Finite Fields and Their Applications **7,** 253–286 (2001)
doi.10.1006/ffta.2000.0281, available online at http://www.idealibrary.com on IDEAL®

A Proof of the Welch and Niho Conjectures on Cross-Correlations of Binary m-Sequences

Henk D. L. Hollmann

Philips Research Laboratories, Prof. Holstlaan 4, 5656 AA Eindhoven, The Netherlands
E-mail: hollmann@natlab.research.philips.com

and

Qing Xiang

Department of Mathematical Sciences, University of Delaware, Newark, Delaware, 19716
E-mail: xiang@math.udel.edu

Communicated by Dieter Jungnickel

Received October 22, 1998; revised February 9, 2000; published online November 18, 2000

Binary m-sequences are widely applied in navigation, radar, and communication systems because of their nice autocorrelation and cross-correlation properties. In this paper, we consider the cross-correlation between a binary m-sequence of length $2^m - 1$ and a decimation of that sequence by an integer t. We will be interested in the number of values attained by such cross-correlations. As is well known, this number equals the number of nonzero weights in the dual of the binary cyclic code $C_{1,t}$ of length $2^m - 1$ with defining zeros α and α^t, where α is a primitive element in GF(2^m). There are many pairs (m, t) for which $C_{1,t}^{\perp}$ is known or conjectured to have only few nonzero weights. The three-weight examples include the following cases:

(a) $t = 1 + 2^r$, if $m/(m, r)$ odd,
(b) $t = 2^{2r} - 2^r + 1$, if $m/(m, r)$ odd,
(c) $m = 2r + 1$ odd, $t = 2^r + 3$, and
(d) m odd, $4r \equiv -1 \bmod m$, $t = 2^{2r} + 2^r - 1$.

We present a method of proving many of these known or conjectured results, including all of the above cases, in a unified way.

1. INTRODUCTION

Maximal length linear feedback shift register sequences (m-sequences) are widely employed in applications such as navigation, radar, and spread-spectrum communication systems. These applications require pairs of binary

1071-5797/01 $35.00

m-sequences a and b of period $2^m - 1$ such that their cross-correlation function

$$\theta_{a,b}(\tau) = \sum_{i=0}^{2^m-2} (-1)^{a_i + b_{i+\tau}} \tag{1}$$

is small. Therefore the cross-correlation properties of binary m-sequences have been studied extensively (see [3, 12, 17, 19, 21]). As is well known [12], the cross-correlation of a pair of distinct m-sequences takes on at least three values. It is thus an interesting problem to determine which pairs of m-sequences result in cross-correlation functions with exactly three values. The problem of determining the *cross-correlation spectrum* of two m-sequences, i.e., the set of values taken by the cross-correlation function together with a count of the number of times that each value occurs, can also be formulated as a problem of determining the weight distribution of certain cyclic codes. In order to explain this connection, we introduce some notation.

Let α be a primitive element of the finite field $\mathrm{GF}(2^m)$. We denote the minimal polynomial of α^i over $\mathrm{GF}(2)$ by $m_i(x)$. Let $h_i(x) = (x^{2^m-1} - 1)/m_i(x)$, and let $h_i^*(x) = x^{\deg(h_i)} h_i(x^{-1})$. In what follows, we will consider various binary linear cyclic codes of length $n = 2^m - 1$. As is customary in coding theory, we identify codewords $c = (c_0, \ldots, c_{n-1})$ with polynomials $c(x) = \sum_{i=0}^{n-1} c_i x^i$ in $\mathscr{R} = \mathrm{GF}(2)[x]/(x^n - 1)$. Let C_i denote the binary cyclic code of length $n = 2^m - 1$ with defining zero α^i. That is, C_i is the code consisting of all polynomials in $\mathscr{R}$ which are multiples of $m_i(x)$. Note that C_i has dimension $n - d_i$ over $\mathrm{GF}(2)$, where d_i is the degree of $m_i(x)$. The dual code $C_i^\perp$ of C_i has dimension d_i and consists of all multiples $a(x)h_i^*(x)$ in $\mathscr{R}$ of the polynomial $h_i^*(x)$.

If the greatest common divisor (i, n) of i and n equals 1, then the code C_i is simply a binary *Hamming code*; its dual $C_i^\perp$ is called a *simplex code*. By definition, an m-sequence of length $n = 2^m - 1$ is a nonzero codeword of a simplex code.

