SIAM J. DISCRETE MATH.
Vol. 13, No. 1, pp. 105–138

WEIGHT DIVISIBILITY OF CYCLIC CODES, HIGHLY NONLINEAR FUNCTIONS ON $\mathbf{F}_{2^m}$, AND CROSSCORRELATION OF MAXIMUM-LENGTH SEQUENCES*

ANNE CANTEAUT†, PASCALE CHARPIN†, AND HANS DOBBERTIN‡

Abstract. We study $[2^m-1, 2m]$-binary linear codes whose weights lie between w_0 and 2^m-w_0, where w_0 takes the highest possible value. Primitive cyclic codes with two zeros whose dual satisfies this property actually correspond to almost bent power functions and to pairs of maximum-length sequences with preferred crosscorrelation. We prove that, for odd m, these codes are completely characterized by their dual distance and by their weight divisibility. Using McEliece's theorem we give some general results on the weight divisibility of duals of cyclic codes with two zeros; specifically, we exhibit some infinite families of pairs of maximum-length sequences which are not preferred.

Key words. cyclic codes, weight divisibility, Boolean functions, nonlinearity, almost bent functions, m-sequences, crosscorrelation

AMS subject classifications. 11T71, 94B15, 94A55, 94A60

PII. S0895480198350057

1. Introduction.

This paper presents a new theoretical approach for studying the weight polynomials of binary cyclic codes with two zeros. Using Pless power moment identities [30] and some ideas due to Kasami [18], we point out the essential role played by the weight divisibility of linear codes of length (2^m-1) and dimension $2m$ in the determination of their weight distributions. We especially focus on $[2^m-1, 2m]$-linear codes which are optimal in the following sense: their weights lie in the range $[w_0, \ldots, 2^m-w_0]$, where w_0 takes the highest possible value. Most notably we prove that, for odd m, these $[2^m-1, 2m]$-optimal codes are completely characterized by their dual distance and by their weight divisibility. The use of McEliece's theorem [24] then reduces the determination of cyclic codes with two zeros whose dual is optimal to a purely combinatorial problem. It especially provides a very fast algorithm for finding such optimal cyclic codes, even for large lengths. These results also enables us to exhibit some infinite families of cyclic codes with two zeros whose dual is not optimal.

This result widely applies in several areas of telecommunications: binary cyclic codes with two zeros whose dual is optimal in the previous sense are especially related to highly nonlinear power functions on finite fields; they also correspond to pairs of maximum-length sequences with preferred crosscorrelation. A function f from $\mathbf{F}_{2^m}$ into $\mathbf{F}_{2^m}$ is said to achieve the highest possible nonlinearity if any nonzero linear combination of its Boolean components is as far as possible from the set of Boolean affine functions with m variables. When m is odd, the highest possible value for the nonlinearity of a function over $\mathbf{F}_{2^m}$ is known and the functions achieving this bound are called almost bent (AB). These functions play a major role in cryptography; in particular, their use in the S-boxes of a Feistel cipher ensures the best resistance to

*Received by the editors December 28, 1998; accepted for publication (in revised form) July 6, 1999; published electronically January 13, 2000.
http://www.siam.org/journals/sidma/13-1/35005.html
†INRIA, projet CODES, Domaine de Voluceau, BP 105, 78153 Le Chesnay Cedex, France (Anne.Canteaut@inria.fr, Pascale.Charpin@inria.fr).
‡German Information Security Agency, P.O. Box 20 03 63, D-53133 Bonn, Germany (dobbertin@skom.rhein.de).

both differential and linear cryptanalyses. It was recently proved [6] that a function f from $\mathbf{F}_{2^m}$ into $\mathbf{F}_{2^m}$ having maximal nonlinearity corresponds to an optimal code of length (2^m-1) and dimension $2m$. In particular when f is a power function, $f: x \mapsto x^s$, this code is the dual of the cyclic code of length (2^m-1) whose zeros are α and α^s (α denotes a primitive element of $\mathbf{F}_{2^m}$). Cyclic codes with two zeros whose dual is optimal also appear in the study of maximum-length sequences (also called m-sequences): the exponents s such that the permutation $x \mapsto x^s$ over $\mathbf{F}_{2^m}$ has maximum nonlinearity coincide with the values of the decimations such that the absolute value of the crosscorrelation function between an m-sequence and its decimation by s is minimum. In this case, any two sequences in the set consisting of all time-shifted versions of an m-sequence and all time-shifted versions of its decimation by s can be easily distinguished. Such pairs of m-sequences are then intensively used in many communication systems, especially in code-division multiple access systems.

The next section recalls some properties of binary cyclic codes; it also exhibits the link between the weight distribution of the duals of cyclic codes with two zeros and both concepts of nonlinearity of a power function from $\mathbf{F}_{2^m}$ into $\mathbf{F}_{2^m}$ and of crosscorrelation of a pair of m-sequences. In section 3 we develop a new theoretical tool for studying the weight distribution of some linear codes, which generalizes some ideas due to Kasami. This method provides new characterizations of AB power mappings and of pairs of m-sequences having some 3-valued correlation spectra, which are presented in section 4. These characterizations use the weight divisibility of the duals of cyclic codes with two zeros which can be derived from McEliece's theorem. Section 5 exhibits some general bounds on the weight divisibility of these codes. Most notably we examine the cyclic codes with two zeros whose dual is at most 8-divisible. Section 6 focuses on power functions $x \mapsto x^s$ over $\mathbf{F}_{2^m}$ for odd m when the exponent s can be written as $s = 2^{\frac{m-1}{2}} + 2^i - 1$. This set of exponents contains the values which appear in both Welch's and Niho's conjectures. Here we prove that for most values of i, $x \mapsto x^{2^{\frac{m-1}{2}}+2^i-1}$ is not AB on $\mathbf{F}_{2^m}$. In section 7 we give some results on the weight divisibility of the duals of cyclic codes with two zeros of length (2^m-1) when m is not a prime. This leads to a very simple necessary condition on the values s of the decimations providing preferred pairs of m-sequences; in this case we are able to eliminate most values of s. We also give the exact weight divisibility of the duals of the binary cyclic codes of length (2^m-1) with a defining set $\{1, s\}$ when m is even and $s \bmod (2^{\frac{m}{2}}-1)$ is a power of 2. All of these results notably generalize two recently proved conjectures on the crosscorrelation of pairs of m-sequences [15, 31, 25, 3]. They also imply that the conjectured almost perfect nonlinear (APN) function $x \mapsto x^s$ with $s = 2^{4g}+2^{3g}+2^{2g}+2^g-1$ over $\mathbf{F}_{2^{5g}}$ is not AB. Finally, we give some numerical results which point out that our theoretical results directly provide the weight divisibility of many infinite families of duals of cyclic codes with two zeros.

2. Cyclic codes with two zeros and related objects. We first give two different formulations of the McEliece theorem which enable us to determine the weight divisibility of the dual of a primitive binary cyclic code with two zeros. These results will be extensively used in the paper.

2.1. Weight divisibility of cyclic codes. Here we consider primitive binary cyclic codes. Let α denote a primitive element of $\mathbf{F}_{2^m}$. Any cyclic code $\mathcal{C}$ of length (2^m-1) can be defined by its generator polynomial whose roots are called the zeros of the code. The defining set of $\mathcal{C}$ is then the set

$$I(\mathcal{C}) = \{i \in \{0, \ldots, 2^m-2\} | \alpha^i \text{ is a zero of } \mathcal{C}\}.$$

Since $\mathcal{C}$ is a binary code, its defining set is a union of 2-cyclotomic cosets modulo $(2^m - 1)$, $Cl(a)$, where $Cl(a) = \{2^j a \bmod (2^m - 1)\}$. From now on the defining set of a binary cyclic code of length $(2^m - 1)$ is identified with the representatives of the corresponding 2-cyclotomic cosets modulo $(2^m - 1)$.

DEFINITION 2.1. *A binary code $\mathcal{C}$ is* 2^ℓ-divisible *if the weight of any of its codewords is divisible by 2^ℓ. Moreover, $\mathcal{C}$ is* exactly 2^ℓ-divisible *if, additionally, it contains at least one codeword whose weight is not divisible by $2^{\ell+1}$.*

The following theorem due to McEliece reduces the determination of the exact weight divisibility of binary cyclic codes to a combinatorial problem.

THEOREM 2.2 (see [24]). *A binary cyclic code is exactly 2^ℓ-divisible if and only if ℓ is the smallest number such that $(\ell + 1)$ nonzeros of $\mathcal{C}$ (with repetitions allowed) have product* 1.

We now focus on primitive cyclic codes with two zeros and on the exact weight divisibility of their duals. We denote by $\mathcal{C}_{1,s}$ the binary cyclic code of length $(2^m - 1)$ with defining set $Cl(1) \cup Cl(s)$. The nonzeros of the cyclic code $\mathcal{C}_{1,s}^\perp$ are the elements α^{-i} with

$$i \in Cl(1) \cup Cl(s).$$

Then $(\ell + 1)$ nonzeros of $\mathcal{C}_{1,s}^\perp$ have product 1 if and only if there exist $I_1 \subset Cl(s)$ and $I_2 \subset Cl(1)$ with $|I_1| + |I_2| = \ell + 1$ and

$$\prod_{k \in I_1 \cup I_2} \alpha^{-k} = 1$$
$$\iff \sum_{k \in I_1 \cup I_2} k \equiv 0 \bmod (2^m - 1).$$

We consider both integers u and v defined by their 2-adic expansions: $u = \sum_{i=0}^{m-1} u_i 2^i$ and $v = \sum_{i=0}^{m-1} v_i 2^i$, where

$$u_i = \begin{cases} 1 & \text{if } 2^i s \bmod (2^m - 1) \in I_1, \\ 0 & \text{otherwise,} \end{cases}$$

$$v_i = \begin{cases} 1 & \text{if } 2^i \bmod (2^m - 1) \in I_2, \\ 0 & \text{otherwise.} \end{cases}$$

Then we have

$$\sum_{k \in I_1 \cup I_2} k \equiv \sum_{i=0}^{m-1} u_i 2^i s + \sum_{i=0}^{m-1} v_i 2^i \bmod (2^m - 1)$$
$$\equiv 0 \bmod (2^m - 1).$$

The size of I_1 (resp., I_2) corresponds to $w_2(u) = \sum_{i=0}^{m-1} u_i$ (resp., $w_2(v)$) which is the 2-weight of u (resp., v). McEliece's theorem can then be formulated as follows.

COROLLARY 2.3. *The cyclic code $\mathcal{C}_{1,s}^\perp$ of length $(2^m - 1)$ is exactly 2^ℓ-divisible if and only if for all (u, v) such that $0 \le u \le 2^m - 1$, $0 \le v \le 2^m - 1$, and*

$$us + v \equiv 0 \bmod (2^m - 1),$$

we have $w_2(u) + w_2(v) \ge \ell + 1$.

Since $v \leq 2^m - 1$, the equation

$$us + v \equiv 0 \bmod (2^m - 1)$$

can be written

$$v = (2^m - 1) - (us \bmod (2^m - 1)).$$

This leads to the following equivalent formulation.

COROLLARY 2.4. *The cyclic code $\mathcal{C}_{1,s}^{\perp}$ of length $(2^m - 1)$ is exactly 2^ℓ-divisible if and only if for all u such that $0 \leq u \leq 2^m - 1$,*

$$w_2(A(u)) \leq w_2(u) + m - 1 - \ell,$$

where $A(u) = us \bmod (2^m - 1)$.

2.2. APN and AB functions. We now point out that some cryptographic properties of power functions over $\mathbf{F}_{2^m}$ are related to the weight enumerators of cyclic codes with two zeros.

Let f be a function from $\mathbf{F}_2^m$ into $\mathbf{F}_2^m$. For any $(a, b) \in \mathbf{F}_2^m \times \mathbf{F}_2^m$, we define

$$\delta_f(a,b) = \#\{x \in \mathbf{F}_2^m : \ f(x+a) + f(x) = b\},$$
$$\lambda_f(a,b) = |\#\{x \in \mathbf{F}_2^m : \ a \cdot x + b \cdot f(x) = 0\} - 2^{m-1}|,$$

where $\cdot$ is the usual dot product on $\mathbf{F}_2^m$. These values are of great importance in cryptography, especially for measuring the security of an iterated block cipher using f as a round permutation. A differential attack [2, 21] against such a cipher exploits the existence of a pair (a, b) with $a \neq 0$ such that $\delta_f(a, b)$ is high. Similarly, a linear attack [22, 23] is successful if there is a pair (a, b) with $b \neq 0$ such that $\lambda_f(a, b)$ is high. The function f can then be used as a round function of an iterated cipher only if both

$$\delta_f = \max_{a \neq 0} \max_b \delta_f(a,b),$$
$$\lambda_f = \max_a \max_{b \neq 0} \lambda_f(a,b)$$

are small. Moreover, if f defines the S-boxes of a Feistel cipher, the values of δ_f and λ_f completely determine the complexity of differential and linear cryptanalyses [29, 28].

Since x is a solution of $f(X + a) + f(X) = b$ if and only if $x + a$ is a solution too, δ_f is always even. Then we have the following.

PROPOSITION 2.5. *For any function $f : \mathbf{F}_2^m \to \mathbf{F}_2^m$,*

$$\delta_f \geq 2.$$

In the case of equality, f is called almost perfect nonlinear (APN).

PROPOSITION 2.6 (see [32, 7]). *For any function $f : \mathbf{F}_2^m \to \mathbf{F}_2^m$,*

$$\lambda_f \geq 2^{\frac{m-1}{2}}.$$

In the case of equality, f is called almost bent (AB).

Note that this minimum value for λ_f can be achieved only if m is odd. For even m, some functions with $\lambda_f = 2^{\frac{m}{2}}$ are known and it is highly conjectured that this value is the minimum [31, p. 603].

From now on the vector space $\mathbf{F}_2^m$ is identified with the finite field $\mathbf{F}_{2^m}$. The function f can then be expressed as a unique polynomial of $\mathbf{F}_{2^m}[X]$ of degree at most (2^m-1). Note that the values of δ_f and λ_f are invariant under both right and left compositions by a linear permutation of $\mathbf{F}_{2^m}$. Similarly, if f is a permutation, $\delta_f = \delta_{f^{-1}}$ and $\lambda_f = \lambda_{f^{-1}}$. We can then assume that $f(0) = 0$ without loss of generality. Both APN property and nonlinearity can also be expressed in terms of error-correcting codes. The proofs of the following results are developed by Carlet, Charpin, and Zinoviev in [6].

THEOREM 2.7. *Let f be a function from $\mathbf{F}_{2^m}$ into $\mathbf{F}_{2^m}$ with $f(0) = 0$. Let $\mathcal{C}_f$ be the linear binary code of length $2^m - 1$ defined by the parity-check matrix*

$$H_f = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^m-2} \\ f(1) & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{2^m-2}) \end{pmatrix}, \tag{2.1}$$

where each entry is viewed as a binary vector and α is a primitive element of $\mathbf{F}_{2^m}$. Then

- *If $\dim \mathcal{C}_f = 2^m - 1 - 2m$,*

$$\lambda_f = \max_{c \in \mathcal{C}_f^\perp, c \neq 0} |2^{m-1} - wt(c)|.$$

  In particular, for odd m, f is AB if and only if for any nonzero codeword $c \in \mathcal{C}_f^\perp$,

$$2^{m-1} - 2^{\frac{m-1}{2}} \leq wt(c) \leq 2^{m-1} + 2^{\frac{m-1}{2}}.$$

- *$\lambda_f = 2^{m-1}$ if and only if $\dim \mathcal{C}_f > 2^m - 1 - 2m$ or $\mathcal{C}_f^\perp$ contains the all-one vector.*
- *f is APN if and only if the code $\mathcal{C}_f$ has minimum distance 5.*

In particular, if f is a power function $x \mapsto x^s$ over $\mathbf{F}_{2^m}$, the code $\mathcal{C}_f$ is the cyclic code of length $(2^m - 1)$ whose zeros are α and α^s.

