Binomial and Monotonic Behavior of the Probability of Undetected Error and the 2^{-r}-Bound

WACKER H. D., BOERCSOEK J.
Development
HIMA Paul Hildebrandt GmbH + Co KG
Albert-Bassermann-Strasse 28, D-68782 Bruehl
GERMANY
h.wacker@hima.com j.boercsoek@hima.com http://www.hima.com

Abstract: - Proper linear codes play an important role in error detection. They are characterized by an increasing probability of undetected error $p_{\text{ue}}(\varepsilon,C)$ and are considered "good for error detection". A lot of CRCs commonly used to protect data transmission via a variety of field busses are known for being proper. In this paper the weight distribution of proper linear codes on a binary symmetric channel without memory is investigated. A proof is given that its components are upper bounded by the binomial coefficients in a certain sense. Secondly an upper bound of the tail of the binomial is given, and the results are then used to derive estimates of $p_{\text{ue}}(\varepsilon,C)$. If a code is not proper, it would be desirable to have at least subintervals, where $p_{\text{ue}}(\varepsilon,C)$ increases, or where it satisfies the 2^{-r}-bound. It is for this reason that next the range of monotonicity and of the 2^{-r}-bound is determined. Finally, applications on safety integrity levels are studied.

Key-Words: - Binary Symmetric Channel, Proper Linear Code, CRC, Probability of Undetected Error, Weight Distribution, Binomiality, Monotonicity, 2^{-r}-bound, Dual Distance, Safety Integrity Level

1 Introduction

Let C be a $[n, k]$ linear code on a binary symmetric channel without memory, where n is the block length and k is the number of data bits. The probability of undetected error of such a code is then given by (see [20] for example):

$$p_{ue}(\varepsilon,\mathrm{C}) = \sum_{l=1}^{n} A_l \varepsilon^l (1-\varepsilon)^{n-l},$$

where
A_l = component of the weight distribution of C
= number of code words of weight l,
ε = bit error probability,
n = block length.
d = minimum distance of C.

Clearly the A_l are upper bounded by the binomial coefficients

$$(1) \qquad A_l \le \binom{n}{l},$$

an inequality representing the so called "worst case".

In several publications ([1], [2], [16], [17], [18]) the range of binomiality of a linear code has been investigated, i.e. the range of all indices l with A_l satisfying

$$(2) \qquad A_l \le \gamma \cdot \frac{\sqrt{n}}{2^r} \cdot \binom{n}{l},$$

where $r = n - k$ is the length of the check sum and $\gamma > 0$ is a positive constant. If C is a cyclic redundancy check (CRC) $r = n - k$ is equal to the degree of the polynomial generating the CRC. A common result of all papers is that there is binomial behavior of A_l when l is taken from some neighborhood of $n/2$. Moreover, in each subinterval large enough there is an index i such that the binomial bound is asymptotically met (see for example [1] or [16]).

But apart from those results, the question arises, if there is a complete class of codes with a weight distribution showing binomial behaviour for all indices l. Until now in literature, there seem to be reported no results of this kind. An answer to this question shall be given in subsection 3.1. Theorem 2 states that binomial behaviour is closely related to the monotonicity of $p_{\text{ue}}(\varepsilon,C)$: Ranges of monotonicity are ranges of binomiality. This issue leads directly to the problem of determining the range of monotonicity, a question being attacked in [9] by Dodunekova and Nikolova. Their results will be improved by ours in section 4.

In addition to theoretical considerations binomial behaviour is of great interest when dealing with estimates of the probability of undetected error. Depending on γ and the block length n, inequality (2) improves (1) by a factor of 2^{-r} being enormous say for a CRC-32. If nothing is known about the code but its minimum distance, you will have to be content with (1) (see Annex G of the committee draft in [15]). Misleadingly in [15], estimate (2) without the factor $n^{1/2}$ is attributed to all proper codes, a fact being false (see [1], [16]). On the other hand, inequality (2) may be applied with benefit in all cases, in which the exact weight distribution of a code is unknown, but its minimum distance and monotonic behaviour can be supposed to be known. And it is a useful instrument, if you want to get a close upper bound on the probability of undetected error without calculating the exact weights of a code. In [13] for example, optical data communication via Wavelength Division Multiplexing (WDM) for security applications is investigated. Now the question arises, to which amount the probability of undetected error is reduced by using those techniques. The results of this paper together with those in [4] are serving in [23] to answer this question. In [21] a safety analysis of fieldbus systems is performed by means of a Markov model. Our results could be used to add an estimate of the probability of undetected error to those ideas, and it turns out that they constitute a considerable improvement of estimates known so far.

Therefore first of all we shall now have a closer look at so called proper codes.

2 Proper Linear Codes

A linear code C is said to be proper if and only if the probability of undetected error $p_{\text{ue}}(\varepsilon,C)$ is an increasing function of ε in the interval [0, 1/2].

Because of

$$(3)\qquad \begin{aligned} p_{ue}(\varepsilon,C) &\le p_{ue}(1/2,C)\\ &\le (2^{\mathrm{k}}-1)/2^{n}\\ &< 1/2^{r} \end{aligned}$$

for all $\varepsilon \in [0, 1/2]$, proper linear codes obey the 2^{-r} bound. Those codes are considered “good for error detection” (see for example [19]), and they are widely used in this field.

A lot of important CRCs used to protect data transmission are known for being proper (at least for most block lengths, see [3], [7], [8], [10], [11], [12]). On the other hand nothing seems to be known about specific properties of the weight distribution of a linear code resulting from properness.

