Is the Class of Cyclic Codes Good?

Conchita Martínez-Pérez
Departamento de Matemáticas
Universidad de Zaragoza,
50009 Zaragoza

Wolfgang Willems
Institut für Algebra und Geometrie
Fakultät für Mathematik
Otto-von-Guericke-Universität
39016 Magdeburg

Abstract- **There is the long standing question whether the class of cyclic codes is good. By an old result of Lin and Weldon, long BCH codes are bad. Berman proved that cyclic codes are bad if only finitely many primes are involved in the lenghts of the codes. Using representation theory we investigate further classes of cyclic codes which also turn out to be bad. Based on reduction arguments we give some evidence that there exists a good sequence of binary cyclic codes in which all lengths are prime numbers provided there is any good sequence of binary cyclic codes.**

Index Terms- **cyclic codes, asymptotically good, representation theory, irreducible modules, tensor products**

1 Introduction

Throughout the paper all codes are assumed to be linear and defined over a finite field of characteristic two (if not otherwise explicitly stated). A sequence of $[n_i, k_i, d_i]$ codes with $n_1 < n_2 < \dots$ is called *good* if there exist $\alpha > 0$ and $\beta > 0$ such that

$$\frac{k_i}{n_i} \geq \alpha \quad \text{and} \quad \frac{d_i}{n_i} \geq \beta$$

for all $i = 1, 2, \dots$. A class of codes, for instance BCH codes or Justesen codes, is called good if there is a good sequence in which all codes belong to the class. By [12], BCH codes are *bad*, i.e. in the class of BCH codes there are no good sequences. However as Berlekamp and Justesen pointed out in [3] the concatination of BCH codes with MDS codes leads to cyclic codes which perform much better than BCH codes. However their construction also leads to sequences which are bad. Kasami proved in [9] that there is a sequence of binary cyclic codes whose error probabilities approach zero and whose transmition ratio approach a limit greater than zero as the lengths of codes grow to infinity provided the (BSC) channel probability of error is small enough.

Justesen was the first to describe explicitely a good sequence of codes (see [8]). However the codes are not cyclic. Meanwhile many other classes have been checked to be good, in particular the class of special quasi-cyclic (not cyclic) codes (see [10], [11]).

At the WCC 2003 meeting in Versailles Kabatianski brought the following old problem again to our attention (see [1]).

Is the class of cyclic codes good?

There is not much known about the problem in general (see [5], p. 1035) and any progess seems to be of interest.

For $n \in \mathbb{N}$ let $\sigma(n)$ denote the set of primes dividing n. Suppose for a moment that $|\cup_{i=1}^{\infty} \sigma(n_i)| < \infty$ for a sequence C_i of binary cyclic $[n_i, k_i, d_i]$ codes with $n_1 < n_2 < \ldots$. Then, by a result due to Berman ([4], Theorem 2.1), the sequence is bad. Thus in order to find a good sequence of binary cyclic codes we have to assume that $|\cup_{i=1}^{\infty} \sigma(n_i)| = \infty$. Under the stronger assumption that even $\lim_{i\to\infty} |\sigma(n_i)| = \infty$ and that the n_i have a special arithmetical structure, i.e. the primes involved in all n_i satisfy particular number theoretical conditions, we prove that good binary cyclic codes do not exist (see Theorem 3.1). Moreover, if a good sequence of binary cyclic codes exists and the arithmetical condition on the lengths n_i is satisfied then there also exists a good sequence of cyclic codes over a finite extention of $\mathbb{F}_2$ such that all lengths n_i are powers of suitable primes (see Theorem 3.2). Supposing some extra condition on the primes the lenghts may be even reduced to primes (see Theorem 3.4).

The methods which we use heavily depend on facts about irreducible representations of cyclic groups of odd order.

