ГОДИШНИК НА СОФИЙСКИЯ УНИВЕРСИТЕТ "СВ. КЛИМЕНТ ОХРИДСКИ"
ФАКУЛТЕТ ПО МАТЕМАТИКА И ИНФОРМАТИКА
Книга 1 — Математика
Том 82, 1988

ANNUAIRE DE L'UNIVERSITE DE SOFIA "ST. KLIMENT OHRIDSKI"
FACULTE DE MATHEMATIQUES ET INFORMATIQUE
Livre 1 — Mathématiques
Tome 82, 1988

ON THE COVERING RADIUS OF SOME BINARY CYCLIC CODES *

EVGUENIA VELIKOVA

Евгения Великова. РАДИУСЫ ПОКРЫТИЯ НЕКОТОРЫХ ДВОИЧНЫХ ЦИКЛИЧНЫХ КОДОВ. Рассматриваются двоичные цикличные коды длины $n = uv$, которые получаются следующим разбиением многочлена $x^{uv} - 1 = (x-1)\left(\frac{x^u-1}{x-1}\right) \times \left(\frac{x^v-1}{x-1}\right) f_1(x)$, где u и v — нечетные взаимно простые числа. Для этих кодов определены радиусы покрытия (для двух из них — только верхняя и нижняя границы радиуса).

Evguenia Velikova. ON THE COVERING RADIUS OF SOME BINARY CYCLIC CODES. The binary cyclic codes of length $u = uv$ obtained by the factorization $x^{uv} - 1 = (x-1) \times \left(\frac{x^u-1}{x-1}\right)\left(\frac{x^v-1}{x-1}\right) f_1(x)$, where u and v are odd relatively prime numbers are considered. For these codes we find the covering radius (for two codes only upper and lower bound on covering radius).

In this paper we study the problem of finding the covering radius of some binary cyclic codes. Let C be an $[n, k]$ binary linear code and with F denote the field with two elements $F = GF(2)$. The covering radius $R = R(C)$ of C is the smallest integer, such that any vector of the space F^n is within Hamming distance R from some code word. The covering radius of cyclic codes of length up to 31 are given in[1] and the covering radius of cyclic codes of length 33, 35 and 39, without 3 codes, are given in [2]. The codes, considered in this paper, are some binary cyclic codes of length which is a product of two relatively prime odd numbers.

*This paper was partially supported by the Bulgarian Comittee of Science under contract 37/1988.

Let u and v be odd integers, such that $gcd(u, v) = 1$ and $u < v$. We consider the binary cyclic codes of length $n = uv$, obtained by the following factorization:

$$x^{uv} + 1 = f_0(x) \cdot f_1(x) \cdot f_u(x) \cdot f_v(x),$$

where

$$\begin{aligned} f_0(x) &= x + 1, \\ f_u(x) &= x^{u-1} + \cdots + x + 1 = \frac{x^u + 1}{x + 1}, \\ f_v(x) &= x^{v-1} + \cdots + x + 1 = \frac{x^v + 1}{x + 1}, \\ f_1(x) &= \frac{x^{uv} + 1}{f_0(x) \cdot f_u(x) \cdot f_v(x)}. \end{aligned}$$

In other words we consider only the codes which generator polynomial is a product of some $f_0(x)$, $f_1(x)$, $f_u(x)$, $f_v(x)$. For each two numbers u and v there are 12 codes of this kind and let the codes be C_i and $g_i(x)$ be the generator polynomial of code C_i, as they are given in the Table 1 and R_i be the covering radius of code C_i.

Some of these codes have a parity polynomial which divides $x^s + 1$ ($s = u$ or $s = v$) and these codes are composed of some repetitions of (in our case) F^s or E_s (E_s is the $[s, s-1, 2]$ even weight code). For such codes we can calculate their covering radius using [3]. In this way we obtain the covering radius of the following codes:

Table 1

Code	Generator polynomial
C_1	$g_1(x) = f_1(x) f_u(x)$
C_2	$g_2(x) \equiv f_0(x) f_1(x) f_u(x)$
C_3	$g_3(x) \equiv f_1(x) f_v(x)$
C_4	$g_4(x) \equiv f_0(x) f_1(x) f_v(x)$
C_5	$g_5(x) \equiv f_0(x) f_v(x)$
C_6	$g_6(x) \equiv f_v(x)$
C_7	$g_7(x) \equiv f_0(x) f_u(x)$
C_8	$g_8(x) \equiv f_u(x)$
C_9	$g_9(x) \equiv f_1(x)$
C_{10}	$g_{10}(x) \equiv f_0(x) f_1(x)$
C_{11}	$g_{11}(x) \equiv f_0(x) f_u(x) f_v(x)$
C_{12}	$g_{12}(x) \equiv f_u(x) f_v(x)$

