Bounds on the error-correction capability of codes beyond half the minimum distance *

Tor Helleseth and Torleiv Kløve,
Department of Informatics, University of Bergen
HIB, N-5020 Bergen, Norway,

Vladimir I. Levenshtein,
Keldysh Institute for Applied Mathematics, RAS,
Miusskaya sq. 4, 125047 Moscow, Russia.

Abstract

We present bounds on the error-correction capability of binary linear codes beyond half the minimum distance which are a part of the results of the recently submitted paper [7].

Key words: error-correction capability, linear codes, minimal words, covering radius, simplex codes, Reed-Muller codes.

1 Introduction

Let F^n be the set of all binary vectors $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ (with coordinates 0 and 1) and F_t^n be the set of all vectors of F^n of the Hamming weight t. For any $\mathbf{x} \in F^n$ we consider the *support* $S(\mathbf{x}) = \{i : x_i = 1\}$ and $m(\mathbf{x}) = \min S(\mathbf{x})$, and define on F^n a partial ordering $\subseteq$ (covering) as follows:

$$\mathbf{x} \subseteq \mathbf{y} \quad \text{if and only if} \quad S(\mathbf{x}) \subseteq S(\mathbf{y}).$$

A linear code $C \subseteq F^n$ of dimension k is referred to as an $[n, k]$ code. We also use the notation $[n, k, d]$ if the code C has minimum distance d_C at least d. We set $t_C = \lfloor (d_C - 1)/2 \rfloor$ and denote the covering radius of C by r_C.

A coset leader of an $[n, k]$ code C is the lexicographically smallest element among the minimum weight vectors in a coset. We denote the set of all 2^{n-k} coset leaders by $E^0(C)$. In (maximum likelihood) decoding *only* error vectors of the set $E^0(C)$ can be corrected and they are *all* corrected for transmission of *any* code word. Therefore, the elements of $E^0(C)$ are called *correctable errors*, and the elements of $E^1(C) = F^n \setminus E^0(C)$ are called *uncorrectable errors*. Let $E_t^0(C) = E^0(C) \cap F_t^n$, be the set of correctable errors of weight t, and $E_t^1(C) = E^1(C) \cap F_t^n$, be the set of uncorrectable errors of weight t.

* The research was supported by The Norwegian Research Council; the work of V.I. Levenshtein is also supported by The Russian Foundation for Basic Research, grant 01-01-00035.

One of the main problems in coding theory is to find, for a given $[n,k,d]$ code C, the function (*the ratio of correctable errors*):

$$\varepsilon_C(t) = \frac{|E_t^0(C)|}{\binom{n}{t}}, \quad t = 0,1,...,n. \tag{1}$$

A significant fact inherent in linear codes is a monotone structure of the sets of correctable and uncorrectable errors, namely that if $\mathbf{x} \subset \mathbf{y}$, then $\mathbf{x} \in E^1(C)$ implies $\mathbf{y} \in E^1(C)$ and $\mathbf{y} \in E^0(C)$ implies $\mathbf{x} \in E^0(C)$. Using this property it is easily proved that for any $[n,k]$ code C and any $t = 0,1,...,n-1$,

$$\varepsilon_C(t+1) \leq \varepsilon_C(t). \tag{2}$$

Thus, $\varepsilon_C(t)$ is a nonincreasing function in t such that $\varepsilon_C(t) = 1$ for $t \leq t_C$ and $\varepsilon_C(t) = 0$ for $t > r_C$ since the covering radius equals to the maximum weight of a correctable error. The function $\varepsilon_C(t)$ for $t \geq d_C/2$ (that is equivalent to $t \geq t_C + 1$ for an integer t) really characterizes the capability of codes to correct errors. However, it is difficult to estimate this function even if the weight distribution $A_i(C)$, $i = 0,1,...,n$, of the code C is known. (Our results in Section 4 show how it is possible to overcome this difficulty in some cases.) It is also worth noticing that the decoding error probability $P_{\mathrm{de}}(C,p)$ of a code $C \subseteq F^n$ on the binary symmetric channel has the following expression:

$$P_{\mathrm{de}}(C,p) = \sum_{t=0}^{n} (1 - \varepsilon_C(t)) \binom{n}{t} p^t (1-p)^{n-t}. \tag{3}$$

