On Upper Bounds for Minimum Distance and Covering Radius of Non-binary Codes

Tero Laihonen

Department of Mathematics, University of Turku,
FIN-20014 Turku, Finland

Simon Litsyn

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

Turku Centre for Computer Science
TUCS Technical Report No 80
December 1996

ISBN 951-650-923-1
ISSN 1239-1891

Abstract

We consider upper bounds on two fundamental parameters of a code; minimum distance and covering radius. New upper bounds on the covering radius of non-binary linear codes are derived by generalizing a method due to S. Litsyn and A. Tietäväinen [9] and combining it with a new upper bound on the asymptotic information rate of non-binary codes. The new upper bound on the information rate is an application of a shortening method of a code. These results improve on the best presently known asymptotic upper bounds on minimum distance and covering radius of non-binary codes in certain intervals.

TUCS Research Group
Coding Theory Group

1 Introduction

Bounds on minimum distance and covering radius attracted a great deal of research (see, e.g. [10, 3]).

In this paper we consider the case of bounds for parameters of non-binary codes. The best presently known upper bounds on the minimum distance is due to M. Aaltonen [2], and was obtained using the linear programming method in the generalized Johnson scheme (see Section 3 for more details). It is known that there the covering radius depends crucially on the distance of the dual code.

In 1973 Delsarte [5] proved that the covering radius of a code is at most the number of nonzero weights in the dual code. Later in the papers [4, 6, 7, 12, 13, 14, 16, 17] a number of bounds have been obtained for the covering radius of a code with a given dual distance.

Especially, Tietäväinen [17] gave the following asymptotic result:

Let $(C_n)_{n=1}^{\infty}$ be a sequence of codes $C_n \subset F_q^n$ with 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

$$\rho \leq \frac{q-1}{q} - \frac{q-2}{2q}\delta' - \frac{1}{q}\sqrt{(q-1)\delta'(2-\delta')}. \tag{1}$$

In the paper [14] Solé and Stokes proved the following asymptotic result for linear codes with certain assumptions (see [14, Section VI]):

$$\rho \leq \frac{H_q\left(\frac{q-1}{q} - \frac{q-2}{q}\delta' - \frac{2}{q}\sqrt{(q-1)\delta'(1-\delta')}\right)}{\log_q\left(\frac{q-1}{(1-\delta')q-1}\right)} \tag{2}$$

where

$$H_q(x) = \begin{cases} 0 & \text{if } x = 0, \\ x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x) & \text{if } 0 < x \leq \frac{q-1}{q}. \end{cases}$$

In the last expression an upper bound on the information rate is implicitly used. The best known bound for non-binary codes was obtained by M.Aaltonen [2] in the frames of linear programming method.

In this paper we generalize a method due to Litsyn and Tietäväinen [9] to non-binary codes and we give a new upper bound on the asymptotic information rate improving on Aaltonen's bound; i.e., a new asymptotic upper bound on the minimum distance is obtained. Combining these two results gives a new asymptotic upper bound on the covering radius of non-binary linear codes which improves on the best presently known bounds (1) and (2) in certain intervals (see Section 4).

2 The generalized method

Let F_q denote the finite field of cardinality of q. Assume that $C \subset F_q^n$ is a linear code of dimension k, minimum distance $d(\geq 3)$, 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 the set $\{\mathbf{h}_1, \ldots, \mathbf{h}_n\}$ by L and the nonzero elements of F_q by $F_q^\star$. Let $N_{\mathbf{a}}(L, s, \mathbf{b})$, where $\mathbf{a} = (a_1, \ldots, a_s) \in (F_q^\star)^s$, be the number of solutions $(\mathbf{x}_1, \ldots, \mathbf{x}_s) \in L^s$ of the equation

$$a_1\mathbf{x}_1 + \ldots + a_s\mathbf{x}_s = \mathbf{b}. \tag{3}$$

Denote also $N(L, s, \mathbf{b}) = \sum_{\mathbf{a}\in(\mathrm{F}_q^\star)^s} N_{\mathbf{a}}(L, s, \mathbf{b})$.

The covering radius R of a linear code C is the smallest integer r such that every syndrome of C is a F_q-linear combination of at most r columns of H.

