The Dual Distance of a CRC and Bounds on the Probability of Undetected Error, the Weight Distribution, and the Covering Radius

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: - Dual codes play an important role in the field of error detecting codes on a binary symmetric channel. Via the MacWilliams Identities they can be used to calculate the original code's weight distribution and its probability of undetected error. Moreover, knowledge of the minimum distance of the dual code provides insight in the properties of the weights of a code. In this paper firstly the order of growth of the dual distance of a CRC as a function of the block length n is investigated, and a new lower bound is proven. Then this bound is used to derive a weaker version of the 2^{-r}-bound on the probability of undetected error, and the relationship of this bound to the 2^{-r}-bound is discussed. Estimates of the range of binomiality and the covering radius are given, depending only on the code rate R and the degree r of the generating polynomial of the CRC. In the case of a CRC, two results of Tietäväinen are improved. Furthermore, wit is shown that there is binomial behavior of the weight distribution, if only n is large enough. Then, by means of an estimate of the tail of the binomial, another bound on the probability of undetected error is verified. Finally a new version of Sidel'nikov's theorem on the normality of the cumulative distribution function of the weights of a code is presented, where the dual distance is replaced by an expression depending on n and the degree r. In this way the conclusions of the present paper may attribute a new meaning to some well known results about codes with known dual distance and give some new insight in this kind of problems.

Key-Words: - CRC, Binary Symmetric Channel, Probability of Undetected Error, Weight Distribution, MacWilliams Identities, Binomiality, Dual Distance, Gaussian Distribution, Covering Radius, Sidel'nikov's theorem.

1 Introduction

Let C_n be a $[n, k]$ linear code on a binary symmetric channel without memory, where n is the block length and k is the dimension of the code. The probability of undetected error of such a code is given by (see[15] for example):

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

where

A_l = component of the weight distribution of C_n
= number of code words of weight l,

ε = bit error probability,

n = block length.

d_n = minimum distance of C_n.

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

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

The dual code is an $[n, n - k]$ linear code. Its weight distribution is closely related to the weight distribution of C_n by the MacWilliams Identities (see [15]). The minimum distance of $C_n^{\perp}$ is the minimum weight of all code words in $C_n^{\perp}$

$$d_n^{\perp} = \min\{w(\boldsymbol{c}) : \boldsymbol{c} \in C_n^{\perp}, \boldsymbol{c} \neq \boldsymbol{0}\},$$

usually being called the "dual distance". If B_l are the components of the weight distribution of $C_n^{\perp}$, the subsequent equation is an easy consequence of those identities (cf. [23] for example):

$$(2) \qquad p_{ue}(\varepsilon, C_n) = 2^{-r}\{1 + \sum_{l=d_n^{\perp}}^{n} B_l (1-2\varepsilon)^l\} - (1-\varepsilon)^n,$$

where $r = n - k$. In the case of a CRC r is the degree of the generating polynomial. This equation turned out to be a useful instrument for calculating the probability of undetected error via the weight distribution of the dual code. This has been done in a lot of papers for a lot of Codes (see for example [5], [6], [7], [8], [9], [10], [22]).

On the other hand we thought it to be the appropriate tool to investigate the properties of the probability of undetected error in a more general way.

2 The Role of the Dual Distance

Because of (2) it was to be expected that $d_n^\perp$ would play a major role when dealing with bounds on $p_{ue}(\varepsilon,C_n)$. But the dual distance on its own is a code parameter deserving closer attention.

In [2], [11] and [12] bounds on the components of the weight distribution can be found for codes with known dual distance. One of the leading parts in this game is occupied by the relative dual distance

$$\delta_n^\perp = \frac{d_n^\perp}{n}.$$

Witzke and Leung in [21] used (2) to show that for a CRC C_n generated by a polynomial of degree r the probability of undetected error converges to the 2^{-r}-bound

$$\lim_{n\to\infty} p_{ue}(\varepsilon, C_n) = 2^{-r} \tag{3}$$

for all $0 < \varepsilon \le ½$. Part of their proof is the fact that the minimum distance $d_n^\perp$ of $C_n^\perp$ "increases without bound" as n (or k) increases. But their proof does not show how exactly $d_n^\perp$ depends on n. Nor it gives any hint as to the order of growth of $d_n^\perp$. Furthermore it contains no statement how fast or how slow convergence in (3) has to be understood, and there is no error estimate.

Because until now there is no general answer to the question, which codes are satisfying the 2^{-r}-bound, we thought it desirable to get bounds on $p_{ue}(\varepsilon,C_n)$ weaker than the 2^{-r}-bound but involving it. That is, the problem is to find the order of growth of $d_n^\perp$ as n increases and then to find bounds on $\delta_n^\perp$ and on $p_{ue}(\varepsilon,C_n)$. This will be done in the next section.

Once determined the order of growth of $d_n^\perp$, it will be an easy task to attribute a new meaning to some results about codes with known dual distance.

3 The Order of Growth of the Dual Distance

3.1 A Lower Bound on $d_n^\perp$

Let us first state our main result. As Witzke's and Leung's proof does, our proof is based on (2) and on the matrix representation of $C_n^\perp$.

As common use, $\lfloor x \rfloor$ has the meaning of the floor function..

Theorem 1: Let C_n be a $[n, k]$ CRC with a generating polynomial g of degree $r = n - k$, then a lower bound on the dual distance $d_n^\perp$ is given by

$$d_n^\perp \ge \left\lfloor \frac{n}{r} \right\rfloor. \tag{4}$$

Proof: Without loss of generality we may assume that

$$g(X) = \lambda_0 + \lambda_1 X + \cdots + \lambda_r X^r$$

with λ_0 and λ_r different from 0.