Tables 2.1 and 2.2 (resp., Tables 2.3 and 2.4) give all known and conjectured values of exponents s (up to equivalence) such that the power function $x \mapsto x^s$ is APN (resp., has the highest known nonlinearity).

TABLE 2.1
Known and conjectured APN power functions x^s on $\mathbf{F}_{2^m}$ with $m = 2t + 1$.

	Exponents s	Status
Quadratic functions	$2^i + 1$ with $\gcd(i, m) = 1$, $1 \leq i \leq t$	proven [13, 27]
Kasami's functions	$2^{2i} - 2^i + 1$ with $\gcd(i, m) = 1$, $2 \leq i \leq t$	proven [19]
Inverse function	$2^{2t} - 1$	proven [27, 1]
Welch's function	$2^t + 3$	proven [11]
Niho's function	$2^t + 2^{\frac{t}{2}} - 1$ if t is even $2^t + 2^{\frac{3t+1}{2}} - 1$ if t is odd	proven [10]
Dobbertin's function	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$ if $m = 5i$	conjectured [10]

TABLE 2.2
Known and conjectured APN power functions x^s on $\mathbf{F}_{2^m}$ with $m = 2t$.

	Exponents s	Status
Quadratic functions	$2^i + 1$ with $\gcd(i, m) = 1$, $1 \le i < t$	proven [13, 27]
Kasami's functions	$2^{2i} - 2^i + 1$ with $\gcd(i, m) = 1$ $2 \le i < t$	proven [19, 17]
Dobbertin's function	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$ if $m = 5i$	conjectured [10]

TABLE 2.3
Known AB power permutations x^s on $\mathbf{F}_{2^m}$ with $m = 2t + 1$.

	Exponents s	Status
Quadratic functions	$2^i + 1$ with $\gcd(i, m) = 1$, $1 \le i \le t$	proven [13, 27]
Kasami's functions	$2^{2i} - 2^i + 1$ with $\gcd(i, m) = 1$ $2 \le i \le t$	proven [19]
Welch's function	$2^t + 3$	proven [5, 4]
Niho's function	$2^t + 2^{\frac{t}{2}} - 1$ if t is even $2^t + 2^{\frac{3t+1}{2}} - 1$ if t is odd	proven [16]

TABLE 2.4
Known power permutations x^s with highest known nonlinearity on $\mathbf{F}_{2^m}$ with $m = 2t$.

Exponents s	Status
$2^{2t-1} - 1$	proven [20]
$2^i + 1$ with $\gcd(i, m) = 2$ $1 \le i < t, m \equiv 2 \bmod 4$	proven [13]
$2^{2i} - 2^i + 1$ with $\gcd(i, m) = 2$ $1 \le i < t, m \equiv 2 \bmod 4$	proven [19]
$\sum_{i=0}^{t} 2^{ik}$ with t even, $0 < k < t$ such that $\gcd(k, m) = 1$	proven [12]
$2^t + 2^{\frac{t+1}{2}} + 1$ t odd	proven [9]
$2^t + 2^{t-1} + 1$ t odd	proven [9]
$2^t + 2^{\frac{t}{2}} + 1$ $t \equiv 2 \bmod 4$	proven [12]

2.3. Crosscorrelation of a pair of binary m-sequences. A binary sequence $(u_i)_{i \ge 0}$ generated by a linear feedback shift register (LFSR) of length m has maximal period when the feedback polynomial of the LFSR is primitive. Such a sequence is called an *m-sequence* of length $(2^m - 1)$. From now on, a binary m-sequence of length $(2^m - 1)$ is identified with the binary vector of length $(2^m - 1)$ consisting of its first $(2^m - 1)$ bits. A further property of m-sequences is that they are almost uncorrelated with their cyclic shifts. This property is important in many communication

systems (such as radar communications or transmissions using spread-spectrum techniques) since it is often required that a signal be easily distinguished from any time-shifted version of itself. It is well known that for any m-sequence u of length (2^m-1) there exists a unique $c \in \mathbf{F}_{2^m} \setminus \{0\}$ such that

$$\forall i,\ 0 \le i \le 2^m-2,\ \ u_i = \mathrm{Tr}(c\alpha^i),$$

where α is a root of the feedback polynomial of the LFSR generating u (i.e., α is a primitive element of $\mathbf{F}_{2^m}$) and Tr denotes the trace function from $\mathbf{F}_{2^m}$ to $\mathbf{F}_2$.

When a communication system uses a set of several signals (usually corresponding to different users), it is also required that each of these signals be easily distinguished from any other signal in the set and its time-shifted versions. This property is of great importance, especially in code-division multiple access systems. The distance between a sequence u and all cyclic shifts of another sequence v can be computed with the crosscorrelation function.

DEFINITION 2.8. *Let u and v be two different binary sequences of length N. The crosscorrelation function between u and v, denoted by $\theta_{u,v}$, is defined as*

$$\theta_{u,v}(\tau) = \sum_{i=0}^{N-1} (-1)^{u_i + v_{i+\tau}}.$$

The corresponding crosscorrelation spectrum is the vector $(T_{-N}, \ldots, T_N)$ with

$$T_\omega = \#\{\tau,\ 0 \le \tau \le N-1,\ \ \theta_{u,v}(\tau) = \omega\}.$$

Since $\theta_{u,v}(\tau) = N - 2wt(u + \sigma^\tau v)$, where σ denotes the cyclic shift operator, the above mentioned applications use pairs of sequences (u, v) such that $|\theta_{u,v}(\tau)|$ is small for all $\tau \in \{0, \ldots, N-1\}$.

If u and v are two different binary m-sequences of length (2^m-1), there exists an integer s in $\{0, \ldots, 2^m-2\}$ and a pair (c_1, c_2) of nonzero elements of $\mathbf{F}_{2^m}$ such that

$$\forall i,\ 0 \le i \le 2^m-2,\ \ u_i = \mathrm{Tr}(c_1\alpha^i) \text{ and } v_i = \mathrm{Tr}(c_2\alpha^{si})\ .$$

If $c_1 = c_2$, the sequence v is said to be a *decimation by s of u*. Writing $c_1 = \alpha^{j_1}$ and $c_2 = \alpha^{j_2}$, the crosscorrelation function for the pair (u, v) is given by

$$\theta_{u,v}(\tau) = \sum_{i=0}^{2^m-2} (-1)^{\mathrm{Tr}(\alpha^{i+j_1} + \alpha^{si+j_2+\tau})} = \sum_{x \in \mathbf{F}_{2^m}^*} (-1)^{\mathrm{Tr}(\alpha^{\tau'}[\alpha^{j_1-\tau'}x + x^s])}\ ,$$

where $\tau' = j_2 + \tau$. It follows that the corresponding crosscorrelation spectrum does not depend on the choice of j_2. It is then sufficient to study the pairs (u, v), where v is a decimation by s of u.

We now recall the well-known link between the crosscorrelation spectrum of pairs of binary m-sequences and the weight distribution of the duals of some cyclic codes with two zeros.

PROPOSITION 2.9. *Let m and s be two positive integers such that $\gcd(s, 2^m-1) = 1$ and s is not a power of 2. Let $(T_{-2^m+1}, \ldots, T_{2^m-1})$ be the crosscorrelation spectrum between an m-sequence of length (2^m-1) and its decimation by s. Let $(A_0, \ldots, A_{2^m-1})$ be the weight enumerator of the dual of the binary cyclic code $\mathcal{C}_{1,s}$ of length (2^m-1)*

with defining set $\{1, s\}$. *Then we have that* $T_\omega = 0$ *for all even values of* ω *and for odd* ω*:*

$$\begin{aligned} T_\omega &= A_{2^{m-1}-\frac{\omega+1}{2}} \text{ for all } \omega \notin \{-1, 2^m - 1\}, \\ T_{-1} &= A_{2^{m-1}} - 2(2^m - 1), \\ T_{2^m-1} &= 0. \end{aligned}$$

In particular, if ω_0 *is the smallest positive integer such that*

$$T_{-\omega} = T_\omega = 0 \text{for all } \omega \text{ such that } \omega > \omega_0,$$

then we have

$$\omega_0 = 2^m - 1 - 2w_0,$$

where w_0 *is the largest integer such that* $0 < w_0 \leq 2^{m-1}$ *and*

$$A_w = A_{2^m-w} = 0 \text{ for all } w \text{ such that } 0 < w < w_0.$$

Proof. The code $\mathcal{C}_{1,s}^\perp$ consists of all codewords $c = (c_0, \ldots, c_{2^m-2})$, where

$$c_i = \mathrm{Tr}(a\alpha^i + b\alpha^{si}) \text{ with } a, b \in \mathbf{F}_{2^m}.$$

If either a or b equals zero, c is a codeword of the simplex code of length $(2^m - 1)$. In this case, its Hamming weight is 2^{m-1} except for $a = b = 0$. Using that $\theta_{u,v}(\tau) = 2^m - 1 - 2wt(u + \sigma^\tau v)$, we obtain the expected result. □

Using Theorem 2.7 we see that

$$\begin{aligned} \omega_0 &= -1 + 2 \max_{c \in \mathcal{C}_{1,s}^\perp, c \neq 0} |2^{m-1} - wt(c)| \\ &= 2\lambda_s - 1, \end{aligned}$$

where λ_s is the linearity of the power permutation $x \mapsto x^s$ over $\mathbf{F}_{2^m}$. In particular, when m is odd the lowest possible value for ω_0 is $2^{\frac{m+1}{2}} - 1$ and the values of s for which this bound is reached exactly correspond to the exponents s such that $x \mapsto x^s$ is an AB permutation over $\mathbf{F}_{2^m}$.

3. Weight polynomials of linear codes of length $2^m - 1$ and dimension $2m$. As previously seen, both notions of nonlinearity of a function from $\mathbf{F}_{2^m}$ into $\mathbf{F}_{2^m}$ and of crosscorrelation spectrum of a pair of binary m-sequences of length $(2^m - 1)$ are related to the weight polynomials of some linear binary codes of length $(2^m - 1)$ and dimension $2m$. Here we give some general results on the weight distributions of linear codes having these parameters. Our method uses Pless power moment identities [30] and some ideas due to Kasami [18, Thm. 13] (see also [6, Thm. 4]).

THEOREM 3.1. *Let* $\mathcal{C}$ *be a* $[2^m - 1, 2m]$*-linear code which does not contain the all-one vector* $\mathbf{1} = (1, \ldots, 1)$. *Assume that the minimum distance of the dual code* $\mathcal{C}^\perp$ *is at least* 3. *Let* $A = (A_0, \ldots, A_{2^m-1})$ *(resp.,* $B = (B_0, \ldots, B_{2^m-1})$*) be the weight enumerator of* $\mathcal{C}$ *(resp.,* $\mathcal{C}^\perp$*). Then, for any positive integer* $x \leq 2^{m-1}$, *we have*

$$\begin{aligned} &\sum_{w=1}^{2^{m-1}-1} (w - 2^{m-1})^2 \left((w - 2^{m-1})^2 - x^2\right) (A_w + A_{2^m-w}) \\ &\quad = 2^{2m-2} \left[6(B_3 + B_4) + (2^m - 1)(2^{m-1} - x^2)\right]. \end{aligned}$$

Most notably this implies the following:

(i) *If w_0 is such that for all $0 < w < w_0$*

$$A_w = A_{2^m - w} = 0,$$

then

$$6(B_3 + B_4) \leq (2^m - 1)\left[(2^{m-1} - w_0)^2 - 2^{m-1}\right],$$

where equality holds if and only if $A_w = 0$ for all $w \notin \{0, w_0, 2^{m-1}, 2^m - w_0\}$.

(ii) *If w_1 is such that for all $w_1 < w < 2^{m-1}$*

$$A_w = A_{2^m - w} = 0,$$

then

$$6(B_3 + B_4) \geq (2^m - 1)\left[(2^{m-1} - w_1)^2 - 2^{m-1}\right],$$

where equality holds if and only if $A_w = 0$ for all $w \notin \{0, w_1, 2^{m-1}, 2^m - w_1\}$.

Proof. The main part of the proof relies on the first Pless power moment identities [30]. The first four power moment identities on the weight distribution of a code of length $2^m - 1$ and dimension $2m$ are

$$\begin{aligned}
&\sum_{w=0}^{n} wA_w = 2^{2m-1}(2^m - 1),\\
&\sum_{w=0}^{n} w^2 A_w = 2^{3m-2}(2^m - 1),\\
&\sum_{w=0}^{n} w^3 A_w = 2^{2m-3}\left((2^m - 1)^2(2^m + 2) - 3!B_3\right),\\
&\sum_{w=0}^{n} w^4 A_w = 2^{2m-4}\left(2^m(2^m - 1)(2^{2m} + 3 \cdot 2^m - 6) + 4!\ (B_4 - (2^m - 1)B_3)\right).
\end{aligned}$$

Let us consider the numbers $I_\ell = \sum_{w=1}^{2^m-1}(w - 2^{m-1})^\ell A_w$. Since for ℓ even

$$(w - 2^{m-1})^\ell = ((2^m - w) - 2^{m-1})^\ell\ ,$$

we have for any even ℓ

$$I_\ell = \sum_{w=1}^{2^m-1}(w - 2^{m-1})^\ell A_w = \sum_{w=1}^{2^{m-1}-1}(w - 2^{m-1})^\ell (A_w + A_{2^m - w}).$$

Note that the codeword of weight zero is not taken into account in the sum above. Recall that C does not contain the all-one codeword.

By using the four power moments, we obtain the following values for I_2 and I_4:

$$\begin{aligned}
I_2 &= 2^{2m-2}(2^m - 1),\\
I_4 &= 2^{2m-2}\left[6(B_3 + B_4) + 2^{m-1}(2^m - 1)\right].
\end{aligned}$$

Let x be a positive integer and let $\mathcal{I}(x)$ denote the value of $I_4 - x^2 I_2$. We have

$$\begin{aligned}
\mathcal{I}(x) &= \sum_{w=1}^{2^{m-1}-1}(w - 2^{m-1})^2\left((w - 2^{m-1})^2 - x^2\right)(A_w + A_{2^m - w})\\
&= 2^{2m-2}\left[6(B_3 + B_4) + (2^m - 1)(2^{m-1} - x^2)\right].
\end{aligned}$$

The wth term in this sum satisfies

$$\begin{array}{lll}(w-2^{m-1})^2\left((w-2^{m-1})^2-x^2\right) & <0 & \text{if } 0<|2^{m-1}-w|<x\\ & =0 & \text{if } w\in\{2^{m-1},2^{m-1}\pm x\}\\ & >0 & \text{if } |2^{m-1}-w|>x.\end{array}$$

This implies that, if $A_w = A_{2^m-w} = 0$ for all w such that $0 < w < w_0$, all the terms in $\mathcal{I}(2^{m-1} - w_0)$ are nonpositive. Then we have

$$6(B_3 + B_4) + (2^m - 1)\left[2^{m-1} - (2^{m-1} - w_0)^2\right] \le 0$$

with equality if and only if all terms in the sum are zero. This can happen only when $A_w = 0$ for all $w \notin \{0, w_0, 2^{m-1}, 2^m - w_0\}$.