Let $q = p^r$ where p is the characteristic of F_q. We recall (see e.g. [5]) that a character $\psi_{\mathbf{u}}$, $\mathbf{u} \in F_q^n$, of $(F_q^n, +)$ is of the form

$$\psi_{\mathbf{u}}(\mathbf{v}) = \omega^{Tr_p^q(\mathbf{u}\cdot\mathbf{v})} \text{ for all } \mathbf{v} \in F_q^n$$

where ω denotes a primitive complex pth root of unity, $\mathbf{u}\cdot\mathbf{v}$ the inner product of the vectors $\mathbf{u}$ and $\mathbf{v}$, and the trace function $Tr_p^q : F_q \to F_p$ is defined by

$$Tr_p^q(x) = x + x^p + \ldots + x^{p^{r-1}}.$$

The next lemma is crucial in the sequel and it generalizes the result presented in [9] to non-binary codes.

Lemma 1 *Assume that for each* $\mathbf{b} \in F_q^{n-k}$ *there is a polynomial of degree at most* r *such that*

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

where $\beta_i(\mathbf{b}) = \sum_{\mathbf{k}\in F_q^{n-k}, w(\mathbf{k}H)=i} \psi_{\mathbf{k}}(-\mathbf{b})$. *Then* $R \leq r$.

Proof. It is well-known (see e.g. [10, p.143]) that

$$\sum_{\mathbf{k}\in F_q^{n-k}} \psi_{\mathbf{k}}(\mathbf{a}) = \begin{cases} q^{n-k} & \text{if } \mathbf{a} = \mathbf{0}, \\ 0 & \text{otherwise,} \end{cases}$$

and therefore, by (3), we obtain

$$q^{n-k} N(L, s, \mathbf{b}) = \sum_{\mathbf{k}\in F_q^{n-k}} \psi_{\mathbf{k}}(-\mathbf{b}) \left(\sum_{\mathbf{x}\in L} \sum_{a\in F_q^\star} \psi_{\mathbf{k}}(a\mathbf{x}) \right)^s$$

Furthermore,
$$\sum_{\mathbf{x}\in L}\sum_{a\in F_q^\star}\psi_{\mathbf{k}}(a\mathbf{x}) = n(q-1) - qw(\mathbf{k}H)$$
where w denotes the Hamming weight.

Since $\mathbf{k}H$ runs through all elements of the dual code C^- of C, when $\mathbf{k}$ runs through the elements of F_q^{n-k}, we have

$$q^{n-k}N(L,s,\mathbf{b}) = \sum_{i=0}^{n}\left(\sum_{\mathbf{k}\in F_q^{n-k}, w(\mathbf{k}H)=i}\psi_{\mathbf{k}}(-\mathbf{b})\right)(n(q-1)-qi)^s$$

and therefore,

$$q^{n-k}N(L,s,\mathbf{b}) = \sum_{i=0}^{n}\beta_i(\mathbf{b})(n(q-1)-qi)^s. \tag{4}$$

We choose next such a polynomial $g(x) = \sum_{s=0}^{r}\gamma_s x^s$ that $g(n(q-1)-qi) = f(i)$. Since $\beta_0(\mathbf{b}) = 1$ for all $\mathbf{b}\in F_q^{n-k}$, we have by (4)

$$\begin{aligned} 0 &< f(0) + \sum_{i=1}^{n}\beta_i(\mathbf{b})f(i) \\ &= q^{n-k}\sum_{s=0}^{r}\gamma_s N(L,s,\mathbf{b}). \end{aligned}$$

Hence $N(L,s,\mathbf{b}) \neq 0$ for at least one s ($s = 0,1,\ldots,r$) and so $R \leq r$. □

We should now find a polynomial of a low degree such that $|f(i)|$ is small compared to $f(0)$ when $i \neq 0$ and $\beta_i(\mathbf{b}) \neq 0$.

The Chebyshev polynomial of the first kind and degree r is defined in [11, p.5] by
$$T_r(x) = \frac{1}{2}\left(\left(x+\sqrt{x^2-1}\right)^r + \left(x-\sqrt{x^2-1}\right)^r\right).$$

So clearly, $x \geq 1$,

$$T_r(x) \leq \frac{1}{2}((x+\sqrt{x^2-1})^r + 1) \tag{5}$$

Assume that $0 \leq a < b$. Among the polynomials $p_r(x)$ of degree at most r such that $p_r(0) = 1$ the one defined by

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

provides (see [15, p.42]) the minimum of $\max_{x\in[a,b]} |p_r(x)|$. Furthermore,

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

In order to apply the polynomial $t_r(x)$ to Lemma 1 efficiently, we need to know something about the asymptotic information rate of non-binary codes. It will be studied in the next section.