2 Preliminaries in representation and coding theory

Throughout this section let K denote a field with 2^t elements. For an odd $n \in \mathbb{N}$ we define $s(n)$ as the smallest positive integer such that $n \mid 2^{s(n)} - 1$. In particular a field with $2^{s(n)}$ elements is the smallest extension field of $\mathbb{F}_2$ containing a primitive n-th root of unity. Let G_n always denote a cyclic group of order n.

Lemma 2.1 *If $n_i \in \mathbb{N}$ for $i = 1, 2$ with* $\gcd(n_1, n_2) = 1$ *then*

$$s(n_1 n_2) = \mathrm{lcm}\,(s(n_1), s(n_2)).$$

Proof: Since $n_1 n_2 \mid 2^{s(n_1 n_2)} - 1$ we have $s(n_i) \mid s(n_1 n_2)$. Thus $\mathrm{lcm}\,(s(n_1), s(n_2))$ divides $s(n_1 n_2)$. Let F_i $(i = 1, 2)$ be fields with $|F_i| = 2^{s(n_i)}$. Then the compositum $F_1 F_2$ contains a primitive $n_1 n_2$-th root of unity as $\gcd(n_1, n_2) = 1$. Since

$|F_1F_2| = 2^{\mathrm{lcm}\,(s(n_1),s(n_2))}$ we get $s(n_1n_2) \mid \mathrm{lcm}\,(s(n_1), s(n_2))$ and the proof is complete. $\square$

Lemma 2.2 *Let $F \geq K$ be a splitting field of the cyclic group $G = G_n$ of odd order n. Then the irreducible KG-modules correspond to orbits of n-th roots of unity under the action of $\Gamma = \mathrm{Gal}(F/K)$. The length of each orbit is the dimension of the corresponding irreducible KG-module. In particular, the dimensions of the irreducible KG-modules are*

$$\frac{s(m)}{\gcd(t, s(m))}$$

where $m \mid n$.

Proof: Let M be an irreducible KG-module. By ([7], Chap. VII, Sec. 1), we have

$$M \otimes F = M_1 \oplus \ldots \oplus M_r$$

where the M_i are pairwise nonisomorphic and irreducible FG-modules. Moreover the M_i are conjugate under Galois automorphisms over K. Clearly, each M_i is of dimension one and a generator of G acts on M_i by a primitive m-th root of unity, say ξ, where $m \mid n$. The number r is the smallest positive integer such that

$$\xi, \xi^q, \ldots, \xi^{q^{r-1}}, \xi^{q^r} = \xi$$

where $q = 2^t$. Now, the last equality is equivalent to $\xi^{2^{tr}-1} = \xi^{q^r-1} = 1$ or $s(m) \mid tr$. Since $r = \frac{s(m)}{\gcd(t,s(m))}$ is obviously the smallest positive integer such that $s(m) \mid tr$ the proof is complete. $\square$

Lemma 2.3 *Let $n, m \in \mathbb{N}$ be odd and coprime. Suppose that U is an irreducible KG_n and W an irreducible KG_m-module. If $\gcd(\dim U, \dim W) = 1$, then $U \otimes W$ is an irreducible KG_{nm}-module.*

Proof: Let $F \geq K$ be a splitting field for $G_{nm} = G_n \times G_m$. Clearly, F is also a splitting field for G_n and G_m as well and the modules U resp. W correspond to orbits of suitable elements, say $\alpha \in F$ resp. $\beta \in F$ under $\Gamma = \mathrm{Gal}(F/K)$. These orbits have lengths $\dim U$ resp. $\dim W$. Since $\gcd(\dim U, \dim W) = 1$ the orbit of $\alpha\beta$ has length $\dim U \dim W$. But this is the dimension of $U \otimes W$ which implies that $U \otimes W$ is irreducible. $\square$

Proposition 2.4 *Let $n, m \in \mathbb{N}$ be odd and coprime. Furthermore suppose that $\gcd(s(n), s(m)) \mid t$. Then the irreducible KG_{nm}-modules are precisely the tensor products $U \otimes W$ where U is an irreducible KG_n and W is an irreducible KG_m-module.*

