Bounds on the Covering Radius of Linear Codes

A. Ashikhmin * A. Barg *

Abstract

Asymptotically bounding the covering radius in terms of the dual distance is a well-studied problem. We will combine the polynomial approach with estimates of the distance distribution of codes to derive new results for linear codes.

1 Introduction

Let $F = \mathbb{F}_2^n$ and let $C \subset F$ be a binary linear code of length $n$. The covering radius of $C$ is defined as

$$r(C) = \max_{x \in F} \min_{y \in C+x} \text{wt}(y),$$

where $\text{wt}(\cdot)$ denotes the Hamming weight. Bounding the covering radius of codes is one of the main extremal problems of coding theory. Let $C' = \{x \in F : (x, c) = 0 \ \forall c \in C\}$ be the dual code of $C$ and $(A'_i, 0 \leq i \leq n)$ be its weight distribution, where $A'_i = |\{x \in C' : \text{wt}(x) = i\}|$. The minimal $i \geq 1$ such that $A'_i > 0$ is called the dual distance of $C$, denoted $d'$. The most developed direction is deriving bounds on $r$ in terms of the strength of $C$ as a design in $F$ or, in other words, in terms of the distance $d'$. This problem received considerable attention through the last decade, see [2], [3, Ch. 12], [4], [6]–[8], [11]–[19], and this is the problem studied in the present paper. Let $r(d') = \max r(C)$ where the maximum is taken over all codes of dual distance at most $d'$. We will be interested in asymptotic upper bounds on $\rho = r/n$ valid for any sequence of codes $C_n$ of growing length and dual distance $d \leq d'n$. A review of the methods used for obtaining such bounds is given in [2], [7], see also [11]. A large part of ideas concentrates around an application of Delsarte’s polynomial method put forward by Tietjävärinen in [19]. The result in that paper has the following form:

$$\rho(d') \leq \varphi(d'/2),$$

where $\varphi(x) = \frac{1}{2} - \sqrt{x(1-x)}$. Ultimately the best upper bounds on $\rho(d')$ known are obtained based on the following theorem. By $K_i(x)$ we denote the Krawtchouk polynomial of degree $i$.

---

* Bell Labs, Lucent Technologies, 600 Mountain Avenue, Murray Hill, NJ 07974, {aea, abarg}@research.bell-labs.com.

1 Research supported in part by the Binational Science Foundation (USA-Israel), grant no. 1999099
Theorem 1 [3, p. 230] Let $s$ be an integer, and let $f(x) = \sum_{i=0}^{n} f_i K_i(x)$ be a polynomial such that $f(i) \leq 0, i = s + 1, \ldots, n$, and

$$f_0 \geq \sum_{j=d'}^{n} |f_j| A_j$$

(2)

Then the covering radius of a linear code $C$ with dual distance $d'$ is at most $s$.

So far applications of this theorem were based on bounding $A_j$ above by the maximal size $A(n, d', j)$ of a code of length $n$, distance $d'$ and constant weight $j$. This enables one to derive an upper bound of the form $\sum_{j=d'}^{n} |f_j| A'_j \leq F$; then to establish (2) for a given polynomial $f(x)$ one only needs to verify that $F < f_0$. Asymptotically this approach amounts to using bounds on the rate $R(\delta', \xi)$ of constant-weight codes with relative distance $\delta'$ and relative weight $\xi = j/n$. In particular [2] relies upon the “JPL” bound [13], and [7] uses an improvement of this bound from [9, 14] to improve the bound on $\rho(\delta')$ for $0.04 \leq \delta' \leq 0.20$. Papers [2], [7] use the polynomial

$$W_t(x) := \frac{(K_{i+1}(x) + K_i(x))^2}{a - x}$$

(3)

where $a$ is the smallest root of the numerator and $t$ an appropriately chosen parameter. This polynomial was first suggested in [13] for bounding the size of codes. Jointly papers [2] and [7] together with [6] contain the best bounds known to-date. The first two bounds are cited in Theorem 4 below and the remarks following its proof; the third one is too cumbersome to reproduce here (see also Theorem 2 in [2]).

In this paper we suggest to replace estimates of $R(\delta', \xi)$ with other bounds on the weight distribution of codes. One option is, for a given choice of the polynomial $f(x)$, to bound the sum $\sum_{j=d'}^{n} |f_j| A'_j$ as a whole. A method for deriving universal bounds of this type was suggested in a recent work [1]. In the same paper we also obtained estimates of individual coefficients $A_i$ which can be used in Theorem 1. Both approaches enable us to improve the cited results. We establish the following new bounds.