3 New upper bounds on the information rate

Let $M_q(n,d)$ denote the number of words in the largest code $C \subset F_q^n$ with minimum distance at least d. We define the asymptotic information rate $R_q(\delta)$ $(0 \le \delta \le 1)$ by

$$R_q(\delta) = \limsup_{n\to\infty} \frac{1}{n} \log_q M_q(n,d),$$

where $\lim_{n\to\infty} d/n = \delta$.

The tightest presently known upper bounds on asymptotic information rate of non-binary codes are the following ones (see [2, p.141]):

$$R_q(\delta) \le 1 - \delta \frac{q}{q-2} \log_q(q-1), \qquad q > 2,\ 0 \le \delta \le \left(\frac{q-2}{q}\right)^2, \tag{6}$$

and

$$R_q(\delta) \le 1 - H_q(\omega) + f_q(\xi,\eta), \tag{7}$$

where the parameters satisfy the following conditions:

$$0 \le \omega \le 1,\ 0 \le \eta \le \frac{q-2}{q-1}\omega,\ 0 \le \xi - \eta \le \min\{\omega - \eta, 1-\omega\},$$

$$\beta = (1-\eta) h\left(\frac{\omega-\eta}{1-\eta}, \frac{\xi-\eta}{1-\eta}\right) \le \omega - \frac{q-1}{q-2}\eta,$$

$$\delta \ge 2\beta + (\omega - \beta) k_{q-1}\left(\frac{\eta}{\omega-\beta}\right)$$

with the following notations:

$$f_q(\xi,\eta) = H_q(\xi) + \xi H_q(\eta/\xi) - (\xi+\eta)\log_q(q-1) + \eta \log_q(q-2),$$

$$k_q(x) = \frac{q-1}{q} - \frac{q-2}{q}x - \frac{2}{q}\sqrt{(q-1)x(1-x)},\ \ (0 \le x \le 1),$$

and

$$h(x,y)=\frac{x(1-x)-y(1-y)}{1+2\sqrt{y(y-1)}},\ (0\le x\le 1,\ 0\le y\le 1).$$

With a certain choice of parameters the bound (7) reduces to a simpler form (see [2, p.141]):

$$R_q(\delta)\le H_q(k_q(\delta)),\ 0\le\delta\le\frac{q-1}{q}, \tag{8}$$

which is useful for when δ is close to $(q-1)/q$ (see [2, p.157]). We are here interested in large values of δ, since the method presented in Lemma 1 improves on the bound (1) when δ' is large.

In order to give a new upper bound on $R_q(\delta)$, we shall need the following theorem, which generalizes the well-known result (see e.g. [10, p.43])

$$M_q(n,d)\le q^t M_q(n-t,d)$$

where $t\le n-d$. Let $B_r(\mathbf{x})$ be the Hamming sphere of radius r and with center at $\mathbf{x}\in F_q^n$. Denote its cardinality by $V_q(n,r)=\sum_{i=0}^{r}\binom{n}{i}(q-1)^i$.

Theorem 1 *Let $0\le d\le n$, $d-2r\le n-t$, $0\le r\le t$ and $0\le r\le \frac{1}{2}d$. Then*

$$M_q(n,d)\le\frac{q^t}{V_q(t,r)}M_q(n-t,d-2r). \tag{9}$$

Proof. Let a code $C\subset F_q^n$ be such that its cardinality is $M_q(n,d)=:M$; i.e., let C be an (n,M,d) code. We shorten the code C choosing t components of codewords and taking those codewords in which the chosen t components belong to a Hamming sphere of radius r. Finally, we delete these t coordinates.

Next we show that in this way we get from C an $(n-t,\ge\frac{M}{q^t}V_q(t,r),\ge d-2r)$ code. The first parameter is clear and the third one follows from the fact that the deleted parts of the selected codewords differ at most in $2r$ positions. Let us now consider the second parameter. We denote the M words (not necessarily distinct) of the t components by $\mathbf{y}_1,\ldots,\mathbf{y}_M\in F_q^t$ in some order. Let

$$\chi_{\mathbf{x}}(\mathbf{y})=\begin{cases}1 & \text{if } \mathbf{y}\in B_r(\mathbf{x}),\\ 0 & \text{otherwise.}\end{cases}$$

Since

$$\begin{aligned}\frac{1}{q^t}\sum_{\mathbf{x}\in F_q^t}\sum_{i=1}^{M}\chi_{\mathbf{x}}(\mathbf{y}_i) &= \frac{1}{q^t}\sum_{i=1}^{M}\sum_{\mathbf{x}\in F_q^t}\chi_{\mathbf{x}}(\mathbf{y}_i)\\ &= \frac{M}{q^t}V_q(t,r),\end{aligned}$$

there exists a sphere of radius r which contains at least $\frac{M}{q^t}V_q(t,r)$ of the words $\mathbf{y}_1,\ldots,\mathbf{y}_M$ and so the claim follows. □

By the previous theorem we get now the following upper bound on the asymptotic information rate.