— $g_1(x) = f_1(x) f_u(x)$ and C_1 is $[uv, v, u]$ $R_1 = \frac{v(u-1)}{2}$ code and C_1 is u repetitions of F^v,

— $g_2(x) = f_0(x) f_1(x) f_u(x)$ and C_2 is $[uv, v-1, 2u]$ $R_2 = 1 + \frac{v(u-1)}{2}$ code and C_2 is u repetitions of E_v,

— $g_3(x) = f_1(x) f_v(x)$ and C_3 is $[uv, u, v]$ $R_3 = \frac{u(v-1)}{2}$ code and C_3 is v repetitions of F^u,

— $g_4(x) = f_0(x) f_1(x) f_v(x)$ and C_4 is $[uv, u-1, 2v]$ $R_4 = 1 + \frac{u(v-1)}{2}$ code and C_4 is v repetitions of E_v.

We will use the following obvious proposition:

Proposition 1. Let C be an $[n, k]$ binary linear code. If $H = (h_1 \dots h_n)$ is a parity check matrix of C, then $R(C)$ is the smallest integer, such that every nonzero vector of F^{n-k} is a sum of at most R columns of the matrix H, i.e.

$$x = h_{i_1} + \dots + h_{i_t}, \qquad t \leqq R, \qquad \forall x \in F^{n-k} \setminus \{0\}.$$

If H has repeated columns, then only one of this columns can be taken for the calculation. Therefore, using this proposition we can calculate the covering radius of the codes dual to $C_1, \dots, C_4$ and namely the covering radius of the following codes:

— $g_5(x) = f_1(x) f_v(x)$ and C_5 is $[uv,\ uv - v,\ 2]$ $R_5 = v$ code and C_5 is the dual to C_1,

— $g_6(x) = f_v(x)$ and C_6 is $[uv,\ uv - v + 1,\ 2]$ $R_6 = \frac{v-1}{2}$ code and C_6 is the dual to C_2,

— $g_7(x) = f_0(x) f_u(x)$ and C_7 is $[uv,\ uv - u,\ 2]$ $R_7 = u$ code and C_7 is the dual to C_3,

— $g_8(x) = f_u(x)$ and C_8 is $[uv,\ uv - u + 1,\ 2]$ $R_8 = \frac{u-1}{2}$ code and C_8 is the dual to C_4.

The minimum distance of each of the rest four codes is given by the following theorem:

Theorem 1. i) If $g_9(x) = f_1(x)$ then C_9 is a $[uv,\ u + v - 1,\ u]$ code and C_9 has a weight enumerator

$$A(z) = \sum_{i=0}^{\frac{1}{2}(u-1)} \binom{u}{2i} \left(z^{2i} + z^{u-2i}\right)^v ,$$

ii) If $g_{10}(x) = f_0(x) f_1(x)$, then C_{10} is the $[uv,\ ,u + v - 2,\ 2u]$ code,

iii) If $g_{11}(x) = f_0(x) f_u(x) f_v(x)$, then C_{11} is the $[uv,\ ,uv - u - v + 1,\ 4]$ code,

iv) If $g_{12}(x) = f_u(x) f_v(x)$, then C_{12} is the $[uv,\ ,uv - u - v + 2,\ 4]$ code.

Proof. i) The code C_9 contains the code C_1 which is u times repeated F^v, as well as the code C_3 which is v times repeated F^u. C_3 is generated by the words x_i, $i = 1, \dots, u$ with support $X_i = \{i,\ i + u,\ \dots,\ i + (v-1)u\}$ and C_1 is generated by words y_j, $j = 1, \dots, v$ with support $Y_j = \{j,\ j + v,\ \dots,\ j + (u-1)v\}$. We can arrange the coordinates $\{1, 2, \dots, n\}$ in a $u \times v$ matrix

$$\begin{pmatrix} i_{11} & \dots & i_{1v} \\ \dots & \dots & \dots \\ i_{u1} & \dots & i_{uv} \end{pmatrix},$$