Proof: First we check that $U \otimes W$ is an irreducible KG_{nm}-module if U is an irreducible KG_n and W an irreducible KG_m-module. Note that, by Lemma 2.2,

$$\frac{s(n')}{\gcd(t, s(n'))} \quad \text{resp.} \quad \frac{s(m')}{\gcd(t, s(m'))}$$

are the dimensions of U resp. W for suitable $n' \mid n$ resp. $m' \mid m$. Since $s(n') \mid s(n)$ and $s(m') \mid s(m)$ we get $\gcd(s(n'), s(m')) \mid t$. Thus

$$\gcd(s(n'), s(m')) \mid \gcd(s(n'), t) \quad \text{und} \quad \gcd(s(n'), s(m')) \mid \gcd(s(m'), t)$$

which implies that

$$\frac{s(n')}{\gcd(t, s(n'))} \quad \text{and} \quad \frac{s(m')}{\gcd(t, s(m'))}$$

are coprime. Hence, by Lemma 2.3, the module $U \otimes W$ is irreducible. The assertion now follows since $KG_{nm} = KG_n \otimes KG_m$. □

Proposition 2.5 *Let $n = n_1 n_2 \ldots n_s \in \mathbb{N}$ where the n_i are pairwise coprime and odd. Suppose that*

$$\gcd(s(n_i), s(n_j)) \mid t$$

for all $1 \leq i \neq j \leq s$. Then every irreducible KG_n-module is a tensor product of the form

$$U_1 \otimes \ldots \otimes U_s$$

where U_i is an irreducible KG_{n_i}-module for $i = 1, \ldots, s$.

Proof: Let $m = n_1 \ldots n_{s-1}$. By 2.1, we have $s(m) = \operatorname{lcm}(s(n_1), \ldots, s(n_{s-1}))$ and the hypothesis implies that

$$\gcd(s(m), s(n_s)) \mid t.$$

Thus we may apply Proposition 2.4 to the groups G_m and G_{n_s}. Finally, an inductive argument yields the assertion. □

Lemma 2.6 *Let C be an $[n, k, d]$ code over a field with q elements. If $k \geq 2$ then*

$$(q + 1)d \leq qn.$$

Proof: The defect of C is defined by $s = n - k + 1 - d$. By Lemma 4.4.3 of [14], we have

$$d \leq q(s + 1) = q(n - k + 2 - d),$$

hence $(q + 1)d \leq q(n - k + 2) \leq qn$. □

Lemma 2.7 *Let F/E denote an extenstion of finite fields and let C be a code over E. We denote by $C \otimes F$ the F-code obtained by extending scalars of C. Then the minimum distance of $C \otimes F$ is equal to the minimum distance of C, i.e.,*

$$\mathrm{d}(C \otimes F) = \mathrm{d}(C).$$

Proof: Let $\Gamma = \mathrm{Gal}(F/E)$ and let $0 \neq w \in C \otimes F$ be of minimum weight. As w is an F-linear combination of words in C we have $w^\sigma \in C \otimes F$ for any $\sigma \in \Gamma$. By multiplying w with a scalar if necessary we may assume that $0 \neq v = \sum_{\sigma \in \Gamma} w^\sigma$. Thus we have $v \in C$ and $0 \neq \mathrm{wt}(v) \leq \mathrm{d}(C \otimes F)$. Therefore $\mathrm{d}(C) \leq \mathrm{d}(C \otimes F)$. The opposite inequality is obvious. □

3 The asymptotic of cyclic codes

First we consider a sequence of binary cyclic $[n_i, k_i, d_i]$ codes C_i with

$$(*) \qquad n_i = n_{i_1} \dots n_{i_{s_i}}$$

where the $0 < n_{i_j}$ are pairwise coprime and odd.

Theorem 3.1 *Let C_i be a sequence of binary cyclic codes as defined in $(*)$ with $\lim_{i\to\infty} s_i = \infty$. For each i we put*

$$t_i = \mathrm{lcm}_{r\neq k}\{\gcd(s(n_{i_r}), s(n_{i_k}))\}.$$

If the sequence t_i is bounded then the sequence C_i is bad.