Theorem 2 *Let* $0 \le \delta \le \frac{q-1}{q}$, $\tau - 2\lambda \le 1-\delta$, $0 \le \lambda \le \frac{1}{2}\delta$ *and* $0 \le \lambda \le \frac{q-1}{q}\tau$. *Denote* $\frac{x}{2} = \frac{\lambda}{\tau}$ *and* $y = \frac{\delta-2\lambda}{1-\tau}$. *Assume that* $x \ne \delta$. *Then*

$$R_q(\delta) \le R(y) + (1 - H_q(x/2) - R(y))\frac{\delta - y}{x - y} \tag{10}$$

where $R(y)$ *is an upper bound on the asymptotic information rate at point* y.

Proof. Let $r = \lfloor \lambda\tau^{-1}\lfloor \tau n\rfloor\rfloor$ and $t = \lfloor \tau n \rfloor$. It is well-known (see e.g. [8, p.55]) that

$$\lim_{n\to\infty} \frac{log_q V_q(n, \lfloor \alpha n\rfloor)}{n} = H_q(\alpha)$$

where $0 \le \alpha \le \frac{q-1}{q}$. Combining this result with Theorem 1 gives

$$R_q(\delta) \le \tau(1 - H_q(\lambda/\tau)) + (1-\tau)R_q\left(\frac{\delta - 2\lambda}{1-\tau}\right).$$

Thus

$$R_q(\delta) \le R(y) + ((1 - H_q(x/2) - R(y))\frac{\delta - y}{x - y}.$$

□

By the Hamming bound (see e.g. [8, p.60]):

$$H(\delta) := 1 - H_q(\delta/2),\ 0 \le \delta \le 1,$$

we may write the bound (10) in the form

$$R_q(\delta) \le R(y) + (H(x) - R(y))\frac{\delta - y}{x - y}$$

with the assumptions of the previous theorem.

Hence Theorem 2 means that $R_q(\delta)$ is on or below any straight line segment between the Hamming bound and a given upper bound, i.e., a straight line between any point on the Hamming bound $(x, H(x))$ and any point on a given upper bound $(y, R(y))$ is also an upper bound on the asymptotic information rate. Clearly, the best improvements are achieved when the line (10) is tangential to the Hamming bound and to the given upper bound.

Table 1: Numerical values for $q = 16$.

δ	(6) & (7)	(10)	δ	(6) & (7)	(10)
0.26	0.70201	0.70192	0.52	0.41955	0.41568
0.28	0.68056	0.67990	0.54	0.39722	0.39366
0.30	0.65908	0.65788	0.56	0.37490	0.37164
0.32	0.63755	0.63586	0.58	0.35257	0.34963
0.34	0.61598	0.61384	0.60	0.33025	0.32761
0.36	0.59435	0.59183	0.62	0.30792	0.30559
0.38	0.57269	0.56981	0.64	0.28560	0.28357
0.40	0.55098	0.54779	0.66	0.26327	0.26155
0.42	0.52923	0.52577	0.68	0.24095	0.23953
0.44	0.50744	0.50375	0.70	0.21862	0.21752
0.46	0.48561	0.48173	0.72	0.19630	0.19550
0.48	0.46374	0.45972	0.74	0.17397	0.17348
0.50	0.44184	0.43770	0.76	0.15165	0.15146

Table 2: The interval [a,b] and parameters x and y.

q	a	b	x	y	q	a	b	x	y
7	0.54	0.56	0.08	0.58	27	0.14	0.84	0.04	0.86
8	0.52	0.60	0.08	0.62	32	0.12	0.86	0.04	0.88
16	0.26	0.76	0.06	0.78	64	0.06	0.92	0.02	0.94

Choosing the given upper bound to be the bound (8), the bound (10) gives a small improvement on the bounds (6) and (7) in a certain interval. In Table 1 the comparing of these bounds is given for $q = 16$ and only those values of δ are given where these improvements occur on best of the bounds (6) and (7).