such that $i_{st} \equiv i_{s\ell} (\mathrm{mod} u)$ and $i_{st} \equiv i_{\ell t} (\mathrm{mod} v)$. Then the words x_i, $i = 1, \dots, u$

and y_j, $j = 1, \ldots, v$ are presented as

$$(1)\ x_i = \begin{pmatrix} 0 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 1 & \cdots & 1 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 0 \end{pmatrix} \text{ — } i\text{–th row}\ , \qquad y_j \ = \begin{pmatrix} 0 & \cdots & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 1 & \cdots & 0 \end{pmatrix}.$$

j–th
column

The word, which is a sum of t words of x_i, $i = 1, \ldots, u$ and s words of y_j, $j = 1, \ldots, v$ has a weight $t(v - s) + s(u - t)$ and in this way we obtain

$$A(z) = \sum_{c \in C_9} z^{wt(c)} = \sum_{i=0}^{\frac{1}{2}(u-1)} \binom{u}{2i} \left(z^{2i} + z^{u-2i}\right)^v,$$

and the minimum distance of the C_9 is equal to u.

ii) The code C_{10} is the even weight subcode of C_9 and the minimum even distance in C_9 is $2u$.

iii) The generator polynomial of code C_{11} is $g_{11}(x) = \dfrac{(x^u + 1)(x^v + 1)}{x + 1}$ and the word $(x + 1)g_{11}(x) = x^{u+v} + x^v + x^u + 1$ belongs to the code C_{11}. Therefore $d_{11} \leqq 4$ but C_{11} is the even weight code and its dual code C_9 is not a repetition code, hence $d_{11} = 4$. We can compute the weight enumerator of C_{11} using the MacWilliams equations (see [4, p. 127]). The weight enumerator of C_{11} is

$$B(z) = \sum_{c \in C_{11}} z^{wt(c)}$$

$$= 2^{1-u-v} \sum_{i=0}^{\frac{1}{2}(u-1)} \binom{u}{2i} \left((1 - z)^{u-2i}(1 + z)^{2i} + (1 - z)^{2i}(1 + z)^{u-2i}\right)^v,$$

iv) The code C_{12} is a self-complementary and its even weight subcode is C_{11}. Hence the minimum distance of C_{12} is equal to $\min\{4, uv - t\}$,

where t is the maximal weight of C_{11}. But the weight enumerator $B(z)$ of code C_{11} has degree less than $uv - 3$. Hence $d_{12} = 4$.

The bounds on the covering radius of the codes C_9 and C_{10} are given by the following theorem:

Theorem 2. i) Let $v_1 = v - \left\lfloor \frac{v}{2^{u-1}} \right\rfloor \cdot 2^{u-1}$ (v_1 is the residual of $v \bmod 2^{u-1}$) and $v_1 = \sum_{i=0}^{r} \binom{u}{i} + t$, where $0 \leqq t \leqq \binom{u}{r+1}$. Then the code C_9 with a generator polynomial $g_9(x) = f_1(x)$ has a covering radius R_9, where

$$\left\lfloor \frac{v}{2^{u-1}} \right\rfloor \sum_{i=0}^{\frac{1}{2}(u-1)} \binom{u}{i} i + \sum_{i=0}^{r} \binom{u}{i} i + t(r + 1) \leqq R_9 \leqq \left\lfloor \frac{v}{2^{u-1}} \sum_{i=0}^{\frac{1}{2}(u-1)} \binom{u}{i} i \right\rfloor.$$

ii) The code C_{10} with a generator polynomial $g_{10}(x) = f_0(x)f_1(x)$ has a covering radius R_{10} where $R_9 + 1 \leqq R_{10} \leqq R_9 + u - 2$.