Theorem 2 For $0 \leq \delta' \leq 1/2$

$$\rho(\delta') \leq \varphi(H^{-1}(1 - H(\varphi(\delta'))))$$

(4)

$$\rho(\delta') \leq 2\varphi(\delta')$$

(5)

where $H(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$.

(Logarithms are base 2 throughout). These results improve the bound of [6] for all $\delta'$ and the bound of [2] in the interval $\delta' \in [\delta'_1, 1/2]$, where $\delta'_1 \approx 0.27$. For $\delta' \leq 0.267\ldots$, (4) is better than (5). For $0 < \delta' \leq \delta'_1$ the results of [2],[7] remain the best known. The improvement of the previous results given by Theorem 2 is rather substantial, as shown in Table 1.

Apart from proving Theorem 2 we also present a new proof of the results of [2], [7] which enables us to formulate them in a more explicit manner than in the original works.
2 Bounds on the weight distribution

In this section we collect the results from [2] that we need. We also prove an extended version of one of the estimates on the weight distribution from [2].

A. Krawtchouk Polynomials (for the proofs see, for instance, [3]). Let $\alpha(i) = 2^{-n} \binom{n}{i}$. We have $\int K_i K_s d\alpha = \binom{n}{i} \delta_{i,s}$ and thus $\|K_i\|^2 = \binom{n}{i}$. This implies that

$$(K_i(i))^2 \leq \binom{n}{i} 2^n / \binom{n}{i}.$$

The Krawtchouk coefficients of any polynomial $f(x) = \sum f_j K_j(x)$ can be computed from $\|K_j\|^2 f_j = \int f K_j d\alpha$. In particular,

$$K_a(x) K_b(x) = \sum_{c=0}^{n} p_{a,b}^c K_c(x),$$  \hspace{1cm} (6)

where

$$p_{a,b}^c = \binom{c}{(b-a+c)/2} \binom{n-c}{(b+a-c)/2} 1_{\{a+b-c \in \mathbb{Z}_+\}}$$  \hspace{1cm} (7)

Note that $p_{a,b}^c = 0$ for $a + b < c$ and $p_{a,b}^0 = \delta_{a,b} \binom{n}{i}$.

With $t = \tau n$ and $i = \mu n$ we see that $n^{-1} \log_2 |K_i(i)| \leq E_1(\tau, \mu) + o(1)$, where

$$E_1(u,v) = \frac{1}{2} (H(u) - H(v) + 1).$$

The zeros of $K_i(x)$ are located inside the segment $[n \varphi(\tau), n(1 - \varphi(\tau))]$ and for the minimum zero we have

$$n \varphi(t/n) \leq x_1 \leq n \varphi(t/n) + t^{1/6} \sqrt{n-t}.$$  \hspace{1cm} (8)

Note that the function $\varphi(x)$ is monotone decreasing for $0 \leq x \leq 1/2$. It is also an involution and so $\varphi^2 = \text{id}$. Let

$$I(\tau, \mu) = \int_0^\mu \log \frac{s + \sqrt{s^2 - 4y(1-y)}}{2 - 2y} \, dy.$$
where \( s = 1 - 2\tau \). It is known [5] that \( n^{-1} \log_2 K_{\tau n}(\mu n) = E_2(\tau, \mu) + o(1) \), where

\[
E_2(\tau, \mu) := (H(\tau) + I(\tau, \mu)) \quad (0 \leq \mu \leq \varphi(\tau)).
\]

(9)

An upper bound on the exponent of \( K_i(i) \) which has a simpler form and is not as crude as \( E_1 \) was derived in [10]. It has the form \( n^{-1} \log_2 K_{\tau n}(\mu n) \leq E_3(\tau, \mu) + o(1) \), where

\[
E_3(\tau, \mu) := \frac{1}{2} \left[ \mu \log \frac{\varphi(\tau)}{1 - \varphi(\tau)} + \log(1 - \varphi(\tau)) + H(\tau) + 1 \right] \quad (0 \leq \mu \leq \varphi(\tau)).
\]

(10)

We note that \( E_3(\tau, \mu) \geq E_2(\tau, \mu) \geq E_1(\tau, \mu) \) for \( 0 \leq \mu \leq \varphi(\tau) \) with equality if and only if \( \mu = \varphi(\tau) \). Moreover, for this \( \mu \) also

\[
(E_1(\tau, \mu))'_\mu = (E_2(\tau, \mu))'_\mu = (E_3(\tau, \mu))'_\mu.
\]

B. Weight distribution. Let \( a_\xi(C) = (\log_2 A_\xi(n))/n \) be the exponent of the weight coefficient of a linear code \( C \) of length \( n \). We denote

\[
a_\xi(\delta) = \max_{C: d(C) = \delta n} a_\xi(C).
\]

Theorem 3 For any sequence of codes of relative distance \( \delta \)

\[
a_\xi \lesssim \begin{cases} 
H(\xi) + H(\varphi(\delta)) - 1 & \delta \leq \xi \leq 1 - \delta \\
-2I(\varphi(\delta), \xi) & 1 - \delta \leq \xi \leq 1.
\end{cases}
\]

(11)

(See Fig. 1).