In subsection (3.1) of this paper we shall prove that the weight distribution of each proper linear code is showing binomial behavior in the sense of (2) for all components A_l with $l \le n/2$. Moreover we shall demonstrate that, if $p_{\text{ue}}(\varepsilon,C)$ increases on the interval [β, 1/2], then each component A_l of the weight distribution of C with $\beta \le l/n \le 1/2$ is showing binomial behavior. In subsection 3.2 we shall give estimates of the tail of the binomial, and use it in 3.3 to derive upper bounds on the probability of undetected error for proper linear codes.

In the sections 4 and 5 we then determine the range of monotonicity and an interval, where the 2^{-r}-bound is satisfied. Finally the consequences of the estimates of $p_{\text{ue}}(\varepsilon,C)$ for the problem of achieving a specific Safety Integrity Level (SIL) are investigated.

.

3 Binomial Behavior and Properness

3.1 The Weight Distribution

In order to demonstrate our main result we took advantage of Stirling’s approximation

$$1 \le \frac{n!}{\sqrt{2\pi n}\,(n/\mathrm{e})^{n}} \le 1 + 1/11n \ \text{ for all } n = 1,2,3,\ldots$$

from which we were able to deduce

Theorem 1: Let C be an arbitrary linear code, then for each component A_l of the weight distribution of C the inequality

$$A_l \le \frac{72}{121}\sqrt{2\pi}\sqrt{n}\cdot p_{ue}(\frac{l}{n},C)\cdot\binom{n}{l}$$

holds.

Proof: For all l = 1,…, n the subsequent inequality is obvious

$$(4)\qquad \begin{aligned} A_l\left(\frac{l}{n}\right)^{l}\left(1-\frac{l}{n}\right)^{n-l} &\le \sum_{i=1}^{n} A_i\left(\frac{l}{n}\right)^{i}\left(1-\frac{l}{n}\right)^{n-i}\\ &= p_{ue}(\frac{l}{n},C). \end{aligned}$$

Consequently

$$\begin{aligned} A_l &\le \frac{1}{\left(\frac{l}{n}\right)^{l}\left(1-\frac{l}{n}\right)^{n-l}}\cdot p_{ue}(\frac{l}{n},C)\\ &= \frac{n^{n}}{l^{l}(n-l)^{n-l}}\cdot p_{ue}(\frac{l}{n},C), \end{aligned}$$

from which, by Stirling's approximation, we get

$$\begin{aligned} A_l &\leq \frac{n!\mathrm{e}^n}{\sqrt{2\pi n}} \frac{\frac{12}{11}\sqrt{2\pi l}}{l!\mathrm{e}^l} \frac{\frac{12}{11}\sqrt{2\pi(n-l)}}{(n-l)!\mathrm{e}^{n-l}} \cdot p_{\mathrm{ue}}(\frac{l}{n},C) \\ &= \frac{144}{121}\sqrt{2\pi}\sqrt{\frac{l(n-l)}{n}} \frac{n!}{l!(n-l)!} \cdot p_{\mathrm{ue}}(\frac{l}{n},C) \\ &= \frac{144}{121}\sqrt{2\pi} \frac{1}{\sqrt{n}} \sqrt{l(n-l)} \cdot \binom{n}{l} \cdot p_{\mathrm{ue}}(\frac{l}{n},C). \end{aligned}$$

And then, by the inequality of the arithmetic and geometric means

$$\begin{aligned} A_l &\leq \frac{144}{121}\sqrt{2\pi} \frac{1}{\sqrt{n}} \frac{l+(n-l)}{2} \cdot \binom{n}{l} \cdot p_{ue}(\frac{l}{n},C) \\ &\leq \frac{72}{121}\sqrt{2\pi}\sqrt{n}\, p_{ue}(\frac{l}{n},C) \cdot \binom{n}{l}. \end{aligned}$$

■

Remark 1: Perry in [19] used (4) to find codes not satisfying the 2^{-r} bound. We pursued a different plan, and therefore continued in a different way.

Now we are able to state our main result:

Theorem 2: Let the probability of undetected error $p_{\mathrm{ue}}(\varepsilon,C)$ of the linear code C be an increasing function of ε on the interval [β, 1/2]. Then each component A_l of the weight distribution of C with $\beta \leq l/n \leq 1/2$ is showing binomial behavior, i.e.:

$$A_l \leq \frac{72}{121}\sqrt{2\pi} \cdot \frac{\sqrt{n}}{2^r} \cdot \binom{n}{l}.$$

In particular the components A_l of the weight distribution of a proper linear code are showing binomial behaviour for all $l = 1,\ldots,\lfloor n/2 \rfloor$.

Proof: For all l with $\beta \leq l/n \leq 1/2$ we have $p_{\mathrm{ue}}(l/n,\ C) \leq p_{\mathrm{ue}}(1/2,\ C) \leq 2^{-r,}$ from which the statement follows by Theorem 1. ■

Remark 2: As the proof shows, Theorem 2 remains valid, if we replace properness by the more general condition of C satisfying the 2^{-r} bound. Because of the importance of the class of proper linear codes and due to the fact that normally properness is used to validate the 2^{-r} bound, we didn't state Theorem 2 under the most general conditions.