Similarly, if $A_w = A_{2^m-w} = 0$ for all w such that $w_1 < w < 2^{m-1}$, all the terms in $\mathcal{I}(2^{m-1} - w_1)$ are positive. Then we have

$$6(B_3 + B_4) + (2^m - 1)\left[2^{m-1} - (2^{m-1} - w_1)^2\right] \ge 0$$

with equality if and only if all terms in the sum are zero, i.e., if $A_w = 0$ for all $w \notin \{0, w_1, 2^{m-1}, 2^m - w_1\}$. □

This theorem obviously gives an upper bound on the value of w_0 for which all nonzero weights of $\mathcal{C}$ lie between w_0 and $2^m - w_0$.

COROLLARY 3.2. *Let $\mathcal{C}$ be a $[2^m - 1, 2m]$-linear code which does not contain the all-one vector $\mathbf{1} = (1, \ldots, 1)$. Assume that the minimum distance of the dual code $\mathcal{C}^\perp$ is at least 3. Let w_0 be the smallest w such that $0 < w < 2^{m-1}$ and*

$$A_w + A_{2^m-w} \neq 0.$$

Then

$$w_0 \le 2^{m-1} - 2^{\frac{m-1}{2}}$$

and equality holds if and only if the weight of every codeword in $\mathcal{C}$ belongs to $\{0, 2^{m-1}, 2^{m-1} \pm 2^{\frac{m-1}{2}}\}$. In this case the weight distribution of $\mathcal{C}$ is the same as the weight distribution of the dual of the 2-error-correcting Bose–Chaudhuri-Hocquenghem (BCH) code, i.e.,

Weight: w	*Number of words: A_w*
0	1
$2^{m-1} - 2^{(m-1)/2}$	$(2^m - 1)(2^{m-2} + 2^{(m-3)/2})$
2^{m-1}	$(2^m - 1)(2^{m-1} + 1)$
$2^{m-1} + 2^{(m-1)/2}$	$(2^m - 1)(2^{m-2} - 2^{(m-3)/2})$

Proof. The first statement directly results from the previous theorem. Moreover, if $w_0 = 2^{m-1} - 2^{\frac{m-1}{2}}$, then A_{w_0}, $A_{2^{m-1}}$, and $A_{2^m-w_0}$ are the only unknown values in the weight distribution of $\mathcal{C}$. They are then completely determined by inverting the linear system formed by $A_{w_0} + A_{2^{m-1}} + A_{2^m-w_0} = 2^{2m} - 1$ and the first two Pless power moments identities. □

Pless power moment identities also imply that if all nonzero codewords of a $[2^m - 1, 2m]$ code have Hamming weight in the set $\{2^{m-1} \pm W, 2^{m-1}\}$, the weight distribution of this code is unique as long as its dual has minimum distance at least 3.

PROPOSITION 3.3. *Let $\mathcal{C}$ be a $[2^m-1, 2m]$-linear code which does not contain the all-one vector $\mathbf{1} = (1, \ldots, 1)$. Assume that the minimum distance of the dual code $\mathcal{C}^\perp$ is at least 3. Assume that the weight of every codeword in $\mathcal{C}$ lies in $\{0, 2^{m-1}, 2^{m-1} \pm W\}$. Then W is divisible by $2^{\lceil \frac{m-1}{2} \rceil}$. Moreover, the weight distribution of $\mathcal{C}$ is completely determined:*

Weight: w	*Number of words: A_w*
0	1
$2^{m-1} - W$	$\frac{2^{m-2}(2^m-1)(2^{m-1}+W)}{W^2}$
2^{m-1}	$\frac{(2^m-1)((2^m+1)W^2-2^{2m-2})}{W^2}$
$2^{m-1} + W$	$\frac{2^{m-2}(2^m-1)(2^{m-1}-W)}{W^2}$

In particular, the number B_3 (resp., B_4) of codewords of weight 3 (resp., 4) in $\mathcal{C}^\perp$ is given by

$$B_3 = \frac{(2^m-1)(W^2-2^{m-1})}{3 \cdot 2^{m-1}},$$
$$B_4 = \frac{(2^m-1)(2^{m-2}-1)(W^2-2^{m-1})}{3 \cdot 2^{m-1}}.$$

Proof. Let $A = (A_0, \ldots, A_{2^m-1})$ (resp., $B = (B_0, \ldots, B_{2^m-1})$) be the weight enumerator of $\mathcal{C}$ (resp., $\mathcal{C}^\perp$). By hypothesis, $B_1 = B_2 = 0$. Using the first two Pless power moment identities, we obtain

$$A_{2^{m-1}-W} + A_{2^{m-1}} + A_{2^{m-1}+W} = 2^{2m} - 1,$$
$$(2^{m-1}-W)A_{2^{m-1}-W} + 2^{m-1}A_{2^{m-1}} + (2^{m-1}+W)A_{2^{m-1}+W} = 2^{2m-1}(2^m-1),$$
$$(2^{m-1}-W)^2A_{2^{m-1}-W} + 2^{2m-2}A_{2^{m-1}} + (2^{m-1}+W)^2A_{2^{m-1}+W} = 2^{3m-2}(2^m-1).$$

Inverting this linear system gives the expected weight distribution. By writing the third and fourth Pless power moment identities, we can compute the number of codewords of weights 3 and 4 in $\mathcal{C}^\perp$:

$$B_3 = \frac{(2^m-1)(W^2-2^{m-1})}{3 \cdot 2^{m-1}},$$
$$B_4 = \frac{(2^m-1)(2^{m-2}-1)(W^2-2^{m-1})}{3 \cdot 2^{m-1}}.$$

Since B_3 is an integer, we have that 2^{m-1} divides $W^2 - 2^{m-1}$ and then W is divisible by $2^{\lceil \frac{m-1}{2} \rceil}$. □

4. AB functions, 3-valued crosscorrelation functions, and weight divisibility.

4.1. A new characterization of AB functions. Let us now suppose that m is odd, $m = 2t+1$. We give a necessary and sufficient condition on $f : \mathbf{F}_{2^m} \to \mathbf{F}_{2^m}$ to achieve the highest possible nonlinearity.

THEOREM 4.1. *Let m be an odd integer and $\mathcal{C}$ be a $[2^m-1, 2m]$-linear code which does not contain the all-one vector $\mathbf{1} = (1, \ldots, 1)$. Assume that the minimum distance*

of the dual code $\mathcal{C}^\perp$ is at least 3. Let $A = (A_0, \ldots, A_{2^m-1})$ be the weight enumerator of $\mathcal{C}$ and let w_0 be the smallest w such that $0 < w < 2^{m-1}$ and

$$A_w + A_{2^m-w} \neq 0.$$

Then

$$w_0 = 2^{m-1} - 2^{\frac{m-1}{2}}$$

if and only if the minimum distance of the dual code $\mathcal{C}^\perp$ is 5 and $\mathcal{C}$ is $2^{\frac{m-1}{2}}$-divisible.

Proof. This condition is sufficient because, if

$$w_0 = 2^{m-1} - 2^{\frac{m-1}{2}},$$

the code $\mathcal{C}$ has the same weight distribution as the 2-error-correcting BCH code (according to Corollary 3.2).

This condition is also necessary since, for any w such that $2^{m-1} - 2^{\frac{m-1}{2}} < w < 2^{m-1}$, both integers w and $2^{m-1} - w$ are not divisible by $2^{\frac{m-1}{2}}$. The condition on the divisibility of the weights of $\mathcal{C}$ then implies that

$$A_w + A_{2^m-w} = 0 \text{ for all } w \text{ such that } 2^{m-1} - 2^{\frac{m-1}{2}} < w < 2^{m-1}\ .$$

If $B_3 = B_4 = 0$, the lower bound given in Theorem 3.1(ii) (applied with $w_1 = 2^{m-1} - 2^{\frac{m-1}{2}}$) is reached. Then the weight of every codeword in $\mathcal{C}$ lies in $\{0, 2^{m-1}, 2^{m-1} \pm 2^{\frac{m-1}{2}}\}$. □

COROLLARY 4.2. *Let m be an odd integer and let f be a function from $\mathbf{F}_2^m$ into $\mathbf{F}_2^m$ such that $\lambda_f \neq 2^{m-1}$. Then f is AB if and only if f is APN and the code $\mathcal{C}_f^\perp$ defined in Theorem 2.7 is $2^{\frac{m-1}{2}}$-divisible.*

When f is a power function, $f : x \mapsto x^s$, the corresponding code C_f is the binary cyclic code $\mathcal{C}_{1,s}$ of length $(2^m - 1)$ with defining set $\{1, s\}$. The weight divisibility of the corresponding dual code can therefore be obtained by applying McEliece's theorem, as expressed in Corollary 2.4. This leads to the following characterization of AB power functions.

COROLLARY 4.3. *Let $m = 2t+1$. Assume that the power function $f : x \mapsto x^s$ on $\mathbf{F}_{2^m}$ satisfies $\lambda_f \neq 2^{m-1}$. Then f is AB on $\mathbf{F}_{2^m}$ if and only if f is APN on $\mathbf{F}_{2^m}$ and*

$$\forall u,\ \ 1 \leq u \leq 2^m - 1,\ \ w_2(A(u)) \leq t + w_2(u), \tag{4.1}$$

where $A(u) = us \bmod (2^m - 1)$.

Note that $\lambda_f = 2^{m-1}$ means that there exists a linear combination of the Boolean components of f which is an affine function.

Condition (4.1) is obviously satisfied when $w_2(u) \geq t+1$. Moreover, if $\gcd(s, 2^m - 1) = 1$ (i.e., if $x \mapsto x^s$ is a permutation), the condition also holds for all u such that $w_2(u) = t$. Using that

$$A(u2^i \bmod (2^m - 1)) = 2^i A(u) \bmod (2^m - 1),$$

we deduce that condition (4.1) must be checked only for one element in each cyclotomic coset. Note that if u is the smallest element in its cyclotomic coset and $w_2(u) < t$, we have $u \leq 2^{m-2} - 1$.

This result provides a fast algorithm for checking whether an APN power function is AB and then for finding all AB power functions on $\mathbf{F}_{2^m}$. There are roughly $\frac{2^{m-1}}{m}$

cyclotomic representatives u such that $w_2(u) \leq t$, and each test requires one modular multiplication on m-bit integers and two weight computations. Condition (4.1) can then be checked with approximately 2^m elementary operations and at no memory cost.

4.2. A new characterization of some pairs of m-sequences with 3-valued crosscorrelation. We now suppose that m is even, $m = 2t$, and we are interested in the values of s such that the crosscorrelation function between an m-sequence of length $(2^m - 1)$ and its decimation by s takes the following three values: $-1, 2W - 1$, and $-2W - 1$. From Proposition 2.9, this means that the weight of every codeword in $\mathcal{C}_{1,s}^{\perp}$ lies in $\{0, 2^{m-1}, 2^{m-1} + W, 2^{m-1} - W\}$. Proposition 3.3 then implies that W is divisible by 2^t. When W is a power of 2, we have $W = 2^{t+e}$. The $[2^m - 1, 2m]$-codes whose weights lie in $\{0, 2^{m-1}, 2^{m-1} \pm 2^{t+e}\}$ are then completely characterized by their weight divisibility and by the number of codewords of weights 3 and 4 in their dual.

THEOREM 4.4. *Let $m = 2t$ be an even integer and $\mathcal{C}$ be a $[2^m - 1, 2m]$-linear code which does not contain the all-one vector $\mathbf{1} = (1, \ldots, 1)$. Assume that the minimum distance of the dual code $\mathcal{C}^{\perp}$ is at least 3. Let $A = (A_0, \ldots, A_{2^m-1})$ be the weight enumerator of $\mathcal{C}$ and let e be an integer. The weight of every codeword in $\mathcal{C}$ lies in $\{0, 2^{m-1}, 2^{m-1} \pm 2^{t+e}\}$ if and only if $\mathcal{C}$ is 2^{t+e}-divisible and the number B_3 (resp., B_4) of codewords of weight 3 (resp., 4) in $\mathcal{C}^{\perp}$ satisfies*

$$B_3 = \frac{(2^m - 1)(2^{2e+1} - 1)}{3},$$
$$B_4 = \frac{(2^m - 1)(2^{m-2} - 1)(2^{2e+1} - 1)}{3}.$$

Proof. Applying Proposition 3.3 shows that this condition is sufficient. It is also necessary since, for any w such that $2^{m-1} - 2^{t+e} < w < 2^{m-1}$, both integers w and $2^{m-1} - w$ are not divisible by 2^{t+e}. The condition on the divisibility of the weights of $\mathcal{C}$ then implies that

$$A_w + A_{2^m-w} = 0 \text{ for all } w \text{ such that } 2^{m-1} - 2^{t+e} < w < 2^{m-1}.$$

For the given values of B_3 and B_4, we have

$$6(B_3 + B_4) = 2^{m-1}(2^m - 1)(2^{2e+1} - 1).$$

It follows that the lower bound given in Theorem 3.1(ii) (applied with $w_1 = 2^{m-1} - 2^{t+e}$) is reached. The weight of every codeword in $\mathcal{C}$ then lies in $\{0, 2^{m-1}, 2^{m-1} \pm 2^{t+e}\}$ and there is at least a codeword in $\mathcal{C}$ having any of these weights since a code with these parameters has at least three different nonzero weights [15, Thm. 4.1]. □

By applying McEliece's theorem (Corollary 2.4), we derive a necessary and sufficient condition to obtain a pair of m-sequences with crosscorrelation values in $\{-1, -1 \pm 2^{t+1+e}\}$. Note that if $e = 0$, $\omega_0 = \max_\tau |\theta_{u,v}(\tau)|$ equals $2^{t+1} - 1$, which is the smallest known value for ω_0. In this case, the 3-valued crosscorrelation function is said to be *preferred* and the corresponding (u, v) is called a *preferred pair of m-sequences.*

COROLLARY 4.5. *Let $m = 2t$ be an even integer and s a positive integer such that $\gcd(s, 2^m - 1) = 1$ and s is not a power of 2. Let e be a positive integer and $\mathcal{C}_{1,s}$ be the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, s\}$. The crosscorrelation function between an m-sequence of length $(2^m - 1)$ and its decimation by s takes exactly 3 values, -1, $-1 + 2^{t+1+e}$, and $-1 - 2^{t+1+e}$ if and only if the number B_3 (resp., B_4)*

of codewords of weight 3 *(resp.,* 4*) in* $\mathcal{C}_{1,s}$ *satisfies*

$$B_3 = \frac{(2^m-1)(2^{2e+1}-1)}{3},$$
$$B_4 = \frac{(2^m-1)(2^{m-2}-1)(2^{2e+1}-1)}{3},$$

and

$$\forall u,\ \ 1 \le u \le 2^m-1,\ \ w_2(A(u)) \le t-1-e+w_2(u),$$

where $A(u) = us \bmod (2^m-1)$.

In particular, the crosscorrelation function is preferred if and only if

$$B_3 = \frac{(2^m-1)}{3},\ \ B_4 = \frac{(2^m-1)(2^{m-2}-1)}{3},$$

and

$$\forall u,\ \ 1 \le u \le 2^m-1,\ \ w_2(A(u)) \le t-1+w_2(u).$$

5. Some general results on the weight divisibility of $\mathcal{C}_{1,s}^{\perp}$. We now show that the weight divisibility of the dual of the cyclic code $\mathcal{C}_{1,s}$ is conditioned by the 2-weight of s. Most notably this implies that $\mathcal{C}_{1,s}^{\perp}$ has a low exact weight divisibility only for particular values of s.

