Is the Class of Cyclic Codes Asymptotically 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 asymptotically good. By an old result of Lin and Weldon, long BCH codes are asymptotically bad. Berman proved that cyclic codes are asymptotically bad if only finitely many primes are involved in the lengths of the codes. We investigate further classes of cyclic codes which also turn out to be asymptotically bad. Based on reduction arguments we give some evidence that there are asymptotically good sequences of binary cyclic codes in which all lengths are prime numbers provided there is any asymptotically good sequence of binary cyclic codes.**

Index Terms- **cyclic codes, asymptotically good codes, Kronecker product**

1 Introduction

Throughout the paper all codes are assumed to be linear and defined over a finite field of characteristic two (if not stated otherwise explicitly). A sequence of $[n_i, k_i, d_i]$ codes with $n_1 < n_2 < \ldots$ is called *asymptotically 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 $i = 1, 2, \ldots$. A class of codes is called asymptotically good if there is an asymptotically good sequence in which all codes belong to the class. By [11], BCH codes are *asymptotically bad*, i.e. in the class of BCH codes there are no asymptotically good sequences. However as Berlekamp and Justesen pointed out in [3] a suitable concatenation of BCH codes with MDS codes leads to cyclic codes which perform much better than BCH codes. However using their construction we get again only sequences which are asymptotically bad. Kasami proved in [8] that there is a sequence of binary cyclic codes whose error probabilities approach zero and whose transsmition ratio approaches 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 an asymptotically good sequence of codes (see [7]). However the codes are not cyclic. Meanwhile many other classes have been checked to be asymptotically good, in particular the class of quasi-cyclic (not cyclic) codes (see [9],[10]).

At the WCC 2003 meeting in Versailles Kabatianski brought again to our attention the following old problem which was already asked by E.F. Assmus, H.F. Mattson and R. Turyn in 1966 (see [1]).

Is the class of cyclic codes asymptotically good?

Not much is known about that problem (see [5], p. 1035), and any progress seems to be of interest.

Note that the automorphism group of a cyclic code of length n contains a cycle of order n. In particular the automorphism group acts transitively on the coordinates. Thus cyclic codes belong to the class of *transitive codes*, i.e. codes which admit a transitive automorphism group. Just recently Stichtenoth proved that the class of transitive codes is asymptotically good (see [14]). His construction is based on a new tower of function fields. However this does not cover the case of cyclic codes which are particular transitive codes.

2 The results

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 $n_1 < n_2 < \ldots$ and all n_i odd. Then, by a result of Berman ([4], Theorem 2.1), the sequence is asymptotically bad. Thus in order to find an asymptotically good sequence of binary cyclic codes we have to assume that $|\cup_{i=1}^{\infty} \sigma(n_i)| = \infty$.

To state our main results we define $s(n)$ for an odd $n \in \mathbb{N}$ as the smallest positive integer such that $n \mid 2^{s(n)} - 1$. Thus the finite field with $2^{s(n)}$ elements is the smallest extension field of $\mathbb{F}_2$ containing a primitive n-th root of unity.

Next we decompose the lengths

$$n_i = n_{i_1} \ldots n_{i_{s_i}}$$

where $0 < n_{i_j} \in \mathbb{N}$ and the n_{i_j} are pairwise coprime (and odd). For each i let

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

With these notations we have

Theorem 2.1 *Let (C_i) be a sequence of binary cyclic codes with* $\lim_{i\to\infty} s_i = \infty$*, i.e. the number of different coprime factors in the lengths grows to infinity for $i \to \infty$. If in addition the sequence (t_i) is bounded then the sequence (C_i) is asymptotically bad.*

Theorem 2.2 *Suppose that there exists an asymptotically good sequence (C_i) of binary cyclic codes with bounded sequence (t_i). Then there exists an asymptotically 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.*

Unfortunately under the assumptions of Theorem 2.2 we were not able to prove the existence of a binary asymptotically good sequence in which all cyclic codes have prime power lengths. However under rather mild number theoretical conditions we can reduce prime powers to primes. More precisely, we have

Theorem 2.3 *Let C_i be an asymptotically 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*

$$s(p_i^a) = p_i^{a-1} s(p_i) \qquad (1)$$

for all positive integers a.
Then there exists an asymptotically 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).

We would like to mention here that there is some evidence that the condition (1) in Theorem 2.3 can be dropped. This can be seen as follows.

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.

In order to prove the results above we need some facts on cyclic codes. Most of them seem to be well-known. However to keep the paper self-contained we will give the proofs here.