The generating matrix $\boldsymbol{H}$ of $C_n^\perp$ consists of an r x r identity part $\boldsymbol{I_{n-k}}$ and a r x k parity part $\boldsymbol{P^T}$ (cf. [15] and [20] for example)**:**

$$\boldsymbol{H} = (\boldsymbol{I_{n-k}} \mid \boldsymbol{P^T}).$$

Let furthermore t be defined by

$$t = \left\lfloor \frac{n}{r} \right\rfloor.$$

Then

$$\boldsymbol{P^T} = \begin{pmatrix} \rho_{1r} \cdots \rho_{12r-1}\rho_{12r} \cdots \rho_{13r-1}\rho_{13r} \cdots \rho_{1tr} \cdots \rho_{1n} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ \rho_{rr} \cdots \rho_{r2r-1}\rho_{r2r} \cdots \rho_{r3r-1}\rho_{r3r} \cdots \rho_{rtr} \cdots \rho_{rn} \end{pmatrix},$$

where the elements of the i^{th} column

$$\begin{pmatrix} \rho_{1i} \\ \vdots \\ \rho_{ri} \end{pmatrix}$$

are the coefficients of a representative of the congruence class $\{X^i\}$ of X^i modulo $g(X)$. Hence the parity part $\boldsymbol{P^T}$ is composed of square matrices $\boldsymbol{P_j}$ and a residue term $\boldsymbol{R_n}$

$$\boldsymbol{P^T} = (\boldsymbol{P_1}\ \boldsymbol{P_2} \cdots \boldsymbol{P_{t\text{-}1}}\ \boldsymbol{R_n})$$

with

$$\boldsymbol{P_j} = \begin{pmatrix} \rho_{1jr} \cdots \rho_{1(j+1)r-1} \\ \vdots \quad\quad \vdots \\ \rho_{rjr} \cdots \rho_{r(j+1)r-1} \end{pmatrix}$$

and

$$\boldsymbol{R_n} = \begin{pmatrix} \rho_{1tr} \cdots \rho_{1n} \\ \vdots \qquad \vdots \\ \rho_{rtr} \cdots \rho_{rn} \end{pmatrix}.$$

First of all we shall prove that the column vectors of $\boldsymbol{P_j}$ are linearly independent for all j =1, 2,…, t - 1 . Assume therefore

$$\alpha_0 \begin{pmatrix} \rho_{1\,jr} \\ \vdots \\ \rho_{rjr} \end{pmatrix} + \alpha_1 \begin{pmatrix} \rho_{1\,jr+1} \\ \vdots \\ \rho_{rjr+1} \end{pmatrix} + \cdots + \alpha_{r\text{-}1} \begin{pmatrix} \rho_{1(j+1)r-1} \\ \vdots \\ \rho_{r(j+1)r-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Because the vectors

$$\begin{pmatrix} \rho_{1\,jr} \\ \vdots \\ \rho_{rjr} \end{pmatrix}, \begin{pmatrix} \rho_{1\,jr+1} \\ \vdots \\ \rho_{rjr+1} \end{pmatrix}, \cdots, \begin{pmatrix} \rho_{1(j+1)r-1} \\ \vdots \\ \rho_{r(j+1)r-1} \end{pmatrix}$$

are the representatives of the congruence classes

$$\{X^{jr}\}, \{X^{jr+1}\}, \cdots, \{X^{(j+1)r-1}\},$$

the congruence class of

$$X^{jr}(\alpha_0 + \alpha_1 X + \cdots + \alpha_{r\text{-}1} X^{r-1})$$

satisfies the equation

$$\begin{aligned} &\{X^{jr}(\alpha_0 + \alpha_1 X + \cdots + \alpha_{r\text{-}1} X^{r-1})\} \\ &\quad = \{\alpha_0 X^{jr} + \alpha_1 X^{jr+1} + \cdots + \alpha_{r\text{-}1} X^{(j+1)r-1}\} \\ &\quad = \alpha_0 \{X^{jr}\} + \alpha_1 \{X^{jr+1}\} + \cdots + \alpha_{r\text{-}1} \{X^{(j+1)r-1}\} \\ &\quad = 0. \end{aligned}$$

Therefore the polynomial

$$X^{jr}(\alpha_0 + \alpha_1 X + \cdots + \alpha_{r\text{-}1} X^{r-1})$$

is divisible by $g(X)$. And because X^{jr} is not contained in $g(X)$ as a factor, the polynomial

$$\alpha_0 + \alpha_1 X + \cdots + \alpha_{r\text{-}1} X^{r-1}$$

(degree r - 1) must be divisible by $g(X)$ (degree r). This can be true only if $\alpha_0 + \alpha_1 X + \cdots + \alpha_{r\text{-}1} X^{r-1}$ is the zero polynomial, i.e. $\alpha_0 = \alpha_1 = \cdots = \alpha_{r\text{-}1} = 0$. Because the row rank of a matrix is equal to its column rank, the row vectors

$$(\rho_{1\,jr}, \cdots, \rho_{1(j+1)r-1}), \ldots, (\rho_{rjr}, \cdots, \rho_{r(j+1)r-1})$$

of $\boldsymbol{P_j}$ are linearly independent too for all j =1, 2,… , t - 1. Now for each code vector $\boldsymbol{c} \in C_n^{\perp}$ there exists a message vector

$$\boldsymbol{m} = (m_1, m_2, \cdots, m_r) \neq \boldsymbol{0}$$

such that

$$\begin{aligned} &\boldsymbol{c} = \boldsymbol{m}(\boldsymbol{I_{n\text{-}k}} \mid \boldsymbol{P}^T) \\ &= (\boldsymbol{m}, m_1\rho_{1r} + \cdots + m_r\rho_{rr}, \cdots, m_1\rho_{12r-1} + \cdots + m_r\rho_{r2r-1}, \\ &\qquad m_1\rho_{12r} + \cdots + m_r\rho_{r2r}, \cdots, m_1\rho_{13r-1} + \cdots + m_r\rho_{r3r-1}, \\ &\qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\qquad m_1\rho_{1(t-1)r} + \cdots + m_r\rho_{r(t-1)r}, \cdots, m_1\rho_{1tr-1} + \cdots + m_r\rho_{rtr-1}, \\ &\qquad m_1\rho_{1tr} + \cdots + m_r\rho_{rtr}, \cdots, m_1\rho_{1n} + \cdots + m_r\rho_{rn}). \end{aligned}$$