The monotonicity (2) allows us to introduce the following definition. For any integer t, $1 \leq t \leq n$, and any ε, $0 < \varepsilon \leq 1$, a binary linear code $C \subseteq F^n$ will be called (t,ε)-*error-correcting code* if $\varepsilon_C(t) \geq \varepsilon$. In particular, for $\varepsilon = 1$ this definition coincides with the standard definition of a t-error-correcting code. As an example, the double-error-correcting BCH $[n = 2^m - 1, k = n - 2m, d = 5]$ codes are $(3,\varepsilon)$-error-correcting codes with $\varepsilon = \frac{3(n+3)}{(n-1)(n-2)}$; that is a consequence of the Gorenstein-Peterson-Zierler result [5] that these codes are quasi-perfect. As it follows from the investigation due to Charpin and Zinoviev [3] the problem to find ε such that a 3-error-correcting BCH code is a $(4,\varepsilon)$-error-correcting code is still open. It is significant to note that, by (2), any (t,ε)-error-correcting code is a (t',ε)-error-correcting code for any integer $t' < t$. This ensures the reasonableness of the definition, for any code C, of the *error-correction capability function* $t_C(\varepsilon)$ as the maximum t such that C is a (t,ε)-error-correcting code.

The first two of our bounds for $\varepsilon_C(t)$ are based on investigation of the monotone structure of correctable and uncorrectable errors for a code C and they are given in Section 2. In Section 3 we find precise and simple bounds for the best $[n,k]$ codes and give asymptotical analysis of these bounds. In Section 4 we obtain bounds on $\varepsilon_{C_n}(t)$ for given sequences of $[n,k(n)]$ codes C_n and prove that some of them are optimal in an asymptotical sense.

2 Bounds based on monotone structure of correctable and uncorrectable errors

First we strengthen (2).

Theorem 1 *For any $[n,k]$ code C and any t, $d_C/2 \le t \le r_C$,*

$$\varepsilon_C(t+1) \le \varepsilon_C(t) - \frac{1}{\binom{n}{t}}. \tag{4}$$

To prove this theorem we show that for any t, $d_C/2 \le t \le r_C$, there exist at least $n-t+1$ pairs $(\mathbf{x},\mathbf{y})$ such that $\mathbf{x} \in E^0_{t-1}(C)$ and $\mathbf{y} \in E^1_t(C)$.

In particular, Theorem 1 implies that $\varepsilon_C(t+1) < \varepsilon_C(t)$ for $t_C \le t \le r_C$. Hence we get the following corollary.

Corollary 1 *For $\varepsilon \in (0,1]$, the error-correction capability function $t_C(\varepsilon)$ is nonincreasing, left continuous, and takes all values $t \in \{t_C, t_C+1, \ldots, r_C\}$.*

Another bound for $\varepsilon_C(t)$ is based on the description of *minimal uncorrectable errors* $\mathbf{y} \in E^1(C)$ such that, if $\mathbf{x} \subseteq \mathbf{y}$ and $\mathbf{x} \in E^1(C)$, then $\mathbf{x} = \mathbf{y}$.

A vector $\mathbf{u} \in F^n$ will be called a *larger half of a codeword* $\mathbf{c} \in C$, $\mathbf{c} \ne \mathbf{0}$, if and only if

$$\mathbf{u} \subseteq \mathbf{c}, \quad ||\mathbf{c}|| \le 2||\mathbf{u}|| \le ||\mathbf{c}|| + 2, \tag{5}$$

$$m(\mathbf{u}) = m(\mathbf{c}), \text{ if } 2||\mathbf{u}|| = ||\mathbf{c}||, \tag{6}$$

$$m(\mathbf{u}) > m(\mathbf{c}), \text{ if } 2||\mathbf{u}|| = ||\mathbf{c}|| + 2. \tag{7}$$

