# Bounds on the Covering Radius of Linear Codes* 

A. ASHIKHMIN

Bell Labs, Lucent Technologies, 600 Mountain Avenue, Murray Hill, NJ 07974
A. BARG
aea@research.bell-labs.com

Bell Labs, Lucent Technologies, 600 Mountain Avenue, Murray Hill, NJ 07974

Communicated by: A. Tietäväinen
Received December 14, 2000; Revised July 12, 2001; Accepted October 12, 2001


#### 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.


Keywords: asymptotics of Krawtchouk polynomials, Christoffel-Darboux kernel, distance distribution, dual distance

Mathematics Subject Classification: 94B65, 33C45

## 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

$$
r(C)=\max _{x \in F} \min _{y \in C+x} \mathrm{wt}(x)
$$

where $\mathrm{wt}(\cdot)$ denotes the Hamming weight. Bounding the covering radius of codes is one of the main extremal problems of coding theory. Let $C^{\prime}=\{x \in F:(x, c)=0 \forall c \in C\}$ be the dual code of $C$ and $\left(A_{i}^{\prime}, 0 \leq i \leq n\right)$ be its weight distribution, where $A_{i}^{\prime}=\mid\left\{x \in C^{\prime}\right.$ : $\mathrm{wt}(x)=i\} \mid$ and $(x, c)$ denotes the dot product. The minimal $i \geq 1$ such that $A_{i}^{\prime}>0$ is called the dual distance of $C$, denoted by $d^{\prime}$.
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 dual distance $d^{\prime}$. 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 $r\left(d^{\prime}\right)=\max r(C)$ where the maximum is taken over all codes of dual distance at least $d^{\prime}$. We will be interested in asymptotic upper bounds on $\rho=r / n$ valid for any sequence of codes $C_{n}$ of growing length $n$ and dual distance $d^{\prime} \geq \delta^{\prime} n$. A review of the methods used for obtaining such bounds is given

[^0]in [2,7], see also [11]. Previous work has been largely concentrated around an application of Delsarte's polynomial method put forward by Tietäväinen in [19]. The result in that paper has the following form:
\[

$$
\begin{equation*}
\rho\left(\delta^{\prime}\right) \leq \varphi\left(\delta^{\prime} / 2\right) \tag{1}
\end{equation*}
$$

\]

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

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

$$
\begin{equation*}
f_{0}>\sum_{j=d^{\prime}}^{n}\left|f_{j}\right| A_{j}^{\prime} \tag{2}
\end{equation*}
$$

Then the covering radius of a linear code $C$ with dual distance $d^{\prime}$ is at most $s$.
So far applications of this theorem were based on bounding $A_{j}^{\prime}$ above by the maximal size $A\left(n, d^{\prime}, j\right)$ of a code of length $n$, distance $d^{\prime}$ and constant weight $j$. This enables one to derive an upper bound of the form $\sum_{j=d^{\prime}}^{n}\left|f_{j}\right| A_{j}^{\prime} \leq F$; 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 $R\left(\delta^{\prime}, \xi\right)$ of constant-weight codes with relative distance $\delta^{\prime}$ 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 $\rho\left(\delta^{\prime}\right)$ for $0.04 \leq \delta^{\prime} \leq 0.20$. Papers [2,7] use the polynomial

$$
\begin{equation*}
W_{t}(x):=\frac{\left(K_{t+1}(x)+K_{t}(x)\right)^{2}}{a-x} \tag{3}
\end{equation*}
$$

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 $R\left(\delta^{\prime}, \xi\right)$ 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 $\sum_{j=d^{\prime}}^{n}\left|f_{j}\right| A_{j}^{\prime}$ 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 (logarithms are base 2 throughout).