3 Some facts on cyclic codes

More generally than we need in the theorems we assume in this section that K is a finite field with $|K| = p^t$ and p any prime. As usual when dealing with cyclic codes we furthermore assume that the lengths of the codes are not divisible by the characteristic p of the underlying field. Remember that a cyclic code of length n is an ideal in the factor algebra $K[x]/(x^n-1)$. The condition $p \nmid n$ forces

$$f = x^n - 1 = \prod_{j=1}^{s} f_i$$

with pairwise coprime and irreducible polynomials $f_i \in K[x]$. Thus, by the Chinese Reminder Theorem, we have

$$K[x]/(x^n-1) \cong K[x]/(f_1) \oplus \ldots \oplus K[x]/(f_s)$$

where the components $K[x](f_i)$ are finite extension fields of K. This shows that the ambient space $K[x]/(x^n-1)$ is a direct sum of irreducible (minimal) ideals. Such an ideal is generated by a polynomial g with $g \mid x^n - 1$ where $(x^n-1)/g$ is irreducible. In particular, we have the following well-known fact which is part of Theorem 7 in ([13], Ch. 8, §3).

Proposition 3.1 *Any cyclic code of length n is a direct sum of irreducible cyclic codes of length n.*

If $n = n_1 \ldots n_s$ with n_i relatively prime then

$$K[x]/(x^n-1) \cong K[x_1]/(x_1^{n_1}-1) \otimes \ldots \otimes K[x_s]/(x_s^{n_s}-1) \tag{2}$$

where the right hand side denotes the Kronecker product. To see that note that each element on the right hand side can be written as

$$f = \sum a_{i_1 \ldots i_s} x_1^{i_1} \otimes \ldots \otimes x_s^{i_s}$$

with $0 \leq i_j < n_j$ and $a_{i_1 \ldots i_s} \in K$. If we choose

$$t(i_1, \ldots, i_s) \equiv i_j \bmod n_j$$

for $j = 1, \ldots, s$ then the isomorphism in (2) is given by

$$f \mapsto \sum a_{i_1 \ldots i_s} x^{t(i_1, \ldots, i_s)}.$$

Thus the Kronecker product of cyclic codes of coprime lengths n_i is again cyclic and of length $n = n_1 \ldots n_s$ (see [13], Ch 18, §2, Theorem 1).

In general the Kronecker product of irreducible cyclic codes of coprime lengths need not to be irreducible. Furthermore an irreducible cyclic code of length $n = n_1 n_2$ with n_1 and n_2 coprime is in general not a Kronecker product of cyclic codes of lengths n_1 and n_2. To overcome these difficulties we have to assume additional conditions.

Proposition 3.2 *An irreducible cyclic code C of length $n = n_1 n_2$ with n_1 and n_2 coprime is a Kronecker product of irreducible cyclic codes C_i of length n_i $(i = 1, 2)$ if and only if $\dim C_1$ and $\dim C_2$ are coprime.*

Proof: This is Theorem 2 of ([13], Ch 18, §3). □

However, all irreducible cyclic codes of length $n = n_1 \dots n_s$ with n_i coprime decompose as a Kronecker product of irreducible cyclic codes of length n_i over a field big enough (a splitting field for the polynomial $x^n - 1$ suffices). The use of this splitting field is the key point in our main theorems. Unfortunately we can not drop the assumption over the field. The objective of the next lemmata is to measure how big the field must be.

Definition 3.3 *Let p be a prime. Then for $n \in \mathbb{N}$ with $p \nmid n$ the number $s(n)$ is defined as the smallest positive integer such that $n \mid p^{s(n)} - 1$.*

Proposition 3.4 *If $|K| = p^t$ then the dimensions of the irreducible cyclic codes over K of length n are*

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

with $m \mid n$.

Proof: We have to find the degrees of irreducible (normed) polynomials $f \in K[x]$ with $f \mid x^n - 1$. Clearly, f has a zero, say ξ in a suitable extension field of K. Thus $\xi^n = 1$ and therefore ξ is of order m with $m \mid n$. Since$f$ is irreducible (and normed) f is the minimal polynomial of ξ over K. This polynomial is known to have degree$\frac{s(m)}{\gcd(t,s(m))}$. □

Proposition 3.5 *Let $n, m \in \mathbb{N}$ be coprime and not divisible by the prime p. Let $|K| = p^t$ and suppose that $\gcd(s(n), s(m)) \mid t$. Then the irreducible cyclic codes of length nm are precisely the Kronecker products of irreducible cyclic codes of length n with irreducible cyclic codes of length m.*

