Europ. J. Combinatorics (1996) **17,** 265–270

Upper Bounds on the Covering Radius of a Code with a Given Dual Distance

S. Litsyn and A. Tietäväinen

We derive new upper bounds on the covering radius of a binary linear code as a function of its dual distance and dual-distance width. These bounds improve on the Delorme–Solé–Stokes bounds, and in a certain interval for binary linear codes they are also better than Tietäväinen's bound.

1. Introduction

Let C be a code of length n, covering radius $R = R(C)$ and dual distance d'. In 1973 Delsarte [2] proved that $R(C)$ is at most the number of non-zero weights in the dual code $C^{\perp}$. Later a number of bounds have been obtained for the covering radius of a code with a given dual distance. In 1978 Helleseth, Kløve and Mykkeltveit [4] proved the so-called Norse bounds which say that, if C is a binary self-complementary code, then

$$R \leqslant \begin{cases} \frac{1}{2}n & \text{if } d' \geqslant 2, \\ \frac{1}{2}(n - \sqrt{n}) & \text{if } d' \geqslant 4. \end{cases}$$

Recently, some remarkable generalizations were found in [6], [11], [7] and [12]. In particular, the following asymptotic results were proved in [12]:
(a) Let $\mathscr{C} = (C_n)_{n=1}^{\infty}$ be a sequence of codes C_n of length n, dual distance $d' = d'(n)$ and covering radius $R = R(n)$, where $R/n \to \rho$ and $d'/n \to \delta'$ when $n \to \infty$. Then

$$\rho \leqslant \frac{q-1}{q} - \frac{(q-2)\delta'}{2q} - \frac{1}{q}\sqrt{(q-1)\delta'(2-\delta')}$$

and therefore in the binary case

$$\rho \leqslant \tfrac{1}{2}(1 - \sqrt{\delta'(2-\delta')}). \tag{1}$$

(b) There are sequences $\mathscr{C}$ such that, for $0 < \delta' < (q-1)/q$,

$$\rho \geqslant H_q^{-1}(1 - H_q(\delta'))$$

where H_q is the q-ary entropy function. Thus in the binary case there are sequences $\mathscr{C}$ for which

$$\rho \geqslant H_2^{-1}(1 - H_2(\delta')) \tag{2}$$

where $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$.

If C is a binary linear code of dimension k, the trivial redundancy bound $R \leqslant n - k$ together with the weak form of the McEliece–Rodemich–Rumsey–Welch bound [5] implies

$$\rho \leqslant H_2(\tfrac{1}{2} - \sqrt{\delta'(1-\delta')}). \tag{3}$$

Furthermore, in the case of even binary linear codes the Delsarte bound mentioned above gives the result

$$\rho \leqslant 1 - 2\delta'. \tag{4}$$

0195-6698/96/020265 + 06 $18.00/0

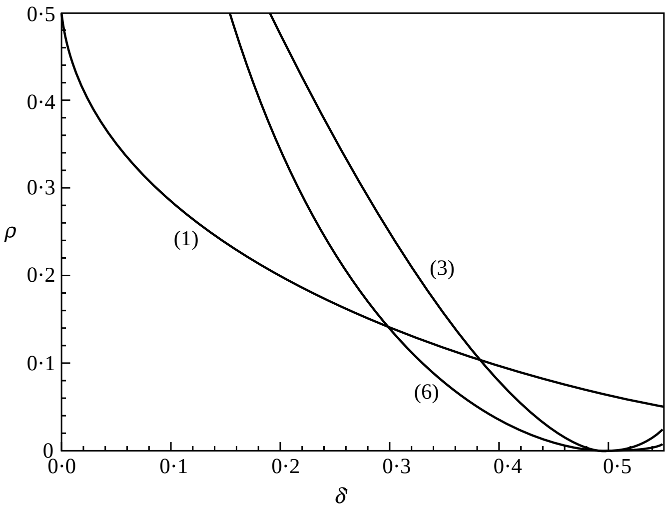

FIGURE 1. The bound (1) and bounds for general linear codes.