Note that if $||\mathbf{c}||$ is odd, $||\mathbf{c}|| = 2h-1$ say, then by (5), $||\mathbf{u}|| = h$ and conditions (6) and (7) do not apply. If $||\mathbf{c}|| = 2h$ is even, we have $||\mathbf{u}|| = h$ or $h+1$; moreover, if $||\mathbf{u}|| = h$, then $m(\mathbf{u}) = m(\mathbf{c})$, and if $||\mathbf{u}|| = h+1$, then $m(\mathbf{u}) > m(\mathbf{c})$. Thus, any codeword $\mathbf{c} \in C$ of norm $i \ge 1$ has $\binom{i}{\lceil \frac{i+1}{2} \rceil}$ larger halves; $\binom{2h-1}{h}$, if $i = 2h-1$, and $\binom{2h-1}{h-1} + \binom{2h-1}{h+1} = \binom{2h}{h+1}$, if $i = 2h$.

A codeword $\mathbf{c} \in C$ is called *minimal*, if $\mathbf{c} \ne \mathbf{0}$ and $\mathbf{a} \subset \mathbf{c}$ with $\mathbf{a} \in C$ implies that $\mathbf{a} = \mathbf{0}$. Denote by $M(C)$ the set of all minimal words of a code C. We give and use some known properties of $M(C)$ (see [1] and references there). Since any $n-k+1$ columns of an $[n,k]$ code C are dependent, the maximum weight of a minimal word of C does not exceed $n-k+1$ and hence we have $||\mathbf{u}|| \le \lceil \frac{n-k+2}{2} \rceil$ for any larger half $\mathbf{u}$ of a codeword. We note that $M(C) = C \setminus \{\mathbf{0}\}$ if and only if any two non-zero code words have intersecting supports. Such code are called intersecting codes, see e.g. [4]. Minimal codewords have found applications e.g. in secret sharing, see [10].

One of our main results in [7] is a proof of the statement that all minimal uncorrectable errors are larger halves of minimal codewords. The following bound is eventually based on this statement and is a refinement of bounds given in [11], [12], and [6].

Theorem 2 *Let C be an $[n,k,d]$ code and $A^M_d(C), \ldots, A^M_{n-k+1}(C)$ be weight distribution of its minimal codewords. Then for any weight t, $d/2 \le t \le n$,*

$$1 - \varepsilon_C(t) \le \sum_{i=d}^{2t} A^M_i(C) \sum_{a=\lceil i/2 \rceil} \frac{\binom{i}{a}\binom{n-i}{t-a}}{\binom{n}{t}} - \sum_{a=\lceil d/2 \rceil}^{t} A^M_{2a}(C) \frac{\binom{2a-1}{a}\binom{n-2a}{t-a}}{\binom{n}{t}}. \tag{8}$$

From our proof it follows that this bound remains valid if one considers $\{A_i^M(C)\}$ as the weight distribution of a (minimal) subset $M \subseteq M(C)$ such that the set of larger halves of codewords of M contains all minimal uncorrectable errors. Such a set M is a test set in the terminology of Ashikhmin and Barg [1] and it is a subset of the test set consisting of the zero-neighbors defined by Levitin and Hartman [9].

3 Bounds for the best codes

Now we give simple and precise bounds for $\varepsilon_C(t)$ using the quantity

$$\sigma(n,k,t) = 2^{k-n} \sum_{i=0}^{t} \binom{n}{i} \tag{9}$$

which plays a significant role in our investigation. Note that $\sigma(n,k,t) \leq 1$ is a necessary condition for the existence of a t-error-correcting $[n,k]$ code (the Hamming bound).

