The Minimum Distance of the Dual of a CRC

WACKER H. D., BOERCSOEK J.
Development
HIMA Paul Hildebrandt GmbH + Co KG
Albert-Bassermann-Strasse 28, D-68782 Bruehl
GERMANY

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 the code. In this paper firstly the order of growth of the dual distance of a CRC as a function of *n* is investigated, and a lower bound is given. Then, on one hand, this bound is used to derive an upper bound on the probability of undetected error of a CRC. On the other hand it is applied to some results about the range of binomiality and the covering radius of a CRC. Finally a new interpretation of Sidel'nikov's theorem on the cumulative distribution function of the weights of a code is given. In this way the conclusions may attribute a new meaning to some results about codes with known dual distance.

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

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 [7] for example):

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

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 [7]). 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. [13] for example):

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

$d_n^{\perp}$ being the minimum distance of $C_n^{\perp}$ (the "dual distance") and $r = n - k$. 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. 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 abstract 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 [1] and [4] 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 [12] 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

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

for all $0 < \varepsilon \leq ½$. 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. But above all we thought it desirable to get bounds on $p_{ue}(\varepsilon,C_n)$ involving the 2^{-r}-bound. 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 $d_n^{\perp}$

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

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

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 $\boldsymbol{I}_{n\text{-}k}$ and a r x k parity part $\boldsymbol{P}^{\mathrm{T}}$ (cf. [7] and [11] for example)**:**

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

Let further 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 member of the congruence class $\{X^i\}$ of X^i modulo $g(X)$. The parity part $\boldsymbol{P}^{\mathrm{T}}$ 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

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

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

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

Because

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

represent the congruence classes

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

this means that the congruence class of

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

satisfies the equation

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

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

$(\rho_{1jr},\cdots,\rho_{1(j+1)r-1}),\ldots,(\rho_{rjr},\cdots,\rho_{r(j+1)r-1})$
of $\boldsymbol{P_j}$ are linearly independent for all $j = 1, 2, \ldots, t-1$.
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

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

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

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

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

$$
\begin{aligned}
& m_1(1^{\text{st}} \text{ row of } \boldsymbol{P_1}) + \cdots + m_r(r^{\text{th}} \text{ row of } \boldsymbol{P_1}) \\
& m_1(1^{\text{st}} \text{ row of } \boldsymbol{P_2}) + \cdots + m_r(\text{r}^{\text{th}} \text{ row of } \boldsymbol{P_2}) \\
& \quad \cdots\cdots\cdots \\
& m_1(1^{\text{st}} \text{ row of } \boldsymbol{P_{t-1}}) + \cdots + m_r(\text{r}^{\text{th}} \text{ row of } \boldsymbol{P_{t-1}})
\end{aligned}
$$

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

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

and

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

■

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

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

Proof: By (4) we get

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

■

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

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

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

Proof: By (2) and (4) we get (cf. Wolf&Blakeney [13])

$$p_{\text{ue}}(\varepsilon, C_n) \leq 2^{-r}\left\{1 + (2^r - 1)(1 - 2\varepsilon)^{d_n^{\perp}}\right\} - (1 - \varepsilon)^n$$

$$\leq 2^{-r} + \frac{2^r - 1}{2^r}(1-2\varepsilon)^{\left\lfloor \frac{n}{r} \right\rfloor} - (1-\varepsilon)^n.$$

∎

From Theorem 3 we then 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 ε ϵ [0, 1/2].

Remark 1: Omitting the factor $(2^r - 1)2^{-r}$, 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 for $n \to \infty$:

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

The convergence cannot be uniform on [0, 1/2]. Otherwise the limit function had to be continuous on [0, 1/2], a fact being evidently false.