Consequently the weight of $\boldsymbol{c}$ amounts to

$$\begin{aligned} &w(\boldsymbol{c}) = w(\boldsymbol{m}) + \\ &w(m_1\rho_{1r} + \cdots + m_r\rho_{rr}, \cdots, m_1\rho_{12r-1} + \cdots + m_r\rho_{r2r-1}) + \\ &w(m_1\rho_{12r} + \cdots + m_r\rho_{r2r}, \cdots, m_1\rho_{13r-1} + \cdots + m_r\rho_{r3r-1}) + \\ &\qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &w(m_1\rho_{1(t-1)r} + \cdots + m_r\rho_{r(t-1)r}, \cdots, m_1\rho_{1tr-1} + \cdots + m_r\rho_{rtr-1}) + \\ &w(m_1\rho_{1tr} + \cdots + m_r\rho_{rtr}, \cdots, m_1\rho_{1n} + \cdots + m_r\rho_{rn}) \\ &\quad = w(\boldsymbol{m}) + \\ &w(m_1(\rho_{1r}, \cdots, \rho_{12r-1}) + \cdots + m_r(\rho_{rr}, \cdots, \rho_{r2r-1})) + \\ &w(m_1(\rho_{12r}, \cdots, \rho_{13r-1}) + \cdots + m_r(\rho_{r2r}, \cdots, \rho_{r3r-1})) + \\ &\qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &w(m_1(\rho_{1(t-1)r}, \cdots, \rho_{1tr-1}) + \cdots + m_r(\rho_{r(t-1)r}, \cdots, \rho_{rtr-1})) + \\ &w(m_1(\rho_{1tr}, \cdots, \rho_{1n}) + \cdots + m_r(\rho_{rtr}, \cdots, \rho_{rn})) \\ &\quad = w(\boldsymbol{m}) + \\ &w(m_1(1^{\text{st}} \text{ row of } \boldsymbol{P_1}) + \cdots + m_r(r^{\text{th}} \text{ row of } \boldsymbol{P_1})) + \\ &w(m_1(1^{\text{st}} \text{ row of } \boldsymbol{P_2}) + \cdots + m_r(\text{r}^{\text{th}} \text{ row of } \boldsymbol{P_2})) + \\ &\qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &w(m_1(1^{\text{st}} \text{ row of } \boldsymbol{P_{t-1}}) + \cdots + m_r(\text{r}^{\text{th}} \text{ row of } \boldsymbol{P_{t-1}})) + \\ &w(m_1(1^{\text{st}} \text{ row of } \boldsymbol{R_n}) + \cdots + m_r(\text{r}^{\text{th}} \text{ row of } \boldsymbol{R_n})). \end{aligned}$$

Because the row vectors of $\boldsymbol{P_j}$ are linearly independent, all the vectors

$m_1(1^{\text{st}}\text{ row of }\boldsymbol{P}_1) + \cdots + m_r(r^{\text{th}}\text{ row of }\boldsymbol{P}_1)$
$m_1(1^{\text{st}}\text{ row of }\boldsymbol{P}_2) + \cdots + m_r(\text{r}^{\text{th}}\text{ row of }\boldsymbol{P}_2)$
$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$
$m_1(1^{\text{st}}\text{ row of }\boldsymbol{P}_{t-1}) + \cdots + m_r(\text{r}^{\text{th}}\text{ row of }\boldsymbol{P}_{t-1})$

are different from **0** and consequently have a minimum weight not less than 1. The weight of $\boldsymbol{m} \neq \mathbf{0}$ too is at least 1. This results in

$$\begin{aligned} w(\boldsymbol{c}) &\geq \underbrace{w(\boldsymbol{m})}_{1} + \underbrace{1+1+1+\cdots+1}_{t-1} + \\ &\quad w\big(m_1(1^{\text{st}}\text{ row of }\boldsymbol{R}_n) + \cdots + m_r(\text{r}^{\text{th}}\text{ row of }\boldsymbol{R}_n)\big) \\ &\geq t. \end{aligned}$$

and consequently

$$\begin{aligned} d_n^{\perp} &= \min\{w(\boldsymbol{c}) : \boldsymbol{c} \in C_n^{\perp}, \boldsymbol{c} \neq \mathbf{0}\} \\ &\geq t \\ &= \left\lfloor \frac{n}{r} \right\rfloor. \end{aligned}$$

■

If $R = k/n$ is the rate of the code, an easy conclusion leads to the subsequent

Corollary 2: Let C_n be a $[n, k]$ CRC with a generating polynomial g of degree $r = n - k$, then the dual distance $d_n^{\perp}$ and the relative dual distance $\delta_n^{\perp}$ satisfy the lower bounds

(5) $\quad d_n^{\perp} \geq n\frac{R}{r}$ and $\delta_n^{\perp} \geq \frac{R}{r}$..

Proof: By (4) we get

$$\begin{aligned} d_n^{\perp} &\geq \left\lfloor \frac{n}{r} \right\rfloor \\ &\geq \frac{n}{r} - 1 \\ &= \frac{R}{r} n \end{aligned}$$

■

Corollary 2 reveals us the order of growth of $d_n^{\perp}$: The dual distance increases at least linearly as a function of the block length n. The relative dual distance (the ratio of this linear dependence) is not less than R/r.