As an easy conclusion of Theorem 1 we now get immediately a first simple estimate of the probability of undetected error:

Theorem 3: Let C be an arbitrary linear code, then for each ε with $0 \leq \varepsilon \leq 1$ the probability of undetected error is upper bounded by

$$p_{ue}(\varepsilon,C) \quad \leq \frac{72}{121}\sqrt{2\pi}\sqrt{n} \cdot \sum_{l=d}^{n} p_{ue}(\frac{l}{n},C) \cdot \binom{n}{l} \varepsilon^l (1-\varepsilon)^{n-l}$$

3.2 The Tail of the Binomial

We now want to apply the statement of Theorem 2 to get an upper bound on the probability of undetected error of proper linear codes. To this end we need an estimate of the tail of the binomial delivered by Theorem 4.

Theorem 4: For all natural numbers q and n with $q \leq n$ and all ε with $0 \leq \varepsilon \leq 1$ the tail of the binomial obeys the following inequality:

$$(5) \qquad \sum_{l=q}^{n} \binom{n}{l} \varepsilon^e (1-\varepsilon)^{n-e} \leq \binom{n}{q} \varepsilon^q \leq \frac{1}{q!} n^q \varepsilon^q .$$

Proof: a) To begin with, let k, n and q be natural numbers satisfying $k + q \leq n$, with the help of which we get an estimate of the binomial coefficients:

$$\begin{aligned} \binom{n}{k+q} &= \frac{n(n-1)\cdots(n-q+1)}{(k+q)\cdots(k+1)} \cdot \frac{(n-q)\cdots(n-k-q+1)}{k!} \\ &= \frac{n(n-1)\cdots(n-q+1)}{(k+q)\cdots(k+1)} \binom{n-q}{k} \\ &\leq \frac{n(n-1)\cdots(n-q+1)}{q!} \binom{n-q}{k} \\ &= \binom{n}{q} \cdot \binom{n-q}{k} \end{aligned}$$

b) When then focusing onto (5) by means of part a), we achieve

$$\begin{aligned} \sum_{l=q}^{n} \binom{n}{l} \varepsilon^l (1-\varepsilon)^{n-l} &= \varepsilon^q \sum_{l=q}^{n} \binom{n}{l} \varepsilon^{l-q} (1-\varepsilon)^{n-l} \\ &= \varepsilon^q \sum_{k=0}^{n-q} \binom{n}{k+q} \varepsilon^k (1-\varepsilon)^{n-k-q} \\ &\leq \varepsilon^q \cdot \sum_{k=0}^{n-q} \binom{n}{q} \cdot \binom{n-q}{k} \varepsilon^k (1-\varepsilon)^{n-k-q} \\ &= \varepsilon^q \binom{n}{q} \cdot \{\varepsilon + (1-\varepsilon)\}^{n-q} \end{aligned}$$

$$= \frac{n \cdot (n-1) \cdots (n-q+1)}{q!} \varepsilon^q$$

$$\le \frac{n^q}{q!} \varepsilon^q .$$

∎

Now, by inequality (1) and Theorem 4 a simple inequality turns out.

Theorem 5: Let *C* be an arbitrary linear code, then for each ε with 0 ≤ ε ≤ 1 the probability of undetected error is upper bounded by

(6) $$p_{ue}(\varepsilon, C) \le \sum_{l=d}^{n} \binom{n}{l} \varepsilon^e (1-\varepsilon)^{n-e} \le \frac{1}{d!} n^d \varepsilon^d \quad ,$$

where *d* is the minimum distance of *C*.

Remark 3: If nothing is known about the code but its minimum distance *d*, Theorem 5 is useful for calculating maximal block lengths in order to achieve a specific upper bound σ on $p_{\mathrm{ue}}(\varepsilon, C)$. In fact, solving

$$\frac{1}{d!} n^d \varepsilon^d < \sigma$$

for *n* yields

(7) $$n_{max} < \varepsilon^{-1} (\sigma d!)^{1/d} .$$

In fact (7) is used when dealing with safety related systems.
Binomial coefficients play an important role in error detection (see for example [26]).Therefore the results of this subsection on its own may have various applications.

3.3 The Probability of Undetected Error

Now we are in a position to estimate the probability of undetected error in the case of proper linear codes. As common use, $\lfloor x \rfloor$ has the meaning of the floor function (highest integer less than or equal to *x*).

Theorem 6: Let *C* be a proper linear code, then for all ε ∈ [0, 1/2] the probability of undetected error obeys

(8) $$p_{ue}(\varepsilon, C) \le \frac{72}{121} \sqrt{2\pi} \sum_{l=d}^{\lfloor n/2 \rfloor} \frac{\sqrt{n}}{2^r} \binom{n}{l} \varepsilon^l (1-\varepsilon)^{n-l} + R_n(\varepsilon) ,$$

where *d* is the minimum distance of *C*, and the remainder term $R_n(\varepsilon)$ satisfies

$$R_n(\varepsilon) \le \binom{n}{\lfloor n/2 \rfloor} \varepsilon^{\lfloor n/2 \rfloor} \le \begin{cases} \left(2\sqrt{\varepsilon}\right)^n & \text{, if n} \ge 3 \text{ and even,} \\ 2\left(2\sqrt{\varepsilon}\right)^{n-1} & \text{, if n} \ge 4 \text{ and odd} \end{cases} .$$