Proof: Note that

$$K[x]/(x^{nm} - 1) \cong K[y]/(y^n - 1) \otimes K[z]/(z^m - 1).$$

Thus, by Proposition 3.2, we only have to check that the dimensions of the irreducible cyclic codes of length n are coprime to those of length m. By Proposition 3.4,

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

are the dimensions of irreducible cyclic codes of length n resp. m 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

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

which implies that

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

are coprime. $\square$

Together with an obvious induction argument we obtain

Proposition 3.6 *Let $|K| = p^t$ and let $n = n_1 n_2 \dots n_s \in \mathbb{N}$ where the n_i are pairwise coprime and not divisible by p. Suppose that*

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

for all $1 \leq i \neq j \leq s$. Then every irreducible cyclic code of length n over K is a Kronecker product of the form

$$C_1 \otimes \dots \otimes C_s$$

where C_i is an irreducible cyclic code of length n_i over K.

Proof: Let $m = n_1 \dots n_{s-1}$. Since the n_i are pairwise coprime we have

$$s(m) = \operatorname{lcm}(s(n_1), \dots, s(n_{s-1}))$$

and the hypothesis implies

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

Thus we may apply Proposition 3.5 to m and n_s. An obvious induction argument yields the assertion. $\square$

Finally we state two more results on codes which are well-known but crucial in the next section when proving the main theorems.

Lemma 3.7 *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: This follows immediately from the Plotkin bound. $\square$

Lemma 3.8 *Let F/E denote an extension 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: The assertion is obvious since the minimal distance of a code can be read off from linear (in)dependency conditions on the columns of a parity check matrix which do not depend on the field. $\square$

4 Proofs of the Theorems

This section is devoted to the proofs of the main results stated in Section 2.

Proof of Theorem 2.1

Let $t = \mathrm{lcm}_i\{t_i\}$ and let F be a field with $q = 2^t$ elements. By Lemma 3.8, 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 $r, k \leq s_i$. By Proposition 3.1, C_i is a direct sum of irreducible cyclic codes of length n_i over F. According to 3.6 the irreducible codes are of the form

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

where U_{i_j} is an irreducible cyclic code of length n_{i_j}. We are going to distinguish two cases according to how many components U_{i_j} of dimension 1 occur in the irreducible summands of C_i.

Assume first that there exists a γ such that for all i the code C_i contains only summands U_i with at least $s_i - \gamma$ components U_{i_j} of dimension 1. Next, we compute a bound for $\dim C_i$. Consider first the code, say M, which is the sum of all those irreducible cyclic codes of length n_i of the form

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

with $\dim U_{i_j} = 1$ for $j = 1, \ldots, s_i - \gamma$. As there are at most $q - 1$ irreducible cyclic codes of a fixed length over F the number $q - 1$ is also a bound for the number of irreducible codes of length n_{i_j} and dimension 1 over F. Thus we obtain

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

To get a bound for $\dim C_i$, note that after a renumbering of n_{i_j} if necessary, we may assume that $n_{i_1} < n_{i_2} < \ldots$. 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

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

Since $n_{i_j} \geq j$ we obtain

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

The obvious inequality

$$\binom{s_i}{\gamma} (q-1)^{s_i-\gamma} \leq (1 + (q-1))^{s_i} = q^{s_i}$$

implies that

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

Finally the assumption $\lim_{i\to\infty} s_i = \infty$ forces $\lim_{i\to\infty} \frac{q^{s_i-\gamma}}{(s_i-\gamma)!} = 0$ which proves that the sequence (C_i) is bad.

Thus we may assume that in each C_i of a suitable subsequence we can 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 bigger than 1 gets larger and larger if i grows. Applying Proposition 3.7 we obtain

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

As $\lim_{i\to\infty} r_i = \infty$ the sequence (C_i) is again bad and the proof is complete since a subsequence of a good sequence is always good. $\square$

Proof of Theorem 2.2

By assumption and Theorem 2.1 the sequence s_i is bounded. So by choosing if necessary a subsequence of (C_i) we may assume that $s_i = s$ for a suitable positive integer s and all i. Extending scalars in C_i we get a good sequence of cyclic codes over $\mathbb{F}_{2^t}$ where $t = \mathrm{lcm}_i\{t_i\}$. We denote that sequence again by (C_i).