5.1. Upper and lower bounds on the weight divisibility of $\mathcal{C}_{1,s}^{\perp}$. We first give some general lower and upper bounds on the exact divisibility of $\mathcal{C}_{1,s}^{\perp}$ which depend on the 2-weight of s. The 2-weight of s obviously gives an upper bound on the weight divisibility of $\mathcal{C}_{1,s}^{\perp}$ (obtained for $u=1$ in Corollary 2.4). Using this result, we immediately recover the condition on the degree of AB functions given in [6, Thm. 1] in the particular case of power functions.

COROLLARY 5.1. *Let* $\mathcal{C}_{1,s}$ *be the binary cyclic code of length* (2^m-1) *with defining set* $\{1,s\}$. *If* $\mathcal{C}_{1,s}^{\perp}$ *is* 2^ℓ*-divisible, then*

$$\ell \le m - w_2(s).$$

Most notably this implies the following:

- *For odd* m*, if the power permutation* $f: x \mapsto x^s$ *is AB on* $\mathbf{F}_{2^m}$*, then*

$$w_2(s) \le \frac{m+1}{2};$$

- *for even* m*, if the crosscorrelation function between an* m*-sequence of length* (2^m-1) *and its decimation by* s *takes the values* $-1, 2^{\frac{m}{2}+1+e}-1, -2^{\frac{m}{2}+1+e}-1$*, then*

$$w_2(s) \le \frac{m}{2} - e.$$

The 2-weight of s also provides a lower bound on the divisibility of $\mathcal{C}_{1,s}^{\perp}$: the cyclic code $\mathcal{C}_{1,s}^{\perp}$ of length (2^m-1) is a subcode of the punctured Reed–Muller code of length (2^m-1) and of order $w_2(s)$, which is exactly 2^ℓ-divisible with $\ell = \lfloor \frac{m-1}{w_2(s)} \rfloor$. When $\gcd(2^m-1, s) = 1$, this bound can be slightly improved.

COROLLARY 5.2. *Let m and s be two positive integers such that $s \leq 2^m - 1$ and $\gcd(2^m - 1, s) = 1$. Let $\mathcal{C}_{1,s}$ be the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, s\}$. Then $\mathcal{C}_{1,s}^{\perp}$ is 2^ℓ-divisible with $\ell = \lceil \frac{m-1}{w_2(s)} \rceil$.*

Proof. We use McEliece's theorem as expressed in Corollary 2.3. Let u and v be two integers in $\{0, \ldots, 2^m - 1\}$ such that $us + v \equiv 0 \bmod (2^m - 1)$. Here we prove that

$$w_2(u) + w_2(v) \geq \left\lceil \frac{m-1}{w_2(s)} \right\rceil + 1. \tag{5.1}$$

Since $s \leq 2^m - 2$, we have that

$$us + v = K(2^m - 1), \text{ where } K \text{ lies in } \{1, \ldots, 2^m - 1\}.$$

By writing

$$K(2^m - 1) = (K-1)2^m + [(2^m - 1) - (K-1)],$$

we obtain that

$$w_2(K(2^m - 1)) = w_2(K-1) + m - w_2(K-1) = m$$

since $0 \leq K - 1 \leq 2^m - 1$. It follows that $w_2(us + v) = m$. We now write that

$$w_2(us + v) \leq w_2(us) + w_2(v) \leq w_2(u)w_2(s) + w_2(v)$$

and we get

$$w_2(u)w_2(s) + w_2(v) \geq m.$$

We therefore obtain

$$w_2(u) + w_2(v) \geq m - (w_2(s) - 1)w_2(u). \tag{5.2}$$

Case 1. $w_2(u) \leq \lceil \frac{m-1}{w_2(s)} \rceil - 1$.
Let $m - 1 = qw_2(s) + r$ with $0 \leq r < w_2(s)$. We have

$$\left\lceil \frac{m-1}{w_2(s)} \right\rceil = \begin{cases} q & \text{if r = 0;} \\ q+1 & \text{otherwise.} \end{cases}$$

When $r = 0$, inequality (5.2) gives

$$\begin{aligned} w_2(u) + w_2(v) &\geq m - (w_2(s) - 1)(q - 1) \\ &\geq m - w_2(s)q + q + w_2(s) - 1 \\ &\geq 1 + q + w_2(s) - 1 \\ &\geq q + 1 \\ &\geq \left\lceil \frac{m-1}{w_2(s)} \right\rceil + 1. \end{aligned}$$

When $r > 0$, inequality (5.2) gives

$$\begin{aligned} w_2(u) + w_2(v) &\geq m - (w_2(s) - 1)q \\ &\geq 1 + r + q \\ &\geq q + 2 \\ &\geq \left\lceil \frac{m-1}{w_2(s)} \right\rceil + 1. \end{aligned}$$

Case 2. $w_2(u) = \lceil \frac{m-1}{w_2(s)} \rceil$.
Since $\gcd(2^m - 1, s) = 1$, there is no integer $u < 2^m - 1$ satisfying $us \equiv 0 \bmod (2^m - 1)$. This implies that $w_2(v) \geq 1$, and therefore

$$w_2(u) + w_2(v) \geq \left\lceil \frac{m-1}{w_2(s)} \right\rceil + 1.$$

Case 3. $w_2(u) \geq \lceil \frac{m-1}{w_2(s)} \rceil + 1$.
In this case, inequality (5.1) obviously holds. □

5.2. Cyclic codes $\mathcal{C}_{1,s}^{\perp}$ with a small weight divisibility. We now focus on the values of s for which the exact weight divisibility of $\mathcal{C}_{1,s}^{\perp}$ is small, i.e., for which $\mathcal{C}_{1,s}^{\perp}$ is exactly 2^ℓ-divisible with $\ell \in \{1, 2, 3\}$.

If $\gcd(s, 2^m - 1) = 1$, the only values of s such that $\mathcal{C}_{1,s}^{\perp}$ is exactly 2-divisible satisfy $w_2(s) = m - 1$ [15, Thm. 4.7]; they all lie in the cyclotomic coset defined by $(2^{m-1} - 1)$. In this case $\mathcal{C}_{1,s}^{\perp}$ is the dual of the Melas code; its weights are all even integers w such that $|w - \frac{2^m - 1}{2}| \leq 2^{\frac{m}{2}}$ [20]. The following proposition similarly exhibits all values of s such that $\mathcal{C}_{1,s}^{\perp}$ is exactly 4-divisible.

PROPOSITION 5.3. *Let m and s be two positive integers such that* $\gcd(s, 2^m - 1) = 1$. *Let $\mathcal{C}_{1,s}$ be the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, s\}$.*

(i) *$\mathcal{C}_{1,s}^{\perp}$ is exactly 2-divisible if and only if $w_2(s) = m - 1$.*
(ii) *$\mathcal{C}_{1,s}^{\perp}$ is exactly 4-divisible if and only if either $w_2(s) = m - 2$ or $w_2(s^{-1}) = m - 2$, where s^{-1} is the only integer in $\{0, \ldots, 2^m - 1\}$ such that $s^{-1}s \equiv 1 \bmod (2^m - 1)$.*

Proof.
(i) This was proved by Helleseth [15].
(ii) Suppose that $w_2(s) < m - 1$. In this case, $\mathcal{C}_{1,s}^{\perp}$ is at least 4-divisible. According to McEliece's theorem (Corollary 2.3) $\mathcal{C}_{1,s}^{\perp}$ is exactly 4-divisible if and only if there exists a pair of integers (u, v) in $\{0, \ldots, 2^m - 1\}$ such that $us + v \equiv 0 \bmod (2^m - 1)$ and $w_2(u) + w_2(v) = 3$. Since $\gcd(s, 2^m - 1) = 1$, we have $w_2(v) \geq 1$. It follows that $(w_2(u), w_2(v)) \in \{(1, 2), (2, 1)\}$.

If $w_2(u) = 1$ and $w_2(v) = 2$, such a pair exists if and only if $w_2(s) = m - 2$; s then lies in the same cyclotomic coset as $2^{m-1} - 2^i - 1$ for some $i \in [0, \ldots, 2^m - 1]$. If $w_2(u) = 2$ and $w_2(v) = 1$, such a pair exists if and only if there exists an element $s' \in Cl(s)$ and two distinct integers i_1 and i_2 in $[0, \ldots, m - 1]$ such that

$$\begin{aligned} & -(2^{i_1} + 2^{i_2})s' \equiv 1 \bmod (2^m - 1) \\ \iff & (2^m - 2^{i_1} - 2^{i_2} - 1)s' \equiv 1 \bmod (2^m - 1). \end{aligned}$$

It follows that s' is the inverse modulo $(2^m - 1)$ of an element whose 2-weight equals $m - 2$. □

We now prove that if $\gcd(2^m - 1, s) = 1$ and if $\mathcal{C}_{1,s}^{\perp}$ is exactly 8-divisible, s should satisfy the following necessary condition.

PROPOSITION 5.4. *Let m and s be two positive integers such that* $\gcd(2^m - 1, s) = 1$. *Let $\mathcal{C}_{1,s}$ be the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, s\}$. If $\mathcal{C}_{1,s}^{\perp}$ is exactly 8-divisible, then s satisfies one of the following conditions:*

(i) *$w_2(s^{-1}) = m - 3$, where s^{-1} is the only integer in $\{0, \ldots, 2^m - 1\}$ such that $s^{-1}s \equiv 1 \bmod (2^m - 1)$;*

(ii) $\lceil \frac{m-2}{2} \rceil \leq w_2(s) \leq m-3$.

Proof. Proposition 5.3 implies that $\mathcal{C}_{1,s}^{\perp}$ is 8-divisible if and only if $w_2(s) \leq m-3$ and $w_2(s^{-1}) \leq m-3$. Let us assume that this condition is satisfied. We now use the same technique as in the previous proof: $\mathcal{C}_{1,s}^{\perp}$ is exactly 8-divisible if and only if there exists a pair of integers $(u,v) \in \{0,\ldots,2^m-1\}$ such that $us+v \equiv 0 \bmod (2^m-1)$ and $w_2(u)+w_2(v)=4$. Since $\gcd(s,2^m-1)=1$, we have that $(w_2(u),w_2(v)) \in \{(1,3),(2,2),(3,1)\}$.

- If $(w_2(u),w_2(v))=(1,3)$, then $w_2(s)=m-3$.
- If $(w_2(u),w_2(v))=(3,1)$, then $w_2(s^{-1})=m-3$ (the proof here is the same as the proof of Proposition 5.3(ii)).
- If $(w_2(u),w_2(v))=(2,2)$, we use inequality (5.2) proved in Corollary 5.2:

$$w_2(u)w_2(s)+w_2(v) \geq m.$$

It follows that

$$w_2(s) \geq \frac{m-2}{2}. \qquad \square$$

Note that Corollary 5.1 and Proposition 5.3 imply that $\mathcal{C}_{1,s}^{\perp}$ is exactly 8-divisible when $w_2(s)=m-3$ or $w_2(s^{-1})=m-3$.

Open problem 5.5. *For any ℓ, $1 \leq \ell \leq \lfloor \frac{m-1}{2} \rfloor$, does there exist an s such that $w_2(s)=m-\ell$ and the cyclic code $\mathcal{C}_{1,s}^{\perp}$ of length (2^m-1) is exactly 2^ℓ-divisible?*

6. Weight divisibility of the code $\mathcal{C}_{1,s}^{\perp}$ of length $(2^{2t+1}-1)$ with $s=2^t+2^i-1$. In his 1968 paper [14], Golomb mentioned a conjecture of Welch stating that for $m=2t+1$, the crosscorrelation function between a binary m-sequence of length (2^m-1) and its decimation by $s=2^t+3$ takes on precisely the three values $-1,-1\pm 2^{t+1}$. Niho [26] stated a similar conjecture for $s=2^t+2^{\frac{t}{2}}-1$ when t is even and $s=2^t+2^{\frac{3t+1}{2}}-1$ when t is odd. These conjectures equivalently assert that, for these values of s, the power function $x \mapsto x^s$ is AB over $\mathbf{F}_{2^m}$. Note that all of these exponents s can be written as 2^t+2^i-1 for some i. Since both Welch's and Niho's functions are APN [11, 10], Corollary 4.3 leads to a new formulation of Welch's and Niho's conjectures.

Conjecture 6.1. *Let $m=2t+1$ be an odd integer. For all u such that $1 \leq u \leq 2^m-1$, we have*

$$w_2((2^t+2^i-1)u \bmod (2^m-1)) \leq t+w_2(u) \tag{6.1}$$

for the following values of i: $i=2$, $i=t/2$ for even t, and $i=(3t+1)/2$ for odd t.

Previously, we proved that condition (6.1) is satisfied in the Welch case ($i=2$) [5, 4]. More recently, Hollmann and Xiang used this formulation for proving Niho's conjecture [16]. Here we focus on all other values of s which can be expressed as $s=2^t+2^i-1$ for some i. We prove that for almost all of these values $\mathcal{C}_{1,s}^{\perp}$ actually contains a codeword whose weight is not divisible by 2^t. This result is derived from both of the following lemmas which give an upper bound on the exact weight divisibility of $\mathcal{C}_{1,s}^{\perp}$.

Lemma 6.2. *Let $m=2t+1$ be an odd integer and $s=2^t+2^i-1$ with $2<i<t-1$. Let $\mathcal{C}_{1,s}$ be the binary cyclic code of length (2^m-1) with defining set $\{1,s\}$. If 2^ℓ denotes the exact divisibility of $\mathcal{C}_{1,s}^{\perp}$, we have*

- *if $t \equiv 0 \bmod i$ and $i \neq t/2$, then $\ell \leq t-1$;*
- *if $t \equiv 1 \bmod i$, then $\ell \leq t-i+2$;*

- *if $t \equiv r \bmod i$ with $1 < r < i$, then $\ell \leq t - i + r$.*

Proof. Let $t = iq + r$ with $r < i$ and $A(u) = (2^t + 2^i - 1)u \bmod 2^m - 1$. McEliece's theorem (Corollary 2.4) implies that $\mathcal{C}_{1,s}^{\perp}$ is at most 2^ℓ-divisible if there exists an integer $u \in \{0, \ldots, 2^m - 1\}$ such that

$$w_2(A(u)) = w_2(u) + 2t - \ell.$$

Here we exhibit an integer u satisfying this condition for the announced values of ℓ.