Proof: a) Firstly, let *n* be even, then by Theorem 2

$$p_{ue}(\varepsilon, C) = \sum_{l=d}^{n/2} A_l \varepsilon^l (1-\varepsilon)^{n-l} + \sum_{l=n/2+1}^{n} A_l \varepsilon^l (1-\varepsilon)^{n-l}$$

$$\le \frac{72}{121} \sqrt{2\pi} \sum_{l=d}^{\lfloor n/2 \rfloor} \frac{\sqrt{n}}{2^r} \cdot \binom{n}{l} \varepsilon^l (1-\varepsilon)^{n-l} + R_n(\varepsilon),$$

where (by Theorem 4 with *q* = *n*/2 and Stirling's approximation)

$$R_n(\varepsilon) = \sum_{l=q+1}^{n} A_l \varepsilon^l (1-\varepsilon)^{n-l}$$

$$\le \sum_{l=q}^{n} A_l \varepsilon^l (1-\varepsilon)^{n-l}$$

$$= \frac{n!}{q!(n-q)!} \varepsilon^q$$

$$\le \frac{2\sqrt{2\pi n}\, n^n \mathrm{e}^{-n}}{\sqrt{2\pi q}\, q^q \mathrm{e}^{-q} \sqrt{2\pi(n-q)}\, (n-q)^{n-q} \mathrm{e}^{-(n-q)}} \varepsilon^q$$

$$= \sqrt{\frac{2n}{\pi (n/2)(n/2)}} \frac{n^n}{(n/2)^{n/2} (n/2)^{n/2}} \varepsilon^{n/2}$$

$$\le \left(2\sqrt{\varepsilon}\right)^n ,$$

if $n \ge 3$. Let now n be odd, then again by Theorem 2

$$p_{ue}(\varepsilon, C) = \sum_{l=d}^{(n-1)/2} A_l \varepsilon^l (1-\varepsilon)^{n-l} + \sum_{l=(n+1)/2}^{n} A_l \varepsilon^l (1-\varepsilon)^{n-l}$$

$$\le \frac{72}{121} \sqrt{2\pi} \sum_{l=d}^{\lfloor n/2 \rfloor} \frac{\sqrt{n}}{2^r} \cdot \binom{n}{l} \varepsilon^l (1-\varepsilon)^{n-l} + R_n(\varepsilon),$$

where, by Theorem 4 with *q* = (*n* - 1)/2, and, as in the proof of the "even case", by Stirling's approximation

$$R_n(\varepsilon) = \sum_{l=q+1}^{n} A_l \varepsilon^l (1-\varepsilon)^{n-l}$$

$$\le \sum_{l=q}^{n} A_l \varepsilon^l (1-\varepsilon)^{n-l}$$

$$\le \binom{n}{q} \varepsilon^q$$

$$= \frac{n!}{q!(n-q)!} \varepsilon^q$$

$$
\begin{aligned}
&= \frac{2q+1}{q+1}\frac{(2q)!}{q!q!}\varepsilon^{q} \\
&\le 2\frac{(2q)!}{q!q!}\varepsilon^{q} \\
&\le \frac{2\cdot 2\sqrt{2\pi 2q}(2q)^{2q}\mathrm{e}^{-2q}\cdot\varepsilon^{q}}{\sqrt{2\pi q}q^{\mathrm{q}}\mathrm{e}^{-q}\sqrt{2\pi(2q-q)}(2q-q)^{2q-q}\mathrm{e}^{-(2q-q)}} \\
&= \frac{2\sqrt{2\pi 2q}(2q)^{2q}\mathrm{e}^{-2q}\cdot\varepsilon^{q}}{\sqrt{2\pi q}q^{q}\mathrm{e}^{-q}\sqrt{2\pi q}(q)^{q}\mathrm{e}^{-q}} \\
&= \frac{2\cdot 2^{2q}\cdot\varepsilon^{q}}{\sqrt{\pi q}} \\
&= \frac{2\cdot 2^{n\text{-}1}\cdot\varepsilon^{\frac{n\text{-}1}{2}}}{\sqrt{\pi\frac{n\text{-}1}{2}}} \\
&\le 2\left(2\sqrt{\varepsilon}\right)^{n-1},
\end{aligned}
$$

if $n \ge 4$. ■

Remark 4: Even for relatively large ε (= 10^{-2}) and relatively small n (= 40, imagine a payload of 1 byte and a CRC-32) the remainder term $R_n(\varepsilon)$ is so small (< 10^{-26}) that it doesn't carry any weight compared with the first term on the right hand side of (8).

Now, as a consequence of Theorems 4 and 6, an analogon of Theorem 5 for proper linear codes emerges.

Theorem 7: Let C be a proper linear code, then for all $\varepsilon \in [0, 1/2]$ the probability of undetected error is upper bounded by:

$$\text{(9)}\qquad p_{ue}(\varepsilon, C) \le \frac{72}{121}\sqrt{2\pi}\frac{\sqrt{n}}{2^{r}}\frac{1}{d!}n^{d}\varepsilon^{d} + R_n(\varepsilon),$$

where d is the minimum distance of C, and the remainder term $R_n(\varepsilon)$ obeys

$$R_n(\varepsilon) \le \binom{n}{\lfloor n/2 \rfloor}\varepsilon^{\lfloor n/2 \rfloor} \le \begin{cases} \left(2\sqrt{\varepsilon}\right)^{n} & \text{,if n} \ge 3 \text{ and even,} \\ 2\left(2\sqrt{\varepsilon}\right)^{n-1} & \text{,if n} \ge 4 \text{ and odd} \end{cases}.$$