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 according to the condition $\lim_{i\to\infty} n_i = \infty$ we may assume that $\lim_{i\to\infty} k_i = \infty$. Since

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

every irreducible cyclic code of length n_i over $\mathbb{F}_{2^t}$ is a Kronecker product of irreducible cyclic codes of lengths k_i and l_i by Proposition 3.5. Thus we may write

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

where the A_j^i are suitable cyclic codes of length k_i and $\{V_1^i, \ldots, V_{m_i}^i\}$ is a full set of irreducible cyclic codes of length l_i. Next we claim that the sequence

$$A_1^1, \ldots, A_{m_1}^1, A_1^2, \ldots, A_1^i, \ldots, A_{m_i}^i, \ldots \tag{3}$$

of cyclic codes has a good subsequence. Since

$$\frac{\mathrm{d}(C_i)}{n_i} \leq \frac{\mathrm{d}(A_j^i)}{k_i}\frac{\mathrm{d}(V_j^i)}{l_i} \leq \frac{\mathrm{d}(A_j^i)}{k_i}$$

for all j and since the sequence (C_i) is good we only have to worry about the dimensions of A_j^i. Assume first that for each $\epsilon > 0$ there exists an i_0 such that

$$\frac{\dim A_j^i}{k_i} < \epsilon$$

for all $i \geq i_0$. Since $\{V_1^i, \ldots, V_{m_i}^i\}$ is a full set of irreducible cyclic codes of length l_i we obviously have $\sum_j \dim V_j^i = l_i$. Thus

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

which contradicts the fact that C_i is a good sequence. Therefore, for some $\epsilon > 0$, there are infinitely many codes in the sequence (3) with

$$\epsilon \leq \frac{\dim\, A_j^i}{k_i}$$

which proves the claim.

Finally, note that either the lengths of these codes are prime powers or their corresponding sequence of t_i's 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. $\square$

Definition 4.1 A cyclic code C of length n over the field F is called *degenerate* if it consists of several repetitions of a code C' of smaller length, say length r, with $r \mid n$. In other words, each $c \in C$ is of the form $c = (c', c', \ldots, c')$ where $c' \in C'$ or each codeword is fixed under a cyclic shift of r coordinates.

Lemma 4.2 *Let C be a cyclic code of length n with check polynomial $h(x)$. Then the following conditions are equivalent.*

a) C is degenerate.

b) $h(x) \mid x^r - 1$ for some $r \mid n,\ r < n$.

Proof: Note that C is degenerate if and only if there exists an $r \mid n$ such that each codeword c is of the form $c = (c', c', \ldots, c')$ where c' is of length $r < n$. This is equivalent to

$$x^r g(x) \equiv g(x) \bmod x^n - 1$$

for the generator polynomial $g(x)$ of C. Thus a cyclic code is degenerate if and only if

$$h(x)g(x) = x^n - 1 \mid (x^r - 1)g(x),$$

hence if and only if

$$h(x) \mid x^r - 1.$$

Lemma 4.3 *Let p be an odd prime and let $t, a \in \mathbb{N}$. Suppose that $p \nmid t$. Furthermore let F be a finite field with $|F| = 2^t$. If $s(p^a) = p^{a-1}s(p)$ then for every primitive p^a-th root of unity α its minimal polynomial over F is a polynomial in $x^{p^{a-1}}$.*

Proof: Let K be a field with $F \leq K$ and $|K| = 2^m$ where $m = \operatorname{lcm}(s(p^a), t)$. Note that K is the smallest splitting field of the polynomial $x^{p^a} - 1$ which contains the field F. Let $\alpha \in K$ be a primitive p^a-th root of unity and let $\mathrm{m}_\alpha(x) \in F[x]$ denote its minimal polynomial over F. If we put $s = \gcd(s(p), t)$ then the condition $p \nmid t$ implies $s = \gcd(s(p^a), t)$. Let $q = p^{a-1}$. Thus, by 2.2 of [12],

$$\deg \mathrm{m}_\alpha(x) = \frac{s(p^a)}{\gcd(s(p^a), t)} = \frac{p^{a-1}s(p)}{s} = \frac{qs(p)}{s}.$$

Clearly,

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

with irreducible normed polynomials $f_i(x) \in F[x]$. Furthermore

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

If we 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. □

Lemma 4.4 *Let p be an odd prime and let $t, a \in \mathbb{N}$ with $p \nmid t$. Furthermore let F be a finite field with $|F| = 2^t$. Suppose that $s(p^a) = p^{a-1}s(p)$. If C is a cyclic non-degenerate irreducible code over F of length p^a then the generator polynomial of C is a polynomial in $x^{p^{a-1}}$.*