Let t be an integer relatively prime to n. The decimation by t of a periodic sequence $a = a_0, a_1, \ldots, a_{n-1}$ with associated polynomial $a(x) = \sum_{i=0}^{n-1} a_i x^i$ in $\mathscr{R}$ is the sequence $b = b_0, b_1, \ldots, b_{n-1}$ whose associated polynomial $b(x) = \sum_{i=0}^{n-1} b_i x^i$ in $\mathscr{R}$ is given by $b(x) = a(x^{t^{-1}})$. Consequently, the zeros of $b(x)$ include β^t for each zero β of $a(x)$. Hence if a is an m-sequence, that is, $a(x) = x^r h_i^*(x)$ for some r and some i with $(i, n) = 1$, then $b(x) \in C_{it}^\perp$, hence $b(x) = x^s h_{it}^*(x)$ for some s. Replacing the primitive element α by α^i, we may assume without loss of generality that $i = 1$. Then we can write the cross-correlation function (1) of a and b to be

$$\theta_{a,b}(\tau) = n - 2 \cdot \mathrm{w_H}(x^\tau a(x) + b(x)) = n - 2 \cdot \mathrm{w_H}(x^{\tau+r} h_1^*(x) + x^s h_t^*(x)), \tag{2}$$

where $\mathrm{w_H}$ is the Hamming weight.

Now let $C_{1,t}$ be the binary cyclic code of length n with defining zeros α and α^t, or equivalently, with generator polynomial $m_1(x)m_t(x)$. Define

$$\Gamma = \{x^i h_1^*(x) + x^j h_t^*(x) | 0 \le i, j < n\}.$$

Note that the set Γ consists of all polynomials $x^r a(x) + b(x)$ together with their cyclic shifts. Since $m_1(x)m_t(x)(x^i h_1(x) + x^j h_t(x)) = 0$ in $\mathscr{R}$ for all i and j, we see that Γ is contained in the dual code $C_{1,t}^{\perp}$ of $C_{1,t}$. In fact it is easy to see that $C_{1,t}^{\perp}$ is the disjoint union of $\{0\}$, $C_1^{\perp}\backslash\{0\}$, $C_t^{\perp}\backslash\{0\}$, and Γ. Since the $2(2^m - 1)$ nonzero words of the two simplex codes $C_1^{\perp}$, $C_t^{\perp}$ all have weight 2^{m-1}, we conclude that the cross-correlation spectrum of the pair $a = x^r h_1^*(x)$, $b = x^s h_t^*(x)$ and the weight distribution of the code $C_{1,t}^{\perp}$ contain exactly the same information.

A pair of m-sequences is called a *preferred pair* if the cross-correlation function only takes on the values -1, $-1 \pm 2^{\lfloor (m+2)/2 \rfloor}$, or equivalently, if the corresponding code $C_{1,t}^{\perp}$ has only three nonzero weights, 2^{m-1}, $2^{m-1} \pm 2^{\lfloor (m+2)/2 \rfloor - 1}$. It has been shown [17] that there are no preferred pairs when $m \equiv 0 \bmod 4$, while for $m \equiv 2 \bmod 4$, the only known examples are those arising from $t = 2^r + 1$, r even, $t = 2^{2r} - 2^r + 1$, r even, $t = 2^{(m+2)/2} + 3$, and $t = 2^{m/2} + 2^{(m+2)/4} + 1$ (for the latter two cases, see [7]). In the case m is odd, the following is a list of all values of t which are known or conjectured to lead to a pair of preferred m-sequences:

(a) $t = 2^r + 1$, if $(r, m) = 1$ (proved by Gold [11], 1968);
(b) $t = 2^{2r} - 2^r + 1$, if $(r, m) = 1$ (proved by Welch [22], 1969, and Kasami [14], 1971);
(c) $m = 2r + 1$ odd, $t = 2^r + 3$ (conjectured by Welch [19], 1972);
(d) m odd, $4r \equiv -1 \bmod m$, $t = 2^{2r} + 2^r - 1$ (conjectured by Niho [19], 1972).

The main purpose of this paper is to provide a uniform treatment of the four cases above. In particular, we prove the Welch and Niho conjectures from 1972. The proofs depend on a combination of three ideas.

Let $C_{1,t}$ be the cyclic code of length $2^m - 1$ defined as above, and let A_i, B_i denote the number of codewords of weight i in $C_{1,t}$ and $C_{1,t}^{\perp}$ respectively. In Section 2, we use the Pless power moment identities to evaluate a certain linear combination of the B_i's in terms of A_3 and A_4. Our interest in this expression stems from the fact that the only negative coefficients in this linear combination are confined to a small interval of weights symmetric about 2^{m-1}, with the coefficient of $B_{2^{m-1}}$ and two other coefficients equal to zero. Therefore if we could show that the code $C_{1,t}^{\perp}$ has no other weights in this interval, and if the aforementioned linear combination of the B_i's can be shown to be zero, then the code $C_{1,t}^{\perp}$ can only have three nonzero weights.