In this case also, Delorme and Solé [1] improved earlier bounds in certain intervals by showing that

$$\rho \leqslant H_2\left(\tfrac{1}{2} - \sqrt{\delta'(1-\delta')}\right) \Big/ \log_2\left(\frac{1}{1-2\delta'}\right). \tag{5}$$

In the paper [8], Solé and Stokes were able to partially generalize the results in [1] for unrestricted codes. They also considered the problem to find bounds of this type when not only the dual distance but also the dual-distance width is known.

In this paper we introduce a new approach which generalizes a method presented in [3] and [10]. Using this approach and Chebyshev polynomials, we show in Theorem 2 that, for binary linear codes,

$$\rho \leqslant H_2\left(\tfrac{1}{2} - \sqrt{\delta'(1-\delta')}\right) \Big/ \log_2\left(\frac{(1+\sqrt{\delta'})^2}{1-\delta'}\right). \tag{6}$$

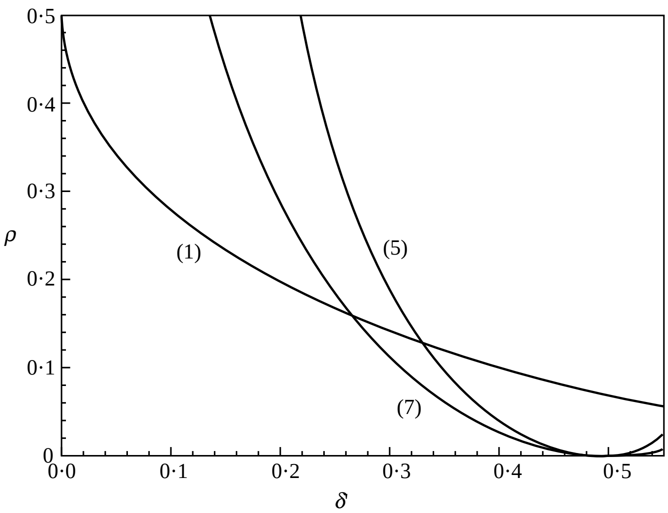

FIGURE 2. The bound (1) and bounds for even-weight linear codes.

Further, we prove in Theorem 3 that, for even binary linear codes,

$$\rho \leqslant H_2\big(\tfrac{1}{2} - \sqrt{\delta(1-\delta')}\big) \Big/ \log_2\Big(\frac{1 + 2\sqrt{\delta'(1-\delta')}}{1 - 2\delta'}\Big). \tag{7}$$

Finally, we find a corresponding bound (Theorem 4) for ρ as a function of the relative dual-distance width. The bound (7) improves on the Delorme–Solé–Stokes bound (5). The bound (6) is better than the redundancy bound (3) for $\delta' > \frac{1}{9}$ and, in the case of linear codes, better than (1) if $\delta' > 0{\cdot}298$.

Generalizations for non-linear and non-binary codes will appear in a forthcoming paper by Litsyn and Solé.

2. A New Approach

Assume that C is a binary linear code of length n, dimension k, minimum distance d ($\geqslant 3$), covering radius R and dual distance d'. Let the $(n-k)\times n$ matrix $H = (\mathbf{h}_1, \ldots, \mathbf{h}_n)$ be a parity check matrix for C, and denote $\{\mathbf{h}_1, \ldots, \mathbf{h}_n\}$ by L. Let $N(L, s, \mathbf{b})$ be the number of solutions $(\mathbf{x}_1, \ldots, \mathbf{x}_s) \in L^s$ of the equation

$$\mathbf{x}_1 + \cdots + \mathbf{x}_s = \mathbf{b}. \tag{8}$$

The covering radius R is the smallest integer r such that every syndrome of C is the sum of at most r columns of H. Hence $R \leqslant r$ if for every $\mathbf{b} \in \mathbf{F}_2^{n-k}$ there is a polynomial $g(x) = \sum_{s=0}^{r} \gamma_s x^s$ such that $\sum_{s=0}^{r} \gamma_s (N(L, s, \mathbf{b}) > 0$.