Theorem 3 *(i) For any $[n,k]$ code C and any t, $t = 0,1,...,n$,*

$$\varepsilon_C(t) \leq \frac{2^{n-k}}{\sum_{i=0}^{t} \binom{n}{i}} = \frac{1}{\sigma(n,k,t)}. \tag{10}$$

(ii) For any n,k, and t, $0 \leq t \leq n$, there exists an $[n,k]$ code C such that

$$\varepsilon_C(t) > 1 - \sigma(n,k,t). \tag{11}$$

The bound (10) is a direct consequence of the monotonicity (2). To prove (11) we used the approach proposed in [8], Theorem 1. We endow F^n with the structure of $GF(2^n)$ and for any $[n,k]$ code $C \subseteq F^n$ and any non-zero $g \in F^n$ denote by gC the code $\{g\mathbf{c} : \mathbf{c} \in C\}$ which is also an $[n,k]$ code. If $\mathbf{z} \in E_t^1(gC)$, then there exists a non-zero $\mathbf{c} \in gC$ such that $\mathbf{w} = \mathbf{z} + \mathbf{c}$ has weight at most t. Therefore,

$$\begin{aligned}
\sum_{g \in F^n \setminus \{\mathbf{0}\}} |E_t^1(gC)| &\leq \sum_{g \in F^n \setminus \{\mathbf{0}\}} \sum_{\mathbf{z} \in E_t^1(gC)} \sum_{\mathbf{c} \in C \setminus \{\mathbf{0}\}} \sum_{\mathbf{w} \in \bigcup_{i=0}^{t} F_i^n} \delta_{g\mathbf{c},\mathbf{z}+\mathbf{w}} \\
&\leq \sum_{\mathbf{z} \in F_t^n} \sum_{\mathbf{c} \in C \setminus \{\mathbf{0}\}} \sum_{\mathbf{w} \in \bigcup_{i=0}^{t} F_i^n} \sum_{g \in F^n \setminus \{\mathbf{0}\}} \delta_{g\mathbf{c},\mathbf{z}+\mathbf{w}} \\
&\leq \sum_{\mathbf{z} \in F_t^n} \sum_{\mathbf{c} \in C \setminus \{\mathbf{0}\}} \sum_{\mathbf{w} \in \bigcup_{i=0}^{t} F_i^n} 1 = \binom{n}{t}(2^k - 1) \sum_{i=0}^{t} \binom{n}{i}.
\end{aligned}$$

Since there are $2^n - 1$ non-zero g in F^n, there exists a g for which

$$|E_t^1(gC)| \leq \binom{n}{t} \frac{2^k - 1}{2^n - 1} \sum_{i=0}^{t} \binom{n}{i} < \binom{n}{t} \sigma(n,k,t).$$

This completes the proof because $|E_t^1(gC)| = \binom{n}{t}(1 - \varepsilon_{gC}(t))$.

Asymptotic consequences of Theorem 3 for a sequence of $[n,k]$ codes C and weights t as $n \to \infty$ follow from the following arguments. If for such a sequence we have $\sigma(n,k,t) \to \infty$,

then $\varepsilon_C(t) \to 0$. On the other hand, if the parameters k, n, t satisfy $\sigma(n,k,t) \to 0$, then there exists a sequence of $[n,k]$ codes C such that $\varepsilon_C(t) \to 1$.

We consider sequences of $[n,k]$ codes $C_n \subseteq F^n$ with $k = k(n) \to \infty$ as $n \to \infty$. If the limit

$$R = \lim_{n\to\infty} \frac{k}{n}$$

exists, we call R the *rate* of the sequence $\{C_n\}$. For any rate $R,\ 0 \le R \le 1$, we denote by $p_R,\ 0 \le p_R \le 1/2$, the parameter which is uniquely defined by the equation $R = 1 - H(p_R)$ where $H(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the Shannon entropy. First, for a sequence of codes C_n of rate R and a fixed $\varepsilon,\ 0 < \varepsilon < 1$, we find the asymptotic behavior of $t_{C_n}(\varepsilon)$ when $n \to \infty$.