To obtain the desired restrictions on the weights that can occur in the code $C_{1,t}^{\perp}$, a deep theorem of McEliece on cyclic codes is used to express the largest

power of 2 that divides the weights of the code $C_{1,t}^{\perp}$ in terms of a number $M(m, t)$ defined as

$$M(m, t) = \max_{a \in \mathbf{Z}_{2^m-1} \setminus \{0\}} |w(ta) - w(a)|, \tag{3}$$

where $w(a)$ is the binary weight of a. This material can be found in Section 4. We remark that on other occasions [3, 17], McEliece's theorem has been used successfully to prove interesting results on the cross-correlation of m-sequences. Even the number $M(m, t)$ has been investigated before. For example, it was shown in [3] that $M(2^r, t) \geq 2^{r-1}$ for all odd t.

In order to show that the linear combination referred to earlier is indeed equal to zero, we need to count the number $A_3 + A_4$ of codewords of weights 3 and 4 in the code $C_{1,t}$. This problem is addressed in Section 3. In the case when t is of the form $t = 2^r + 1$, this is easy. For the case where $t = 2^{2r} - 2^r + 1$, we use results from [14, 15] to determine $A_3 + A_4$ under the condition that $m/(r, m)$ is odd. In the other two cases of interest we make use of the recent breakthrough results from [8, 9], which essentially state that the minimum distance of the code $C_{1,t}$ is 5 in these cases.

In Section 5 we collect the required results concerning $M(m, t)$. We develop a method involving add-with-carry algorithms in $\mathbf{Z}_{2^m-1}$ to investigate this number. In all four cases, this method actually succeeds in obtaining the exact values of $M(m, t)$. We remark that these problems involving binary weights can sometimes be rephrased as tiling problems. Therefore it is possible to approach the problem of determining $M(m, t)$ from the tiling point of view (see [6]).

Finally, in Section 6 we prove our main results on the three-valued cross-correlation of binary m-sequences using the results obtained in previous sections. In particular, we give a proof for the Welch and Niho conjectures mentioned above.

We note that the techniques developed in this paper can be useful for investigating many other (known or conjectured) instances of cyclic codes with few nonzero weights. To mention just a couple of examples: Recently, in [6], Chang *et al.* conjectured that the cyclic code C_{1,t,t^2} of length $n = 2^m - 1$ with defining zeros α, α^t, and α^{t^2} in $\mathrm{GF}(2^m)$, with $t = 1 + 2^{(m+1)/2}$, has the same weight distribution as the 3-error-correcting primitive BCH code of the same length. We can prove this conjecture by using some results in [6] and straightforward generalisations of the techniques in this paper. Similarly, we can give a solution for research problem 9.7, Chapter 9.11 in [18]. We will give details of these results in a forthcoming paper.

After submitting this paper, we became aware through discussions with Charpin and Dobbertin that for the past few years they have been working systematically towards solving the Welch conjecture along the same lines as

in this paper (the idea of using Pless power moment identities and McEliece's theorem seems first to have occurred to Charpin [5], while the distance results [8, 9] were published by Dobbertin). However, for obvious reasons they did not wish to reveal this promising way of attacking the Welch conjecture to others. During a meeting in Oberwolfach the second author was informed by Dobbertin that solving the binary weight problem in Section 5, which looked similar to a binary weight problem from [10], was probably sufficient to prove the Welch conjecture; no details concerning this proof were revealed. After finishing [10], we used the methods developed there to solve the binary weight problem; then, intrigued by the Welch and Niho conjectures, we succeeded in deriving the complete proof for the Welch and Niho conjectures presented here. After hearing of our results, Canteaut *et al.*, also succeeded in completing their own proof of the Welch conjecture (see [4]). Perhaps unfortunately, our offer to write a joint paper could not be effectuated at that point of time. We hope that the above lines serve to give the proper credit to all the people that have been involved in this proof through the years.

2. POWER MOMENT IDENTITIES AND CODES WITH FEW WEIGHTS

As in Section 1, we use $C_{1,t}$ to denote the binary cyclic code of length $n = 2^m - 1$ with defining zeros α and α^t, where α is a primitive element in GF(2^m). The number of codewords of weight i in $C_{1,t}$ and its dual code $C_{1,t}^{\perp}$ will be denoted by A_i and B_i, respectively.

For later use, we observe the following.

LEMMA 1. *With the above notation, we have that* $A_1 = A_2 = 0$.

Proof. Note that $C_{1,t}$ is a subcode of the binary Hamming code, which has minimum distance 3; therefore $A_1 = A_2 = 0$. ■

As we mentioned in Section 1, for certain special values of t, the code $C_{1,t}^{\perp}$ is known or conjectured to be a three-weight code. We will show how such results can be proved in a uniform manner from information on A_3, A_4, and certain divisibility conditions on the weights of $C_{1,t}^{\perp}$ by powers of 2.

We proceed as follows, using some ideas of Kasami [13]. In fact we will treat a more general situation first, then specialize to the aforementioned codes $C_{1,t}^{\perp}$.