ThEOREM 2. For $0 \leq \delta^{\prime} \leq 1 / 2$

$$
\begin{align*}
& \rho\left(\delta^{\prime}\right) \leq \varphi\left(H^{-1}\left(1-H\left(\varphi\left(\delta^{\prime}\right)\right)\right)\right)  \tag{4}\\
& \rho\left(\delta^{\prime}\right) \leq 2 \varphi\left(\delta^{\prime}\right) \tag{5}
\end{align*}
$$

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

Table 1. Bounds on $\rho\left(\delta^{\prime}\right)$.

| $\delta^{\prime}$ | 0.28 | 0.32 | 0.36 | 0.4 | 0.44 | 0.48 |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| $(4)$ | 0.1047 | 0.0754 | 0.0499 | 0.0285 | 0.0120 | 0.00177 |
| $(5)$ | 0.102 | 0.067 | 0.04 | 0.020 | 0.0072 | 0.00080 |
| $[2]$ | 0.105 | 0.0769 | 0.051 | 0.029 | 0.0125 | 0.00178 |
| $[6]$ | 0.149 | 0.096 | 0.057 | 0.029 | 0.0103 | 0.0011 |

Both (4) and (5) improve the known results (see Table 1). In particular the bound of [6] is improved for all $\delta^{\prime}$ and the bound of [2] in the interval $\delta^{\prime} \in\left[\delta_{1}^{\prime}, 1 / 2\right)$, where $\delta_{1}^{\prime} \approx 0.27$. For $\delta^{\prime} \leq 0.267 \ldots$, (4) is better than (5). For $0<\delta^{\prime} \leq \delta_{1}^{\prime}$ the results of [2,7] remain the best known. As shown in Table, the improvement of the previous results given by Theorem 2 is rather substantial.

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 $\sum_{i=0}^{n} K_{t}(i) K_{s}(i) \alpha(i)=\binom{n}{t} \delta_{t, s}$ and thus $\left\|K_{t}\right\|^{2}:=\sum_{i=0}^{n}\left(K_{t}(i)\right)^{2} \alpha(i)=\binom{n}{t}$. This implies that

$$
\begin{equation*}
\left(K_{t}(i)\right)^{2} \leq\binom{ n}{t} 2^{n} /\binom{n}{i} . \tag{6}
\end{equation*}
$$

The Krawtchouk coefficients of any polynomial $f(x)=\sum f_{j} K_{j}(x)$ can be computed from $\left\|K_{j}\right\|^{2} f_{j}=\sum_{i=0}^{n} f(i) K_{j}(i) \alpha(i)$. In particular,

$$
\begin{equation*}
K_{a}(x) K_{b}(x)=\sum_{c=0}^{n} p_{a, b}^{c} K_{c}(x) \tag{7}
\end{equation*}
$$

where

$$
\begin{equation*}
p_{a, b}^{c}=\binom{c}{(b-a+c) / 2}\binom{n-c}{(b+a-c) / 2} \chi\{a+b-c \in 2 \mathbb{Z}\} \tag{8}
\end{equation*}
$$

Note that $p_{a, b}^{c}=0$ for $a+b<c$ and $p_{a, b}^{0}=\delta_{a, b}\binom{n}{a}$.
With $t=\tau n$ and $i=\mu n$ we see from (6) that $n^{-1} \log \left|K_{t}(i)\right| \leq E_{1}(\tau, \mu)+o(1)$, where

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

Let $\tau<1 / 2$. The zeros of $K_{t}(x)$ are located inside the segment $[n \varphi(\tau), n(1-\varphi(\tau))]$ and for the minimum zero we have

$$
\begin{equation*}
n \varphi(t / n) \leq x_{t} \leq n \varphi(t / n)+t^{1 / 6} \sqrt{n-t} \tag{9}
\end{equation*}
$$

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

$$
I(\tau, \mu)=\int_{0}^{\mu} \log \frac{s+\sqrt{s^{2}-4 y(1-y)}}{2-2 y} d y
$$

where $s=1-2 \tau$. It is known [5] that $n^{-1} \log K_{\lfloor\tau n\rfloor}(\mu n)=E_{2}(\tau, \mu)+o(1)$, where

$$
\begin{equation*}
E_{2}(\tau, \mu):=H(\tau)+I(\tau, \mu) \quad(0 \leq \mu \leq \varphi(\tau)) \tag{10}
\end{equation*}
$$