- We first consider the case $r \neq 0$. Let $u = 2^t + 2^{r-1} \sum_{k=1}^{q} 2^{ik} + 1$. Then $w_2(u) = q + 2$ and we have

$$\begin{aligned} A(u) &= 2^{2t} + 2^{t+r-1} \sum_{k=1}^{q} 2^{ik} + 2^t + 2^{t+i} - 2^t + 2^{r-1} \left(2^{(q+1)i} - 2^i\right) + 2^i - 1 \\ &= 2^{2t} + 2^{t+r-1} \sum_{k=1}^{q} 2^{ik} + 2^{t+i} + (2^{t+i-1} - 2^{i+r-1}) + (2^i - 1). \end{aligned} \tag{6.2}$$

  If $r > 1$, we have for all k such that $1 \leq k \leq q$,

$$t + i < t + r - 1 + ik \leq 2t - 1.$$

  We then deduce that all terms in (6.2) are distinct. It follows that

$$\begin{aligned} w_2(A(u)) &= 1 + q + 1 + (t - r) + i \\ &= w_2(u) + t - r + i. \end{aligned}$$

  If $r = 1$, we obtain

$$A(u) = 2^{2t} + 2^t \sum_{k=2}^{q} 2^{ik} + 2^{t+i+1} + 2^{t+i-1} - 1.$$

  In this case

$$\begin{aligned} w_2(A(u)) &= 1 + (q - 1) + 1 + (t + i - 1) \\ &= w_2(u) + t + i - 2. \end{aligned}$$

- Suppose now that $r = 0$ and $i \neq t/2$. Since $i < t$, we have $q > 2$. Let $u = 2^{t+i} + 2^{t+2} + 2^t + 2^{i+2} \sum_{k=0}^{q-2} 2^{ik} + 1$. Using that $i > 2$, we deduce that, for all $k \leq q - 2$,

$$\begin{aligned} i + 2 + ik &\leq i(q - 1) + 2 \\ &\leq t - i + 2 < t. \end{aligned}$$

  It follows that $w_2(u) = q + 3$. Let us now expand the corresponding $A(u)$:

$$\begin{aligned} A(u) &\equiv 2^{2t+i} + 2^{2t+2} + 2^{2t} + 2^{t+i+2} \sum_{k=0}^{q-2} 2^{ik} + 2^t + 2^{t+2i} - 2^{t+i} + 2^{t+i+2} \\ &\quad -2^{t+2} + 2^{t+i} - 2^t + 2^{i+2} \left(2^{(q-1)i} - 1\right) + 2^i - 1 \\ &= 2^{i-1} + 2 + 2^{2t} + 2^{t+i+2} \sum_{k=1}^{q-2} 2^{ik} + 2^{t+2i} + 2^{t+i+3} + 2^{i+2} \left(2^{(q-1)i} - 1\right) \\ &\quad +2^i - 1 \\ &= 2^{2t} + \sum_{k=0}^{q-3} 2^{t+2+(k+2)i} + 2^{t+2i} + 2^{t+i+3} - 2^{i+2} + 2^i + 2^{i-1} + 1. \end{aligned} \tag{6.3}$$

If $i > 2$, all values of k such that $0 \leq k \leq q-3$ satisfy

$$t + 2i < t + 2 + (k+2)i < 2t.$$

We then deduce that, if $q > 2$, all the terms in (6.3) are distinct except if $i = 3$. It follows that, for any $i > 3$,

$$\begin{aligned} w_2(A(u)) &= 1 + (q-2) + 1 + (t+1) + 3 \\ &= w_2(u) + t + 1. \end{aligned}$$

For $i = 3$, we have

$$A(u) = 2^{2t} + \sum_{k=0}^{q-3} 2^{t+3k+8} + 2^{t+7} - 2^5 + 2^3 + 2^2 + 1.$$

In this case

$$\begin{aligned} w_2(A(u)) &= 1 + (q-2) + (t+2) + 3 \\ &= t + q + 4 \\ &= w(u) + t + 1. \qquad \square \end{aligned}$$

LEMMA 6.3. *Let $m = 2t+1$ be an odd integer $s = 2^t + 2^i - 1$ with $t+1 < i < 2t$. Let $\mathcal{C}_{1,s}$ be the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, s\}$. If 2^ℓ denotes the exact divisibility of $\mathcal{C}_{1,s}^\perp$, we have*

- *if $t+1 < i < \frac{3t+1}{2}$, then $\ell \leq m - i$;*
- *if $\frac{3t+1}{2} < i < 2t-1$, then $\ell \leq 2(m-i) - 1$;*
- *if $i = 2t-1$, then $\ell \leq 3$.*

Proof. Let $A(u) = (2^t + 2^i - 1)u \bmod (2^m - 1)$. Exactly as in the proof of the previous lemma, we exhibit an integer $u \in \{0, \ldots, 2^m - 1\}$ such that

$$w_2(A(u)) = w_2(u) + 2t - \ell$$

for the announced values of ℓ. We write $i = t + j$, where $1 < j < t$.

- We first consider the case $t+1 < i < \frac{3t+1}{2}$. Let $u = 2^t + 2^{j-1} + 1$. Then $w_2(u) = 3$ and

$$\begin{aligned} A(u) &\equiv 2^{2t} + 2^{t+j-1} + 2^t + 2^{2t+j} + 2^{t+2j-1} + 2^{t+j} - 2^t - 2^{j-1} - 1 \\ &= 2^{2t} + 2^{t+2j-1} + 2^{t+j} + 2^{t+j-1} - 1. \end{aligned} \tag{6.4}$$

  Since $j < \frac{t+1}{2}$, we have that $2t > t + 2j - 1$. All the terms in (6.4) are therefore distinct. We deduce

$$\begin{aligned} w_2(A(u)) &= 3 + (t + j - 1) \\ &= w_2(u) + i - 1. \end{aligned}$$

- We now focus on the case $\frac{3t+1}{2} < i \leq 2t-1$. Let $u = 2^t + 2^j + 1$. Then $w_2(u) = 3$ and

$$\begin{aligned} A(u) &= 2^{2t} + 2^{j-1} - 2^t + 2^{t+j} + 2^{2j-t-1} - 2^j + 2^t + 2^{t+j} - 1 \\ &= 2^{2t} + 2^{t+j+1} - 2^{j-1} + 2^{2j-t-1} - 1. \end{aligned} \tag{6.5}$$

Since $\frac{t+1}{2} < j < t$, we have $0 < 2j - t - 1 < j - 1$. If $j \neq t-1$, all the exponents in (6.5) are distinct. It follows that

$$\begin{aligned} w_2(A(u)) &= 1 + (t+2) + (2j - t - 1) \\ &= w_2(u) + 2(i-t) - 1. \end{aligned}$$

If $j = t - 1$, we have

$$A(u) = 2^{2t+1} - 2^{j-1} + 2^{2j-t-1} - 1.$$

In this case

$$\begin{aligned} w_2(A(u)) &= (2t+1) - (t-j) \\ &= w_2(u) + 2t - 3. \end{aligned}$$ □

For $i = 2t - 1$, we actually obtain the exact divisibility of $\mathcal{C}_{1,s}^{\perp}$.

PROPOSITION 6.4. *Let $m > 3$ be an odd integer. The dual of the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, 2^{m-2} + 2^{\frac{m-1}{2}} - 1\}$ is exactly 2^3-divisible.*

Proof. Let $s = 2^{m-2} + 2^{\frac{m-1}{2}} - 1$. The previous lemma implies that $\mathcal{C}_{1,s}^{\perp}$ is at most 2^3-divisible. Since

$$(2^{\frac{m+1}{2}} + 1)s \equiv 2^{\frac{m-3}{2}}(2^{\frac{m-1}{2}} - 1) \bmod (2^m - 1),$$

we obtain that $\gcd(2^m - 1, s)$ divides both $(2^m - 1)$ and $(2^{\frac{m-1}{2}} - 1)$ which are coprime. It follows that $\gcd(2^m - 1, s) = 1$.

From Proposition 5.3 we know that the divisibility of $\mathcal{C}_{1,s}^{\perp}$ is less than 2^3 if either $w_2(s) \geq m - 2$ or $w_2(s^{-1}) \geq m - 2$. None of these conditions is satisfied here: $w_2(s) = \frac{m+1}{2}$ and s^{-1} lies in the same cyclotomic coset as $2^{m-2} - 2^{\frac{m-1}{2}} - 1$ since

$$\begin{aligned} (2^{m-2} - 2^{\frac{m-1}{2}} - 1)(2^{m-2} + 2^{\frac{m-1}{2}} - 1) &\equiv (2^{m-2} - 1)^2 - 2^{m-1} \bmod (2^m - 1) \\ &\equiv 2^{m-4} \bmod (2^m - 1). \end{aligned}$$

It follows that $w_2(s^{-1}) = m - 3$ and therefore that $\mathcal{C}_{1,s}^{\perp}$ is exactly 8-divisible. □

From Lemmas 6.2 and 6.3 we deduce that $\mathcal{C}_{1,s}^{\perp}$ is not 2^t-divisible for most values of $s = 2^t + 2^i - 1$.

THEOREM 6.5. *Let $m = 2t + 1$ be an odd integer and let $s = 2^t + 2^i - 1$ with $i \in \{1, \ldots, 2t\}$. Let $\mathcal{C}_{1,s}$ be the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, s\}$. The only values of i such that $\mathcal{C}_{1,s}^{\perp}$ is 2^t-divisible are $1, 2, \frac{t}{2}, t, t+1, \frac{3t+1}{2}, 2t$, and maybe $t - 1$.*

Proof. If $i \notin \{1, 2, \frac{t}{2}, t-1, t, t+1, \frac{3t+1}{2}, 2t\}$, $\mathcal{C}_{1,s}^{\perp}$ is not 2^t-divisible since the upper bounds given in both previous lemmas are strictly less than t. Moreover, $\mathcal{C}_{1,s}^{\perp}$ is 2^t-divisible for $i \in \{1, 2, \frac{t}{2}, t, t+1, \frac{3t+1}{2}, 2t\}$:

- $i = 1$ corresponds to a quadratic value of s.
- $i = 2$ corresponds to the Welch's function.
- $i = t$ corresponds to the inverse of a quadratic exponent since $(2^{t+1} - 1)(2^t + 1) \equiv 2^t \bmod 2^m - 1$.
- $i = t + 1$ corresponds to a Kasami's function since $2^t(2^{t+1} + 2^t - 1) \equiv 2^{2t} - 2^t + 1 \bmod 2^m - 1$.
- $i = 2t$ gives an s which is in the same 2-cyclotomic coset as $2^{t+1} - 1$.
- $i = \frac{t}{2}$ or $i = \frac{3t+1}{2}$ corresponds to Niho's function. □

The only unresolved case is then $i = t - 1$. In accordance with our simulation results we formulate the following conjecture.

CONJECTURE 6.6. *Let $m = 2t + 1$ be an odd integer, $m > 3$. The dual of the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, 2^t + 2^{t-1} - 1\}$ is exactly 2^t-divisible.*

Note that an equivalent assertion is that the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, 2^{t+2} + 3\}$ is exactly 2^t-divisible, since $2^{t+2} + 3$ lies in the same cyclotomic coset as the inverse of $2^t + 2^{t-1} - 1$. We checked this conjecture by computer for $m \leq 39$. Note that it is obviously satisfied for $m = 5$ and $m = 7$ since the function $x \mapsto x^s$ for $s = 2^t + 2^{t-1} - 1$ corresponds, resp., to a quadratic function and to the Welch function. On the contrary it is known that the corresponding function is not APN when 3 divides m since $\mathcal{C}_{1,s}$ has minimum distance 3 in this case.

PROPOSITION 6.7 (see [8]). *Let $m = 2t + 1$ be an odd integer, $m > 3$. The binary cyclic code of length $(2^m - 1)$ with defining set $\{1, 2^t + 2^{t-1} - 1\}$ has minimum distance 3 if and only if $m \equiv 0 \bmod 3$. In this case, the number of codewords of weight 3 is*

$$B_3 = 2^m - 1.$$

Proof. This comes from [8, Thm. 5]. This cyclic code has minimum distance 3 if and only if

$$\gcd(m, t - 1) = 1.$$

Since $m = 2t - 1$, it follows that $\gcd(m, t - 1) = 3$ when $m \equiv 0 \bmod 3$ and that $\gcd(m, t - 1) = 1$ otherwise. □

Table 6.1 gives the weight distributions of $\mathcal{C}_{1,s}^{\perp}$, where $s = 2^t + 2^{t-1} - 1$ for $m \in \{9, 11, 13\}$ and the corresponding number B_3 (resp., B_4) of codewords of weight 3 (resp., 4) in $\mathcal{C}_{1,s}$.

TABLE 6.1
Weight distribution of some codes $\mathcal{C}_{1,s}^{\perp}$ with $s = 2^t + 2^{t-1} - 1$.

m	s	B_3	B_4	w	A_w
9	23	511	9709	224	4599
				240	55188
				256	146657
				272	55188
				288	511
11	47	0	180136	960	45034
				992	900680
				1024	2368379
				1056	835176
				1088	45034
13	95	0	2981524	3968	745381
				4032	14055756
				4096	38030813
				4160	13531532
				4224	745381

7. Weight divisibility of $\mathcal{C}_{1,s}^{\perp}$ when m is not a prime. We now focus on the binary cyclic codes $\mathcal{C}_{1,s}$ of length $(2^m - 1)$ when m is not a prime. We show that in this case the weight divisibility of $\mathcal{C}_{1,s}^{\perp}$ is closely related to the exact weight divisibility of the cyclic code $\mathcal{C}_{1,s_0}^{\perp}$ of length $(2^g - 1)$ where g is a divisor of m and $s_0 = s \bmod (2^g - 1)$.

7.1. A general result. We first derive a lower and an upper bound on the exact weight divisibility of $\mathcal{C}_{1,s}^{\perp}$ from the exact weight divisibility of the code $\mathcal{C}_{1,s_0}^{\perp}$ of length (2^g-1). These bounds allow us to give a necessary condition on the decimations which provide preferred pairs of m-sequences of length (2^m-1) when m is not a prime. This general condition generalizes the Sarwate–Pursley conjecture [31, 25] on the nonexistence of preferred pairs of m-sequences of length (2^m-1) when 4 divides m.

THEOREM 7.1. *Let g be a divisor of m. Let $\mathcal{C}_{1,s}$ be the binary cyclic code of length (2^m-1) with defining set $\{1,s\}$ and $\mathcal{C}_0$ the binary cyclic code of length (2^g-1) with defining set $\{1,s_0\}$, where $s_0 = s \bmod (2^g-1)$. Assume that $\mathcal{C}_0^{\perp}$ is exactly 2^ℓ-divisible. Then we have the following:*

(i) *$\mathcal{C}_{1,s}^{\perp}$ is 2^ℓ-divisible. In particular, if there exists i such that $s \equiv 2^i \bmod (2^g-1)$, then $\mathcal{C}_{1,s}^{\perp}$ is 2^{g-1}-divisible.*

(ii) *$\mathcal{C}_{1,s}^{\perp}$ is not $2^{\frac{m}{g}(\ell+1)}$-divisible.*

Proof. Let $s = s_0 + a(2^g-1)$. Here we use McEliece's theorem as expressed in Corollary 2.3.

(i) Let u and v be two integers in $\{0,\dots,2^m-1\}$ such that $us+v = k(2^m-1)$. Then we have

$$us + v = au(2^g-1) + (us_0+v) = k(2^m-1).$$

This implies that

$$us_0 + v \equiv 0 \bmod (2^g-1).$$

Let $u_0 = u \bmod (2^g-1)$ and $v_0 = v \bmod (2^g-1)$. For any integer x, we have $w_2(x) \geq w_2(x \bmod (2^g-1))$: by writing $x = x_2 2^g + x_1$ with $0 \leq x_1 < 2^g$, we obtain that $x \bmod (2^g-1) = x_1 + x_2$. It follows that

$$\begin{aligned} w_2(x \bmod (2^g-1)) &= w_2(x_1+x_2) \\ &\leq w_2(x_1) + w_2(x_2) = w_2(x). \end{aligned}$$

This implies that

$$w_2(u) + w_2(v) \geq w_2(u_0) + w_2(v_0) \geq \ell + 1$$

since $\mathcal{C}_0^{\perp}$ is 2^ℓ-divisible.