Let $C^{\perp}$ be a binary $[n, k]$ linear code. We still use B_i and A_i to denote the number of codewords of weight i in $C^{\perp}$ and C respectively. For later use, we need the Pless power moment identities for the B_i's [20; see also 18, p. 131].

To keep things simple, we will assume that C has minimum distance at least 3 (which will be the case for all our applications). Then, we have that

$$P_0 := \sum_{w=0}^{n} B_w = 2^k,$$

$$P_1 := \sum_{w=0}^{n} wB_w = 2^{k-1}n,$$

$$P_2 := \sum_{w=0}^{n} w^2 B_w = 2^{k-2}n(n+1),$$

$$P_3 := \sum_{w=0}^{n} w^3 B_w = 2^{k-3}(n^2(n+3) - 3!A_3),$$

$$P_4 := \sum_{w=0}^{n} w^4 B_w = 2^{k-4}(n(n+1)(n^2+5n-2) + 4!(A_4 - nA_3)).$$

Let $0 < w_1 \le w_2 \le w_3 \le w_4 \le n$ be given integers, and let

$$g(x) = (x - w_1)(x - w_2)(x - w_3)(x - w_4).$$

We will be interested in the linear combination E of the B_w's defined by

$$E = \sum_{w=1}^{n} g(w)B_w. \tag{4}$$

Note that by using the above formulae for P_i, $i = 0, 1, \ldots, 4$, the value of E for given w_1, w_2, w_3, w_4 can be expressed in terms of n, k, A_3, and A_4. Moreover, we have the following.

THEOREM 1. *With the above notation and assumptions, if $C^\perp$ has no codewords of weight w in the intervals (w_1, w_2) and (w_3, w_4), then $E \ge 0$ with equality if and only if $C^\perp$ has no nonzero weights except w_1, w_2, w_3, and w_4.*

Proof. We note that $g(x)$ is positive outside the interval $[w_1, w_4]$ and inside the interval (w_2, w_3). Also $g(x)$ is negative in the intervals (w_1, w_2) and (w_3, w_4). If $C^\perp$ has no codewords of weight w in the intervals (w_1, w_2) and

(w_3, w_4), then clearly we have $E \geq 0$, and $E = 0$ if and only if $B_w = 0$ for all nonzero w not equal to w_i, $i = 1, 2, 3, 4$. This completes the proof. ■

This simple theorem is actually quite useful for proving that certain codes have only three or four weights. In this paper, we will concentrate on applications of Theorem 1 in proving three-weight code results. But we remark that this theorem can also be used in a similar way to prove four-weight code results.

From now on, we always assume that the length n of the code $C^\perp$ is odd, and $w_1 = w_2 - d$, $w_2 = w_3 = (n+1)/2$, $w_4 = w_2 + d$. We have the following immediate corollary of Theorem 1.

COROLLARY 1. *Suppose that $C^\perp$ has no codewords of weight w in the interval $(n+1)/2 - d < w < (n+1)/2 + d$ except for $w = (n+1)/2$. Then $E \geq 0$, and $E = 0$ if and only if $C^\perp$ is a three-weight code with nonzero weights $(n+1)/2 - d$, $(n+1)/2$, and $(n+1)/2 + d$.*

Proof. In Theorem 1, let $w_1 = w_2 - d$, $w_2 = w_3 = (n+1)/2$, $w_4 = w_2 + d$. Then the corollary follows immediately from Theorem 1. ■

COROLLARY 2. (i) *Suppose that d divides $(n+1)/2$. Then $C^\perp$ is a three-weight code with weights $(n+1)/2 - d$, $(n+1)/2$, and $(n+1)/2 + d$ if and only if $E = 0$ and the weight of every codeword of $C^\perp$ is divisible by d.*

(ii) *If $d | \frac{(n+1)}{2}$, if C has minimum distance at least 3, and if $C^\perp$ is a three-weight code with weights $(n+1)/2 - d$, $(n+1)/2$, and $(n+1)/2 + d$, then $d | 2^{k-1}$, where k is the dimension of $C^\perp$. If, in addition, $n = 2^m - 1$, then $2^{k-m-1} | d^2$ when $k < 3m$, and $d = 2^{m-1}$ when $k \geq 3m$.*

Proof. For part (i), we observe that if the weight of every codeword of $C^\perp$ is divisible by d and $d | \frac{n+1}{2}$, then $C^\perp$ has no codewords of weight w in the interval $(n+1)/2 - d < w < (n+1)/2 + d$ except for $w = (n+1)/2$. Now the conclusion in part (i) follows from Corollary 1.