On the other hand, Table 2 shows (for some q's) the interval [a,b] in which the bound (10) improves on the bounds (6) and (7) (note that q is at least 7). In Table 2 the parameters x and y are also shown.

If we choose $x = 0$ and $R(y)$ to be the bound (8) and we minimize the right-hand side of the inequality (10) (for minimization see [1, p.156]), we obtain the bound (6).

4 New upper bounds for covering radius

We are now in a position to state the results for covering radius. Theorem 3 is valid in the whole interval $[0, 1]$ whereas Theorem 4 improves it in a certain part of this interval.

Theorem 3 *Let $(C_n)_{n=1}^{\infty}$ be a sequence of nonbinary 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 $n \to \infty$. If $0 \le \delta' \le \left(\frac{q-2}{q}\right)^2$, then*

$$\rho \le \frac{1 - \delta' \frac{q}{q-2} \log_q(q-1)}{log_q\left(\frac{(1+\sqrt{\delta'})^2}{1-\delta'}\right)}, \tag{11}$$

and, if $\left(\frac{q-2}{q}\right)^2 \le \delta' \le \frac{q-1}{q}$, then

$$\rho \le \frac{H_q(k_q(\delta'))}{log_q\left(\frac{(1+\sqrt{\delta'})^2}{1-\delta'}\right)}. \tag{12}$$

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

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

Thus

$$\begin{aligned} f(0) + \sum_{i=1}^{n} \beta_i(\mathbf{b}) f(i) &\ge 1 - (q^{n-k} - 1) \max_{i \in [d', n]} |f(i)| \\ &> 1 - \frac{q^{n-k}}{T_r\left(\frac{n+d'}{n-d'}\right)}. \end{aligned}$$

Therefore, by Lemma 1, we have $R \le r$ if

$$q^{n-k} \le T_r\left(\frac{n+d'}{n-d'}\right). \tag{13}$$

Combining the results (13) and (5) with the dual forms of the bounds (6) and (8); i.e.,

$$\limsup_{n\to\infty} \frac{n-k}{n} \le 1 - \delta' \frac{q}{q-2} \log_q(q-1), \; 0 \le \delta' \le \left(\frac{q-2}{q}\right)^2,$$

$$\limsup_{n\to\infty} \frac{n-k}{n} \le H_q(k_q(\delta')), \; 0 \le \delta' \le \frac{q-1}{q}$$

gives the desired result. □

Note that the bounds (11) and (12) coincide at $((q-2)/q)^2$.

Table 3: Numerical values for $q = 16$.

δ'	(11) & (12)	(15)	δ'	(11) & (12)	(15)
0.42	0.95387	0.94417	0.68	0.28522	0.28355
0.44	0.88317	0.87433	0.70	0.25049	0.24922
0.46	0.81671	0.80867	0.72	0.21755	0.21666
0.48	0.75410	0.74682	0.74	0.18635	0.18582
0.50	0.69501	0.68845	0.76	0.15683	0.15664
0.52	0.63917	0.63328	0.78	0.12909	0.12909
0.54	0.58633	0.58107	0.80	0.10347	-
0.56	0.53626	0.53161	0.82	0.08005	-
0.58	0.48879	0.48470	0.84	0.05895	-
0.60	0.44375	0.44020	0.86	0.04034	-
0.62	0.40099	0.39795	0.88	0.02450	-
0.64	0.36038	0.35783	0.90	0.01186	-
0.66	0.32183	0.31973	0.92	0.00314	-

If we replace the dual forms of the bounds (6) and (8) with the dual form of the bound (10) where we have chosen $R(y) = H_q(k_q(y))$; i.e.,

$$\limsup_{n\to\infty} \frac{n-k}{n} \leq \frac{H_q(k_q(y)) - 1 + H_q(x/2)}{y-x}(\delta' - x) + 1 - H_q(x/2) \qquad (14)$$

where $0 \leq x \leq \delta' \leq y \leq \frac{q-1}{q}$, $x \neq y$, the same argument as in the previous proof gives the following result.

We denote the right-hand side of (14) by $L_{x,y}(\delta')$.