Proof: a) By Theorem 6 we obtain

$$
\begin{aligned}
p_{\mathrm{ue}}(\varepsilon, C) &\le \frac{72}{121}\sqrt{2\pi}\sum_{l=d}^{\lfloor n/2 \rfloor}\frac{\sqrt{n}}{2^{r}}\cdot\binom{n}{l}\varepsilon^{l}\left(1-\varepsilon\right)^{n-l} + R_n(\varepsilon) \\
&\le \frac{72}{121}\sqrt{2\pi}\frac{\sqrt{n}}{2^{r}}\sum_{l=d}^{n}\binom{n}{l}\varepsilon^{l}\left(1-\varepsilon\right)^{n-l} + R_n(\varepsilon) \\
&\le \frac{72}{121}\sqrt{2\pi}\frac{\sqrt{n}}{2^{r}}\frac{1}{d!}n^{d}\varepsilon^{d} + R_n(\varepsilon),
\end{aligned}
$$

the last inequality emerging from Theorem 4. ■

Finally let us state the subsequent Remarks, pointing out the influence of properness on the size of the probability of undetected error on one hand, and on maximal block lengths on the other hand.

Remark 5: In the case of a CRC of length r and for all n not too large, inequality (9) improves inequality (6) by a factor of

$$\frac{72}{121}\frac{\sqrt{2\pi n}}{2^{r}}.$$

Remark 6: Similar to (6) inequality (9) too is useful for calculating maximal block lengths in order to achieve a specific upper bound σ on $p_{\mathrm{ue}}(\varepsilon,C)$:

$$\text{(10)}\qquad p_{ue}(\varepsilon, C) \le \frac{72}{121}\sqrt{2\pi}\frac{\sqrt{n}}{2^{r}}\frac{1}{d!}n^{d}\varepsilon^{d} + R_n(\varepsilon) < \sigma.$$

As in the case of Remark 3, solving

$$\frac{72}{121}\sqrt{2\pi}\frac{\sqrt{n}}{2^{r}}\frac{1}{d!}n^{d}\varepsilon^{d} < \sigma.$$

for n yields

$$n_{max} < \left(\varepsilon^{-d}\cdot\sigma\cdot d!\cdot\frac{121}{72}\frac{1}{\sqrt{2\pi}}2^{r}\right)^{1/(d+0.5)}.$$

I.e., apart from $R_n(\varepsilon)$, being small compared with the other term on the right hand side of (9), you only have to choose

$$\text{(11)}\qquad n_{max} < \left(\varepsilon^{-d}\cdot\sigma\cdot d!\cdot\frac{121}{72}\frac{1}{\sqrt{2\pi}}2^{r}\right)^{1/(d+0.5)},$$

and ensure $R_n(\varepsilon)$ to be small enough such that (10) is fulfilled.

In the case of a CRC of length r, inequality (11) improves inequality (7) by an order of magnitude of

$$\left(\frac{121}{72}\frac{1}{\sqrt{2\pi}}2^r\right)^{1/(d+0.5)} .$$

4 The Range of Monotonicity of $p_{\mathrm{ue}}(\varepsilon,C)$

With respect to Theorem 2 we thought it useful to investigate the question of intervals, where $p_{\mathrm{ue}}(\varepsilon,C)$ is an increasing function of ε. In [9] Dodunekova and Nikolova determined intervals, where $p_{\mathrm{ue}}(\varepsilon,C)$ increases. Let us first take a glance upon their results.

The dual code $C^\perp$ of C is defined as the space of all n-tuples orthogonal to all code words of C:

$$C^\perp = \{\boldsymbol{x} : \boldsymbol{x}\cdot\boldsymbol{c} = 0 \text{ for all } \boldsymbol{c}\in C\} \qquad .$$

The dual code is an $[n, n - k]$ linear code. Its weight distribution is closely related to the weight distribution of C by the MacWilliams Identities.

Let now C be a binary linear code and $d^\perp$ the minimum distance of its dual $C^\perp$ (the "dual distance"), then according to Dodunekova and Nikolova the following results hold:

1. If

$$(12) \qquad d^\perp \ge \left\lfloor \frac{n}{2} \right\rfloor + 1,$$

then C are $C^\perp$ proper in [0, 1/2].

2. If $\lceil x \rceil$ represents the ceiling function (smallest integer not less than x) and

$$(13) \qquad \left\lceil \frac{n}{3} \right\rceil \le d^\perp \le \left\lfloor \frac{n}{2} \right\rfloor,$$

then C is proper in the interval

$$(14) \qquad \left[\frac{n+1-2d^\perp}{n-d^\perp}, \frac{1}{2}\right].$$

One aim of this section is to generalize the conditions (12) and (13) and to spare them in the case of a CRC. On the other hand, for a CRC, we shall give a new interval of monotonic behavior instead of (14), pointing out the association to the degree of the CRC-polynomial more clearly.

Theorem 8 states a clear relationship between the order of growth of the dual distance and the range of monotonicity of a binary linear code.