3.2 An Upper Bound on the Probability of Undetected Error

From Theorem 1 we immediately get an upper bound on $p_{ue}(\varepsilon, C_n)$

Theorem 3: Let C_n be a $[n, k]$ CRC with a generating polynomial g of degree $r = n - k$, then the probability of undetected error satisfies the upper bound

(6) $$p_{\text{ue}}(\varepsilon, C_n) \leq 2^{-r} + \frac{2^r - 1}{2^r}(1-2\varepsilon)^{\left\lfloor \frac{n}{r} \right\rfloor} - (1-\varepsilon)^n$$

for all $\varepsilon \in [0, 1/2]$.

Proof: By (2) and (4) we get (cf. Wolf et al.[23])

$$\begin{aligned} p_{\text{ue}}(\varepsilon, C_n) &\leq 2^{-r}\{1 + (2^r - 1)(1-2\varepsilon)^{d_n^{\perp}}\} - (1-\varepsilon)^n \\ &= 2^{-r}\{1 + (2^r - 1)(1-2\varepsilon)^{\delta_n^{\perp} n}\} - (1-\varepsilon)^n \\ &\leq 2^{-r} + \frac{2^r - 1}{2^r}(1-2\varepsilon)^{\left\lfloor \frac{n}{r} \right\rfloor} - (1-\varepsilon)^n. \end{aligned}$$

■

From Theorem 3 we then easily deduce:

Corollary 4: Let C_n be a $[n, k]$ CRC with a generating polynomial g of degree $r = n - k$, then the probability of undetected error satisfies the upper bound

$$p_{\text{ue}}(\varepsilon, C_n) \leq 2^{-r} + \frac{2^r - 1}{2^r}(1-2\varepsilon)^{\frac{R}{r} n} - (1-\varepsilon)^n$$

for all $\varepsilon \in [0, 1/2]$.

Remark 1: Omitting the factor $(2^r - 1)2^{-r}$ being close to 1 for r big enough, from (2) and Corollary 4 we get

$$2^{-r} - (1-\varepsilon)^n \leq p_{\text{ue}}(\varepsilon, C_n) \leq 2^{-r} + (1-2\varepsilon)^{\frac{R}{r} n} - (1-\varepsilon)^n,$$

pointing out once more Witzke's&Leung's result: The sequence of functions $(p_{ue}(\varepsilon, C_n))$ converges point wise on $[0, 1/2]$ for $n \to \infty$:

$$p_{\text{ue}}(\varepsilon, C_n) \to h(\varepsilon) = \begin{cases} 2^{-r}, & \text{if } 0 < \varepsilon \leq 1/2 \\ 0, & \text{if } \varepsilon = 0 \end{cases}.$$

The convergence cannot be uniform on $[0, 1/2]$. Otherwise the limit function had to be continuous on $[0, 1/2]$ by the uniform convergence theorem (see Apostol [1]). But evidently $h(\varepsilon)$ is discontinuous at $\varepsilon = 0$.

Remark 2: For a couple of years it was supposed that CRCs satisfy the 2^{-r}-bound. This is not true (for codes violating the 2^{-r}-bound see Wolf et al. [23]). Theorem 3

holds for each CRC, and consequently the bound of Theorem 3 (or Corollary 4) has to be weaker then the 2^{-r}-bound. But anyway, Corollary 4 contains an estimate, how far away the probability of undetected error can be from the 2^{-r}-bound: $p_{ue}(\varepsilon,C_n)$ exceeds 2^{-r} by a maximal amount of

$$\Phi(\varepsilon) := \frac{2^r - 1}{2^r}(1-2\varepsilon)^{\frac{R}{r}n} - (1-\varepsilon)^n .$$

The typical shape of Φ is represented by Fig.1 (n = 544, k = 512, r = 32).

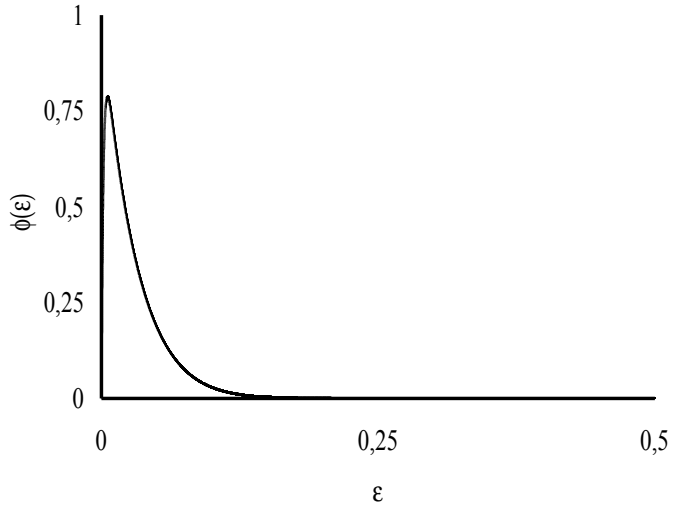

Fig. 1

The Graph of Φ shows a peak of approximately 0.79 near ε =0.0055. It is below peaks of this kind that the humps of the probability of undetected error hide, which are responsible for the violation of the 2^{-r}-bound.