Write $e(a) = (-1)^a$ for $a \in \mathbf{F}_2$. Then, for all $\mathbf{k} \in \mathbf{F}_2^{n-k}$, the mapping $\psi_{\mathbf{k}}$ defined by

$$\psi_{\mathbf{k}}(\mathbf{a}) = e(\mathbf{k}\cdot\mathbf{a}) \qquad \text{for all } \mathbf{a} \in \mathbf{F}_2^{n-k}$$

is an additive character of $\mathbf{F}_2^{n-k}$, and the characters ψ_k form the dual group of $\mathbf{F}_2^{n-k}$. Thus

$$\sum_{\mathbf{k}\in\mathbf{F}_2^{n-k}} e(\mathbf{k}\cdot\mathbf{a}) = \begin{cases} 2^{n-k} & \text{if } \mathbf{a} = \mathbf{0}, \\ 0 & \text{otherwise}, \end{cases}$$

and

$$\begin{aligned} 2^{n-k}(L, s, \mathbf{b}) &= \sum_{\mathbf{x}_1\in L} \cdots \sum_{\mathbf{x}_s\in L} \sum_{\mathbf{k}\in\mathbf{F}_2^{n-k}} e(\mathbf{k}\cdot(\mathbf{x}_1 + \cdots + \mathbf{x}_s + \mathbf{b})) \\ &= \sum_{\mathbf{k}\in\mathbf{F}_2^{n-k}} e(\mathbf{k}\cdot\mathbf{b}) \sum_{\mathbf{x}_1\in L} e(\mathbf{k}\cdot\mathbf{x}_1) \cdots \sum_{\mathbf{x}_s\in L} e(\mathbf{k}\cdot\mathbf{x}_s) \\ &= \sum_{\mathbf{k}\in\mathbf{F}_2^{n-k}} e(\mathbf{k}\cdot\mathbf{b}) \Big(\sum_{\mathbf{x}\in L} e(\mathbf{k}\cdot\mathbf{x})\Big)^s. \end{aligned} \tag{9}$$

Furthermore,

$$\sum_{\mathbf{x}\in L} e(\mathbf{k}\cdot\mathbf{x}) = n - 2wt(\mathbf{k}H), \tag{10}$$

where wt means the Hamming weight. When $\mathbf{k}$ runs through the elements of $\mathbf{F}_2^{n-k}$, then $\mathbf{k}H$ runs through all elements of the dual $C^\perp$ of C. Therefore, by (9) and (10),

$$2^{n-k}N(L, s, \mathbf{b}) = \sum_{i=0}^{n} \beta_i(\mathbf{b})(n-2i)^s,$$

where

$$\beta_i(\mathbf{b}) = \sum_{\mathbf{k}:\, wt(\mathbf{k}H)=i} e(\mathbf{k}\cdot\mathbf{b}). \tag{11}$$

This implies that

$$2^{n-k} \sum_{s=0}^{r} \gamma_s N(L, s, \mathbf{b}) = \sum_{s=0}^{r} \gamma_s \sum_{i=0}^{n} \beta_i(\mathbf{b})(n-2i)^s$$
$$= \sum_{i=0}^{n} \beta_i(\mathbf{b}) \sum_{s=0}^{r} \gamma_s(n-2i)^s$$
$$= \sum_{i=0}^{n} \beta_i(\mathbf{b}) f(i),$$

where $f(i) = g(n-2i)$. Since $\beta_0(\mathbf{b}) = 1$, we have proved the following result.

THEOREM 1. *Assume that there is a polynomial f of degree r such that, for each $\mathbf{b} \in \mathbf{F}_2^{n-k}$,*

$$f(0) + \sum_{i=1}^{n} \beta_i(\mathbf{b}) f(i) > 0,$$

where $\beta_i(\mathbf{b})$ is defined by (11). *Then $R \leqslant r$.*

3. CHEBYSHEV POLYNOMIALS

In order to use Theorem 1 efficiently we should find a polynomial f of a low degree such that $|f(i)|$ is small compared to $f(0)$ whenever $i \neq 0$ and $\beta_i(\mathbf{b}) \neq 0$. The Chebyshev polynomial of the first kind and of degree r is defined by