Proof: Let $g(x)$ denote the generator polynomial and $h = h(x)$ the check polynomial of C. Put $q = p^{a-1}$. Since C is non-degenerate $h \nmid x^q - 1$, by Lemma 4.2. Furthermore, h is irreducible as a polynomial over F since C is irreducible. Thus h is the minimal polynomial over F of a primitive p^a-th root of unity. According to Lemma 4.3 the polynomial h is a polynomial in x^q, i.e. $h(x) = \tilde{h}(x^q)$. Finally, $g(x)$ is a polynomial in x^q since $\tilde{h}(x^q)g(x) = (x^q)^p - 1$. □

Lemma 4.5 *Let C be a cyclic code over F of length n. Suppose that the generator polynomial of C is a polynomial in x^r where $r \mid n$. Then there exists a cyclic code, say $\tilde{C}$, of length $\frac{n}{r}$ such that*

(i) $\mathrm{d}(\tilde{C}) = \mathrm{d}(C)$

(ii) $\dim \tilde{C} = \frac{\dim C}{r}$.

One says that C is r-induced from $\tilde{C}$.

Proof: Let $g(x^r)$ denote the generator polynomial of C. If we put

$$\tilde{C} = g(x^r)F[x^r]/(x^n - 1) \cong g(y)F[y](y^{\frac{n}{r}} - 1)$$

then

$$C = g(x^r)F[x]/(x^n - 1) = \tilde{C} \oplus \tilde{C}x \oplus \ldots \oplus \tilde{C}x^{r-1}.$$

The assertions on $\mathrm{d}(\tilde{C})$ and $\dim \tilde{C}$ are obvious. $\square$

Proof of Theorem 2.3

By Berman [4], we know that infinitely many primes are involved in the lengths of the C_i defined over $F = \mathbb{F}_{2^t}$ since the sequence (C_i) is assumed to be asymptotically good. Taking a subsequence of the sequence (C_i), if necessary, we may assume that $p_i \nmid t$ for all primes p_i which occur in the lengths.

(1) We claim that we may further assume that each C_i is a sum of non-degenerate irreducible cyclic codes of length n_i.

In order to prove that we write $C_i = W_i \oplus W_i'$ where W_i resp. W_i' denotes the sum of all irreducible non-degenerate resp. irreducible degenerate direct summands of C_i. Since a degenerate irreducible cyclic code of length $p_i^{a_i}$ corresponds to a uniquely determined irreducible cyclic code of the same dimension but of length $p_i^{a_i-1}$ we deduce that $p_i^{a_i-1}$ is a bound for $\dim W_i'$. Hence

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

which converges to 0 for $i \to \infty$. Thus we obtain

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

for all i. Furthermore $\mathrm{d}(W_i) \geq \mathrm{d}(C_i)$ which proves the claim.

(2) Now let each C_i be a direct sum of irreducible non-degenerate cyclic codes of length p^{a_i} where $a_i \geq 2$. According to Lemma 4.4 the generator polynomial of C_i is a polynomial in x^{q_i} where $q_i = p^{a_i-1}$. Thus, by Lemma 4.5, there exists a cyclic code $\tilde{C}_i$ of length p_i with $\mathrm{d}(\tilde{C}_i) = \mathrm{d}(C_i)$ and $\dim\, \tilde{C}_i = \frac{\dim\, C_i}{q_i}$. Since

$$\frac{\dim\, \tilde{C}_i}{p_i} = \frac{\dim\, C}{p_i q_i} = \frac{\dim\, C}{p_i^{a_i}}$$

the sequence $(\tilde{C}_i)$ of cyclic codes of length p_i is good.

Remark 4.6 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 lengths of the considered codes are prime to p.

Acknowledgment We would like to thank the anonymous refrees whose comments improved the presentation of the results to a large extent. In an earlier version large parts were written in the language of representation theory for finite groups. Actually such an approach can more widely be used, i.e. in all cases of group codes. However, in case of cyclic codes a direct approach as given now seems to be more appropriate.

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

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

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

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

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

[12] C. Martínez-Pérez and W. Willems. Self-dual codes and modules for groups in characteristic two. IEEE Trans. Inform. Theory 50 (2004), 2379-2389.

[13] F.J. MacWilliams and N.J.A. Sloane. The theory of error-correcting codes. North-Holland, Amsterdam, London, New York, Tokio, 1993.

[14] H. Stichtenoth. Transitive and self-dual codes attaining the Tsfasman-Vladut-Zink bound. Preprint 2005.