Proof: Let $t = \mathrm{lcm}_i\{t_i\}$ and let F be a field with $q = 2^t$ elements. By 2.7, we may assume that the codes C_i are defined over F. Since $t_i \mid t$ for each i we have $\gcd(s(n_{i_r}), s(n_{i_k})) \mid t$ for $r \neq k$ and $r, k \leq s_i$. Let G_i be a cyclic group of order n_i. According to 2.5 all irreducible FG_i-modules are of the form $U_i = U_{i_1} \otimes U_{i_2} \otimes \dots \otimes U_{i_{s_i}}$ where U_{i_j} is an irreducible module for a cyclic group of order n_{i_j}.

Assume that there exists a γ such that for all i the code C_i contains only summands U_i with at most γ components U_{i_j} of dimension strictly larger than 1. Then $\dim C_i$ is bounded by the dimension of the direct sum of all those modules. Next we compute that dimension. Consider first the module, say M, which is the sum of all those irreducible modules which have a one dimensional module in the first $s_i - \gamma$ positions as a component, i.e., M is the sum of all irreducible FG_i-modules of the form

$$U_i = U_{i_1} \otimes U_{i_2} \otimes \dots \otimes U_{i_{s_i}}$$

with $\dim U_{i_j} = 1$ for $j = 1, \dots, s_i - \gamma$. As for any cyclic group there are at most $q-1$ irreducible modules over F we obtain

$$\frac{\dim M}{n_i} \leq \frac{(q-1)^{s_i-\gamma} \dim\left(FG_{i_{s_i-\gamma+1}} \otimes \dots \otimes FG_{i_{s_i}}\right)}{n_i}.$$

After a renumbering of n_{i_j} if necessary we may assume that $n_{i_1} < n_{i_2} < \dots$. Taking into account that we may choose the γ factors at arbitrary positions and that the product of any $s_i - \gamma$ numbers n_{i_j} is greater than $\prod_{j=1}^{s_i-\gamma} n_{i_j}$ we get

$$\frac{\dim\ C_i}{n_i} \leq \binom{s_i}{\gamma} \frac{(q-1)^{s_i-\gamma}}{\prod_{j=1}^{s_i-\gamma} n_{i_j}}.$$

Note that $n_{i_j} \geq j$. Thus

$$\frac{\dim\ C_i}{n_i} \leq \binom{s_i}{\gamma} \frac{(q-1)^{s_i-\gamma}}{(s_i-\gamma)!} \leq \frac{q^{s_i}}{(s_i-\gamma)!} = q^{\gamma} \frac{q^{s_i-\gamma}}{(s_i-\gamma)!}.$$

Now, as $\lim_{i\to\infty} s_i = \infty$ we get $\lim_{i\to\infty} \frac{q^{s_i-\gamma}}{(s_i-\gamma)!} = 0$ which proves that the sequence C_i is bad.

Thus, if the sequence C_i is assumed to be good then in each C_i of a suitable subsequence we find a summand $U_{i_1} \otimes U_{i_2} \otimes \ldots \otimes U_{n_{s_i}}$ such that the number r_i of components U_{i_j} of dimension strictly larger than 1 gets larger and larger if i grows. Applying Proposition 2.6 we obtain

$$\frac{\mathrm{d}(C_i)}{n_i} \leq \prod_{j=1}^{s_i} \frac{\mathrm{d}(U_{i_j})}{n_{i_j}} \leq \left(\frac{q}{q+1}\right)^{r_i}.$$

As $\lim_{i\to\infty} r_i = \infty$ the sequence C_i is bad and the proof is complete. $\square$

Given a sequence of binary cyclic $[n_i, k_i, d_i]$ codes C_i we may write

$$n_i = p_{i_1}^{a_{i_1}} p_{i_2}^{a_{i_2}} \ldots p_{i_{s_i}}^{a_{i_{s_i}}}$$

where the p_{i_j} are pairwise different odd primes. As before let

$$t_i = \mathrm{lcm}_{r\neq k}\{\gcd(s(p_{i_r}^{a_{i_r}}), s(p_{i_k}^{a_{i_k}}))\}.$$