An upper bound on the exponent of $K_{t}(i)$ which has a simpler form and is not as crude as $E_{1}$ was derived in [10]. It has the form $n^{-1} \log K_{\lfloor\tau n\rfloor}(\mu n) \leq E_{3}(\tau, \mu)+o(1)$, where
$E_{3}(\tau, \mu):=\frac{1}{2}\left[\mu \log \frac{\varphi(\tau)}{1-\varphi(\tau)}+\log (1-\varphi(\tau))+H(\tau)+1\right] \quad(0 \leq \mu \leq \varphi(\tau))$.
We note that $E_{1}(\tau, \mu) \geq E_{3}(\tau, \mu) \geq E_{2}(\tau, \mu)$ for $0 \leq \mu \leq \varphi(\tau)$ with equality if and only if $\mu=\varphi(\tau)$. Moreover, for this $\mu$ also

$$
\left(E_{1}(\tau, \mu)\right)_{\mu}^{\prime}=\left(E_{2}(\tau, \mu)\right)_{\mu}^{\prime}=\left(E_{3}(\tau, \mu)\right)_{\mu}^{\prime}
$$

B. Weight Distribution. Let $a_{\xi}(C)=\left(\log A_{\xi n}\right) / n$ 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 $\delta$

$$
a_{\xi} \lesssim \begin{cases}H(\xi)+H(\varphi(\delta))-1 & \delta \leq \xi \leq 1-\delta  \tag{12}\\ -2 I(\varphi(\delta), \xi) & 1-\delta \leq \xi \leq 1\end{cases}
$$

(See Figure 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

$$
\begin{equation*}
\sum_{i=d}^{n} g(i) A_{i} \leq z_{0}|C|-Z(0) \tag{13}
\end{equation*}
$$



Figure 1. Upper estimate of the exponent $a_{\xi}$ of the distance spectrum for a family of codes with distance $\delta=0.3$.
(b) Take $\tau=\varphi(\delta)$ and $t=\tau n$. As in [1], we take

$$
\begin{aligned}
& g(i)=\left(K_{w}(i)\right)^{2}, \\
& Z(i)=\left(K_{w}(i)\right)^{2}-\frac{t+1}{2} \frac{\binom{n}{w}}{\binom{n}{t}} W_{t}(i),
\end{aligned}
$$

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 (13) we get

$$
\begin{equation*}
\sum_{i=d}^{n}\left(K_{w}(i)\right)^{2} A_{i} \leq \frac{n^{2}(t+1)}{2 a t^{2}}\binom{n}{w}\binom{n}{t}-\binom{n}{w}^{2} \tag{14}
\end{equation*}
$$

(c) Let $\delta \leq \xi \leq 1 / 2$ and take $\omega=\varphi(\xi)$. Then we have $\omega<\tau=\varphi(\delta)$. Taking logarithms in (14) and bounding the exponent of $K_{w}(i)$ by $E_{1}(\omega, \xi)$ we obtain the first inequality in (12).
(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 $\left|K_{k}(x)\right|=\left|K_{k}(n-x)\right|$.
(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 (10), and we get the second inequality of the statement.

Note that (14) implies the following estimate of the left-hand side: for any sequence of codes with distance $d$

$$
\begin{equation*}
n^{-1} \log \sum_{i=d}^{n}\left(K_{w}(i)\right)^{2} A_{i} \lesssim H(\omega)+H(\tau) \quad(\omega \leq \tau) . \tag{15}
\end{equation*}
$$

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

$$
\begin{equation*}
n^{-1} \log \sum_{i=d}^{n} p_{t, t}^{i} A_{i} \lesssim 2 H(\tau)-H(\delta / 2) \quad(\delta / 2 \leq \tau) \tag{16}
\end{equation*}
$$

## 3. Bounds on the Covering Radius

We will use the estimates of the previous section for the weight distribution ( $A_{i}^{\prime}, d^{\prime} \leq i \leq n$ ) of the code $C^{\prime}$. By abuse of notation we let $a_{\xi}=n^{-1} \log A_{i}^{\prime}$ and denote by $a_{\xi}\left(\delta^{\prime}\right)$ a generic upper bound on $a_{\xi}$ that holds for any family of codes with relative distance $\delta^{\prime}$. 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

$$
\begin{equation*}
\max _{\delta^{\prime} \leq \xi \leq 2 \tau}\left\{(1-\xi) H\left(\frac{\tau-\xi / 2}{1-\xi}\right)-H(\tau)+\xi+a_{\xi}\left(\delta^{\prime}\right)\right\}<0 \tag{17}
\end{equation*}
$$