Theorem 8: Let C be a binary linear code and suppose that there is natural number r such that

$$(15) \qquad d^\perp \ge \frac{n}{r} - 1$$

for all $n > 2r$. Then, if $n > 2r$, $p_{\mathrm{ue}}(\varepsilon,C)$ increases on the interval

$$J = \left[\frac{1}{2}\left(1 - \frac{1}{2^\rho - 1}\right), \frac{1}{2}\right],$$

where the number ρ is given by

$$\rho = r\frac{n-1}{n-2r}.$$

Proof: According to Dodunekova and Nikolova in [9], the following inequality

$$\frac{\frac{\mathrm{d}}{\mathrm{d}\varepsilon} p_{ue}(\varepsilon,C)}{n(1-\varepsilon)^{n-l}} = 1 - \frac{2^k}{n}\sum_{l=d^\perp}^{n} lB_l\delta^{l-1}(1-\delta)^{n-l}$$
$$\ge 1 - 2^{n-1}\delta^{d^\perp - 1}(1-\delta)^{n-d^\perp},$$

holds for the derivative of $p_{\mathrm{ue}}(\varepsilon,C)$, where

$$(16) \qquad \delta = 1 - \frac{1}{2(1-\varepsilon)}$$

(ε and δ being always between 0 and 0.5). It is at this point that our prove continues in a manner different from Dodunekova's and Nikolova's in [9], and thus (15) yields

$$\frac{\frac{\mathrm{d}}{\mathrm{d}\varepsilon} p_{ue}(\varepsilon,C)}{n(1-\varepsilon)^{n-1}} \ge 1 - 2^{n-1}\delta^{d^\perp - 1}$$
$$\ge 1 - 2^{n-1}\delta^{\frac{n}{r}-2}.$$

If now ε is taken from J, then

$$\varepsilon \ge \frac{1}{2}\left(1 - \frac{1}{2^\rho - 1}\right),$$

and therefore because of (16)

$$\begin{aligned}\delta &\le 1-\frac{1}{2\left(1-\frac{1}{2}\left(1-\frac{1}{2^{\rho}-1}\right)\right)}\\ &=1-\frac{1}{1+\frac{1}{2^{\rho}-1}}\\ &=1-\frac{2^{\rho}-1}{2^{\rho}}\\ &=\frac{1}{2^{\rho}}.\end{aligned}$$

Hence

$$\begin{aligned}1-2^{n-1}\delta^{\frac{n}{r}-2} &\ge 1-2^{n-1}\left(\frac{1}{2^{\rho}}\right)^{\frac{n}{r}-2}\\ &=1-2^{n-1}\left(2^{-r\frac{n-1}{n-2r}}\right)^{\frac{n-2r}{r}}\\ &=1-1\\ &=0,\end{aligned}$$

leading finally to

$$\frac{\frac{\mathrm{d}}{\mathrm{d}\varepsilon}p_{ue}(\varepsilon,C)}{n(1-\varepsilon)^{n-1}}\ge 0.$$ ■

On the other hand, in [22] we proved that a lower bound on the dual distance $d^{\perp}$ of a CRC is given by

$$d_n^{\perp}\ge\left\lfloor\frac{n}{r}\right\rfloor\ge\frac{n}{r}-1,$$

where r is the degree of its generating polynomial. That is, for a CRC the assumptions of Theorem 8 are satisfied, with r being the degree of its generating polynomial. This remark yields

Theorem 9: Let C be a CRC with a generating polynomial of degree r and $n > 2r$. Then $p_{\mathrm{ue}}(\varepsilon,C)$ increases on the interval

$$\left[\frac{1}{2}\left(1-\frac{1}{2^{\rho}-1}\right),\frac{1}{2}\right], \tag{17}$$

where the number ρ is given by

$$\rho=r\frac{n-1}{n-2r}.$$

Remark 7: For large n, ρ tends to r

$$\lim_{n\to\infty}\rho=r,$$

a fact revealing, in which way the range of monotonicity depends on the degree r of the CRC-polynomial.

Remark 8: Inequality (15) corresponds to (12) and (13) of Dodunekova and Nikolova in [9] respectively replaces them. However, the relationship between our interval (17) and Dodunekova's and Nikolova's interval (14) is more difficult to understand.

5 The 2^{-r}-Bound on $p_{\mathrm{ue}}(\varepsilon,C)$

According to Remark 2 and the last section, we shall now investigate the problem of finding intervals, where $p_{\mathrm{ue}}(\varepsilon,C)$ satisfies the 2^{-r}-bound. For a couple of years it was supposed that CRCs satisfy the 2^{-r}-bound on [0, 1/2]. Unfortunately this is not true (for codes violating the 2^{-r}-bound see Witzke&Leung [24] or Wolf&Blakeney [25]). In [22] we managed to prove a weaker form of the 2^{-r}-bound for CRCs:

$$p_{\mathrm{ue}}(\varepsilon,C_n)\le 2^{-r}+\frac{2^r-1}{2^r}(1-2\varepsilon)^{\frac{R}{r}n}-(1-\varepsilon)^n, \tag{18}$$

where $R = k/n = (n - r)/n$ is the rate of the CRC. With the help of (18) we now get the subsequent Theorem showing an interval, where $p_{\mathrm{ue}}(\varepsilon,C)$ obeys the 2^{-r}-bound.

Theorem 10: Let C be a CRC with a generating polynomial of degree r. Then $p_{\mathrm{ue}}(\varepsilon,C)$ satisfies the 2^{-r}-bound on the interval

$$J=\left[\frac{1}{2}\left(1-\frac{1}{2^{\sigma}-\sigma}\right),\frac{1}{2}\right], \tag{19}$$

where the number σ is given by

$$\sigma=\frac{r}{R}.$$

Proof: To proof the Theorem it is sufficient to show

$$(1-2\varepsilon)^{\frac{R}{r}n}\le(1-\varepsilon)^n$$

or (being the same)