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&Blakeney [13]). Consequently the bound of Theorem 3 (or Corollary 4) is weaker then the 2^{-r}-bound. But anyway, Corollary 4 contains an error estimate: $p_{ue}(\varepsilon, C_n)$ exceeds 2^{-r} by a maximal amount of

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

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

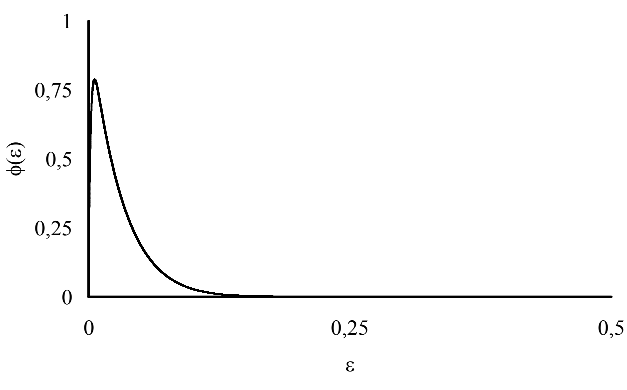

Fig. 1

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.

3.3 The Range of Binomiality of the Distance Distribution and the Covering Radius

In several publications ([1], [2], [4], [5], [6]) the range of binomiality of a linear code has been investigated, i.e. the range of all indices l with A_l satisfying

$$(7) \qquad A_l \leq \gamma \cdot \frac{\sqrt{n}}{2^r} \cdot \binom{n}{l},$$

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 [1] or [4]). Krasikov and Litsyn call this property "asymptotically binomial distance distribution". One part of these results is dealing with codes of known dual distance. First of all, let us state exemplarily one of the results of Ashikhmin, Barg&Litsyn ([1]):
A linear code C_n has asymptotically binomial distance distribution for all indices l with

$$(8) \qquad \frac{n}{2}\left(1 - \sqrt{\delta_n^{\perp}(2-\delta_n^{\perp})}\right) \leq l \leq \frac{n}{2}\left(1 + \sqrt{\delta_n^{\perp}(2-\delta_n^{\perp})}\right)$$

(cf. [1], Theorem 6).
From Corollary 2 we now easily deduce

Theorem 5: Let C_n be a $[n, k]$ CRC with a generating polynomial g of degree $r = n - k$. Then C_n has asymptotically binomial distance distribution for all indices l with

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

Proof: a) The function

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

is increasing in [0, 1], and the result then follows from (5) and (8). ∎

In a similar way Corollary 2 may be applied to other theorems of Ashikmin, Barg&Litsyn. in [1] or Krasikov&Litsyn in [4].
Relations between covering radius and dual distance of a CRC have been studied by Tietäväinen in [9],[10] or by Ashikmin, Honkala, Laihonen&Litsyn in [3]. Corollary 2 may be applied to them as done above, giving those results a new interpretation too.

3.4 Sidel'nikov's Theorem

Last but not least let us focus our interest on Sidel'nikovs Theorem proven in [8]. It states that for each [n, k] linear code with n > 3 and $d_n^{\perp} \geq 3$ its weight distribution is asymptotically normal in the following sense

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

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 $a_l = A_l / 2^k$, and $\mu = \sum_{l=0}^{n} l a_l$ 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. Now by (5) we get the subsequent version of Sidel'nikov's Theorem

Theorem 5: Let C 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 ([14]). It depends on the length r of the check sum whether the bound of Theorem 5 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, and a lower bound has been found. Firstly, this bound yielded an upper bound on the probability of undetected error. Secondly, it served to determine the range of binomialty of a CRC helping to interprete the results of Krasikov&Litsyn and Ashikhmin, Barg&Litsyn. An application to the covering radius was mentioned. Finally it was applied to Sidel'nikov's theorem about asymptotical normality of the weight distribution.

5 Acknowledgment

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

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] 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.

[4]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.

[5]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.

[6]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.

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

[8]Sidel'nikov, V.M., "Weight spectrum of binary Bose–Chaudhuri–Hocquenghem codes," *Problems Inform. Transmissions,* vol. 7, no. 1, pp. 11–17, 1971.

[9]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.

[10]Tietäväinen, A, "Covering Radius and Dual Distance," *Des.Codes Cryptogr.*, vol. 1 pp. 31–46, 1991.

[11]Wicker, S. B., "Error Control Systems for Digital Communication and Storage" Prentice Hall, Upper Saddle River, New Jersey.

[12]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.

[13]Wolf, J. K., and 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. pp. 287-292.

[14]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.