Proof (outline).

(a) The starting point is the following result of [1]. Let \( g(x) \) be a function and \( Z(x) \) a polynomial over \( \mathbb{R} \). Suppose that \( Z(x) = \sum_i z_i K_i(x) \) and that \( z_i \leq 0, 0 \leq i \leq n \). If \( Z(i) \geq g(i), d \leq i \leq n \) then

\[
\sum_{i=d}^n g(i) A_i \leq z_0 |C| - Z(0).
\]

(12)

(b) Take \( \tau = \varphi(\delta) \) and \( t = \tau n \). As in [1], we take

\[
g(i) = (K_w(i))^2,
\]

\[
Z(i) = (K_w(i))^2 - \frac{t + 1}{2} \left( \begin{array}{c} n \\ t \end{array} \right) W_i(i),
\]

for a suitably chosen \( w \). It is proved in [1], Prop.2 that for large \( n \) and \( \frac{w}{n} = \omega < \frac{t}{n} = \tau \), this choice satisfies the conditions of (a). Computing the right-hand side of (12) we get

\[
\sum_{i=d}^n (K_w(i))^2 A_i \leq \frac{n^2(t + 1)}{2at^2} \left( \begin{array}{c} n \\ w \end{array} \right) \left( \begin{array}{c} n \\ t \end{array} \right) - \left( \begin{array}{c} n \\ w \end{array} \right)^2.
\]

(13)
(c) Let $\delta \leq \xi \leq 1/2$ and take $\omega = \varphi(\xi)$. Then we have $\omega < \tau = \varphi(\delta)$. Taking logarithms in (13) and bounding the exponent of $K_w(i)$ by $E_1(\omega, \xi)$ we obtain the first inequality in (11).

(d) Let $1/2 \leq \xi \leq 1 - \delta$. Then we take the same polynomials $g(i)$ and $Z(i)$ with $\tau = \varphi(\delta)$ but choose $\omega = 1 - \varphi(\xi)$. The argument of (c) is then repeated which is possible since $|K_k(x)| = |K_k(n - x)|$.

(e) Now let $1 - \delta \leq \xi \leq 1$. Since we want to ensure that $\omega < \tau$, we replace the above choice of $\omega$ by a number arbitrarily close to $\tau$. Then a better estimate of $K_w(i)$ is given in (9), and we get the second inequality of the statement.

Note that (13) implies the following estimate of the left-hand side: for any sequence of codes with distance $d$

$$n^{-1} \log \sum_{i=d}^{n} (K_w(i))^2 A_i \leq H(\omega) + H(\tau) \quad (\omega \leq \tau).$$

(14)

One more result from [1] that we use is as follows:

$$n^{-1} \log \sum_{i=d}^{n} p_{i,t}^j A_i \leq 2H(\tau) - H(\delta/2) \quad (\delta/2 \leq \tau).$$

(15)

3 Bounds on the covering radius

We will use the estimates of the previous section for the weight distribution $(A_i', d \leq i \leq n)$ of the code $C'$. By abuse of notation we let $a_\xi = n^{-1} \log A_i'$ and denote by $a_\xi(\delta')$ a generic upper bound on $a_\xi$ that holds for any family of codes with relative distance $\delta'$. The following theorem gives results of [2], [7] in an analytic form, replacing a numerical procedure employed there.

**Theorem 4** Let $\tau$ be the minimal number such that

$$\max_{\delta' \leq \xi \leq 2\tau} \{ (1 - \xi)H(\frac{\tau - \xi/2}{1 - \xi}) - H(\tau) + \xi + a_\xi(\delta') \} < 0,$$

(16)

Then $\rho \leq \varphi(\tau)$.

This theorem will follow immediately if we establish the asymptotic behavior of the Krawtchouk coefficients of $f(x)$ from (3).