Remark 3: Let us finally have a closer look at the part, the dual distance is playing in our bound. Following the proof of Theorem 3, the inequality

$$(7) \qquad p_{\mathrm{ue}}(\varepsilon, C_n) \le 2^{-\mathrm{r}} + \Psi(\varepsilon, \delta_n^{\perp})$$

holds with

$$\Psi(\varepsilon,\delta') = \frac{2^r - 1}{2^r}(1-2\varepsilon)^{\delta_n^{\perp} n} - (1-\varepsilon)^n .$$

Now , as long as

$$\delta_n^{\perp} < 1/2 ,$$

there are ε ϵ [0, 1/2] with

$$\Psi(\varepsilon, \delta_n^{\perp}) > 0 ,$$

as elementary calculus shows. On the other hand, for

$$\delta_n^{\perp} \ge 1/2$$

the opposite inequality holds:

$$\Psi(\varepsilon, \delta_n^{\perp}) \le 0 .$$

This means that for $\delta_n^{\perp} < ½$ the 2^{-r}-bound is violated by the upper bound contained in (7), whereas for $\delta_n^{\perp} \ge ½$ it is met. This fact is in total accordance with the fact that cyclic Hamming codes obey the 2^{-r}-bound. Namely, Hamming codes are CRCs generated by a primitive polynomial, and their duals are Simplex codes with dual distance

$$\delta_n^{\perp} = \frac{n+1}{2} > \frac{1}{2} .$$

And it is in accordance with Massey's statement in [14], that "there is good reason to believe that, for most codes, worst-case undetected error probability will not occur for ε = 1/2".

But Remark 3 gives a good reason to turn the tables. The 2^{-r}-bound being violated in so many cases, let us investigate now, if there is some subinterval of [0,1/2], where a CRC satisfies the 2^{-r}-bound in a more general sense. Is

$$p_{\mathrm{ue}}(\varepsilon, C_n) \le \frac{\gamma}{2^r}$$

true for certain ε and n? Eventually, for practical purposes, i.e. to estimate the probability of undetected error, this would be sufficient. The answer is given by

Theorem 5: Let C_n be a [n, k] CRC with a generating polynomial g of degree $r = n - k$, $\alpha > 0$, $0 < \beta < 1$, and

$$n(r,\alpha,\beta) := \frac{r^2 - r\log\alpha}{-\log\beta} + r .$$

Then C_n satisfies the generalized 2^{-r}-bound

$$p_{ue}(\varepsilon, C) \le \frac{1+\alpha}{2^r}$$

for all

$$\varepsilon \in [\frac{1}{2}(1-\beta), \frac{1}{2}] \text{ and all } n \geq n(r, \alpha, \beta) .$$

Proof: a) According to Corollary 4, for (1/2)(1 - β) ≤ ε ≤ 1/2 we have

$$\begin{aligned} p_{ue}(\varepsilon, C_n) &\leq 2^{-r} + (1-2\varepsilon)^{\frac{R}{r}n} \\ &\leq 2^{-r} + \beta^{\frac{R}{r}n} \\ &= 2^{-r} + \beta^{\frac{n-r}{r}} \\ &\leq 2^{-r} + \beta^{\frac{\log \alpha - r}{\log \beta}} \\ &= \frac{1+\alpha}{2^r}. \end{aligned}$$

∎

Theorem 5 will serve us in subsection 3.3 by providing upper bounds on the components of the weight distribution.

3.3 The Range of Binomiality of the Weight Distribution

In several publications ([2], [3], [11], [12], [13]) the range of binomiality of a linear code has been investigated, i.e. the range of all indices l with A_l satisfying

$$(8) \qquad A_l \leq \gamma \cdot \frac{\sqrt{n}}{2^r} \cdot \binom{n}{l},$$

where γ > 0 is a positive constant. 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 [2], [11] or [12]). Krasikov and Litsyn call this property "asymptotically binomial distance distribution" (for linear codes, weight distribution and distance distribution are the same thing). About half of these results is dealing with codes of known dual distance.

First of all, let us state exemplarily one of the results of Krasikov & Litsyn ([12]): A linear code C_n has asymptotically binomial distance distribution for all indices l with

$$(9) \qquad \frac{n}{2}(1-\sqrt{\delta_n^{\perp}(2-\delta_n^{\perp})}) \leq l \leq \frac{n}{2}(1+\sqrt{\delta_n^{\perp}(2-\delta_n^{\perp})}) .$$

From Corollary 2 we now easily deduce

Theorem 6: Let C_n be a $[n, k]$ CRC with a generating polynomial g of degree $r = n - k$. Then C_n has asymptotically binomial weight distribution for all indices l with

$$\frac{n}{2}(1-\sqrt{\frac{R}{r}(2-\frac{R}{r})}) \leq l \leq \frac{n}{2}(1+\sqrt{\frac{R}{r}(2-\frac{R}{r})}) .$$

Proof: a) The function $f(\lambda) = \sqrt{\lambda(2-\lambda)}$ is increasing in [0, 1], and the result then follows from (5) and (9). ∎

In a similar way Corollary 2 may be applied to other theorems of Ashikmin, Barg&Litsyn in [2] or Krasikov&Litsyn in [11] and [12].

As for the left hand side of (9), the paper of Ashikmin, Barg&Litsyn ([2]) contains "a substantial improvement" of the estimate of the range of binomiality over the known results. To illustrate this fact, let for the moment be ξ_1 defined by

$$\xi_1 = \frac{n}{2}(1-\sqrt{\delta_n^{\perp}(2-\delta_n^{\perp})}) ,$$

and let ξ_2 be the root of the equation

$$(10) \qquad R = (2-\delta_n^{\perp}) H\left(\frac{\omega^* - \delta_n^{\perp}/2}{1-\delta_n^{\perp}}\right) + 1 + \delta_n^{\perp} - \mathrm{H}(\omega^*)$$

(or $\xi_2 = 0$, if the root is negative), where $H(x)$ is the binary entropy function:

$$H(x) = -x \cdot \log x - (1-x) \cdot \log(1-x) .$$

Ashikmin, Barg&Litsyn then demonstrate that there is binomial behaviour for all l with

$$l \in [n \cdot \min(\xi_1, \xi_2), n/2] .$$

In their proof, the relative dual distance $\delta_n^{\perp}$ may be replaced by any non negative lower bound d' on $\delta_n^{\perp}$. The only assumption that must be fulfilled is

$$B_l = 0 \text{ for all } l < d',$$

where the numbers B_l represent the dual weight distribution. And so, by (5), we get