(ii) If $\mathcal{C}_0^{\perp}$ is exactly 2^ℓ-divisible, there exists a pair of integers (u_0,v_0) with $u_0 \leq 2^g-1$ and $v_0 \leq 2^g-1$ such that

$$u_0 s_0 + v_0 \equiv 0 \bmod 2^g-1 \text{ and } w_2(u_0) + w_2(v_0) = \ell + 1.$$

Let us now consider both integers u and v defined by

$$u = u_0 \frac{2^m-1}{2^g-1} \text{ and } v = v_0 \frac{2^m-1}{2^g-1}.$$

For $s = s_0 + a(2^g-1)$, the pair (u,v) satisfies

$$\begin{aligned} us + v &= ua(2^g-1) + us_0 + v \\ &= u_0 a(2^m-1) + \frac{2^m-1}{2^g-1}(u_0 s_0 + v_0) \\ &\equiv 0 \bmod (2^m-1). \end{aligned}$$

Since $\frac{2^m-1}{2^g-1} = \sum_{i=0}^{m/g-1} 2^{ig}$ and both u_0 and v_0 are less than $2^g - 1$, we have

$$w_2(u) + w_2(v) = \frac{m}{g}\left(w_2(u_0) + w_2(v_0)\right) = \frac{m}{g}(\ell + 1).$$

We then deduce that $\mathcal{C}_{1,s}^{\perp}$ is not $2^{\frac{m}{g}(\ell+1)}$-divisible. □

COROLLARY 7.2. *Let g be a divisor of m. Let $\mathcal{C}_{1,s}$ be the binary cyclic code of length (2^m-1) with defining set $\{1, s\}$ and $\mathcal{C}_0$ the binary cyclic code of length (2^g-1) with defining set $\{1, s_0\}$, where $s_0 = s \bmod (2^g-1)$. If $\mathcal{C}_{1,s}^{\perp}$ is $2^{\lfloor \frac{m}{2} \rfloor}$-divisible, then $\mathcal{C}_0^{\perp}$ is $2^{\lfloor \frac{g}{2} \rfloor}$-divisible.*

Proof. We denote by 2^ℓ the exact divisibility of $\mathcal{C}_0^{\perp}$. Following Theorem 7.1(ii), we have that $\mathcal{C}_{1,s}^{\perp}$ is not $2^{\frac{m}{g}(\ell+1)}$-divisible. If $\mathcal{C}_{1,s}^{\perp}$ is $2^{\lfloor \frac{m}{2} \rfloor}$-divisible, it therefore follows that

$$\left\lfloor \frac{m}{2} \right\rfloor \leq \frac{m}{g}(\ell + 1) - 1.$$

For odd m, this gives

$$\ell + 1 \geq \frac{g(m+1)}{2m} > \frac{g-1}{2}$$

since $(m+1)g > m(g-1)$.

For even m, we similarly get

$$\ell + 1 \geq \frac{g(m+2)}{2m} > \frac{g}{2} \geq \left\lfloor \frac{g}{2} \right\rfloor.$$

This implies in both cases that $\ell \geq \lfloor \frac{g}{2} \rfloor$; $\mathcal{C}_0^{\perp}$ is then $2^{\lfloor \frac{g}{2} \rfloor}$-divisible. □

We now deduce a necessary condition on the values of the decimations which provide preferred pairs of m-sequences (or equivalently on the exponents which correspond to AB power permutations when m is odd).

PROPOSITION 7.3. *Let m and s be two positive integers such that $\gcd(2^m-1, s) = 1$ and s is not a power of 2. The pair formed by an m-sequence of length (2^m-1) and its decimation by s is not preferred if there exists a divisor g of m with $g > 2$ satisfying one of the following conditions:*

1. $\exists i,\ 0 \leq i < g,\ \ s \equiv 2^i \bmod (2^g-1)$;
2. $s_0 = s \bmod (2^g-1) \neq 2^i$ *and the dual of the cyclic code of length (2^g-1) with defining set $\{1, s_0\}$ is not $2^{\lfloor \frac{g}{2} \rfloor}$-divisible.*

Proof. Theorems 4.1 and 4.4 provide a necessary condition for obtaining a preferred crosscorrelation: $\mathcal{C}_{1,s}^{\perp}$ has to be $2^{\lfloor \frac{m}{2} \rfloor}$-divisible and the number B_3 of codewords of weight 3 in $\mathcal{C}_{1,s}$ should be

$$\begin{aligned} B_3 &= \frac{(2^m-1)}{3} \text{ if } m \text{ is even} \\ &= 0 \text{ if } m \text{ is odd.} \end{aligned}$$

When $s \equiv 2^i \bmod (2^g-1)$, it is known [8] that the cyclic code $\mathcal{C}_{1,s}$ has minimum distance 3 and that the number B_3 of codewords of weight 3 satisfies

$$B_3 \geq \frac{(2^m-1)(2^{g-1}-1)}{3}.$$

This implies that the crosscorrelation is not preferred if $g > 2$.

If $s_0 = s \bmod (2^g - 1)$ is such that the dual of the cyclic code of length $(2^g - 1)$ with defining set $\{1, s_0\}$ is not $2^{\lfloor \frac{g}{2} \rfloor}$-divisible, $\mathcal{C}_{1,s}^{\perp}$ is not $2^{\lfloor \frac{m}{2} \rfloor}$-divisible according to Corollary 7.2. □

This proposition is a generalization of the following result conjectured by Sarwate and Pursley [31] and recently proved in [25].

COROLLARY 7.4 (see [31, 25]). *There is no pair of preferred m-sequences of length* $(2^m - 1)$ *when* 4 *divides* m.

Proof. We consider the pair formed by an m-sequence of length $(2^m - 1)$ and its decimation by s. Let $s_0 = s \bmod 15$. Since 4 divides m, we should have $s_0 \in \{1, 2, 4, 8\} \cup \{7, 11, 13, 14\}$; otherwise s and $2^m - 1$ are not coprime. The previous proposition then applies with $g = 4$ for any such s: condition 1 is satisfied when $s_0 \in \{1, 2, 4, 8\}$ and condition 2 holds when $s_0 \in \{7, 11, 13, 14\}$ since the dual of the cyclic code of length 15 with defining set $\{1, 7\}$ is not 4-divisible. □

7.2. Exact weight divisibility of the code $\mathcal{C}_{1,s}^{\perp}$ of length $(2^{2t} - 1)$ with $s \equiv 2^i \bmod (2^t - 1)$. When $m = 2t$ and $s \equiv 2^i \bmod (2^t - 1)$, all the weights of $\mathcal{C}_{1,s}^{\perp}$ are divisible by 2^{t-1}. This particular case of Theorem 7.1(i) was already treated in [26] and in [12, Lemma 1]. We now prove that this bound actually corresponds to the exact divisibility of $\mathcal{C}_{1,s}^{\perp}$.

THEOREM 7.5. *Let $m = 2t$ be an even integer and let s be an integer such that*

$$s \equiv 2^i \bmod (2^t - 1) \text{ with } 0 \le i < t$$

and s is not a power of 2. Let $\mathcal{C}_{1,s}$ be the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, s\}$. Then $\mathcal{C}_{1,s}^{\perp}$ is exactly 2^{t-1}-divisible.

Proof. Since Theorem 7.1(i) implies that the weights of $\mathcal{C}_{1,s}^{\perp}$ are divisible by 2^{t-1}, it is sufficient to find a pair (u, v) such that $us + v \equiv 0 \bmod (2^m - 1)$ and $w_2(u) + w_2(v) = t$. By cyclotomic equivalence, we have only to consider the values of s such that

$$s = a(2^t - 1) + 2^{t-1},$$

where $a \le 2^t$ and $a \notin \{0, 2^{t-1}\}$ (otherwise s is a power of 2).

- If $a < 2^{t-1}$, we write $a = 2^j a'$ with a' odd. Then s lies in the same 2-cyclotomic coset as $s' = a'(2^t - 1) + 2^{t-j-1}$. Let us choose $u = 2^t + 1 - 2^{t-j-1}$. Then we have

$$\begin{aligned} us' &\equiv a'(2^{2t} - 1) + 2^{t-j-1}\left[-a'(2^t - 1) + 2^t + 1 - 2^{t-j-1}\right] \bmod (2^{2t} - 1) \\ &\equiv 2^{t-j-1}\left[2^t(1 - a') + (a' + 1 - 2^{t-j-1})\right] \bmod (2^{2t} - 1). \end{aligned}$$

  Then $us' + v \equiv 0 \bmod 2^m - 1$ implies that

$$v \equiv 2^{t-j-1}\left[2^t(a' - 1) + (2^{t-j-1} - 1 - a')\right] \bmod (2^m - 1).$$

  Therefore, we obtain

$$\begin{aligned} w_2(v) &\le w_2\left(2^t(a' - 1) + (2^{t-j-1} - 1 - a')\right) \\ &\le w_2(a' - 1) + w_2(2^{t-j-1} - 1 - a') \\ &\le w_2(a' - 1) + t - j - 1 - w_2(a') \\ &\le t - j - 2 \end{aligned}$$

  since $a' \le 2^{t-j-1} - 1$ and a' is odd. Using that $w_2(u) = j + 2$, we finally get

$$w_2(u) + w_2(v) \le t.$$

- If $2^{t-1} < a \leq 2^t$, we choose $u = 1$. By writing

$$s = (a-1)2^t + (2^t - 1) - (a - 1 - 2^{t-1}),$$

we obtain that

$$w_2(s) = w_2(a-1) + t - w_2(a - 1 - 2^{t-1}).$$

Since $2^{t-1} \leq a-1 \leq 2^t-1$, we clearly have that $w_2(a-1-2^{t-1}) = w_2(a-1)-1$. It follows that

$$w_2(s) = w_2(a-1) + t - (w_2(a-1) - 1) = t + 1.$$

For $v = 2^m - 1 - s$, we then have $w_2(u) + w_2(v) = t$. □

Most values of s for which the weight distribution of $\mathcal{C}_{1,s}^{\perp}$ is completely determined satisfy $s \equiv 2^i \bmod (2^t - 1)$. Theorem 7.5 most notably covers the following well-known cases:

(i) $s = 2^t + 1$ since $s = (2^t - 1) + 2$. In this case the weights of $\mathcal{C}_{1,s}^{\perp}$ take the following values: $2^{m-1} - 2^{t-1}, 2^{m-1}, 2^{m-1} + 2^{t-1}$ [19].

(ii) $s = 2^t + 3$ since $s = (2^t - 1) + 4$. The weights of $\mathcal{C}_{1,s}^{\perp}$ take the following values: $2^{m-1} - 2^t - 2^{t-1}, 2^{m-1} - 2^t, 2^{m-1} + 2^{t-1}, 2^{m-1}, 2^{m-1} - 2^{t-1}$ [15, Thm. 4.8].

(iii) $s = \sum_{i=0}^{t} 2^{ik}$, where $0 < k < t$ and $\gcd(m, k) = 1$. Since k is odd, we have

$$\begin{aligned} s = \sum_{i=0}^{t} 2^{ik} &\equiv \frac{2^{(t+1)k} - 1}{2^k - 1} \bmod (2^m - 1) \\ &\equiv \frac{2^{t+k} - 1}{2^k - 1} \bmod (2^m - 1). \end{aligned}$$

It follows that

$$s \equiv 2^k d(2^t - 1) + 1 \bmod (2^m - 1),$$

where d satisfies $d(2^k - 1) \equiv 1 \bmod (2^m - 1)$. The weights of $\mathcal{C}_{1,s}^{\perp}$ take the following values: $2^{m-1} - 2^t, 2^{m-1} - 2^{t-1}, 2^{m-1}, 2^{m-1} + 2^{t-1}$ [12, Prop. 1].

(iv) $s = (2^t + 1)(2^{\frac{t}{2}} - 1) + 2$ when t is even. In this case, $s = (2^{\frac{t}{2}} - 1)(2^t - 1) + 2^{\frac{t}{2}+1}$. The weights of $\mathcal{C}_{1,s}^{\perp}$ take the following values: $2^{m-1} - 2^{\frac{3t}{2}-1}, 2^{m-1} - 2^{t-1}, 2^{m-1}, 2^{m-1} + 2^{t-1}$ [26].

(v) $s = \frac{(2^m-1)}{3} + 2^i$ with $i \in \{0, 1\}$ when t is odd. In this case, 3 divides $(2^t + 1)$. It follows that

$$s = \frac{(2^t + 1)}{3}(2^t - 1) + 2^i.$$

The weights of $\mathcal{C}_{1,s}^{\perp}$ take the following values [15, Thm. 4.11]:

- $2^{m-1} - \frac{2^{t-1}(2^t+1)}{3}, 2^{m-1} - \frac{2^t(2^{t-1}-1)}{3}, 2^{m-1} - 2^t, 2^{m-1} - 2^{t-1}, 2^{m-1}, 2^{m-1} + 2^{t-1}$, when $\frac{2^{m-i}(2^m-1)}{3} \equiv 0 \bmod 3$.
- $2^{m-1} - \frac{2^{t+1}(2^{t-2}+1)}{3}, 2^{m-1} - \frac{2^t(2^{t-1}-1)}{3}, 2^{m-1} - 2^t, 2^{m-1} - 2^{t-1}, 2^{m-1}, 2^{m-1} + 2^{t-1}$, when $\frac{2^{m-i}(2^m-1)}{3} \equiv 1 \bmod 3$.

Tables 7.1, 7.2, and 7.3 give the complete weight distribution of all codes $\mathcal{C}_{1,s}^{\perp}$ of length $(2^m - 1)$ for $m \in \{6, 8, 10\}$ when s satisfies $s \equiv 2^i \bmod (2^{\frac{m}{2}} - 1)$.

TABLE 7.1
Weight distribution of $\mathcal{C}_{1,s}^{\perp}$ *with* $s \equiv 2^i \bmod (2^{\frac{m}{2}}-1)$ *for* $m=6$.

	A_w							
s	20	24	28	32	36	B_3	B_4	ref.
9			252	63	196	63	945	(i)
11, 23	126	252	756	1827	1134	84	252	(ii),(v)
15		588	504	1827	1176	63	63	(iii)

TABLE 7.2
Weight distribution of $\mathcal{C}_{1,s}^{\perp}$ *with* $s \equiv 2^i \bmod (2^{\frac{m}{2}}-1)$ *for* $m=8$.

	A_w								
s	96	104	112	120	128	136	B_3	B_4	ref.
17				2040	255	1800	595	37485	(i)
19, 47		2040	2040	16320	22695	22440	595	3825	(ii)
31, 91			10200	4080	30855	20400	595	1785	(iii)
53	1020			24480	15555	24480	595	6885	(iv)
23, 61	510		5100	14280	23205	22440	595	4335	

TABLE 7.3
Weight distribution of $\mathcal{C}_{1,s}^{\perp}$ *with* $s \equiv 2^i \bmod (2^{\frac{m}{2}}-1)$ *for* $m=10$.