Theorem 4 *(i) For any $R,\ 0 < R < 1$, and any $n \ge 1$ there exist an $[n,k]$ code C with $k = \lfloor nR \rfloor$ and a positive constant c_R such that*

$$t_C\left(1 - \frac{c_R}{\sqrt{n}}\right) \ge \lfloor np_R \rfloor. \tag{12}$$

(ii) For any sequence of $[n,k]$ codes C_n of rate $R,\ 0 \le R < 1$, and any fixed $\varepsilon,\ 0 < \varepsilon < 1$,

$$t_{C_n}(\varepsilon) \lesssim np_R \quad \textit{as} \quad n \to \infty. \tag{13}$$

Now, for a sequence of $[n,k]$ of codes C_n of rate $R = 0$, that is, $k = k(n) = o(n)$, we investigate the asymptotic behavior of $t_{C_n}(\varepsilon)$ for a fixed $\varepsilon,\ 0 < \varepsilon < 1$, as $n \to \infty$. Note that from (13) it follows that $t_{C_n}(\varepsilon) \lesssim n/2$ under our assumption that $k = k(n) \to \infty$. Thus, $t_{C_n}(\varepsilon) \sim n/2$ can hold only for a sequence of codes C_n with rate zero. In order to investigate the convergence $t_{C_n}(\varepsilon) \to n/2$ when $k = o(n)$ we introduce for a code $C \subseteq F^n$ the parameter

$$s_C(\varepsilon) = n - 2t_C(\varepsilon).$$

Note that $s_{C_n}(\varepsilon) = o(n)$ when $t_{C_n}(\varepsilon) \to n/2$.

Theorem 5 *i) For any n and k, $0 < 9k\ln 4 \le n$, there exists an $[n,k]$ code C such that*

$$t_C\left(1 - \frac{1}{\sqrt{k\pi\ln 4}}\right) \ge \left\lfloor \frac{n - \sqrt{nk\ln 4}}{2} \right\rfloor. \tag{14}$$

ii) If for a subsequence of $[n,k]$ codes C_n there exists $\varepsilon,\ 0 < \varepsilon < 1$, such that

$$t_{C_n}(\varepsilon) \sim n/2 \quad \textit{as} \quad n \to \infty,$$

then

$$s_{C_n}(\varepsilon) = n - 2t_{C_n}(\varepsilon) \gtrsim \sqrt{nk\ln 4}. \tag{15}$$

A sequence of $[n,k]$ codes C_n where $k = o(n)$ as $n \to \infty$ is called *asymptotically optimal* if for any fixed $\varepsilon,\ 0 < \varepsilon < 1$,

$$s_{C_n}(\varepsilon) = n - 2t_{C_n}(\varepsilon) \sim \sqrt{nk\ln 4}.$$

From Theorem 5 it follows that asymptotically optimal sequences of $[n,k]$ codes exist for any function $k = k(n)$ such that $k(n) = o(n)$ and $k(n) \to \infty$ as $n \to \infty$.

4 Bounds for given sequences of codes

The inequalities (12) and (14) characterize the maximum weight such that almost all errors of this weight can be corrected for codes with positive and zero rate respectively. However, these results are not constructive: they are based on the existence, for any n, k, and t, of an $[n,k]$ code C for which (11) is valid and on asymptotic analysis of the conditions for $\sigma(n,k,t) \to 0$.

A significant problem is to find, for known classes of $[n,k,d]$ codes C such as the primitive BCH $[n = 2^m - 1, k = n - mh, d = 2h+1]$ codes $B_{m,h}$ and Reed-Muller $[n = 2^m, k = \sum_{i=0}^{r} \binom{m}{i}, d = 2^{m-r}]$ codes $RM_{m,r}$ of order r, an upper bound for $1-\varepsilon_C(t)$ when $t \geq t_C+1 = \lceil d/2 \rceil$. In this section we present bounds similar to (11) for an $[n,k,d]$ code C when $t \geq t_C+1$. The first bound is valid under an additional restriction on the weight distribution $\{A_i^M(C)\}$ of the minimal words of the code C.

Given a positive valued function $\mu(n)$, an $[n,k]$ code C is called $\mu(n)$-*binomial*, if for all i,

$$A_i^M(C) \leq \mu(n) 2^{k-n} \binom{n}{i}. \tag{16}$$

By the recent result of Blinovsky [2], there exists a constant c such that for any $n \geq 2$ and $k \leq n$ there exists an $[n,k]$ code which is $(c\sqrt{n \ln n})$-binomial. (This result is proved using the weight distribution of all, not necessarily minimal, codewords of weight $i > 0$.)