For part (ii), we set $s = (n+1)/2$. Using the power moment identities listed above, we have

$$P_0 = 2^k,$$

$$P_1 = 2^k s - 2^{k-1},$$

$$P_2 = s^2 2^k - 2^{k-1} s = sP_1,$$

$$P_3 = 2^{k-3}(2(2s-1)^2(s+1) - 6A_3),$$

and

$$B_{s-d} = (s+d)(2^{k-1} - s)/(2d^2),$$

$$B_s = (2^k - 1) - s(2^{k-1} - s)/d^2,$$

$$B_{s+d} = (s-d)(2^{k-1} - s)/(2d^2).$$

Since $B_{s-d} - B_{s+d} = (2^{k-1} - s)/d$ is an integer and by assumption $d|s$, we see that $d|2^{k-1}$; hence d is a power of 2.

Using the above expressions for B_{s-d}, B_s, B_{s+d}, we also find that

$$P_3 = s^3(2^k - 1) - d^2(2^{k-1} - s),$$

$$A_3 = (s^3 - (3s-1)2^{k-2} + d^2(2^{k-1} - s))/(3 \cdot 2^{k-2}).$$

Since A_3 is an integer, we conclude that $2^{\lfloor (k-m-1)/2 \rfloor} | d$ if $n = 2^m - 1$, $k < 3m$, and $d = 2^{m-1}$ if $n = 2^m - 1$ and $k \geq 3m$. ■

Next we express E in terms of n, k, A_3, and A_4. (Note that we assume $A_1 = A_2 = 0$.) By the definition of E, we have that

$$E = P_4 - P_3 \sum_{i=1}^{4} w_i + P_2 \sum_{1 \leq i < j \leq 4} w_i w_j$$

$$- P_1 \sum_{i<j<k} w_i w_j w_k + (P_0 - 1) w_1 w_2 w_3 w_4.$$

We assumed that $w_1 = w_2 - d$, $w_2 = w_3 = (n+1)/2$, $w_4 = w_2 + d$. With this assumption, we find using the power moment identities that

$$E = P_4 - 4w_2 P_3 + (6w_2^2 - d^2)P_2 - (4w_2^3 - 2d^2 w_2)P_1$$

$$+ (w_2^4 - d^2 w_2^2)(P_0 - 1) \tag{5}$$

$$= 3 \cdot 2^{k-1}(A_3 + A_4) - (n+1)^4/16 + 2^{k-4}(n+1)(3n+1)$$

$$+ d^2(n+1)^2/4 - 2^{k-2} d^2 (n+1). \tag{6}$$

We now specialize to the case where $n = 2^m - 1$ and $k = 2m$. With these assumptions, we obtain that

$$E = 2^{2m-2}(6(A_3 + A_4) - (d^2 - 2^{m-1})(2^m - 1)).$$

In order to apply Corollary 2, part (i), we need d to be a power of 2. Setting $d^2 = 2^{m-2+e}$, we conclude from the above equation that $E = 0$ if and only if $A_3 + A_4 = (2^{e-1} - 1)2^{m-1}(2^m - 1)/6$. Combining this with Corollary 2, we now have the following.

THEOREM 2. *Let $n = 2^m - 1$, and let $C_{1,t}$ be the binary cyclic code of length n with defining zeros α and α^t, where α is a primitive element of $\mathrm{GF}(2^m)$. Suppose that $C_{1,t}^{\perp}$ has dimension $2m$. Let d be the largest power of 2 dividing the weight of every codeword of $C_{1,t}^{\perp}$, and let e be such that $d^2 = 2^{m-2+e}$. Then*

$$A_3 + A_4 \geq (2^{e-1} - 1)2^{m-2}(2^m - 1)/3,$$

with equality if and only if $C_{1,t}^{\perp}$ is a three-weight code with nonzero weights $2^{m-1} + \varepsilon 2^{(m-2+e)/2}$, $\varepsilon = -1, 0, 1$, where A_i denotes the number of codewords of weight i in $C_{1,t}$.

3. THE NUMBER OF WORDS OF WEIGHT 3 OR 4 in $C_{1,t}$

Let $n = 2^m - 1$ and let α be a primitive element in $\mathrm{GF}(2^m)$. Given a function $f: \mathrm{GF}(2^m) \to \mathrm{GF}(2^m)$ with $f(0) = 0$, we use C_f to denote the binary cyclic code of length 2^m with parity check matrix

$$H_f = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ f(0) & f(1) & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{n-1}) \end{pmatrix}.$$

We will index the coordinate positions of C_f using the elements of $\mathrm{GF}(2^m)$, in such a way that the column of H_f with index $x \in \mathrm{GF}(2^m)$ will be $(1, x, f(x))^{\mathrm{T}}$. Let C_f^* denote the subcode of C_f consisting of all words having a zero in the position indexed by 0. Denote the number of codewords of weight w in C_f^* by A_w. We remark that if $f(x) = x^t$, then the code C_f^* is just $C_{1,t}$. Note also that if $S = \{x | c_x \neq 0\}$ is the set of supports of a codeword of weight $2w$ in C_f, then $S \backslash \{0\}$ is the set of supports of a codeword in C_f^*, of weight $2w$ if $0 \notin S$ or weight $2w - 1$ if $0 \in S$; moreover, all sets of supports of words in C_f^* arise in one of these two ways.