Proof. i) If we arrange the coordinates in a $u \times v$ matrix as in the proof of Theorem 1 i), then the words x_i, $i = 1, \dots, u$ and y_j, $j = 1, \dots, v$ from (1) generate the code C_9. Let I_j, $j = 1, \dots, v$ be the block of coordinate places on the j-th column in that matrix. Then the word with support I_j belongs to C_9. From each block I_j we take away the element, which is on the last row and from the parity check matrix H of the code take away the columns with this numbers. In this way we obtain new blocks $\widetilde{I}_j$ and matrix H. The code $\widetilde{C}$ with the parity check matrix $\widetilde{H}$ is $[uv - v,\ u - 1]$ code and it is generated by the words

$$\left.\left(\begin{array}{ccc} 0 & \cdots & 0 \\ \multicolumn{3}{c}{\dots\dots\dots} \\ 1 & \cdots & 1 \\ \multicolumn{3}{c}{\dots\dots\dots} \\ 0 & \cdots & 0 \end{array}\right)\right\} u - 1$$

Then we can apply the upper bound on the covering radius of self-complementary code from [3] and obtain that $R_9 \leqq \left\lfloor \frac{v}{2^{u-1}} \sum_{i=0}^{\frac{1}{2}(u-1)} \binom{u}{i} i \right\rfloor$.

The lower bound on R_9 is constructive. Let us consider the word $a \in F^{uv}$. We take $\left\lfloor \frac{v}{2^{u-1}} \right\rfloor$ copies of each column of length u and weight no exceeding $\frac{u-1}{2}$ and the other $v_1 = v - \left\lfloor \frac{v}{2^{u-1}} \right\rfloor \cdot 2^{u-1}$ columns are distinct and have the minimum possible weight. The word a has a weight $w = \left\lfloor \frac{v}{2^{u-1}} \right\rfloor \sum_{i=0}^{\frac{1}{2}(u-1)} \binom{u}{i} i + \sum_{i=0}^{r} \binom{u}{i} i + t(r+1)$ and it is a leader of the coset $a + C_9$. Hence $R_9 \geqq w$.

ii) The code C_{10} is the even weight subcode of C_9 and then $R_{10} \geqq R_9 + 1$ (see [5]). Let x be a leader of coset of C_9 and

$$x = (x^1, \dots, x^v) = \begin{pmatrix} x_{11} & \cdots & x_{1v} \\ \multicolumn{3}{c}{\dots\dots\dots\dots} \\ x_{u1} & \cdots & x_{uv} \end{pmatrix}$$

and let $x^i \neq 0$. The the words $(x^1, \dots, x^i, \dots, x^v)$ and $(x^1, \dots, \overline{x}^i, \dots, x^v)$ belong to the distinct cosets to C_{10} and they have weight $w = wt(x)$ and $w_1 \leqq w - 1 + u - 1 = w + u - 2$. Therefore, $R_{10} \leqq R_9 + u - 2$.

Corollary 1. When $u = 3$ then $R_9 = \left\lfloor \frac{3v}{4} \right\rfloor$ and $R_{10} = 1 + \left\lfloor \frac{3v}{4} \right\rfloor$.

This corollary follows from the fact that the upper and lower bounds on R_9 and R_{10} from Theorem 2 are equal.

Theorem 3. The code C_{11} with generator polynomial $g_{11}(x) = f_0(x)f_u(x)f_v(x)$ has a covering radius $R_{11} = v$.

Proof. The coefficients of the generator polynomial of this code are g_{11}: $\underbrace{11\dots1}_{u}\underbrace{0\dots0}_{v-u}\underbrace{1\dots1}_{u}$ and then $R_{11} \leqq R' = v$, where R' is the covering radius of $[u + v,\ 1]$ code generated by the vector g_{11} (see [3]) a C_{11} is a subcode of code C_5

with $R_5 = v$. Then from the Supercode Lemma [5] follows that $R_{11} \geqq v$. Hence $R_{11} = v$.

The covering radius of the code C_{12} is obtained using the Proposition 1, as it is given in the following theorem:

Theorem 4. The code C_{12} with a length $n = uv$, $u < v$ generator polynomial $g_{12}(x) = f_u(x)f_v(x)$ has a covering radius

$$R_{12} = \begin{cases} \frac{1}{2}(v-1) & \text{if} \quad u \leqq \frac{1}{2}(v-1), \\ u & \text{if} \quad \frac{1}{2}(v-1) < u < v. \end{cases}$$

