) To prove the assertion in b) we may assume that $t' = t+1$. Taking into account that for positive real numbers $a, b, c, d$ the inequality $\frac{a}{a+b} < \frac{c}{c+d}$ is equivalent to $\frac{a}{b} < \frac{c}{d}$ the assertion can be reformulated according to 2.1 as

$$\frac{P_{ue}(C,t,p)}{P(Y \in B_t(0) \mid X = 0)} < \frac{P_{ue}(C,t+1,p)}{P(Y \in B_{t+1}(0) \mid X = 0)}.$$

According to 3.1 this is equivalent to

$$\frac{\sum_{i=d}^{n} A_i \sum_{j=0}^{t} \alpha(i,j)}{\mathrm{P}(Y \in B_t(0) \mid X=0)} < \frac{\sum_{i=d}^{n} A_i \sum_{j=0}^{t+1} \alpha(i,j)}{\mathrm{P}(Y \in B_{t+1}(0) \mid X=0)}$$

where $\alpha(i,j) = \sum_{s=0}^{j} \left[ \binom{i}{s} \left(\frac{p}{q-1}\right)^{i-s} \left(1-\frac{p}{q-1}\right)^{s} \binom{n-i}{j-s} p^{j-s}(1-p)^{n-i-j+s} \right]$.
So it is enough to prove for each $i \in \{d,\ldots,n\}$ that

$$\frac{\sum_{j=0}^{t} \alpha(i,j)}{\mathrm{P}(Y \in B_t(0) \mid X=0)} < \frac{\sum_{j=0}^{t+1} \alpha(i,j)}{\mathrm{P}(Y \in B_{t+1}(0) \mid X=0)},$$

which means

$$\frac{\mathrm{P}(Y \in B_{t+1}(0) \mid X=0)}{\mathrm{P}(Y \in B_t(0) \mid X=0)} < \frac{\sum_{j=0}^{t+1} \alpha(i,j)}{\sum_{j=0}^{t} \alpha(i,j)}. \qquad (1)$$

Next we put $D_j(c) = \{w \in \mathbb{F}_q^n \mid d(c,w) = j\}$ for $j = 0,1,\ldots,n$ and $c \in \mathbb{F}_q^n$. Then (1) can be written as

$$1 + \frac{\mathrm{P}(Y \in D_{t+1}(0) \mid X=0)}{\sum_{j=0}^{t} P(Y \in D_j(0) \mid X=0)} < 1 + \frac{\alpha(i,t+1)}{\sum_{j=0}^{t} \alpha(i,j)}$$

for $d \le i \le n$. Since for positive real numbers $a, b, a_j, b_j$ obviously $\frac{a}{a_j} < \frac{b}{b_j}$ implies $\frac{a}{\sum a_j} < \frac{b}{\sum b_j}$ the inequality (1) holds true if, for $i,j$ with $d \le i \le n$ and $0 \le j \le t$, we have

$$\frac{\mathrm{P}(Y \in D_{t+1}(0) \mid X=0)}{P(Y \in D_j(0) \mid X=0)} < \frac{\alpha(i,t+1)}{\alpha(i,j)}. \qquad (2)$$

Moreover since for positive real numbers $a_j, b_j$ the inequalities $\frac{a_{j+1}}{a_j} < \frac{b_{j+1}}{b_j}$ ( $j = 0,\ldots,t$) imply $\frac{a_{t+1}}{a_j} < \frac{b_{t+1}}{b_j}$ it is enough to prove (2) for $j = t$.

Now we fix $i \in \{d,\ldots,n\}$ and take $c \in \mathbb{F}_q^n$ with $d(c,0) = i$. Observe that $\alpha(i,j) = P(Y \in D_j(c) \mid X=0)$. So we are left to show that

$$\frac{\mathrm{P}(Y \in D_{t+1}(0) \mid X=0)}{P(Y \in D_t(0) \mid X=0)} < \frac{\mathrm{P}(Y \in D_{t+1}(c) \mid X=0)}{P(Y \in D_t(c) \mid X=0)} \qquad (3).$$