In what follows, we will be interested in the number $A_3 + A_4$ of codewords of weight 3 or 4 in C_f^*. Note that by the previous remark, $A_3 + A_4$ equals the number of words of weight 4 in C_f and therefore is the number of sets $\{x_1, x_2, x_3, x_4\} \subseteq \mathrm{GF}(2^m)$ of size 4 such that

$$x_1 + x_2 + x_3 + x_4 = 0, \tag{7}$$

$$f(x_1) + f(x_2) + f(x_3) + f(x_4) = 0. \tag{8}$$

Writing $x_2 = x$, $x_1 = x + a$, and $x_4 = y$, we see that $A_3 + A_4$ is the number of sets of the form $\{x, x + a, y, y + a\}$, $a \neq 0$, $y \neq x, x + a$, such that

$$f(x + a) + f(x) = f(y + a) + f(y). \tag{9}$$

The function f is said to be *Almost Perfect Nonlinear* (APN) if for each $a \in \mathrm{GF}(2^m)\backslash\{0\}$, the function

$$\Delta_{f,a}(x) = f(x + a) - f(x)$$

is two-to-one from $\mathrm{GF}(2^m)$ to itself—that is, if (9) only has the trivial solutions $a = 0$, $y = x$, or $y = x + a$.

As a consequence of the preceding analysis, we have obtained the main part of the following theorem.

THEOREM 3 [5]. *The code C_f^* has minimum distance 5 if and only if f is APN.*

(The fact that C_f^* has minimum distance at most 5 follows from a sharpening of the Johnson bound [1].)

COROLLARY 3. *The function f is APN if and only if $A_3 + A_4 = 0$.*

From now on, we only consider functions f of the form $f(x) = x^t$ for some t. In that case, for given x the number of solutions y of (9) only depends on whether $a = 0$ or $a \neq 0$. (To see this, in (9) divide both sides of the equation by a^t if $a \neq 0$.) As a consequence, the set of supports of codewords of weight 4 in the extended code of $C_{1,t}$ are precisely the sets of the form

$$\{ax, a(x + 1), ay, a(y + 1)\}, \qquad a \neq 0,\ y \neq x, x + 1 \tag{10}$$

with x and y satisfying

$$(x + 1)^t + x^t = (y + 1)^t + y^t. \tag{11}$$

Let $v_t(x)$ denote the number of solutions y of the equation (11). Note that $v_t(x) \geq 2$ for all x.

THEOREM 4. *The sets of supports of codewords of weight* 3 *or* 4 *in* $C_{1,t}$ *are precisely the sets* $S\backslash\{0\}$ *for which* S *has the form* (10) *with* x *and* y *satisfying* (11). *The number* $A_3 + A_4$ *of such codewords satisfies*

$$A_3 + A_4 = (2^m - 1) \sum_{x \in \mathrm{GF}(2^m)} (v_t(x) - 2)/4!$$

Proof. For each $a \neq 0$, Eq. (9) has precisely $v_t(x)$ solutions y for given x; all but two of these lead to a valid support set $\{x, x + a, y, y + a\}$. ■

We remark that the support sets of words of weight 4 in the code C_f, $f(x) = x^t$, form a 2-design if and only if $v_t(x)$ does not depend on $x \in \mathrm{GF}(2^m)$.

In what follows, we will apply the previous results to determine $A_3 + A_4$ for various pairs (m, t).

3.1. *The Gold Case*

First we consider the case where $t = 1 + \sigma$, $\sigma = 2^r$. Write $e = (r, m)$.

THEOREM 5. *All words of weight* 3 *or* 4 *in* $C_{1,1+\sigma}$ *have zeros* $\alpha^{1+2^{ej}}$ *for all* j. *The number* $A_3 + A_4$ *of such words satisfies*

$$A_3 + A_4 = 2^{m-2}(2^m - 1)(2^{e-1} - 1)/3.$$

Proof. We apply Theorem 4. Note that the map $z \mapsto z^\sigma$ from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2^m)$ is linear, hence $(1 + z)^{1+\sigma} + z^{1+\sigma} = z^\sigma + z + 1$. Moreover, x and y satisfy (11) precisely when $\gamma = x + y$ satisfies $\gamma^\sigma = \gamma$. It is easily seen that this holds if and only if

$$\gamma^{2^e} = \gamma. \tag{12}$$

As a consequence, the sets of supports of codewords of weight 3 or 4 in $C_{1,1+\sigma}$ are precisely the sets

$$\{ax, a(x + 1), a(x + \gamma), a(x + \gamma + 1)\}\backslash\{0\} \tag{13}$$

with $a \neq 0$, $\gamma \neq 0$, 1 and γ satisfying (12) (i.e., $\gamma \in \mathrm{GF}(2^e)$). The number $A_3 + A_4$ of such sets is easily seen to be $(2^m - 1)2^m(2^e - 2)/4!$.