Theorem 7: Let C_n be a $[n, k]$ CRC with a generating polynomial g of degree $r = n - k$. Then C_n has asymptotically binomial weight distribution for all indices l with

$$. \; l \in \left[n \cdot \min(\xi_1, \xi_2), n/2 \right] ,$$

where

$$\xi_1 = \frac{1}{2}(1 - \sqrt{\frac{R}{r}(2 - \frac{R}{r})}) ,$$

and ξ_2 is the root of the equation

$$R = (2 - \frac{R}{r}) H\left(\frac{\omega^* - \frac{R}{2r}}{1 - \frac{R}{r}} \right) + 1 + \frac{R}{r} - \mathrm{H}(\omega^*) ,$$

or $\xi_2 = 0$, if the root is negative.

We could have proven Theorem 6 in the same manner, but we wanted to outline the basic idea of the proof in two different ways.

Apart from the results listed so far, there is an alternative access to the issue of binomiality, opened by Theorem 5 of the preceding subsection. To this end, we have to outline an idea of [19], where we investigated binomial behavior from a completely different point of view. We then proved that the weight distribution of an arbitrary linear code satisfies

$$(11) \qquad A_l \le \frac{72}{121} \sqrt{2\pi} \sqrt{n} \cdot p_{ue}(\frac{l}{n}, C) \cdot \binom{n}{l}$$

for all l = 1,…n.

Theorem 5 together with (11) now yields

Theorem 8: Let C_n be a $[n, k]$ CRC with a generating polynomial g of degree $r = n - k$, $\alpha > 0$, $0 < \beta < 1$, and

$$n(r, \alpha, \beta) := \frac{r^2 - r \log \alpha}{-\log \beta} + r .$$

Then the weight distribution of C_n is showing at most asymptotically binomial behavior in the following sense:

$$A_l \le \frac{72}{121} \sqrt{2\pi} \cdot (1 + \alpha) \frac{\sqrt{n}}{2^r} \cdot \binom{n}{l}$$

for all indices l with

$$(12) \qquad \frac{n}{2}(1 - \beta) \le l \le \frac{n}{2} \text{ and all } n \ge n(r, \alpha, \beta)$$

Proof: By (12)

$$\frac{1}{2}(1 - \beta) \le \frac{l}{n} \le \frac{1}{2} ,$$

and therefore the claim turns out to be true by Theorem 5 and (11). ∎

3.4 A Bound on the Weight Distribution in the General Case

In [19] we investigated proper linear codes, i.e. linear codes with $p_{ue}(\varepsilon, C_n)$ increasing on [0, 1/2]. Inequality (11), in the case of proper linear codes, yielded

$$(13) \qquad A_l \le \frac{72}{121} \sqrt{2\pi} \cdot \frac{\sqrt{n}}{2^r} \cdot \binom{n}{l}$$

for each component of the weight distribution of C, a result from which we deduced (by estimating the tail of the binomial)

$$(14) \quad p_{ue}(\varepsilon, C) \le \frac{72}{121} \sqrt{2\pi} \sum_{l=d}^{\lfloor n/2 \rfloor} \frac{\sqrt{n}}{2^r} \binom{n}{l} \varepsilon^l (1 - \varepsilon)^{n-l} + R_n(\varepsilon) .$$

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

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

Inequality (14) turned out to be a useful instrument to provide estimates of the probability of undetected error. Now by means of Theorem 3 or Corollary 4 we are in a state to transfer (13) and (14) to the case of an arbitrary CRC:

Theorem 9: Let C_n be a $[n, k]$ CRC with a generating polynomial of degree $r = n - k$, then the weight distribution of C obeys the upper bound:

$$(15) \qquad A_l \le \frac{72}{121} \sqrt{2\pi} \sqrt{n} \cdot \left(\frac{1}{2^r} + \frac{2^r - 1}{2^r} \left(1 - 2\frac{l}{n}\right)^{R \cdot n / r} - \left(1 - \frac{l}{n}\right)^n \right) \binom{n}{l}$$

Proof: Inequality (11) and Corollary 4. ∎

Theorem 10: Let C_n be a $[n, k]$ CRC with a generating polynomial of degree $r = n - k$, then the probability of undetected error obeys the upper bound

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

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: Exactly in the same way as in the case of (14) in [19] by estimating the tail of the binomial (with (15) instead of (13)). ∎

Surely the bounds in Theorem 9 and 10 are far weaker than those in (13) and (14). But more could not be expected in the general case. Anyway, for small ε they may represent a tool for upper bounding the probability of undetected error, which might be helpful in practical problems.

3.5 The Covering Radius

Given the n-tuples $x = (x_1,\ldots,x_n)$ and $y = (y_1,\ldots,y_n)$, the Hamming distance of x and y is defined as

$$d(x,y) = |\{l = 1,\ldots,n : x_l \ne y_l\}|.$$

The Hamming distance induces a metric on the n-dimensional linear space GF(2)^n of all n-tuples. The covering radius $R_{\mathrm{cov}}(C)$ of C is defined as "smallest radius ρ such that the spheres of radius ρ around the code words cover the linear space of all words of length n":

$$R_{\mathrm{cov}}(C) = \max\{\min\{d(x,c) : c \in C\} : x \in \mathrm{GF}(2)^n\}.$$

The covering radius is an essential geometric characteristic of a code. It can be taken as a measure of the error correcting performance. For instance, it is an important tool in the field of data compression and write once memories.