Note that all words of $RM_{m,1}$ except $\mathbf{0}$ and $\mathbf{1}$ have weight $n/2$ and are minimal. Since $\binom{n}{n/2} \sim \sqrt{2/(\pi n)} 2^n$ as $n \to \infty$, the code $RM_{m,1}$ is $\mu(n)$-binomial where $\mu(n) \sim \sqrt{\pi n/2}$ as $n = 2^m \to \infty$.

Theorem 6 *If an $[n,k,d]$ code C is $\mu(n)$-binomial, then for any t, $t \geq d/2$,*

$$1 - \varepsilon_C(t) \leq \mu(n)\sigma(n,k,t) = \mu(n) 2^{k-n} \sum_{i=0}^{t} \binom{n}{i}. \tag{17}$$

To prove this statement we used Theorem 2 and two combinatorial identities. The first is the well known relation

$$\binom{n}{i}\binom{i}{a}\binom{n-i}{t-a} = \binom{n}{t}\binom{t}{a}\binom{n-t}{i-a}. \tag{18}$$

The other identity is

$$\sum_{i=0}^{2t} \sum_{a=\lceil i/2 \rceil} \binom{t}{a}\binom{n-t}{i-a} = \sum_{i=0}^{t} \binom{n}{i}. \tag{19}$$

We include the proof of (19). Since $0 \leq i-a \leq a \leq t$ and $0 \leq i \leq 2t$, the sum $S = \sum_{i=0}^{2t} \sum_{a=\lceil i/2 \rceil} \binom{t}{a}\binom{n-t}{i-a}$ is equal to the number of pairs (U,V) of subsets where $U \subseteq \{1,2,...,t\}$, $V \subseteq \{t+1,t+2,...,n\}$, and $0 \leq |V| \leq |U| \leq t$. Therefore, $S = \sum_{j=0}^{t} \binom{n-t}{j} \sum_{a=j}^{t} \binom{t}{a}$. If one considers the generating functions

$$(1+x^{-1})^{n-t} = \sum_{j=0}^{n-t} \binom{n-t}{j} x^{-j} \quad \text{and} \quad (1+x)^t = \sum_{a=0}^{t} \binom{t}{a} x^a,$$

then it is easily seen that S equals the sum of the coefficients at nonnegative degrees of x in the product

$$(1+x^{-1})^{n-t}(1+x)^t = (1+x)^n x^{t-n}.$$

Hence $S = \sum_{j=n-t}^{n} \binom{n}{j} = \sum_{i=0}^{t} \binom{n}{i}$. This proves (19).

The asymptotic results obtained in Section 3 are based on finding conditions for

$$-\log_2 \sigma(n,k,t) = n - k - \log_2 \sum_{i=0}^{t} \binom{n}{i} \to \infty.$$

Therefore, asymptotic properties of good codes whose existence was proved using random selection are preserved for $\mu(n)$-binomial codes if $\ln \mu(n) = o(k)$ as $n \to \infty$. In this case it is sufficient to replace k by $k - \log_2 \mu(n)$ in the previous proofs.

Now we present a bound similar to (11) for an arbitrary $[n,k,d]$ code C. Note that we can assume that $t \le (n - \sqrt{n})/2$ due to (13) and (15).