Theorem 3.2 *Suppose that there exists a good sequence C_i of binary cyclic codes with a bounded sequence t_i. Then there exists a good sequence of cyclic codes C_i' over the field $\mathbb{F}_{2^t}$ with $t = \mathrm{lcm}_i\{t_i\}$ where the length of each C_i' is a power of a suitable prime.*

Proof: By assumption and Theorem 3.1 the sequence s_i is bounded. Note that a subsequence of a good sequence is good as well. So by choosing if necessary a subsequence of C_i we may assume that $s_i = s$ for a suitable positive integer s. Now we proceed by induction on s. We only have to consider the case $s > 1$. Thus we may split

$$n_i = k_i l_i$$

with $1 < k_i$ and $1 < l_i$ coprime and both k_i and l_i a product of a fixed number of primes for each i. Note that by condition $\lim_{i\to\infty} n_i = \infty$ we may assume that $\lim_{i\to\infty} k_i = \infty$. Let G_i be a cyclic group of order n_i and write $G_i = X_i \times Y_i$ with groups X_i, Y_i and $|X_i| = k_i$. Since

$$\gcd(s(k_i), s(l_i)) \mid t$$

every irreducible FG_i-module is a tensor product of an irreducible FX_i-module and an irreducible FY_i-module. Extending scalars in C_i we get a good sequence of cyclic codes over F. For those codes (which we also denote by C_i) we have

$$C_i = (A_1^i \otimes V_1^i) \oplus (A_2^i \otimes V_2^i) \oplus \ldots \oplus (A_{m_i}^i \otimes V_{m_i}^i)$$

where the A_j^i are suitable FX_i-modules and $\{V_1^i, \ldots, V_{m_i}^i\}$ is a full set of irreducible FY_i-modules. In particular,

$$\frac{\dim\, C_i}{n_i} = \sum_{j=1}^{m_i} \frac{\dim\, A_j^i}{k_i} \frac{\dim\, V_j^i}{l_i}$$

and

$$\frac{\mathrm{d}(C_i)}{n_i} \leq \frac{\mathrm{d}(A^i_j)}{k_i}\frac{\mathrm{d}(V^i_j)}{l_i} \leq \frac{\mathrm{d}(A^i_j)}{k_i} \quad \text{for all } j.$$

Next we consider the sequence

$$A^1_1, \ldots, A^1_{m_1}, A^2_1, \ldots, A^i_1, \ldots, A^i_{m_i}, \ldots$$

of cyclic codes over F and take $\epsilon > 0$. If there are infinitely many codes in this sequence with

$$\epsilon \leq \frac{\dim\ A^i_j}{k_i}$$

then, by choosing that subsequence, we get a good sequence of cyclic codes over F. Suppose that the lengths are not prime powers. Their corresponding sequence of t_i's obviously satisfies $\mathrm{lcm}_i\{t_i\} = t' \mid t$ and we may apply the inductive hypothesis to get a good sequence of cyclic codes over $\mathbb{F}_{2^{t'}}$ hence over $\mathbb{F}_{2^t}$ in which all lengths are prime powers.

Thus to finish the proof we may assume that there exists an i_0 such that

$$\frac{\dim A^i_j}{k_i} < \epsilon$$

for all $i \geq i_0$. But then it follows that

$$\frac{\dim\ C_i}{n_i} < \sum_j (\frac{\dim\ V^i_j}{l_i})\epsilon = \epsilon$$

which contradicts the fact that C_i is a good sequence.