$$T_r(x) = \tfrac{1}{2}((x + \sqrt{x^2-1})^r + (x - \sqrt{x^2-1})^r),$$

and for $x \geqslant 1$ equivalently by

$$T_r(x) = \cosh(r \cosh^{-1}(x)). \tag{12}$$

It has the following optimality property (see [9, p. 42]). Let $0 \leqslant a < b$. Let P_r be the set of all polynomials $p_r(x)$ of degree r or less such that $p_r(0) = 1$. Then,

$$t_r(x) = T_r\left(\frac{b+a-2x}{b-a}\right) \Big/ T_r\left(\frac{b+a}{b-a}\right)$$

provides the minimum over the polynomials in P_r of

$$\max_{x \in [a,b]} |p_r(x)|.$$

Moreover,

$$\max_{x \in [a,b]} |t_r(x)| = 1 \Big/ T_r\left(\frac{b+a}{b-a}\right).$$

Furthermore, for $x \geqslant 1$,

$$\cosh^{-1}(x) = \ln(x + \sqrt{x^2-1}). \tag{13}$$

Thus, fox $x \gg 1$,

$$\cosh^{-1}(x) \approx \ln(2x). \tag{14}$$

4. Asymptotic results

Choose $f(x) = t_r(x)$, $a = d'$ and $b = n$. Then

$$\max_{x \in [d', n]} |f(x)| = 1 \Big/ T_r\Big(\frac{n + d'}{n - d'}\Big)$$

Therefore, by (11),

$$f(0) + \sum_{i=1}^{n} \beta_i(\mathbf{b}) f(i) \geq 1 - (2^{n-k} - 1) \max_{i \in [d', n]} |f(i)|$$

$$> 1 - 2^{n-k} \Big/ T_r\Big(\frac{n + d'}{n - d'}\Big),$$

and so Theorem 1 and the equation (12) yield the result

$$R \leq r \qquad \text{if } 2^{n-k} \leq T_r\Big(\frac{n + d'}{n - d'}\Big) = \cosh\Big(r \cosh^{-1}\Big(\frac{n + d'}{n - d'}\Big)\Big). \tag{15}$$

by the McEliece–Rodemich–Rumsey–Welch bound (5),

$$(n - k)/n \lesssim H_2(\tfrac{1}{2} - \sqrt{\delta'(1 - \delta')}), \qquad \text{when } n \to \infty \quad \text{and} \quad d'/n \to \delta'. \tag{16}$$

Combining the result (15) with the formulae (16), (13) and (14) gives the following theorem.

Theorem 2. *Let $(C_n)_{i=1}^{\infty}$ be a sequence of binary linear codes C_n of length n, dual distance d' and covering radius R, where $R/n \to \rho$ and $d'/n \to \delta'$, when $n \to \infty$. Then*

$$\rho \leq H_2(\tfrac{1}{2} - \sqrt{\delta'(1 - \delta')}) \Big/ \log_2\Big(\frac{(1 + \sqrt{\delta'})^2}{1 - \delta'}\Big).$$

Assume then that the weights of the codewords of C are all even. Then $\mathbf{1} \in C^{\perp}$ and hence there is a unique $\mathbf{k}_1 \in \mathbf{F}_2^{n-k}$ such that $\mathbf{k}_1 H = \mathbf{1}$. Thus, for each $\mathbf{b} \in \mathbf{F}_2^{n-k}$, $\beta_n(\mathbf{b}) = e(\mathbf{k}_1 \cdot \mathbf{b})$ and $\beta_i(\mathbf{b}) = 0$ when $i \in (0, d') \cup (n - d', n)$. Now we take $a = d', b = n - d'$ and $f(x) = t_r(x)$, and choose the parity of r in such a way that $\beta_n(\mathbf{b}) f(n)$ is positive (and so equal to 1). Therefore

$$f(0) + \sum_{i=1}^{n} \beta_i(\mathbf{b}) f(i) \geq 2 - (2^{n-k} - 2) \max_{i \in [d', n-d']} |f(i)|$$

$$> 2 - 2^{n-k} \Big/ T_r\Big(\frac{n}{n - 2d'}\Big),$$

and the same argument as before Theorem 2 gives the following result.