Since (12) implies that $\gamma^{2^{ej}} = \gamma$ for all j, the preceding analysis shows that each set (13) is in fact the set of supports of a word that is contained in all codes $C_{1,1+2^{ej}}$. ■

We remark that as a consequence of Theorem 4 and Theorem 5, the function $x \mapsto x^{2^r+1}$ on $\mathrm{GF}(2^m)$ is APN if and only if $(m, r) = 1$.

3.2. *The Kasami Case*

Next, we consider the case where $t = \sigma^2 - \sigma + 1$, $\sigma = 2^r$. Again we write $e = (r, m)$. We have not been able to find a simple method to count the number of words of weight at most 4 in $C_{1,\sigma^2-\sigma+1}$ for *all* values of r; the following approach works in the case where m/e is odd.

Let $C_{1+\sigma,1+\sigma^3}$ denote the binary cyclic code of length $n = 2^m - 1$ with defining zeros $\alpha^{1+\sigma}$, $\alpha^{1+\sigma^3}$. Remark that if m/e is odd, or, equivalently, if $(1 + \sigma, 2^m - 1) = 1$, then the map $\alpha \mapsto \alpha^{1+\sigma}$ induces a permutation on $\mathrm{GF}(2^m)\backslash\{0\}$ and hence the codes $C_{1,\sigma^2-\sigma+1}$ and $C_{1+\sigma,1+\sigma^3}$ are equivalent. We will show later on that the following holds.

LEMMA 2. (i) *A word of weight* 3 *or* 4 *in the code* $C_{1,\sigma^2-\sigma+1}$ *has additional zeros* $\alpha^{(\sigma^{2j+1}+1)/(\sigma+1)}$ *for all* j.

(ii) *A word of weight* 3 *or* 4 *in the code* $C_{1+\sigma,1+\sigma^3}$ *has additional zeros* $\alpha^{1+2^{e(2j+1)}}$ *for all* j.

This has the following consequence.

THEOREM 6. *Let* m/e *be odd. Then the sets of words of weight at most* 4 *in the codes* $C_{1+\sigma,1+\sigma^3}$ *and* $C_{1,1+\sigma}$ *are equal. Moreover, the number* $A_3 + A_4$ *of words of weight* 3 *or* 4 *in* $C_{1,\sigma^2-\sigma+1}$ *satisfies*

$$A_3 + A_4 = 2^{m-2}(2^{e-1} - 1)(2^m - 1)/3.$$

Proof. By Theorem 5, the words of weight 3 or 4 in $C_{1,1+\sigma}$ have zeros $\alpha^{1+2^{ej}}$ for all j. So in particular, such words have zeros $\alpha^{1+\sigma}$ and $\alpha^{1+\sigma^3}$ and hence are contained in $C_{1+\sigma,1+\sigma^3}$.

Conversely, if m/e is odd, then by Lemma 2, a word of weight 3 or 4 in $C_{1+\sigma,1+\sigma^3}$ has zeros $\alpha^{1+2^{e(2j+1)}}$ for all j; therefore α^2, and hence α, is a zero and such a word is contained in $C_{1,1+\sigma}$. Since the codes $C_{1+\sigma,1+\sigma^3}$ and $C_{1,\sigma^2-\sigma+1}$ are equivalent if m/e is odd, the second claim in the theorem follows from Theorem 5. ■

We now give a proof of Lemma 2. In fact, part (ii) of Lemma 2 has already been proved in [14]. Here we sketch a short proof of Lemma 2, based on results from [14] and [15].

Let $c(X) = \sum_{i=1}^{k} X^{u_i}$ with $0 \le u_1 < u_2 < \cdots < u_k < n$. For each $i \in \mathbf{Z}_n$, define the vector $v(i)$ in $\mathrm{GF}(2^m)^k$ by

$$v(i) = (\alpha^{iu_1}, \alpha^{iu_2}, \ldots, \alpha^{iu_k}).$$

Let A be a subset of $\mathbf{Z}_n$. We will say that A is independent if the corresponding set of vectors $V(A) = \{v(a) | a \in A\}$ is independent over GF(2^m), or, equivalently, if the set of residue classes $\{X^a | a \in A\}$ modulo the polynomial $p_c(X) = \prod_{i=1}^{k}(X - \alpha^{u_i})$ is independent. Note that an independent set has size at most k.