Theorem 7 *For any $[n,k,d]$ code C and any t, $t_C + 1 \le t \le (n - \sqrt{n})/2$,*

$$1 - \varepsilon_C(t) \le 2^k \frac{\binom{t}{t_C+1}\binom{n-t}{t_C+1}}{\binom{n}{2t_C+2}} \frac{n - t - t_C}{n - 2t + 1}. \tag{20}$$

To investigate (20) we proved that for even i and $0 < i < 2t \le n$,

$$\frac{\binom{t}{i/2}\binom{n-t}{i/2}}{\binom{n}{i}} < \sqrt{\frac{8(n-i)t(n-t)}{\pi i(2t-i)(2n-2t-i)n}} 2^{-ng(\xi,\tau)} \tag{21}$$

where $\xi = i/n$, $\tau = t/n$, and

$$g(\xi,\tau) = H(\xi) - \tau H\left(\frac{\xi}{2\tau}\right) - (1-\tau) H\left(\frac{\xi}{2(1-\tau)}\right).$$

While τ increases from $\xi/2$ to $1/2$, the function $g(\xi,\tau)$ decreases from $g(\xi,\xi/2) > \xi(1-\xi)/\ln 4$ to $g(\xi,1/2) = 0$.

Corollary 2 *For a sequence of $[n,k,d]$ codes C_n, for which $\frac{d}{n} \to \delta > 0$, $\frac{k}{n} \to R$, where $0 < R < g(\delta,\delta/2)$, let τ_0 be the (unique) solution of the equation $R = g(\delta,\tau)$. Then for any $\tau < \tau_0$, $\varepsilon_{C_n}(\lfloor n\tau \rfloor) \to 1$ as $n \to \infty$.*

Consider a sequence of $[n,k,d]$ codes C_n ($k \to \infty$) for which $t_{C_n}(\varepsilon) \sim n/2$ for an ε, $0 < \varepsilon < 1$, and hence $s_{C_n}(\varepsilon) = n - 2t_{C_n}(\varepsilon) = o(n)$. By Theorems 4 and 5, we have $k = o(n)$ and $s_{C_n}(\varepsilon) \ge \sqrt{n}$. For such sequences of codes one can use the following useful inequality

$$g(\xi,\tau) > \frac{\xi(1-2\tau)^2}{(1-\xi)\ln 4} \quad \text{when} \quad 0 < \xi \le 2\tau < 1. \tag{22}$$

Corollary 3 *Let $\{C_n\}$ be a sequence of $[n,k,d]$ codes such that $d/n \to \delta$ as $n \to \infty$ where $0 < \delta \le 1/2$. Then for any $s = s(n)$ such that $s \ge \sqrt{n}$ and $s = o(n)$,*

$$1 - \varepsilon_{C_n}\left(\left\lfloor \frac{n-s}{2} \right\rfloor\right) \lesssim \frac{1}{s}\sqrt{\frac{(1-\delta)n}{2\pi\delta}} 2^k e^{-\frac{\delta s^2}{2(1-\delta)n}}. \tag{23}$$

This is a refinement of the Sidelnikov-Pershakov estimate [12] for Reed-Muller codes $RM_{m,r}$ of a fixed order r when $n \to \infty$. Equation (23) implies that for any sequence of $[n,k,d]$ codes C_n, for which the conditions of Corollary 3 are satisfied (in particular, for the codes $RM_{m,r}$), and for any fixed ε, $0 < \varepsilon < 1$,

$$s_{C_n}(\varepsilon) \lesssim \sqrt{\frac{n-d}{d} nk \ln 4}. \tag{24}$$

Note that (24) implies the asymptotic optimality of the Reed-Muller codes $RM_{m,1}$ of first order. On the other hand, it gives only $s_{RM_{m,2}}(\varepsilon) \lesssim \sqrt{3nk \ln 4}$ for Reed-Muller codes $RM_{m,2}$ of second order.

Using Theorem 2, (21), and (22) we prove the following sufficient condition for asymptotical optimality of zero rate codes.

Theorem 8 *Let $\{C_n\}$ be a sequence of $[n, k = k(n)]$ codes such that $k = o(n)$, $k \to \infty$, and*

$$\delta n \le w \le \Delta n$$

for all weights w of minimal codewords where δ and Δ are constants such that $0 < \delta \le \Delta < 1$, and let

$$i_n = \frac{n}{2}\left(1 - \frac{1}{k \ln 4 - 1}\right).$$

If

$$\frac{2^{-k\delta/(1-\delta)}}{\sqrt{k}} \sum_{i=d}^{\lfloor i_n \rfloor} A_i^M(C) \to 0 \quad \textit{when} \quad n \to \infty, \tag{25}$$

then

$$\varepsilon_{C_n}\left(\left\lfloor \frac{n - \sqrt{nk \ln 4}}{2} \right\rfloor\right) \to 1 \quad \textit{when} \quad n \to \infty, \tag{26}$$

and so $\{C_n\}$ is asymptotically optimal.