□

In the sequel we further reduce under some extra condition the lengths of the codes C'_i in Theorem 3.2 to primes. In order to prove that we need

Lemma 3.3 *Let p be an odd prime and let t, a be non-negative integers with $p \nmid t$. Let $F \leq K$ be finite fields with $|F| = 2^t$ and $|K| = 2^{\mathrm{lcm}(t, s(p^a))}$. If $s(p^a) = p^{a-1}s(p)$ then*

$$\sum_{\gamma \in \mathrm{Gal}(K/F)} \alpha^\gamma = 0$$

for every primitive p^a-th root of unity $\alpha \in K$.

Proof: Note that K is the smallest splitting field of $x^{p^a} - 1$ which contains the field F. Let $\alpha \in K$ be a primitive p^a-th root of unity. If $\mathrm{m}_\alpha(x) \in F[x]$ is the minimal polynomial of α over F then, by 2.2 of [13],

$$\begin{aligned} \deg\ \mathrm{m}_\alpha(x) &= \tfrac{s(p^a)}{\gcd(s(p^a),t)} \\ &= \tfrac{s(p^a)}{\gcd(s(p),t)} \qquad \text{since } \gcd(t,p) = 1 \\ &= \tfrac{p^{a-1}s(p)}{s} \end{aligned}$$

where $s = \gcd(s(p), t)$. Clearly

$$x^p - 1 = (x-1) \prod_i f_i(x)$$

with irreducible polynomials $f_i(x) \in F[x]$. Again we have

$$\deg f_i(x) = \frac{s(p)}{\gcd(s(p), t)} = \frac{s(p)}{s}.$$

If we put $q = p^{a-1}$ and replace x by x^q we obtain

$$x^{p^a} - 1 = (x^q - 1) \prod_i f_i(x^q).$$

Note that $f_i(x^q)$ is of degree $\frac{qs(p)}{s}$. Thus we get $\mathrm{m}_\alpha(x) = f_i(x^q)$ for some i. Moreover

$$\sum_{\gamma \in \mathrm{Gal}(K/F)} \alpha^\gamma$$

is the coefficient at $x^{\frac{s(p^a)}{s}-1}$ in $f_i(x^q)$ which obviously turns out to be 0. $\square$

Theorem 3.4 *Let C_i be a good sequence of cyclic codes over a finite field F of characteristic 2. Suppose that the length of each C_i is a prime power, say $p_i^{a_i}$, for a suitable odd prime p_i which satisfies $s(p_i^a) = p_i^{a-1}s(p_i)$ for all positive integers a. Then there exists a good sequence C_i' of cyclic codes over F in which the length of each C_i' is a prime (actually equal to p_i).*

Proof: By Berman [4], we may assume that infinitely many primes are involved in the lenghts of the C_i. Taking a subsequence of the sequence C_i, if necessary, we may further assume that $p_i \nmid t$ for all primes p_i which occur in the lenghts.
(1) We claim that each C_i can be replaced by the sum of the faithful irreducible modules contained in C_i:

If $C_i \leq FG_i$ where G_i is a cyclic group of order $p_i^{a_i}$ then the dimension of the sum, say W_i, of all non-faithful irreducible submodules of C_i is bounded by $p_i^{a_i-1}$. In particular

$$\frac{\dim\, W_i}{p_i^{a_i}} \leq \frac{1}{p_i}$$

which converges to 0 for $i \to \infty$. Thus for the dimension of the sum of all irreducible faithful submodules of C_i, say W_i', we have

$$\frac{\dim\, W_i'}{p_i^{a_i}} \geq \alpha > 0$$

for all i. Furthermore $\mathrm{d}(W_i') \geq \mathrm{d}(C_i)$ which proves the claim.
(2) By (1) each code C_i is a direct sum of irreducible faithful FG_i-modules. To get rid of the indices put $C = C_i$, $G = G_i$, $p = p_i$ and $a = a_i$. Let $V = eFG$ be an irreducible faihtful FG-submodule of C with idempotent e and let H be a subgroup of G of index p. If $g \in G$ but $g \notin H$ then g has order p^a. Let K be