$$(20) \qquad 1-2\varepsilon \le f(\varepsilon)\,.$$

where

$$f(\varepsilon) = (1-\varepsilon)^{\sigma}\,.$$

Now for all $\varepsilon \in J$

$$\begin{aligned} 1+(\sigma\cdot 2^{-\sigma+1}-2)\varepsilon &= 1-2^{-\sigma+1}(2^{\sigma}-\sigma)\varepsilon \\ &\le 1-2^{-\sigma+1}(2^{\sigma}-\sigma)\frac{1}{2}\left(1-\frac{1}{2^{\sigma}-\sigma}\right). \\ &= 1-2^{-\sigma}(2^{\sigma}-\sigma)+2^{-\sigma} \\ &= \sigma\cdot 2^{-\sigma}+2^{-\sigma} \end{aligned}$$

and hence

$$\begin{aligned} 1-2\varepsilon &\le \sigma\cdot 2^{-\sigma}+2^{-\sigma}-\sigma\cdot 2^{-\sigma+1}\varepsilon \\ &= 2^{-\sigma}-\sigma\cdot 2^{-\sigma+1}(\varepsilon-1/2) \\ &= \tau(\varepsilon) \end{aligned}$$

where

$$\tau(\varepsilon) = 2^{-\sigma}-\sigma\cdot 2^{-\sigma+1}(\varepsilon-1/2)$$

is the tangent at the function $f(\varepsilon)$ in $\varepsilon = ½$. Now, because $f(\varepsilon)$ is a convex function on [0,1], we have

$$\tau(\varepsilon) \le f(\varepsilon)$$

on [0,1], yielding (20). ■

Remark 9: As in Remark 7, for large n σ tends to r

$$\lim_{n\to\infty} \sigma = r\,,$$

and therefore the size of (19) for large n and r is approximately the same as (17).

6 Application to Safety Integrity Levels

As an application of our results, let us now have a closer look at data integrity according to IEC 68508. According to Remark 6 in subsection 3.3 we wanted to analyze the effect of properness on maximal block lengths achievable for a specific Safety Integrity Level (SIL). Safety Integrity Levels are defined by means of the number Λ of undetected errors per hour:

$$\Lambda = 3600\cdot p_{ue}(\varepsilon, C)\cdot v\cdot(m\text{-}1)\cdot 100$$

where

ν = number of safety related messages per second
m = number of communicating devices
100 = 1%-rule

(See IEC 61508 2000, [14]. A more detailed analysis of safety networks and the used items can be found in [5] and [6].) For our example, we decided to choose $\nu = 100$, a value suggested by experience, and $m = 2$. In this way we get

$$(21) \qquad \Lambda = 3{,}6\cdot 10^{7}\cdot p_{ue}(\varepsilon, C)\,.$$

If no details are known about the quality of the transmission especially about the electromagnetic compatibility (EMC), and nothing can be said about the bit-error probability ε, the Technical Control Board of Germany requires to do all calculations concerning Λ with $\varepsilon = 10^{-2}$. Therefore for our analysis we took account of this bad value of ε.

If on the other hand no details are known about the weight distribution of the code C, the only chance of estimating the probability of undetected error is to use (6) or (9).

We based our calculations on the results of Castagnoli et al. in [7] about the CRC-32/6 polynomial. According to [7], CRC-32/6 is proper for all n ≤ 32767. It is exemplary for a lot of other CRCs, for which similar results are known (see for example [3], [7], [8], [10], [11], [12]).

By means of (7) and (11) we then derived the content of table 1 from the results in [7] about the minimum distance d as a function of n.

Table 1: Maximal block lengths for CRC-32/6

SIL	Λ high demand	$n_{\max}$ by (7)	$n_{\max}$ by (11)
4	10^{-8}	37	56
3	10^{-7}	37	66
2	10^{-6}	39	87
1	10^{-5}	43	114

Using (7) SIL 3 and 4 are achievable with a payload of only 5 bits. In contrast to this fact, with the help of (11) they are achievable with a payload of 34 respectively 24 bits. This result shows the improvement of (11) compared with (7) with regard of practical application.

7 Conclusions

Firstly, via monotonicity, the binomiality of the weight distribution of a linear code has been investigated. Then an upper bound on the probability of undetected error of a class of codes has been proven, which is important for practical applications in safety related systems. The bound can be calculated without knowledge of the complete weight distribution of the code. Only the knowledge of the minimum distance is required. It improves a bound used so far in this field.

Next results of Dodunekova and Nikolova have been analyzed and improved by determining intervals, where the probability of undetected error is an increasing function of the bit error probability ε. Especially the relationship between those intervals and the degree of the generating polynomial of a CRC becomes evident.

Then, in an analogous way, the question of the validness of the 2^{-r}-bound was investigated. Intervals have been deduced, where the 2^{-r}-bound is satisfied. Those intervals turned out to be very similar to those concerning monotonicity.

Finally numerical examples have been given for block lengths being maximal for achieving specific safety integrity levels. The improvement of those block lengths compared with older results has been shown.

References:

[1] Ashikhmin, A., Barg, A., and Litsyn, S., "Estimates of the Distance Distribution of Codes and Designs," *IEEE Trans. Inform. Theory*, vol. 47, no. 3, March 2001. pp. 1050–1061.

[2] Ashikhmin, A., Cohen, G.D., Krivelevich, M. and Litsyn, S., "Bounds on Distance Distributions on Codes of Known Size," *IEEE Trans. Inform. Theory*, vol. 51, no. 1, Jan. 2005. pp. 250–258.

[3] Baicheva, T., Dodunekov, S., and Kazakov, P., "Undetected error probability performance of cyclic redundancy-check codes of 16-bit redundancy," *IEE Proc.- Commun.*, Vol. 147, No. 5, October 2000.