Theorem 3. *Let $(C_n)_{n=1}^{\infty}$ be a sequence of binary linear even-weight codes satisfying the conditions of Theorem 2. Then*

$$\rho \leq H_2(\tfrac{1}{2} - \sqrt{\delta'(1 - \delta')}) \Big/ \log_2\Big(\frac{1 + 2\sqrt{\delta'(1 - \delta')}}{1 - 2\delta'}\Big).$$

The restriction that all the weights in C are even is not very essential because, in any case, this is true for the even-weight subcode C_0. Let us define (see [1]) $w = w(C)$, dual-distance width of C, as the smallest integer w such that all the weights in $C^{\perp}$ belong to the set

$$\{0\} \cup \left[\frac{n}{2} - \frac{w}{2}, \frac{n}{2} + \frac{w}{2}\right] \cup \{n\}.$$

Assume that in the sequence $(C_n)_{n=1}^{\infty}$, $w/n \to \omega$ when $n \to \infty$. Since $R(C) \leqslant R(C_0)$, $w(C) = w(C_0)$ and $d'(C_0) = \frac{1}{2}(n - w(C_0))$, we then see that Theorem 3 implies the following corollary.

THEOREM 4. *If the sequence $(C_n)_{n=1}^{\infty}$ satisfies the assumptions of Theorem 2, we have*

$$\rho \leqslant H_2(\tfrac{1}{2}(1 - \sqrt{1-\omega^2})) \Big/ \log_2\left(\frac{1 + \sqrt{1-\omega^2}}{\omega}\right).$$

Acknowledgements

The authors would like to thank the referees who provided reference [9] and mentioned that the optimality properties of Chebyshev polynomials have been used by Lubotszky, Phillips and Sarnak (Ramanujan graphs, *Combinatorica,* **8** (1988), 261–277) and by Chung, Faber and Manteufel (An upper bound on the diameter of a graph from eigenvalues associated with its Laplacian, *SIAM J. Discr. Math.,* **7** (1994), 443–457) in a combinatorial context but in different directions.

References

1. C. Delorme and P. Solé, Diameter, covering index, covering radius and eigenvalues, *Europ. J. Combin.,* **12** (1991), 95–108.
2. P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, *Inform. Control,* **23** (1973), 407–438.
3. T. Helleseth, On the covering radius of cyclic linear codes and arithmetic codes, *Discr. Appl. Math.,* **11** (1985), 157–173.
4. T. Helleseth, T. Kløve and J. Mykkeltveit, On the covering radius of binary codes, *IEEE Trans. Inform. Theory,* **24** (1978) 627–628.
5. R. J. McEliece, E. R. Rodemich, H. C. Rumsey, Jr. and L. R. Welch, New upper bounds on the rate of a code via the Delsarte–MacWilliams inequalities, *IEEE Trans. Inform. Theory,* **23** (1977), 157–166.
6. P. Solé, Asymptotic bounds on the covering radius of binary codes, *IEEE Trans. Inform. Theory,* **36** (1990), 1470–1472.
7. P. Solé and K. G. Mehrotra, Generalization of the Norse bounds to codes of higher strength, *IEEE Trans. Inform. Theory,* **37** (1991), 190–192.
8. P. Solé and P. Stokes, Covering radius, codimension, and dual-distance width, *IEEE Trans. Inform. Theory,* **39** (1993), 1195–1203.
9. G. Szegö, *Orthogonal Polynomials,* American Mathematical Society, Colloquium Publications, Volume XXIII, Providence, Rhode Island, fourth edition, 1975.
10. A. Tietäväinen, *Codes and Character Sums,* Springer Lecture Notes in Computer Science, vol. 388 1989, pp. 3–12.
11. A. Tietäväinen, An upper bound on the covering radius as a function of its dual distance, *IEEE Trans. Inform. Theory,* **36** (1990), 1472–1474.
12. A. Tietäväinen, Covering radius and dual distance, *Designs, Codes and Cryptography,* **1** (1991), 31–46.

Received 20 *January* 1995 *and accepted in revised form* 13 *March* 1995

S. LITSYN
Department of EE-systems, Tel-Aviv University,
Ramat-Aviv 69978, Israel

A. TIETÄVÄINEN
Department of Mathematics, University of Turku,
FIN-20500 Turku, Finland