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

$$
\begin{equation*}
\log f_{j} \sim \log p_{t, t}^{j} \tag{18}
\end{equation*}
$$

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

$$
n^{-1} \log f_{j}=(1-\xi) H\left(\frac{\tau-\xi / 2}{1-\xi}\right)+\xi+o(1)
$$

Proof. The expression for $f_{j}$ has the form [13]:

$$
\begin{equation*}
f_{j}=\frac{2}{(t+1) K_{t}(a)}\binom{n}{t} \sum_{i=0}^{t} \frac{K_{i}(a)}{\binom{n}{i}}\left(p_{t, i}^{j}+p_{t+1, i}^{j}\right), \tag{19}
\end{equation*}
$$

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 (19) below by the last term, we get

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

which implies the expression of the Lemma as a lower bound. Let us prove that this is also an upper bound. Since ${ }^{1}$

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

we can rewrite (19) as

$$
\begin{equation*}
f_{j}=\frac{2}{(t+1) K_{t}(a)} \frac{\binom{n}{t}}{\binom{n}{a}} \sum_{i=0}^{t} K_{a}(i)\left(p_{t, i}^{j}+p_{t+1, i}^{j}\right) \tag{20}
\end{equation*}
$$

Note that the main term of the minimal zero $x_{a}$ of $K_{a}(x)$ behaves as $n \varphi(a / n)$, 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 $\exp \left(n E_{3}(\varphi(\tau), \xi)\right.$ ) (see (11)) and take logarithms. Putting $i=\mu n$ and recalling that $\varphi$ is an involution we can bound the exponent of the summation term in (20) as follows:

$$
\begin{equation*}
\frac{1}{2}\left[\mu \log \frac{\tau}{1-\tau}+\log (1-\tau)+H(\varphi(\tau))+1\right]+\xi H\left(\frac{\tau-\mu+\xi}{2 \xi}\right)+(1-\xi) H\left(\frac{\tau+\mu-\xi}{2(1-\xi)}\right) \tag{21}
\end{equation*}
$$

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

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

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 these zeros, which satisfy the expression

$$
\frac{(\xi+\tau-\mu)(2-\xi-\tau-\mu) \tau}{(\xi-\tau+\mu)(\tau+\mu-\xi)(1-\tau)}=1
$$

and therefore are equal to

$$
\mu_{1,2}=\frac{ \pm \sqrt{\xi^{2}-4(1-\tau) \tau\left(\xi^{2}-\tau(1-\tau)\right)}-\tau}{1-2 \tau}
$$

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 (21) attains its maximum on $\mu$ for $\mu=\tau$ and we finally obtain

$$
n^{-1} \log f_{j} \lesssim E_{3}(\varphi(\tau), \tau)+n^{-1} \log p_{t, t}^{j}
$$

Finally since $E_{3}(\tau, \varphi(\tau))=E_{1}(\tau, \varphi(\tau))$, we can substitute $E_{1}$ together with the logarithm of $p_{t, t}^{j}$. 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 $A_{j}^{\prime}$ by $a_{\xi}\left(\delta^{\prime}\right)$. Asymptotically the sum $\sum_{j} f_{j} A_{j}^{\prime}$ is dominated by the largest term, $j_{0}$ say, such that its exponent attains the maximum on $\xi=j / n$ for $\delta^{\prime} \leq \xi \leq 2 \tau$. It is also immediate from Lemma 5 that

$$
\log f_{0}=n\left(H(\tau)+2 E_{1}(\tau, \varphi(\tau))\right)+o(n) .
$$

Computing $\log f_{0}-\log \left(f_{j_{0}} A_{j_{0}}\right)$, we obtain the expression under the maximum in (17). Together with Theorem 1 this establishes the claim.