**Lemma 5** Let $f(x)$ be the polynomial (3) and let $f(x) = \sum_{j=0}^{n} f_j K_j(x)$ be its Krawtchouk expansion. Then

$$\log f_j \sim \log p_{i,t}^j.$$ 

(17)

Suppose that $j = \xi n$ and $t = \tau n$. Then

$$n^{-1} \log_2 f_j = (1 - \xi)H(\frac{\tau - \xi/2}{1 - \xi}) + \xi + o(1)$$

5
Proof. The expression for $f_j$ has the form [13]:

$$f_j = \frac{2}{(t+1)K_t(a)} \left( \binom{n}{t} \sum_{i=0}^{t} K_i(a) \left( p_{t,i}^j + p_{t+1,i}^j \right) \right), \quad (18)$$

and $f_j \geq 0$ for all $0 \leq j \leq n$. Note that for any $i$ if $p_{t,i}^j \neq 0$ then $p_{t,i+1}^j = 0$ and vice versa. Estimating (18) below by the last term, we get

$$f_j \geq \frac{2}{t+1} p_{t,i}^j (1 + O(n))$$

which implies the expression of the Lemma as a lower bound. Let us prove that this is also an upper bound. Since\(^1\)

$$\binom{n}{a} K_t(a) = \binom{n}{t} K_t(t)$$

we can rewrite (18) as

$$f_j = \frac{2}{(t+1)K_t(a)} \binom{n}{t} \sum_{i=0}^{t} K_i(i) \left( p_{t,i}^j + p_{t+1,i}^j \right). \quad (19)$$

Note that the main term of the minimal zero $x_a$ of $K_a(x)$ behaves as $n \varphi(a)$, and by definition $a = n \varphi(t) + o(n)$. Hence $x_a \sim t$, and so the sum on $i$ ranges over the segment $0 < i < x_a$. Now let us estimate $K_a(i)$ from above by $\exp(nE_3(\varphi(\tau), \xi))$ (see 10) and take logarithms. Putting $i = \mu n$ and recalling that $\varphi$ is an involution we can bound the exponent of the summation term in (19) as follows:

$$\frac{1}{2} \left[ x \log \frac{\tau}{1 - \tau} + \log(1 - \tau) + H(\varphi(\tau)) + 1 \right] + \xi H \left( \frac{\tau - \mu + \xi}{2\xi} \right)$$

$$+ (1 - \xi) H \left( \frac{\tau + \mu - \xi}{2(1 - \xi)} \right). \quad (20)$$

The derivative of this expression on $\mu$ has the form

$$M(\mu) = \log \left( \frac{(\xi + \tau - \mu)(2 - \xi - \tau - \mu)\tau}{(\xi - \tau + \mu)(\tau + \mu - \xi)(1 - \tau)} \right).$$

Note that $0 \leq \mu \leq \tau \leq 1/2$. We easily check that $M(\tau) \geq 0$ for any $0 \leq \xi \leq 2\tau$. Next we prove that $M(\mu)$ has no zeros for $\tau - \xi \leq \mu \leq \tau$. If it does then the values of $\mu$ that satisfy the expression

$$\frac{(\xi + \tau - \mu)(2 - \xi - \tau - \mu)\tau}{(\xi - \tau + \mu)(\tau + \mu - \xi)(1 - \tau)} = 1,$$
which are
\[
\mu_{1,2} = \frac{\pm \sqrt{\xi^2 - 4(1 - \tau)\tau(\xi^2 - \tau(1 - \tau)) - \tau}}{1 - 2\tau}
\]
fall in the segment \( \tau - \xi \leq \mu \leq \tau \). However, \( \mu_2 < 0 \) and it is checked directly that \( \mu_1 > \tau \). Hence the term in (20) attains its maximum on \( \mu = \tau \) and we finally obtain
\[
n^{-1} \log f_j \leq E_3(\varphi(\tau), \tau) + n^{-1} \log \rho_{i,t}^j.
\]
Finally since \( E_3(\tau, \varphi(\tau)) = E_1(\tau, \varphi(\tau)) \), we can substitute \( E_1 \) together with the logarithm of \( \rho_{i,t}^j \). This implies that the expression in the statement of the lemma is also an upper bound on the exponent of \( f_j \) and completes the proof.

**Proof** of Theorem 4. For \( j = \xi n \) we bound above the exponent of \( A_j \) by \( a_\xi(\delta') \). Asymptotically the sum \( \sum_j f_j A_j \) is dominated by the largest term, \( j_0 \) say, such that its exponent attains maximum on \( \xi = j/n \) for \( \delta' \leq \xi \leq 2\tau \). It is also immediate from Lemma 5 that
\[
\log f_0 = n(H(\tau) + 2E_1(\tau, \varphi(\tau)) + o(n).
\]
Comuting \( \log f_0 - \log(f_{j_0} A_{j_0}) \), we obtain the expression under the maximum in (16). Together with Theorem 1 this establishes the claim.