We have

$$\frac{\mathrm{P}(Y \in D_{t+1}(0) \mid X=0)}{P(Y \in D_t(0) \mid X=0)} = \frac{\sum_{w \in D_{t+1}(0)} P(Y=w \mid X=0)}{\sum_{v \in D_t(0)} P(Y=v \mid X=0)} =$$

$$= \frac{\binom{n}{t+1}(q-1)^{t+1}\left(\frac{p}{q-1}\right)^{t+1}(1-p)^{n-t-1}}{\binom{n}{t}(q-1)^{t}\left(\frac{p}{q-1}\right)^{t}(1-p)^{n-t}} = \frac{(n-t)p}{(t+1)(1-p)}$$

and

$$\frac{P(Y \in D_{t+1}(c) \mid X = 0)}{P(Y \in D_t(c) \mid X = 0)} = \frac{\sum_{w \in D_{t+1}(0)} P(Y = c + w \mid X = 0)}{\sum_{v \in D_t(0)} P(Y = c + v \mid X = 0)}.$$

To finish the proof we set

$$\Gamma = \{(w, v) \mid w \in D_{t+1}(0),\ v \in D_t(0),\ d(w, v) = 1\}.$$

Then

$$(t + 1)|D_{t+1}(0)| = |\Gamma| = (n - t)(q - 1)|D_t(0)|.$$

Thus our last inequality (3) can be rewritten as

$$\frac{(n-t)p}{(t+1)(1-p)} < \frac{\frac{1}{t+1}\sum_{(w,v)\in\Gamma} P(Y = c + w \mid X = 0)}{\frac{1}{(n-t)(q-1)}\sum_{(w,v)\in\Gamma} P(Y = c + v \mid X = 0)}.$$

Clearly, for positive integers $a, b, c_i, d_i$ $(1 \le i \le m)$, the inequalities $\frac{a}{b} \le \frac{c_i}{d_i}$ imply $\frac{a}{b} \le \frac{\sum_{i=1}^m c_i}{\sum_{i=1}^m d_i}$. Thus it is enough to prove that

$$\frac{p}{(q-1)(1-p)} \le \frac{P(Y = c + w \mid X = 0)}{P(Y = c + v \mid X = 0)} \qquad (4)$$

for each $(w, v) \in \Gamma$, with strict inequality for suitable $(w, v) \in \Gamma$. Since

$$|d(c + v, 0) - d(c + w, 0)| \le 1$$

the right side of (4) can take the values $\frac{p}{(q-1)(1-p)}, 1$ or $\frac{(q-1)(1-p)}{p}$. Finally note that $\frac{p}{(q-1)(1-p)} < \frac{(q-1)(1-p)}{p}$ and that to $0 \ne c \in C$ we always find some $(w, v) \in \Gamma$ such that

$$\frac{P(Y = c + w \mid X = 0)}{P(Y = c + v \mid X = 0)} = \frac{(q-1)(1-p)}{p}.$$

**Remark** One easily checks that all results of this paper hold true for distance invariant codes. Only some minor changes in the proofs are necessary.

# References


[1] T. Baicheva, I. Bouyukliev, S. Dodunekov and W. Willems, Teaching linear codes. Matematica Balkanika, New Series, Vol. 19 (2005), Fasc. 1-2, 3-16.

[2] E.R. Berlekamp, Algebraic coding theory. Revised 1984 edition, Aegean Park Press, 1984.

[3] I. Bouyukliev, On the binary projective codes with dimension 6. Bulgarian Academy of Sciences, Preprint No 1/2004, Sofia, 2004.

[4] I. Bouyukliev, S. Bouyuklieva, T.A. Gulliver and P.R.J. Östergård, Clssification of optimal binary self-orthogonal codes. to appear in AAECC.

[5] A. Faldum, Trustworthiness of error-correcting codes. to appear.

[6] F.-W. Fu, T. Kløve and V.K.-W. Wei, On the undetected error probability for binary codes. IEEE Trans. Inform. Theory 49(2) (2003), 382-390.

[7] T. Helleseth, T. Kløve and V. Levenshtein, The Simplex codes and even weight binary codes for error correction. IEEE Trans. Inform. Theory 50 (2004), 2818-2823.

[8] T. Helleseth, T. Kløve and V. Levenshtein, Error-correction capability of binary linear codes and the discrete simplex problem. Preprint version 2004.

[9] T. Kløve and V. Korzhik, Error detecting codes: General theory and their application in feedback communication systems. Kluwer Academic Publishers, 1995.

[10] G. Poltyrev, Bounds on the decoding error probability of binary linear codes via their spectra. IEEE Trans. Inform. Theory 40 (1994), 1284-1292.

[11] W. Willems, Codierungstheorie. DeGruyter, Berlin, 1999.