Corollary 4 *The sequence of codes $RM_{m,2}$ is asymptotically optimal when $n = 2^m \to \infty$.*

To prove this corollary we used the known weight distribution of $RM_{m,2}$. Note that Ashikhmin and Barg [1] found the weight distribution of minimal words in $RM_{m,2}$ but we do not use this result in our proof.

Corollary 5 *Let $\{C_m\}$ be the sequence of the dual of the primitive BCH codes of length $n = 2^m - 1$, designed distance $2t+1$, and dimension $k = mt$ ($2t + 1 < 2^{\lceil m/2 \rceil} + 3$). Then the sequence $\{C_m\}$ is asymptotically optimal when $n = 2^m - 1 \to \infty$ if t is a constant or grows slowly ($t^2 = o\left(\frac{\sqrt{n}}{\ln n}\right)$).*

For this sequence we have $d > i_n$ and the condition (25) is fulfilled.

References

[1] A. Ashikhmin and A. Barg, "Minimal vectors in linear codes", *IEEE Trans. on Inform. Theory*, vol. 44, pp. 2010–2017, 1998.

[2] V.M. Blinovsky, "Uniform estimate for linear code spectrum", *Problemy Peredachi Informatsii*, vol. 37, no. 3, pp. 3-5, 2001 (in Russian). English translation in *Probl. Inform. Transm.*, vol. 37, no. 3, pp. 187–189, 2001.

[3] P. Charpin, V.A. Zinoviev, "On coset weight distributions of the 3-error-correcting BCH codes", *SIAM J. of Discrete Math.*, Vol. 10, no. 1, pp. 128–145, 1997.

[4] G.D. Cohen and A. Lempel, "Linear intersecting codes," *Discr. Math.*, vol. 56, pp. 35–43, 1984.

[5] D.C. Gorenstein, W.W. Peterson, and N. Zierler, "Two-error correcting Bose-Chaudhuri codes are quasi-perfect", *Info. and Control*, vol. 3, pp. 291–294, 1960.

[6] T. Helleseth and T. Kløve, "The Newton radius of codes", *IEEE Trans. on Inform. Theory*, vol. 43, pp. 1820–1831, 1997.

[7] T. Helleseth, T. Kløve, V.I. Levenstein "Error-correction capability of binary linear codes and the discrete simplex problem", submitted to *IEEE Trans. on Inform. Theory.*

[8] V.I. Levenshtein, "Bounds on the probability of undetected error" *Problemy Peredachi Informatsii*, vol. 13, no. 1, pp. 3–18, 1977 (in Russian). English translation in *Probl. Inform. Transm.*, vol. 13, no. 1, pp. 1–12, 1977.

[9] L. Levitin and C.R.P. Hartman, "A new approach to the general minimum distance decoding problem: The zero-neighbors algorithm", *IEEE Trans. on Inform. Theory*, vol. 31, pp. 378–384, 1985.

[10] J. Massey, "Minimal codewords and secret sharing," in *Proc. 6th Joint Swedish-Russian Workshop on Information Theory* (Molle Sweden, 1993), pp. 276–279.

[11] G. Poltyrev, "Bounds on the decoding error probability of binary linear codes via their spectra", *IEEE Trans. on Inform. Theory*, vol. 40, pp. 1284–1292, 1994.

[12] V.M. Sidelnikov, A.S. Pershakov, "Decoding Reed-Muller codes with a large number of errors", *Problemy Peredachi Informatsii*, vol. 28, no. 3, pp. 80-94, 1992 (in Russian). English translation in *Probl. Inform. Transm.*, vol. 28, no. 3, pp. 269–281, 1992.