Theorem 4 *Let $(C_n)_{n=1}^{\infty}$ be a sequence of nonbinary linear codes $C_n \subset F_q^n$ with dual distance d' and covering radius R where $R/n \to \rho$ and $d'/n \to \delta'$ when $n \to \infty$. Assume also that $x \leq \delta' \leq y$, $x \neq y$ where $x, y \in [0, (q-1)/q]$. Then*

$$\rho \leq \frac{L_{x,y}(\delta')}{\log_q\left(\frac{(1+\sqrt{\delta'})^2}{1-\delta'}\right)}. \qquad (15)$$

Table 3 shows that the values of the bounds (11) & (12) and (15) for $q = 16$. In the Table 3 the values less than 1 are given and the bound (15) is included when $x \leq \delta' \leq y$. As q grows the improvement of the bound (15) becomes small compared to the bounds (11) & (12), however these bounds still improve essentially on the well-known bounds (1) and (2).

It should be emphasized that in the binary situation further improvements are possible (see [7]).

Acknowledgements. We are very grateful to M.Aaltonen for inspiring discussions, and for providing programs for calculating asymptotical bounds on the size of non-binary codes. The authors thank heartily also I. Honkala and A. Tietäväinen for their valuable suggestions.

References

[1] M. Aaltonen, Bounds on the information rate of a tree code as a function on the code's feedback decoding minimum distance, *Ann. Univ. Turku. Ser. A I*, Vol. 181 (1981).

[2] M. Aaltonen, A new upper bound on nonbinary block codes, *Discrete Math.*, Vol. 83 (1990), pp. 139–160.

[3] G. Cohen, S. Litsyn, A. Lobstein and H. Mattson, Jr., Covering radius 1985–1994. Technical Raport 94-D-025, Ecole Nationale Supérieure des Télécommunications, Paris, 1994, submitted to AAECC Journal.

[4] C. Delorme and P. Solé, Diameter, covering index, covering radius and eigenvalues,*Europ. J. Combin.*, Vol 12 (1991), pp. 95–108.

[5] P. Delsarte, Four fundamental parametres of a code and their combinatorial significance,*Information and Control*, Vol. 23, (1973), pp. 407–438.

[6] T. Helleseth, T. Kløve, and J. Mykkeltveit, On the covering radius of binary codes, *IEEE Trans. Inform. Theory*, Vol. 24 (1978), pp. 627–628.

[7] I. Honkala, S. Litsyn, and A. Tietäväinen, On algebraic methods in covering radius problems, In: Cohen, G., Giusti M., Mora, T. (eds.) Applied Algebra, Albegraic Algoritms and Error-Correcting Codes. Lecture Notes in Computer Science, Vol 948. Berlin, Heidelberg, New York: Springer (1995).

[8] J. van Lint, *Introduction to Coding Theory*, Berlin, Heidelberg, New York: Springer-Verlag (1982).

[9] S. Litsyn and A. Tietäväinen, Upper bounds on the covering radius of a code with a given dual distance, *Europ. J. Combin.*, to appear.

[10] F. J. MacWilliams and N. J. A. Sloane,*The Theory of Error-Correcting Codes*, Amsterdam: North-Holland (1977).

[11] T. Rivlin, *The Chebyshev polynomials*, New York: John Wiley & Sons (1974).

[12] P. Solé, Asymptotic bounds on the covering radius of binary codes, *IEEE Trans. Inform. Theory*, Vol. 36, (1990), pp. 1470–1472.

[13] P. Solé and K. Mehrotra, Generalization of the Norse bounds to codes of higher strenght, *IEEE Trans. Inform. Theory*, Vol. 37, (1991), pp. 190–192.

[14] P. Solé and P. Stokes, Covering radius, codimension, and dual-distance width,*IEEE Trans. Inform. Theory*, Vol. 39, (1993), pp. 1195–1203.

[15] G. Szegö, *Orthogonal Polynomials*, Amer. Math. Soc. Colloq. Publ., v,. 23, Providence, RI, (1975).

[16] A. Tietäväinen, An upper bound on the covering radius as a function of its dual distance, *IEEE Trans. Inform. Theory*, Vol. 36, (1990), pp. 1472–1474.

[17] A. Tietäväinen, Covering radius and dual distance, *Designs, Codes and Cryptography*, Vol. 1, (1991), pp. 31–46.

Turku Centre for Computer Science
Lemminkäisenkatu 14
FIN-20520 Turku
Finland

http://www.tucs.abo.fi

University of Turku
- **Department of Mathematical Sciences**

Åbo Akademi University
- **Department of Computer Science**
- **Institute for Advanced Management Systems Research**

Turku School of Economics and Business Administration
- **Institute of Information Systems Science**