	A_w								
s	320	336	352	448	464	480	496	512	528
33							16368	1023	15376
35					40920	16368	245520	377487	368280
63, 219						169136	32736	508431	338272
171		2046	1023			41261	225060	471603	307582
343	1023		2046			40920	225060	472626	306900
39, 159				5115	10230	77066	196416	390786	368962
47, 109, 125, 221				5115	10230	87978	163680	423522	358050
101, 157					30690	57288	184140	418407	358050
187			93		20460	82863	163680	422499	358980

s	B_3	B_4	Ref.
33	5115	1304325	(i)
35	5456	81840	(ii)
63, 219	5115	35805	(iii)
171	20460	1616340	(iv)
343	20801	1677720	(iv)
39, 159	5115	71610	
47, 109, 125, 221	5456	76725	
101, 157	5456	71610	
187	5456	92070	

OPEN PROBLEM 7.6. *Let* $m=2t$ *be an even integer and let* s *be an integer such that*

$$s \equiv 2^i \bmod (2^t-1) \text{ with } 0 \le i < t.$$

Let $\mathcal{C}_{1,s}$ *be the binary cyclic code of length* (2^m-1) *with defining set* $\{1,s\}$. *Let* $A=(A_0,\ldots,A_{2^m-1})$ *denote the weight enumerator of* $\mathcal{C}_{1,s}^{\perp}$. *Find the largest integer* w_0

such that

$$A_w = A_{2^m-w} = 0 \text{ for all } w \text{ such that } 0 < w < w_0.$$

7.3. $2^{\frac{m}{2}}$-divisible cyclic codes of length $(2^m - 1)$ when m is a multiple of 4. By combining Theorem 7.5 and Corollary 7.2 we are now able to exhibit a necessary condition on s under which the cyclic code $\mathcal{C}_{1,s}^{\perp}$ of length $(2^m - 1)$ is $2^{\frac{m}{2}}$-divisible. This condition depends on the value of the highest power of 2 which divides m.

PROPOSITION 7.7. *Let $m = 2^a m'$ with m' odd and $a \geq 2$. Let s be a positive integer such that $\gcd(2^m - 1, s) = 1$ and let $\mathcal{C}_{1,s}$ be the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, s\}$. If $\mathcal{C}_{1,s}^{\perp}$ is $2^{\frac{m}{2}}$-divisible, then*

$$s \equiv 2^i \bmod (2^{2^a} - 1) \text{ for some } i$$

and the number B_3 of codewords of weight 3 in $\mathcal{C}_{1,s}$ satisfies

$$B_3 \geq \frac{(2^m - 1)(2^{2^a-1} - 1)}{3}.$$

Proof. Assume that $\mathcal{C}_{1,s}^{\perp}$ is $2^{\frac{m}{2}}$-divisible. For $j \in \{2, \ldots, a\}$, we set $s_j = s \bmod (2^{2^j} - 1)$ and we denote by $\mathcal{C}_j$ the binary cyclic code of length $(2^{2^j} - 1)$ with defining set $\{1, s_j\}$. From Corollary 7.2 we have that $\mathcal{C}_a^{\perp}$ is $2^{2^{a-1}}$-divisible.

We now prove by induction on j that if $\mathcal{C}_j^{\perp}$ is $2^{2^{j-1}}$-divisible, then s_j is a power of 2.

- If $j = 2$, we have that $s_2 \notin \{3, 6, 9, 12\} \cup \{5, 10\}$ since $\gcd(s, 2^m - 1) = 1$ implies that $\gcd(s_{j-1}, 2^4 - 1) = 1$. Moreover, if $s_2 \in \{7, 11, 13, 14\}$, $\mathcal{C}_2$ is not 4-divisible. It follows that $s_2 \in \{1, 2, 4, 8\}$.
- Induction step: Let us suppose that $\mathcal{C}_j^{\perp}$ is $2^{2^{j-1}}$-divisible. According to Corollary 7.2 we have that $\mathcal{C}_{j-1}^{\perp}$ is $2^{2^{j-2}}$-divisible. By an induction hypothesis s_{j-1} is a power of 2, i.e.,

  $$s_j \equiv 2^i \bmod (2^{2^{j-1}} - 1) \text{ for some } i.$$

  Now Theorem 7.5 implies that, in this case, $\mathcal{C}_j$ is exactly $2^{2^{j-1}-1}$-divisible if s_j is not a power of 2.

We now deduce that if $\mathcal{C}_a^{\perp}$ is $2^{2^{a-1}}$-divisible, then

$$s \equiv 2^i \bmod (2^{2^a} - 1) \text{ for some } i. \qquad \square$$

When m is a power of 2, Proposition 7.7 implies the following corollary.

COROLLARY 7.8. *Let $\mathcal{C}_{1,s}$ be the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, s\}$ (s is not a power of 2). If m is a power of 2 and if $\gcd(2^m - 1, s) = 1$, then $\mathcal{C}_{1,s}^{\perp}$ is not $2^{\frac{m}{2}}$-divisible.*

By using Corollary 4.5, we see that this result actually corresponds to the following weak version of the Helleseth conjecture [15] which was proved by Calderbank, McGuire, and Poonen [3].

COROLLARY 7.9 (see [15, 3]). *If m is a power of 2, then there are no pairs of binary m-sequences of length $(2^m - 1)$ with crosscorrelation values -1, $-1 + 2D$, $-1 - 2D$.*

When 4 divides m (and m is not a power of 2) Proposition 7.7 allows us to find all values of s for which $\mathcal{C}_{1,s}^{\perp}$ is $2^{\frac{m}{2}}$-divisible very fast, even for large values of m. We search for all such values for $m \in \{12, 10, 24\}$ and our numerical results lead us to formulate the following conjecture.

CONJECTURE 7.10. *Let $m = 2^a m'$ with $a \geq 2$, m' odd, and $m' > 1$. Let s be a positive integer such that $\gcd(s, 2^m - 1) = 1$ (s is not a power of 2) and let $\mathcal{C}_{1,s}$ be the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, s\}$. The cyclic code $\mathcal{C}_{1,s}^{\perp}$ is $2^{\frac{m}{2}}$-divisible if and only if either s or s^{-1} takes one of the following values (up to cyclotomic equivalence):*

$$2^{i2^a} + 1 \quad or \quad 2^{i2^{a+1}} - 2^{i2^a} + 1$$

with $1 \leq i \leq \lfloor \frac{m'}{2} \rfloor$.

It is known that for these values of s, $\mathcal{C}_{1,s}^{\perp}$ is exactly 2^{ℓ}-divisible with $\ell = \frac{m}{2} - 1 + 2^{a-1} \gcd(m', i)$ [13, 19]. The previous conjecture equivalently asserts that these values are the only decimations which provide a symmetric 3-valued crosscorrelation, i.e., a crosscorrelation function which takes its values in $\{-1, -1 + 2D, -1 - 2D\}$.

7.4. Dobbertin's function. We now obtain an upper bound on the divisibility of the weights of $\mathcal{C}_{1,s}^{\perp}$ in the following particular case.

PROPOSITION 7.11. *Let $\mathcal{C}_{1,s}$ be the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, s\}$. Let g be a divisor of m such that s satisfies:*

$$s \equiv -s_0 \bmod \frac{2^m - 1}{2^g - 1} \text{ with } 0 < s_0 < \frac{2^m - 1}{2^g - 1}.$$

Then $\mathcal{C}_{1,s}^{\perp}$ is not $2^{g(w_2(s_0)+1)}$-divisible.

Proof. Here we use McEliece's theorem as formulated in Corollary 2.4. Let $u = 2^g - 1$. Then we have

$$A(u) = us \bmod 2^m - 1 = (2^m - 1) - (2^g - 1)s_0.$$

We obtain that

$$w_2(A(u)) = m - w_2((2^g - 1)s_0).$$

Since $w_2((2^g - 1)s_0) \leq g w_2(s_0)$, this implies that

$$\begin{aligned} w_2(A(u)) &\geq m - g w_2(s_0) \\ &\geq w_2(u) + m - g(w_2(s_0) + 1). \end{aligned}$$

We then deduce that $\mathcal{C}_{1,s}^{\perp}$ is not $2^{w_2(u)(w_2(s_0)+1)}$-divisible. □

COROLLARY 7.12. *Let m be an odd integer. If there exists a divisor g of m such that s satisfies*

$$s \equiv -s_0 \bmod \frac{2^m - 1}{2^g - 1} \text{ with } 0 < s_0 < \frac{2^m - 1}{2^g - 1}$$

and

$$w_2(s_0) \leq \frac{1}{2}\left(\frac{m}{g} - 3\right),$$

then the power function $x \mapsto x^s$ is not AB on $\mathbf{F}_{2^m}$.

The third author conjectured that for $m = 5g$ the power function $x \mapsto x^s$ with $s = 2^{4g} + 2^{3g} + 2^{2g} + 2^g - 1$ is APN on $\mathbf{F}_{2^m}$ [10]. The previous corollary implies the following.

PROPOSITION 7.13. *Let m be an odd integer such that $m = 5g$. The power function $x \mapsto x^s$ with $s = 2^{4g} + 2^{3g} + 2^{2g} + 2^g - 1$ is not AB on $\mathbf{F}_{2^m}$.*

Proof. Since $s = \frac{2^{5g}-1}{2^g-1} - 2$, we apply the previous corollary with $s_0 = 2$ and $m/g = 5$ using that

$$w_2(s_0) = 1 = \frac{1}{2}\left(\frac{m}{g} - 3\right). \qquad \square$$

Note that Proposition 7.11 implies that, for $m = 5g$ and $s = 2^{4g}+2^{3g}+2^{2g}+2^g-1$, $\mathcal{C}_{1,s}^{\perp}$ is not 2^{2g}-divisible. This means, for example, that for $m = 15$ and $s \in Cl(3657)$, $\mathcal{C}_{1,s}^{\perp}$ is at most 2^5-divisible; this bound actually corresponds to the exact divisibility of the code.

7.5. Numerical results. We now give some examples for $m = 10$ and 14. As above, $\mathcal{C}_{1,s}$ denotes the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, s\}$ and 2^ℓ denotes the exact weight divisibility of $\mathcal{C}_{1,s}^{\perp}$. Table 7.4 recalls some values of s for which the value of ℓ is known.

Tables 7.5 and 7.6 compare the true exact weight divisibility of $\mathcal{C}_{1,s}^{\perp}$ (given in the second column of each table) with the theoretical bounds derived from the previous results.

$m = 10$.

- We always have $\ell \le 10 - w_2(s)$ (Corollary 5.1) and if $\gcd(s, 1023) = 1$, we also get $\ell \le 10 - w_2(s^{-1})$, where s^{-1} is defined by $ss^{-1} \equiv 1 \bmod 1023$. Maoreover, Proposition 5.3 implies that if $w_2(s) > 8$ and $w_2(s^{-1}) > 8$, we have $\ell \ge 3$.
- If $\gcd(s, 1023) = d > 1$, we have $\ell \le w_2(\frac{2^m-1}{d}) - 1$. This is derived from $us + v \equiv 0 \bmod 1023$ with $u = \frac{2^m-1}{d}$ and $v = 0$. Note that if s and 1023 are not coprime, $\ell \le 4$ since the 2-weight of any divisor of 1023 is at most 4.
- If $s \bmod 31 \in \{1, 2, 4, 8, 16\}$, then $\ell = 4$ (Theorem 7.5).
- If $s \bmod 31 \in \{15, 23, 27, 29, 30\}$, then $\ell \le 3$. This comes from Theorem 7.1 using the fact that the code $\mathcal{C}_{1,15}^{\perp}$ of length 31 is not 4-divisible.
- Proposition 5.4 implies that $\ell \ge 4$ when $\gcd(2^m - 1, s) = 1$, $w_2(s) \le 3$, and $w_2(s^{-1}) \le 6$.

TABLE 7.4

Exact weight divisibility of the duals of some cyclic codes of length $(2^m - 1)$ with defining set $\{1, s\}$.

s	ℓ	Ref.
$2^i + 1$, $1 \le i \le \lfloor \frac{m}{2} \rfloor$	$\frac{m+\gcd(m,i)}{2} - 1$ if $\frac{m}{\gcd(m,i)}$ is odd $\frac{m}{2} - 1$ if $\frac{m}{\gcd(m,i)}$ is even	[13, 19]
$2^{2i} - 2^i + 1$, $2 \le i \le \lfloor \frac{m}{2} \rfloor$	$\frac{m+\gcd(m,i)}{2} - 1$ if $\frac{m}{\gcd(m,i)}$ is odd $\frac{m}{2} - 1$ if $\frac{m}{\gcd(m,i)}$ is even	[19]
$\frac{(2^m-1)}{3} + 2^i$, m even	$\frac{m}{2} - 1$	[15]
$2^{\frac{m}{2}} + 2^{\frac{m}{4}} + 1$, $m \equiv 0 \bmod 4$	$\frac{m}{2} - 1$	[12]
$2^{\frac{m}{2}} + 2^{\frac{m+2}{2}} + 1$, $m \equiv 2 \bmod 4$	$\frac{m}{2} - 1$	[9]
$2^{\frac{m+2}{2}} + 3$, $m \equiv 2 \bmod 4$	$\frac{m}{2} - 1$	[9]

TABLE 7.5
Exact weight divisibility of $\mathcal{C}_{1,s}^{\perp}$ for $m = 10$.

s (representatives of cosets)	ℓ		Argument
511	1	$\ell = 1$	$w_2(s) = 9$
31 93 155 341	2	$\ell = 1$	31 divides $\gcd(1023, s)$
173 179 255 383 447 479 495	2	$\ell = 2$	$w_2(s) = 8$ or $w_2(s^{-1}) = 8$
15 23 27 29 61 77 85 89 91 123 151 213 215 247	3	$\ell = 3$	$s \bmod 31 \in \{15, 23, 27, 29, 30\}$
7 53 59 73 127 167 191 223 235 239 251 253 351 367 375 379 439	3	$\ell = 3$	$w_2(s) = 7$ or $w_2(s^{-1}) = 7$
19 175	4	$\ell = 4$	$w_2(s) = 3$ and $w_2(s^{-1}) = 6$
33 35 39 47 63 95 101 109 125 157 159 171 187 219 221 343	4	$\ell = 4$	$s \bmod 31 \in \{1, 2, 4, 8, 16\}$
3 9 57	4	$\ell = 4$	see Table 7.4
71 111 245	3	$3 \le \ell \le 4$	$w_2(s) = 6$ or $w_2(s^{-1}) = 6$
43 115 119 183 189 207 231 237 347 363	4		
45 51 55 75 99 147 165	3	$3 \le \ell \le 4$	$\gcd(1023, s) \in \{3, 11, 33\}$
11 21 69 87 105 117 121	4		
37 83	4	$4 \le \ell \le 5$	$w_2(s) = 3$ and $w_2(s^{-1}) \le 6$
103 149	3	$3 \le \ell \le 5$	
5 205 13 79 17 181 25 41 49 107	5	$\ell = 5$	see Table 7.4

- There is no 8-divisible code $\mathcal{C}_{1,s_0}^{\perp}$ of length 31 with $\gcd(s_0, 31) = 1$. It follows from Theorem 7.1(ii) that, for any s such that $\gcd(s, 2^{10} - 1) = 1$, the code $\mathcal{C}_{1,s}^{\perp}$ of length $(2^{10} - 1)$ is at most 2^5-divisible.