[4] Boercsoek, J., Hoelzel, J., Wacker, H.D. „Probability of Undetected Error with Redundant Data Transmission on Binary Symmetric and Non-symmetric Channels without Memory", *WSEAS Transactions on Communications*, Issue 2, Volume 6, February 2007 ISSN 1109-2742.

[5] Börcsök, J., Schwarz M.H., Holub P., "Concepts of Safety Networks in Industries", *WSEAS Transactions on Communications,* Issue 8, Volume 5, August 2006 ISSN 1109-2742

[6] Börcsök, J., Ugljesa E., Holub P., "Concepts of Safety Networks in Industries – Part II", *WSEAS Transactions on Communications,* Issue 8, Volume 5, August 2006 ISSN 1109-2742

[7] Castagnoli, G., Braeuer, S., and Herrman, M., "Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits," *IEEE Trans. on Communications*, Vol. 41, No. 6, June 1993. pp. 883-992.

[8] Castagnoli, G., Ganz. J., and Graber, P., "Optimum Cyclic Redundancy-Check Codes with 16-Bit Redundancy," *IEEE Trans. on Communications*, Vol. 38, No. 1, 1990, pp. 111-114.

[9] Dodunekova, R., and Nikolova, E., "Sufficient Conditions for Monotonicity of the Undetected Error Probability for Large Channel Error Probabilities," *IEE Proc.- CommunProblems of Information Transmission*, Vol. 41, No. 3, 2005. Translated from *Problemy Peredachi Informatii*, No. 3, 2005, pp. 3-16. Original Russian Text Copyright © 2005 by Dodunekova, Nikolova.

[10] Fujiwara, T., Kasami, T., and Lin, S., "Error Detecting Capabilities of the Shortened Hamming Codes Adopted for Error Detection in IEEE Standard 802.3," *IEEE Trans. on Communications*, Vol. 37, No. 9, Sept. 1989. p. 986-989.

[11] Fujiwara, T., Kasami, T., and Lin, S., "On the Undetected Error Probability for Shortened Hamming Codes," *IEEE Trans. on Communications*, Vol. COM-33, No. 6, Sept. 1985. pp. 570-574.

[12] Funk, G., "Determination of Best Shortened Linear Codes," *IEEE Trans. on Communications*, Vol. 4, No. 1, Jan. 1996. pp. 1-6.

[13] Hillmer, H., Wang, Y., Kusserow, T., Irmer, S., Dharmarasu, N., Hasse, A., Mikami, O., Bartels, M., „Wavelength Division Multiplexing (WDM) for Secure Optical Data Communication in Industrial Computers, Process Control and Fabrication Systems", *WSEAS Trans. on Communications*, Issue 2, Volume 6, February 2007 ISSN 1109-2742.

[14] IEC 61508, International Standard 61508: Functional safety of electrical/electronic/ Programmable electronic safety-related systems, Geneva, International Electrotechnical Commission, 2000

[15] IEC 61784-3 Ed.1: Digital data communications for measurement and control - Part3: Profiles for functional safety communications in industrial networks

[16] Krasikov, I., and Litsyn, S., "Bounds on Spectra of Codes with Known Dual Distance," *Des.Codes Cryptogr.*, vol. 13, no. 3, pp. 285–297, 1998.

[17] Krasikov, I. and Litsyn, S., "Estimates for the Range of Binomiality in Codes Spectra," *IEEE Trans. on Information Theory*, vol. 43, no. 3, May 1997. pp. 987–990.

[18] Krasikov, I. and Litsyn, S., "Linear Programming Bounds for Doubly-Even Self-Dual Codes," *IEEE Trans. on Information Theory*, vol. 43, no. 4July 1997. pp. 1238–1244.

[19] Perry, P., "Necessary Conditions for Good Error Detection," *IEEE Trans. Inform. Theory*, vol. 37, no. 2, March. 1991. pp. 375–378.

[20] Peterson, W. W. and Weldon, E. J., *Error Correcting Codes*. The MIT Press Cambridge, Massachusetts , and London, England, Second Edition 1972.

[21] Velten-Philipp, W., Houtermans, M.J.M., Fieldbus: A solution for safety and availability? *Proceedings of the 6th WSEAS International Conference on Applied Computer Science* (ACS'06), Tenerife, Canary Islands, Spain, December 16-18, 2006

[22] Wacker, H., D., Boercsoek, J., "The Minimum Distance of the Dual of a CRC", *Proceedings of the 5th WSEAS International Conference Computational Intelligence, Man-Machine Systems and Cybernetics (CIMMACS '07)*, Puerto De La Cruz, Tenerife, Canary Islands, Spain, December 14-16, 2007.

[23] Wacker, H., D., Boercsoek, J., Hillmer, H. "Redundant Optical Data Transmission Using Semiconductor Lasers", *Proceedings of The 6th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA-08)*, Doha, Qatar March 31 - April 4, 2008, accepted.

[24] Witzke, K. A., and Leung, C., "A Comparison of Some Error Detecting CRC Code Standards," *IEEE Trans. on Communications*, Vol. COM-33, No. 9, Sept. 1985. pp. 996-998.

[25] Wolf, J. K., Michelson, A. M., Levesque, A. H., "On the probability of undetected error for linear block codes," *IEEE Trans. on Communications*, Vol. COM-30, No. , Febuary. 1982. pp. 317-324.

[26] Zivic, N., Ruland, C., "Channel Coding as a Cryptography Enhancer", *Proceedings of the 11th WSEAS International Conference on Communications*, Agios Nikolaos, Crete Island, Greece, July 26-28, 2007