Obtaining bounds on \( \rho(\delta') \) with this theorem is a matter of choosing a suitable bound \( a_\xi(\delta') \). An obvious idea is to use upper bounds on constant weight codes:
\[
a_\xi(\delta') \leq R(\delta', \xi).
\]
Substituting the bound on \( R(\delta', \xi) \) from [13] we obtain the result of [2]\(^2\). An improved bound from [14] gives the result of [7].

A better result for large \( \delta' \) is obtained if we combine Theorem 4 with Theorem 3. The result can be expressed in a closed form. We need to substitute the bound (11) into (16) and optimize on \( \xi, \delta' \leq \xi \leq 1 \). Depending on whether \( \xi \leq 1 - \delta' \) or not the expression whose maximum on \( \xi \) is sought is different. First we remark that this maximum is always attained for \( \delta' \leq \xi \leq 1 - \delta' \). Indeed, suppose that \( 1 - \delta' \leq \xi \leq 1 \), then substituting the second inequality in (11) we observe that the part of the expression that depends on \( \xi \) equals \( n^{-1} \log \rho_{i,t}^{\xi n} - 2I(\varphi(\delta), \xi) \). The first logarithm is the falling function of \( \xi \) since its derivative equals
\[
\frac{d}{d\xi}((1 - \xi)H(\frac{\tau - \xi/2}{1 - \xi}) + \xi) = \frac{1}{2} \log \frac{(2\tau - \xi)(2 - 2\tau - \xi)}{(1 - \xi)^2},
\]
which has no zeros and is negative for \( 0 \leq \xi \leq 2\tau \). The function \(-2I(\varphi(\delta'), \xi) \) is also directly checked to be falling on \( \xi \). Thus the maximum in this case is attained for \( \xi = 1 - \delta' \) but for this \( \xi \)
\(^2\)In fact, [2] does a little more: the authors there substitute the bound from [13] and some recurrence relations on the function \( R(\delta', \xi) \) to improve the result for small \( \delta' \).
the bound is the same as in the first case of (11). It remains to analyze the case \( \delta' \leq \xi \leq 1 - \delta' \).
Substituting the first upper bound (11) into the expression to be maximized in (16), we obtain

\[
(1 - \xi)H\left(\frac{\tau - \xi/2}{1 - \xi}\right) - H(\tau) + \xi + H(\xi) - H(\phi(\delta)) + 1.
\]

This function has a unique maximum on \( \xi = 2\tau(1 - \tau) \). Substituting this value of \( \xi \), we get, upon simplification, the expression

\[
H(\tau) - 1 + H(\phi(\delta)).
\]

The minimum \( \tau \) for which this is negative is thus arbitrarily close to \( \tau_0 := H^{-1}(1 - H(\phi(\delta))) \). Thus \( \rho(\delta') \leq \varphi(\tau_0) \), which proves the first part of Theorem 2.

To prove the second part of this theorem, let us take in Theorem 1 the polynomial \( f(x) \) given by \( f(i) = 2^tp_i^t \), where \( t/n = \tau = \phi(\delta') \). By (6)-(7) we get \( f(i) = 0 \ (2t + 1 \leq i \leq n) \) and \( f_i = (K_i(i))^2 \). Now from (14) we have

\[
n^{-1}\log \sum_{i=d}^n(K_i(i))^2A_i \leq 2H(\tau)(1 + o(1)).
\]

Since \( n^{-1}\log f_0 \sim 2H(\tau) \), this choice of \( f(x) \) satisfies for large \( n \) the conditions of Theorem 1. So \( \rho \leq 2\tau = 2\varphi(\delta') \), as was to be proved.

**Remark.** If we take \( f(x) = W(x) \) then by (6) \( \log f_i \sim \log p_i^t \), and so

\[
f_0 \sim \left(\frac{n}{t}\right) = \exp(nH(\tau) + o(n)).
\]

Hence together with (15) we see that (2) is satisfied if \( \tau \) is arbitrarily close to but less than \( \delta'/2 \). The first zero of \( f(x) \) behaves as \( n\varphi(\delta'/2) \) and for greater \( x \), \( f(x) \) stays nonpositive; hence \( \varphi(\delta'/2) \) is an upper bound on \( \rho \). This gives another proof of (1).

**References**


Figure 1: Upper estimate of the exponent $a_\xi$ of the distance spectrum for a family of codes with distance $\delta = 0.3$