the field as in Lemma 3.3. Note that the coefficient of g in e is a Galois sum over F of primitive p^a-th roots of unity in K. Thus, by 3.3, this coefficient is 0. In particular, $e \in FH$. Therefore we have

$$V = eFG = eFH \oplus eFHg_2 \oplus \ldots \oplus eFHg_p$$

where $\{1 = g_1, g_2, \ldots, g_p\}$ is a full set of transversals of H in G. This shows that V is a module induced from FH. In particular $C = C_i = W_i^{G_i}$ where W_i is a submodule of FH_i with $H_i = H$. Note that

$$\frac{\dim W_i}{p_i^{a_i-1}} = \frac{\dim C_i}{p_i^{a_i}},$$

and obviously $\mathrm{d}(W_i) = \mathrm{d}(C_i)$. Thus we may replace the good sequence C_i of cyclic codes with lengths $p_i^{a_i}$ by a good sequence W_i of cyclic codes with lengths $p_i^{a_i-1}$ and an induction argument completes the proof. $\square$

Remark 3.5 Let p be an odd prime. If $s(p^3) > s(p^2)$ then by a result of Berlekamp

$$s(p^a) = p^{a-1}s(p)$$

for all non-negative integers $a \geq 3$ (see Theorem 6.52 in [2]). Up to 2^{12} there is no prime p with $s(p^3) = s(p^2)$. Up to 4×10^{12} there are only two primes, namely $p = 1093$ and $p = 3511$ which satisfy $s(p^2) = s(p)$. Note that $s(p^2) = s(p)$ is equivalent to the condition $2^{p-1} \equiv 1 \bmod p^2$ which means that p is a Wieferich prime (see [6]). To date, the only known Wieferich primes are 1093 and 3511.

Remark 3.6 Throughout the paper we actually never used explicitly the fact that the underlying field is of characteristic two. So all the results remain true in odd characteristic p provided that the lenghts of the considered codes are prime to p.

References

[1] E.F. Assmus, H.F. Mattson and R. Turyn. Cyclic codes. AF Cambridge Research Labs. Bedford Mass., Summary Sci. Rept. AFCRL-66-348, March 1966.

[2] E.R. Berlekamp. Algebraic coding theory. Revised 1984 edition, Aegean Park Press, 1984.

[3] E.R. Berlekamp and J. Justesen. Some long cyclic linear binary codes are not so bad. IEEE Trans. Inform. Theory 20 (1974), 351-356.

[4] S.D. Berman. Semisimple cyclic and abelian codes II. Cybernetics 3 (1967), 17-23.

[5] P. Charpin. Open problems on cyclic codes. In: Handbook of coding theory. Editors: V.S. Pless and W.C. Huffman, Elsevier, Amsterdam 1998, pp 963-1063.

[6] R. Crandall, K. Dilcher and C. Pommerance. A search for Wieferich and Wilson primes. Math. Comput. 66 (1997), 433-449.

[7] B. Huppert and N. Blackburn. Finite groups II, Springer, Berlin, Heidelberg, New York, 1982.

[8] J. Justesen. A class of constructive asymptotically good algebraic codes. IEEE Trans. Inform. Theory 18 (1972), 652-656.

[9] T. Kasami. An upper bound on k/n for affine-invariant codes with fixed d/n. IEEE Trans. Inform. Theory 15 (1969), 174-176.

[10] T. Kasami. A Gilbert-Varshamov bound for quasi-cyclic codes at rate 1/2. IEEE Trans. Inform. Theory 20 (1974), 679.

[11] S. Lin and P. Solé. Good self-dual quasi-cyclic codes exist. IEEE Trans. Inform. Theory 49 (2003), 1052-1053.

[12] S. Lin and E.J. Weldon Jr.. Long BCH codes are bad. Inform. and Control 11 (1967), 445-451.

[13] C. Martínez-Pérez and W. Willems. Self-dual codes and modules for groups in characteristic two. `http://fma2.math.uni-magdeburg.de/~willems`

[14] W. Willems. Codierungstheorie. DeGruyter, Berlin, New York, 1999.