Obtaining bounds on $\rho\left(\delta^{\prime}\right)$ with this theorem is a matter of choosing a suitable bound on $a_{\xi}\left(\delta^{\prime}\right)$. An obvious idea is to use upper bounds on constant weight codes:

$$
a_{\xi}\left(\delta^{\prime}\right) \leq R\left(\delta^{\prime}, \xi\right)
$$

Substituting the bound on $R\left(\delta^{\prime}, \xi\right)$ from [13] we obtain the result of [2]. ${ }^{2}$ An improved bound from [14] gives the result of [7].

A better result for large $\delta^{\prime}$ 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 (12) into (17) and optimize on $\xi, \delta^{\prime} \leq \xi \leq 1$. The expression whose maximum on $\xi$ is sought, is different for $\xi \leq 1-\delta^{\prime}$ and $\xi>1-\delta^{\prime}$. However in both cases this maximum is attained for $\delta^{\prime} \leq \xi \leq 1-\delta^{\prime}$. Indeed, suppose that $1-\delta^{\prime} \leq \xi \leq 1$, then substituting the second inequality in (12) into (17), we observe that the part of the expression that depends on $\xi$ equals $\left(n^{-1} \log p_{t, t}^{\xi n}\right)-2 I(\varphi(\delta), \xi)$. The first logarithm is the falling function of $\xi$ since its derivative equals

$$
\frac{d}{d \xi}\left((1-\xi) H\left(\frac{\tau-\xi / 2}{1-\xi}\right)+\xi\right)=\frac{1}{2} \log \frac{(2 \tau-\xi)(2-2 \tau-\xi)}{(1-\xi)^{2}}
$$

which has no zeros and is negative for $0 \leq \xi \leq 2 \tau$. The function $-2 I\left(\varphi\left(\delta^{\prime}\right), \xi\right)$ is also directly checked to be falling on $\xi$. Thus the maximum in this case is attained for $\xi=1-\delta^{\prime}$ but for this $\xi$ the bound is the same as in the first case of (12). It remains to analyze the case $\delta^{\prime} \leq \xi \leq 1-\delta^{\prime}$. Substituting the first upper bound (12) into the expression to be maximized in (17), we obtain

$$
(1-\xi) H\left(\frac{\tau-\xi / 2}{1-\xi}\right)-H(\tau)+\xi+H(\xi)-H(\varphi(\delta))+1
$$

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

$$
H(\tau)-1+H(\varphi(\delta))
$$

The minimum $\tau$ for which this is negative is thus arbitrarily close to $\tau_{0}:=H^{-1}(1-$ $H(\varphi(\delta)))$. Thus $\rho\left(\delta^{\prime}\right) \leq \varphi\left(\tau_{0}\right)$, 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 $f(i)=2^{n} p_{t, t}^{i}$, where $t / n=\tau=\varphi\left(\delta^{\prime}\right)$. By (7)-(8) we get $f(i)=0(2 t+1 \leq i \leq n)$ and $f_{i}=\left(K_{t}(i)\right)^{2}$. Now from (15) we have

$$
n^{-1} \log \sum_{i=d^{\prime}}^{n}\left(K_{t}(i)\right)^{2} A_{i} \leq 2 H(\tau)(1+o(1))
$$

Since $n^{-1} \log f_{0} \sim 2 H(\tau)$, this choice of $f(x)$ satisfies for large $n$ the conditions of Theorem 1. So $\rho \leq 2 \tau=2 \varphi\left(\delta^{\prime}\right)$, as was to be proved.

Remark. If we take $f(x)=W_{t}(x)$ then by (7) $\log f_{i} \sim \log p_{t, t}^{i}$, and so

$$
f_{0} \sim\binom{n}{t}=\exp (n H(\tau)+o(n))
$$

Hence together with (16) we see that (2) is satisfied if $\tau$ is arbitrarily close to but less than $\delta^{\prime} / 2$. The first zero of $f(x)$ behaves as $n \varphi\left(\delta^{\prime} / 2\right)$ and for greater $x, f(x)$ stays nonpositive; hence $\varphi\left(\delta^{\prime} / 2\right)$ is an upper bound on $\rho$. This gives another proof of (1).