Relations between covering radius and dual distance of a CRC have been studied by Tietäväinen, who in [17] and [18] has proved two remarkable results. The first one yields upper bounds on the covering radius, astonishingly depending on the dual distance:

Let C be a binary linear code with block length n and dual distance $d^{\perp} \ge d$', then the covering radius satisfies the subsequent upper bounds ([17],[18])

$$R_{\mathrm{cov}}(C) \le \begin{cases}\frac{1}{2}n & \text{if } d'=2,\\ \frac{1}{2}(n-1) & \text{if } d'=3,\\ \frac{1}{2}(n-\sqrt{n}) & \text{if } d'=4,\\ \frac{1}{2}(n-1-\sqrt{n-1}) & \text{if } d'=5,\\ \frac{1}{2}(n-\sqrt{3n-2}) & \text{if } d'=6,\\ \frac{1}{2}(n-1-\sqrt{3n-5}) & \text{if } d'=7,\\ \frac{n}{2}-(\sqrt{u}-\sqrt[6]{u})\sqrt{n-u} & \text{if } d'=2u,\\ \frac{n-1}{2}-(\sqrt{u}-\sqrt[6]{u})\sqrt{n-1-u} & \text{if } d'=2u-1,\end{cases}$$

As we did in the case of the range of binomiality, let us a now replace in Tietäväinen's result his lower bond d' by our lower bound $\left\lfloor \frac{n}{r} \right\rfloor$. Together with Theorem 1, this leads to

Theorem 11: Let C_n be a $[n, k]$ CRC with a generating polynomial of degree $r = n - k$, then the covering radius satisfies the upper bounds

$$R_{\mathrm{cov}}(C_n) \le \begin{cases}\frac{1}{2}n & \text{if } \frac{n}{3} < r \le \frac{n}{2},\\ \frac{1}{2}(n-1) & \text{if } \frac{n}{4} < r \le \frac{n}{3},\\ \frac{1}{2}(n-\sqrt{n}) & \text{if } \frac{n}{5} < r \le \frac{n}{4},\\ \frac{1}{2}(n-1-\sqrt{n-1}) & \text{if } \frac{n}{6} < r \le \frac{n}{5},\\ \frac{1}{2}(n-\sqrt{3n-2}) & \text{if } \frac{n}{7} < r \le \frac{n}{6},\\ \frac{1}{2}(n-1-\sqrt{3n-5}) & \text{if } \frac{n}{8} < r \le \frac{n}{7},\\ \frac{n}{2}-(\sqrt{u}-\sqrt[6]{u})\sqrt{n-u} & \text{if } \frac{n}{2u+1} < r \le \frac{n}{2u},\\ \frac{n-1}{2}-(\sqrt{u}-\sqrt[6]{u})\sqrt{n-1-u} & \text{if } \frac{n}{2u+2} < r \le \frac{n}{2u+1},\end{cases}$$

Proof: If t is an integer, then

$$\left\lfloor \frac{n}{r} \right\rfloor = t$$

is equivalent to

$$\frac{n}{t+1} < r \le \frac{n}{t}.$$

Now, by Theorem 1, the assumption of Tietäväinen is satisfied with

$$d' = \left\lfloor \frac{n}{r} \right\rfloor,$$

and the statement of the theorem becomes obvious. ∎

Tietäväinen's second result is an asymptotic one ([18]).Let (C_n) be a sequence of binary codes of block length n, dual distance $d_n^\perp$ and covering radius $R_{\mathrm{cov}}(C_n)$, with the following limits existing

$$\lim_{n\to\infty} \delta_n^\perp = \delta^\perp \text{ and } \lim_{n\to\infty} \frac{R_{\mathrm{cov}}(C_n)}{n} = \rho.$$

Then

$$\rho \le \frac{1}{2}(1 - \sqrt{\delta^\perp(2-\delta^\perp)}).$$

By Corollary 2 this result gets a new interpretation too.

Theorem 12: Let (C_n) be a sequence of CRCs of block length n with generating polynomials of degree r_n, dual distance $d_n^\perp$ and covering radius $R_{\mathrm{cov}}(C_n)$, where the sequence of degrees (r_n) is bounded above

(16) $$r_n \le r,$$

and

$$\lim_{n\to\infty} \frac{R_{\mathrm{cov}}(C_n)}{n} = \rho$$

exists. Then

$$\rho \le \frac{1}{2}(1 - \sqrt{\frac{1}{r}(2-\frac{1}{r})}).$$

Proof: Because of Corollary 2 and (16) we have

$$1 \ge \delta_n^\perp \ge \frac{n-r_n}{n}\frac{1}{r_n} \ge \frac{n-r}{n}\frac{1}{r}.$$

Therefore the sequence $(\delta_n^\perp)$ is bounded, and by the Bolzano-Weierstrass-Theorem (see for example [1]) it contains a convergent subsequence. Hence, without loss of generality, we may assume that $(\delta_n^\perp)$ itself converges

$$\lim_{n\to\infty} \delta_n^\perp = \delta^\perp,$$

and according to the begin of the proof

$$\begin{aligned} 1 &\ge \delta^\perp \\ &= \lim_{n\to\infty} \delta_n^\perp \\ &\ge \lim_{n\to\infty} \frac{n-r}{n}\frac{1}{r} \\ &= \frac{1}{r}. \end{aligned}$$

Finally by Tietäväinen's result, and because

$$f(\lambda) = \sqrt{\lambda(2-\lambda)}$$

increases on [0,1], we get

$$\begin{aligned} \rho &\le \frac{1}{2}(1 - \sqrt{\delta^\perp(2-\delta^\perp)}) \\ &\le \frac{1}{2}(1 - \sqrt{\frac{1}{r}(2-\frac{1}{r})}). \end{aligned}$$

∎

In a similar way the results of Ashikmin, Honkala, Laihonen&Litsyn in [4] may be transferred to the case of a CRC.