$m = 14$. Here we examine only the values of s such that $\gcd(2^{14} - 1, s) = 1$. Note that if $\gcd(2^{14} - 1, s) > 1$, $\mathcal{C}_{1,s}^{\perp}$ is not 2^7-divisible since the 2-weight of any factor of $(2^{14} - 1)$ is at most 7. Table 7.6 is derived from the following theoretical results:

- Proposition 5.3 implies that $\ell \ge 3$ for any s such that $w_2(s) \le 12$ and $w_2(s^{-1}) \le 12$.
- From Corollary 5.1, we have $\ell \le 14 - w_2(s)$.
- For any s such that $w_2(s) = 3$ or $w_2(s^{-1}) = 3$, we have $\ell \ge 5$ according to Corollary 5.2.
- Proposition 5.4 implies that $\ell \ge 4$ when $w_2(s) \le 5$ and $w_2(s^{-1}) \le 10$.
- According to Theorem 7.1(ii) we always have that $\ell \le 7$ since the cyclic code $\mathcal{C}_{1,s_0}^{\perp}$ of length $(2^7 - 1)$ is at most 2^3-divisible when s_0 is not a power of 2.
- The cyclic code $\mathcal{C}_{1,s_0}^{\perp}$ of length $(2^7 - 1)$ is exactly 2-divisible when $s_0 \in Cl(63)$ ($Cl(i)$ here denotes the 2-cyclotomic coset modulo 127). It follows that $\ell \le 3$ for any s such that $s \bmod 127 \in Cl(63)$ (Theorem 7.1(ii)).
- The codes $\mathcal{C}_{1,s_0}^{\perp}$ of length $(2^7 - 1)$ are exactly 4-divisible for $s_0 \in \mathcal{E} = Cl(7) \cup Cl(19) \cup Cl(21) \cup Cl(31) \cup Cl(47) \cup Cl(55)$. Theorem 7.1(ii) then implies that $\mathcal{C}_{1,s}^{\perp}$ is at most 2^5-divisible for any s such that $s \bmod 127 \in \mathcal{E}$.
- If $s \equiv 2^i \bmod 127$ for some i, $\mathcal{C}_{1,s}^{\perp}$ is exactly 2^6-divisible according to Theorem 7.5.

TABLE 7.6
Exact weight divisibility $\mathcal{C}_{1,s}^{\perp}$ *for* $m = 14$ *with* $\gcd(2^{14} - 1, s) = 1$.

s (representatives of cosets)	ℓ		Argument
8191	1	$\ell = 1$	$w_2(s) = 13$
2741 2861 2867 6143 7679 8063	2	$\ell = 2$	$w_2(s) = 12$ or $w_2(s^{-1}) = 12$
95 119 125 253 317 349 365 373 377 379 571 619 631 761 857 881 887 1015 1111 1127 1135 1139 1141 1381 1523 1619 1643 1897 1901 1903 2381 2405 2411 2539 2651 2663 3047 3413 3421 3935 4063	3	$\ell = 3$	$s \bmod 127 \in Cl(63)$
283 511 655 703 1003 1117 1177 1259 1273 1375 1435 1679 1919 2047 2479 2527 2797 2971 3071 3583 3703 3757 3839 3967 4031 4079 4087 4091 4093 5851 5887 6079 6127 6139 7039 7103 7135 7151 7159 7663	3	$\ell = 3$	$w_2(s) = 11$ or $w_2(s^{-1}) = 11$
47 59 83 149 197 203 329 341 355 625 1109 1301 3055 3067 3551 3775 3835 4015 4075 5503 5627 5855 5983 6007	4	$\ell = 4$	$w_2(s) \leq 5$ and $w_2(s^{-1}) = 10$
175 461 691 811 967 1019 1213 1253 1277 1385 1391 1535 1615 1685 1847 1957 2015 2035 2039 2045 2347 2453 2507 2765 2771 2807 2815 3007 3455 3517 3575 3581 3823 3959 3965 4027 4055 4061 5567 5599 5615 5623 5879 5999 6011 6071 6107 7031	4	$3 \leq \ell \leq 4$	$w_2(s) = 10$ or $w_2(s^{-1}) = 10$
7 19 25 31 37 41 67 73 97 245 443 529 869 983 1123 1205 2341 3547	5	$\ell = 5$	$s \bmod 127 \in \mathcal{E}$ and $w_2(s) = 3$
115 239 463 533 617 809 1631 2005	4	$4 \leq \ell \leq 5$	$s \bmod 127 \in \mathcal{E}$ and $w_2(s) \leq 5$ and $w_2(s^{-1}) < 10$
55 61 79 91 103 107 109 121 155 169 209 211 227 275 295 313 361 395 409 419 457 475 481 539 563 569 581 587 595 601 611 649 677 709 745 781 787 793 799 803 841 871 971 1013 1171 1193 1225 1307 1343 1387 1531 1597 1621 1645 1775 1895 1967 1999 2383 2407 2779 2903 3323 3389 3419 3829	5		
251 455 719 1735 2389 3925	3	$3 \leq \ell \leq 5$	$s \bmod 127 \in \mathcal{E}$
431 437 493 503 605 629 685 697 853 1237 1243 1255 1325 1331 1357 1363 1373 1481 1693 1837 1865 2455 2717 2813 2983 2995 3805 4013	4		
221 347 371 491 499 505 575 599 623 757 821 823 829 859 877 883 917 931 965 973 1001 1007 1103 1133 1181 1199 1261 1267 1337 1367 1379 1439 1447 1453 1459 1471 1507 1519 1627 1639 1727 1751 1769 1871 1885 1943 1961 1979 1981 2023 2027 2029 2359 2395 2495 2525 2647 2743 2749 2767 2791 2909 2911 2935 3005 3031 3287 3293 3485 3503 3511 3541 3563 3767 3901 3931 4021 5815	5		
289	5	$\ell = 5$	$w_2(s) = 3$ and $w_2(s^{-1}) = 9$
689 2687	4	$4 \leq \ell \leq 5$	$w_2(s) \leq 5$ and $w_2(s^{-1}) = 9$
77 85 157 269 305 307 323 325 391 401 451 613 647 913 1021 1093 1279 1787 1915 1951 2975 3391 3451 3535 3709 3773 3949 5471 5495 5591	5		

TABLE 7.6
(Continued)

s (representatives of cosets)	ℓ		Argument
959 3059	3	$3 \le \ell \le 5$	$w_2(s) = 9$ or $w_2(s^{-1}) = 9$
715 895 991 1183 1223 1469 1759 1783 2419 2431 2555 2557 2677 3023 3415 3515 3791 3803 5551 5563 5819	4		
235 343 427 487 743 751 767 797 847 875 935 995 1009 1231 1319 1495 1663 1747 1789 1853 1855 1939 1975 2011 2041 2357 2471 2519 2543 2551 2783 2879 2927 2939 2941 2999 3035 3037 3061 3295 3319 3325 3383 3439 3487 3559 3565 3707 3743 3797 3799 3821 3947 5611	5		
131 143 191 383 389 397 413 445 509 637 667 763 893 905 953 1145 1147 1151 1175 1207 1271 1399 1405 1429 1525 1655 1715 1907 1909 1913 2429 2477 2669 2671 2675 2683 2731 2923 3431 3437 3445	6	$\ell = 6$	$s \bmod 127 \in Cl(1)$
11 1501	6	$5 \le \ell \le 6$	$w_2(s) = 3$ and $w_2(s^{-1}) = 8$
955 1187 1321 2719	4	$4 \le \ell \le 6$	$w_2(s) \le 5$ and $w_2(s^{-1}) = 8$
89 101 163 181 185 331 541 553 1499 1511 2747 2933 2987 3317 3407 3509	5		
353 535 583 1723 1883 2423	6		
479 1351	3	$3 \le \ell \le 6$	$w_2(s) = 8$ or $w_2(s^{-1}) = 8$
407 839 943 1303 1369 1465 1661 1711 1771 2003 2549 2803 2863 2875	4		
287 439 607 695 827 845 863 997 1327 1403 1463 1483 1487 1517 1529 1595 1687 1705 1757 1781 1949 1963 1973 1997 2009 2363 2399 2653 2711 2735 2989 3029 3307 3499 3701 3755 5819	5		
497 683 1823 1831 1835 1879 2483 2491 5467 5483	6		
5 13 17 65 113 145 193 205 241 319 979 1339 1613 2773 2893 3277	7	$\ell = 7$	see Table 7.4
35 49 137 161 265 335 433 469 919 1355 2515	6	$5 \le \ell \le 7$	$w_2(s) = 3$ or $w_2(s^{-1}) = 3$
167 187 199 229 247 263 299 425 707 805 911 1097 1099 1195 1445 1589 1609 1625 1717 1843 1867 1877	4	$4 \le \ell \le 7$	$w_2(s) \le 5$ and $w_2(s^1) < 10$
29 71 139 151 173 217 223 233 271 281 403 421 547 551 557 565 589 593 653 659 661 665 721 739 749 785 923 947 977 1129 1165 1189 1309 1423 1607 1691 1829 2461	5		
23 53 179 277 293 337 713 727 937 1163 1315 1451 1657 1739 2869 2899	6		
1241 1703 2459 2645	3	$3 \le \ell \le 7$	
415 679 701 733 755 815 907 941 949 985 1115 1211 1427 1433 1637 1721 1753 2485	4		
311 359 367 467 485 671 791 851 925 1229 1235 1421 1493 1513 1709 1741 1765 1945 1993 2351 2387 2533	5		
133 725 2509	6		

REFERENCES

[1] T. BETH AND C. DING, *On almost perfect nonlinear permutations*, in Advances in Cryptology–EUROCRYPT '93, Lecture Notes in Comput. Sci. 765, Springer-Verlag, New York, 1993, pp. 65–76.

[2] E. BIHAM AND A. SHAMIR, *Differential cryptanalysis of DES-like cryptosystems*, J. Cryptology, 4 (1991), pp. 3–72.

[3] A. Calderbank, G. McGuire, and B. Poonen, *On a conjecture of Helleseth regarding pairs of binary m-sequences*, IEEE Trans. Inform. Theory, 42 (1996), pp. 988–990.
[4] A. Canteaut, P. Charpin, and H. Dobbertin, *Binary m-sequences with three-valued cross-correlation: A proof of Welch's conjecture*, IEEE Trans. Inform. Theory, to appear.
[5] A. Canteaut, P. Charpin, and H. Dobbertin, *Couples de suites binaires de longueur maximale ayant une corrélation croisée à trois valeurs: Conjecture de Welch*, C. R. Acad. Sci. Paris Sér. I Math., 328 (1999), pp. 173–178.
[6] C. Carlet, P. Charpin, and V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Des. Codes Cryptogr., 15 (1998), pp. 125–156.
[7] F. Chabaud and S. Vaudenay, *Links between differential and linear cryptanalysis*, in Advances in Cryptology–EUROCRYPT '94, Lecture Notes in Comput. Sci. 950, Springer-Verlag, New York, 1995, pp. 356–365.
[8] P. Charpin, A. Tietäväinen, and V. Zinoviev, *On binary cyclic codes with minimum distance $d = 3$*, Problems Inform. Transmission, 33 (1997), pp. 287–296.
[9] T. Cusick and H. Dobbertin, *Some new 3-valued crosscorrelation functions of binary m-sequences*, IEEE Trans. Inform. Theory, 42 (1996), pp. 1238–1240.
[10] H. Dobbertin, *Almost perfect nonlinear power functions on $GF(2^n)$: The Niho case*, Inform. and Comput., 151 (1999), pp. 57–72.
[11] H. Dobbertin, *Almost perfect nonlinear power functions on $GF(2^n)$: The Welch case*, IEEE Trans. Inform. Theory, 45 (1999), pp. 1271–1275.
[12] H. Dobbertin, *One-to-one highly nonlinear functions on finite field with characteristic* 2, Appl. Algebra Engrg. Comm. Comput., 9 (1998), pp. 139–152.
[13] R. Gold, *Maximal recursive sequences with 3-valued recursive crosscorrelation functions*, IEEE Trans. Inform. Theory, 14 (1968), pp. 154–156.
[14] S. Golomb, *Theory of transformation groups of polynomials over $GF(2)$ with applications to linear shift register sequences*, Inform. Sci., 1 (1968), pp. 87–109.
[15] T. Helleseth, *Some results about the cross-correlation function between two maximal linear sequences*, Discrete Math., 16 (1976), pp. 209–232.
[16] H. Hollmann and Q. Xiang, *A Proof of the Welch and Niho Conjectures on Crosscorrelations of Binary m-sequences*, preprint, 1998.
[17] H. Janwa and R. Wilson, *Hyperplane sections of Fermat varieties in P^3 in char.* 2 *and some applications to cyclic codes*, in Applied Algebra, Algebraic Algorithms and Error-Correcting Codes–Proceedings AAECC-10, Lecture Notes in Comput. Sci. 673, Springer-Verlag, Berlin, 1993, pp. 180–194.
[18] T. Kasami, *Weight distributions of Bose-Chaudhuri-Hocquenghem codes*, in Proceedings of the Conference on Combinatorial Mathematics and Its Applications, The Univ. of North Carolina Press, Chapel Hill, NC, 1969, pp. 335–357.
[19] T. Kasami, *The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes*, Inform. and Control, 18 (1971), pp. 369–394.
[20] G. Lachaud and J. Wolfmann, *The weights of the orthogonal of the extended quadratic binary Goppa codes*, IEEE Trans. Inform. Theory, 36 (1990), pp. 686–692.
[21] X. Lai, J. Massey, and S. Murphy, *Markov ciphers and differential cryptanalysis*, in Advances in Cryptology–EUROCRYPT '91, Lecture Notes in Comput. Sci. 547, Springer-Verlag, New York, 1991, pp. 17–38.
[22] M. Matsui, *Linear cryptanalysis method for DES cipher*, in Advances in Cryptology–EUROCRYPT '93, Lecture Notes in Comput. Sci. 765, Springer-Verlag, New York, 1994, pp. 386–397.
[23] M. Matsui, *The first experimental cryptanalysis of the data encryption standard*, in Advances in Cryptology–CRYPTO '94, Lecture Notes in Comput. Sci. 839, Springer-Verlag, New York, 1995, pp. 1–11.
[24] R. McEliece, *Weight congruence for p-ary cyclic codes*, Discrete Math., 3 (1972), pp. 177–192.
[25] G. McGuire and A. Calderbank, *Proof of a conjecture of Sarwate and Pursley regarding pairs of binary m-sequences*, IEEE Trans. Inform. Theory, 41 (1995), pp. 1153–1155.
[26] Y. Niho, *Multi-valued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequences*, Ph.D. thesis, Univ. Southern California, Los Angeles, CA, 1972; Tech. report 409, Dept. Electrical Engineering, Univ. Southern California, Los Angeles, CA, 1972.
[27] K. Nyberg, *Differentially uniform mappings for cryptography*, in Advances in Cryptology–EUROCRYPT '93, Lecture Notes in Comput. Sci. 765, Springer-Verlag, New York, 1993, pp. 55–64.
[28] K. Nyberg, *Linear approximation of block ciphers*, in Advances in Cryptology–EUROCRYPT '94, Lecture Notes in Comput. Sci. 950, Springer-Verlag, New York, 1994, pp. 439–444.

[29] K. Nyberg and L. Knudsen, *Provable security against differential cryptanalysis*, in Advances in Cryptology–CRYPTO '92, Lecture Notes in Comput. Sci. 740, Springer-Verlag, New York, 1993, pp. 566–574.
[30] V. Pless, *Power moment identities on weight distributions in error-correcting codes*, Inform. and Control, 3 (1963), pp. 147–152.
[31] D. Sarwate and M. Pursley, *Crosscorrelation properties of pseudorandom and related sequences*, Proc. IEEE, 68 (1980), pp. 593–619.
[32] V. Sidelnikov, *On mutual correlation of sequences*, Soviet Math. Dokl., 12 (1971), pp. 197–201.