## Notes

1. Strictly speaking, for this to be true, $a$ must be an integer. However since our aim is asymptotic results, the effect of rounding is insignificant.
2. In fact, [2] does a little more: the authors there substitute the bound from [13] and some recurrence relations on the function $R\left(\delta^{\prime}, \xi\right)$ to improve the result for small $\delta^{\prime}$.

## References

1. A. Ashikhmin, A. Barg and S. Litsyn, Estimates of the distance distribution of codes and designs, IEEE Trans. Inform. Theory, Vol. 47, No. 3 (2001) pp. 1050-1061.
2. A. Ashikhmin, I. Honkala, T. Laihonen and S. Litsyn, On relations between covering radius and dual distance, IEEE Trans. Inform. Theory, Vol. 45, No. 6 (2001) pp. 1808-1816.
3. G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, Covering Codes, Elsevier Science, Amsterdam (1997).
4. G. Fazekas and V. I. Levenshteĭn, On upper bounds for code distance and covering radius of designs in polynomial metric spaces, J. Combin. Theory Ser. A, Vol. 70, No. 2 (1995) pp. 267-288.
5. G. Kalai and N. Linial, On the distance distribution of codes, IEEE Trans. Inform. Theory, Vol. 41, No. 5 (1995) pp. 1467-1472.
6. T. Laihonen, Covering radius of self-complementary codes and BCH codes, Proc. IEEE Int'l Sympos. Inform. Theory (ISIT 1998), Cambridge, MA.
7.     - On an algebraic method for bounding the covering radius, In (A. Barg and S. Litsyn, eds.), Codes and Association Schemes, AMS, Providence (2001) pp. 213-221.
8. T. Laihonen and S. Litsyn, New bounds on covering radius as a function of dual distance, SIAM J. Discrete Math. Vol. 12, No. 2 (1999) pp. 243-251.
9. V. I. Levenshtein, On the minimal redundancy of binary error-correcting codes, Information and Control, Vol. 28, No. 4 (1975) pp. 268-291.
10. S. Litsyn, New upper bounds on error exponents, IEEE Trans. Inform. Theory, Vol. 45, No. 2 (1999) pp. 385-398.
11. S. Litsyn, P. Solé and R. Struik, On the covering radius of an unrestricted code as a function of the rate and dual distance, Discrete Applied Math., Vol. 82 (1998) pp. 177-191.
12. S. Litsyn and A. Tietäväinen, Upper bounds on the covering radius of a code with a given dual distance, European J. Combin., Vol. 17, Nos. 2-3 (1996) pp. 265-270.
13. R. J. McEliece, E. R. Rodemich, H. Rumsey and L. R. Welch, New upper bound on the rate of a code via the Delsarte-MacWilliams inequalities, IEEE Trans. Inform. Theory, Vol. 23, No. 2 (1977) pp. 157-166.
14. A. Samorodnitsky, On the optimum of Delsarte's linear program, J. Combin. Theory Ser. A, Vol. 96, No. 2 (2001) pp. 261-287.
15. P. Solé, Asymptotic bounds on the covering radius of binary codes, IEEE Trans. Inform. Theory, Vol. 36, No. 6 (1990) pp. 1470-1472.
16. -, Packing radius, covering radius, and dual distance, IEEE Trans. Inform. Theory, Vol. 41, No. 1 (1995) pp. 268-272.
17. P. Solé and P. Stokes, Covering radius, codimension, and dual-distance width, IEEE Trans. Inform. Theory, Vol. 39, No. 4 (1993) pp. 1195-1203.
18. A. Tietäväinen, Covering radius and dual distance, Des. Codes Cryptogr., Vol. 1, No. 1 (1991) pp. 31-46.
19.     - An upper bound on the covering radius as a function of the dual distance, IEEE Trans. Inform. Theory, Vol. 36, No. 6 (1990) pp. 1472-1474.

[^0]:    *Research supported in part by the Binational Science Foundation (USA-Israel), Grant no. 1999099.