3.6 Sidel'nikov's Theorem

Last but not least let us focus our interest on Sidel'nikovs Theorem proven in [16]. It states that for each $[n, k]$ linear code with n > 3 and $d_n^\perp \ge 3$ its weight distribution is asymptotically normal in the sense of the next inequality

$$|A(z) - \mathrm{F}(z)| \le \frac{20}{\sqrt{d_n^\perp}},$$

for all real z ∈ (-∞, ∞). Here $A(z)$ has the meaning of the cumulative distribution function of the weights of C

$$A(z) = \sum_{l=|\mu-\sigma z|} a_l,$$

where

$$a_l = A_l / 2^k,$$

$$\mu = \sum_{l=0}^{n} l a_l$$

is the mean weight of all code words, and

$$\sigma^2 = \sum_{l=0}^{n} (\mu - l)^2 a_l$$

is the variance. F(z) is the cumulative distribution function of the Gaussian distribution:

$$F(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-\frac{t^2}{2}} dt, \ -\infty < z < +\infty .$$

Now by (5) we get the subsequent version of Sidel'nikov's Theorem

Theorem 13: Let C_n be a [n, k] CRC with n > 3 and $d_n^{\perp} \geq 3$. Then the weight distribution of C_n is asymptotically normal in the following sense

$$| A(z) - \mathrm{F}(z) | \leq \frac{20}{\sqrt{n}} \sqrt{\frac{r}{R}} .$$

This version of Sidel'nikov's Theorem bears some resemblance to a Theorem of Yue and Yang ([24]). Seemingly, it depends on the length r of the check sum whether the bound of Theorem 13 or the bound of Yue and Yang is the better one.

4 Conclusions

Via the MacWilliams Identities the minimum distance of the dual of a CRC has been investigated, its order of growth has been detected yielding a new lower bound. Firstly, this bound resulted in an upper bound on the probability of undetected error. The bound and its relationship to the 2^{-r}-bound have been discussed extensively. The result was that most CRCs do not obey the 2^{-r}-bound. Secondly, it served to determine the range of binomiality of a CRC as a function of the degree r of the generating polynomial, in this way helping to interpret the results of Krasikov&Litsyn and Ashikhmin, Barg&Litsyn. Moreover, a new estimate of the range of binomiality has been given, and one more new bound on the probability of undetected by estimating the tail of the binomial. Then two theorems of Tietäväinen, containing upper bounds on the covering radius as functions of the relative dual distance, have been examined. The bounds of Tietäväinen have been replaced by such ones depending only on the degree r and the code rate. Finally the results have been applied to Sidel'nikov's theorem about asymptotical normality of the weight distribution. Just as in the other cases, the dual distance has been replaced by a parameter depending on the block length n and the degree r.

5 Acknowledgment

We are much obliged to Mr. Jochen M. Breuer, who has helped us in creating the graphics.

References:

[1] Apostol, Tom M., *Mathematical Analysis*, Addison-Wesley, 2nd ed., 1974.

[2] 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.

[3] 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.

[4] Ashikhmin, A., Honkala, I., Laihonen T. and Litsyn, S., "On Relations Between Covering Radius and Dual Distance," *IEEE Trans. Inform. Theory*, vol. 45, no. 6, Sept. 1999. pp. 1808–1816.

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

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

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

[8] Fujiwara, T., Kasami, T., 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.

[9] Fujiwara, T., Kasami, T., Lin, S., On the Undetected Error Probability for Shortened Hamming Codes,
IEEE Trans. on Communications, Vol. COM-33, No. 6, Sept. 1985.

[10] Funk, G., Determination of Best Shortened Linear Codes, *IEEE Trans. on Communications*, Vol. 4, No. 1, Jan. 1996.

[11] 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.
[12] 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.
[13] 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.
[14] Massey, J.L., "Coding Techniques for Digital Data Networks," *Proceedings of the Int. Conf. on Info. Th. and Systems*, NTG-Fachberichte vol. 65, Berlin, Sept. 18-20, 1978.
[15] Peterson, W. W. and Weldon, E. J., *Error Correcting Codes*. The MIT Press Cambridge, Massachusetts , and London, England, Second Edition 1972.
[16] Sidel'nikov, V.M., "Weight spectrum of binary Bose–Chaudhuri–Hocquenghem codes," *Problems Inform. Transmissions,* vol. 7, no. 1, pp. 11–17, 1971.
[17] Tietäväinen, A., "An upper bound on the covering radius as a function of its dual distance," *IEEE Trans. on Information Theory*, vol. 36, pp. 1472–1474, 1990.
[18] Tietäväinen, A, "Covering Radius and Dual Distance," *Des.Codes Cryptogr.*, vol. 1 pp. 31–46, 1991.
[19] Wacker, H., D.& Boercsoek, J., "Some Inequalities Concerning Binomial Coefficients and the Weight Distribution of Proper Linear Codes", *Proceedings of the 7th WSEAS International Conference on Applied Computer Science (ACS '07)*, Venice, Italy, November 21-23, 2007.
[20] Wicker, S. B., "*Error Control Systems for Digital Communication and Storage*" Prentice Hall, Upper Saddle River, New Jersey.
[21] 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.
[22] Wolf, J.K., Blakeney, R.D., An exact Evaluation of the Probability of Undetected Error for certain Shortened Binary CRC Codes, Qual.Comm, Inc., San Diego, CA 92121. *Proc. Milcom IEEE* 1988.
[23] Wolf, J. K., Michelson, A. M., and Levesque, A. H., "On the Probability of Undetected Error for Linear Block Codes," *IEEE Trans. on Communications*, Vol. COM-30, No. 2, Feb. 1982. pp. 317-324.
[24] Yue, D., and Yang, E., "Asymptotically Gaussian Weight Distribution and Performance of Multicomponent Turbo Block Codes and Product Codes," *IEEE Trans. on Communications*, Vol. 52, No. 5, May 2004. pp. 728-736.