Proof. This code is dual to code C_{10}. The code C_{10} contains the code C_2 which is u repetitions of E_v and code C_4 which is v repetitions of E_u. Therefore a parity check matrix of code C_{12} is equivalent to

$$H = \left(\begin{array}{c|c|c|c|c} 1\cdots1 & 0\cdots0 & & 0\cdots0 & 1\cdots1 \\ 0\cdots0 & 1\cdots1 & & \vdots & 1\cdots1 \\ \vdots & 0\cdots0 & & \vdots & \vdots \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ \vdots & \vdots & & 0\cdots0 & \vdots \\ 0\cdots0 & 0\cdots0 & & 1\cdots1 & 1\cdots1 \\ \hline L & L & \cdots & L & L \end{array} \right) = \left(\frac{h'_1 h'_2 \cdots h'_n}{h''_1 h''_2 \cdots h''_n} \right) = \left(\frac{H_1}{H_2} \right)$$

where L is the $(u-1) \times u$-matrix

$$L = \begin{pmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & \cdots & 0 & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 1 \end{pmatrix}.$$

Let $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ be an arbitrary syndrom of the code C_{12} and $y_1 \in F^{v-1}$, $y_2 \in F^{u-1}$ Let t_1 and t_2 be the smallest numbers such that y_i, $i = 1, 2$ is the sum of t_i columns of H_i. Then y_i can be represented as a sum of $t_i + 2m$ columns of H_i if we add m pairs of equal columns of H_i. There are two cases:

a) $t_1 \equiv t_2 (\mathrm{mod} 2)$ and let $t = \max\{t_1, t_2\}$. Then y_1 and y_2 can be represented as a sum of t columns of H_1 or H_2 respectively: $y_1 = h'_{i_1} + \cdots + h'_{i_t}$ and $y_2 = h''_{j_1} + \cdots + h''_{j_t}$ and we obtain that:

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} h'_{i_1} \\ h''_{j_1} \end{pmatrix} + \cdots + \begin{pmatrix} h'_{i_t} \\ h''_{j_t} \end{pmatrix},$$

and $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ is a sum of t columns of H and $t \leqq \frac{v-1}{2}$;

b) $t_1 \not\equiv t_2 (\mathrm{mod} 2)$. Then $t'_2 = u - t_2$ and if $y_2 = h''_{j_1} + \cdots + h''_{j_{t_2}}$, then y_2 is equal to the sum of the other t'_2 columns of L, because $\sum\limits_{i=1}^{u} h''_i = 0$. Therefore $t''_2 \equiv t_1 (\mathrm{mod} 2)$

and (as in the case a)) we can obtain that $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ is the sum of $t = \max\{t_1, t_2'\}$ columns of H. We have $t_1 \leqq \frac{v-1}{2}$ and $t_2' \leqq u$, hence $t \leqq \max\{\frac{v-1}{2}, u\}$.

In this way we obtain that $R_{12} \leqq \max\{\frac{v-1}{2}, u\}$. On the other hand, $R_{12} \geqq \frac{v-1}{2}$ because the covering radius of the code with parity check matrix H_1 is equal to $\frac{v-1}{2}$ and $R_{12} \geqq u$ because the vector $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ with $y_1 = (1, 0, \ldots, 0)^T$ and $y_2 = (0, \ldots, 0)^T$ is the sum of u and no less than u columns of H. Therefore, we obtain that $R_{12} = \max\{\frac{v-1}{2}, u\}$ which is equal to

$$R_{12} = \begin{cases} \frac{1}{2}(v-1) & \text{if} \quad u \leqq \frac{1}{2}(v-1), \\ u & \text{if} \quad \frac{1}{2}(v-1) < u < v. \end{cases}$$

This paper was presented in part at the International Workshop on Algebraic and Combinatorial Coding Theory, Varna, Bulgaria '88 — [6].

REFERENCES

1. Downey, D., N.J.A. Sloane. The covering radius of cyclic codes of length up to 31. — IEEE Trans. Inform. Theory, IT–31, 446–447, 1985.
2. Velikova, E., K. Manev. Covering radius of cyclic codes of lengths 33, 35 and 39 (to appear in Annuaire de l'Universite de Sofia, Faculte des Mathematiques, 1987).
3. Velikova, E. Bounds on covering radius of linear codes. — Comptes rendus de l'Academie Bulgare des Sciences. 41, № 6, 13–16, 1988.
4. MacWilliams, F.J., N.J.A. Sloane. The Theory of Error-Correcting Codes. Amsterdam, 1977.
5. Cohen, G., M. Karpovsky, H. Mattson. Covering radius — survey and recent results. — IEEE Trans. Inform. Theory, IT–31, 328–343, 1985.
6. Velikova, E. Covering radius of some cyclic codes. — Proceedings of the International Workshop on Algebraic and Combinatorial Coding Theory, Varna, 1988.

Received 5.IV.1989