Let $R = \{r \in \mathbf{Z}_n | c(\alpha^r) = 0\}$. The first step in our proof is mostly a reformulation of Lemma 1 in [14]; see also [15].

1. For all $r, s \in \mathbf{Z}_n$, we have that $v(r)v(s)^\top = c(\alpha^{r+s})$. So if A is independent, $A \subseteq R$, and $s \notin R$, then $A \cup \{s\}$ is independent.

Indeed, $v(r)v(s)^\top = \sum_{i=1}^{k} \alpha^{ru_i}\alpha^{su_i} = \sum_{i=1}^{k} \alpha^{(r+s)u_i} = c(\alpha^{r+s})$. So if $A \subseteq R$ is independent and $s \notin R$, then the vector $v(0)$ is orthogonal to all the vectors in $V(A)$ but not orthogonal to $v(s)$, and therefore $A \cup \{s\}$ is independent.

The next step can be found in Theorem 11 of [15].

2. If A is independent and $s \in \mathbf{Z}_n$, then the set $s + A = \{s + a | a \in A\}$ is independent. This statement is obvious when considered in terms of residue classes $X^a \bmod p_c(X)$.

The next step is again in [14].

3. If A is independent and l is any integer, then the set $2^l A = \{2^l a | a \in A\}$ is independent.

Essentially, this statement is a direct consequence of the fact that for each l, the map $z \mapsto z^{2^l}$ is linear on GF(2^m).

4. Now suppose that for some a, $\tau \in \mathbf{Z}_n$, $\tau = 2^i$, the sequence $\{v_j\}_{j \geq 0}$ in $\mathbf{Z}_n$ satisfies $v_{j+1} = a + \tau v_j$ for all $j \geq 0$ and the set R contains v_j for $j = 0, \ldots, k-1$. Then $v_j \in R$ for all j.

To see this, suppose that $v_j \in R$ for $j = 0, \ldots, u-1$ and $v_u \notin R$. By step 1 with $A = \emptyset$, the set $\{v_u\}$ is independent, and then by a sequence of applications of step 2 (with $s = -a$), step 3 (with $l = -i$), and step 1 (with $s = v_u$), we conclude that the sets $\{v_{u-1}, v_u\}, \{v_{u-2}, v_{u-1}, v_u\}, \ldots, \{v_0, v_1, \ldots, v_u\}$ are independent, which is only possible if $u + 1 \leq k$.

5. Now we apply the above to a codeword $c \in C_{1,\sigma^2-\sigma+1}$ of weight $k \leq 4$. The sequence $v_j = (\sigma^{2^j-3} + 1)/(\sigma + 1)$ satisfies $v_{j+1} = 1 - \sigma + \sigma^2 v_j$ for all $j \geq 0$; moreover, note that $v_0 = \sigma^{-3}(\sigma^2 - \sigma + 1)$, $v_1 = \sigma^{-1}$, $v_2 = 1$, and $v_3 = \sigma^2 - \sigma + 1$ are all zeros of c. Then part (i) of Lemma 2 follows from an application of the result in step 4 above with $a = 1 - \sigma$ and $\tau = \sigma^2$. Similarly, part (ii) of Lemma 2 follows by considering the sequence of numbers $v'_j = (\sigma + 1)v_j$.

3.3. *The Welch Case*

Next, we consider the case where $m = 2r + 1$ is odd and $t = \sigma + 3$, with $\sigma = 2^r$. The results in Section 3.3 and 3.4 are due to Dobbertin [8, 9]. Here, we use Theorem 4 to translate his results into coding language.

Consider the function

$$\Delta(x) = (x+1)^{\sigma+3} + x^{\sigma+3}.$$

Writing $(x+1)^{\sigma+3} = (x+1)^{\sigma}(x+1)^2(x+1)$, it follows easily that $\Delta(x) = 1 + (x + x^{\sigma})(x^2 + x + 1)$. Hence $\Delta(x)$ can be written in terms of the polynomial

$$q(y) = y(y^{2\sigma} + y^2 + 1)$$

as

$$\Delta(x) = 1 + q(x + x^{\sigma}).$$

Since $(r, m) = 1$, the map $x \mapsto x + x^{\sigma}$ is two-to-one on $\mathrm{GF}(2^m)$. The preceding analysis is from [8], where the following result was also proved.

THEOREM 7 [8]. *The polynomial* $q(y) = y(y^{2^{r+1}} + y^2 + 1)$ *is a permutation polynomial on* $\mathrm{GF}(2^m)$, $m = 2r + 1$.

As a consequence, the number $v_{\sigma+3}(x)$ of solutions y to $\Delta(x) = \Delta(y)$ equals 2 for all x; hence by Theorem 4, we have the following.

THEOREM 8. *Let* $m = 2r + 1$ *and* $t = \sigma + 3$, *with* $\sigma = 2^r$. *Then the code* $C_{1,t}$ *has minimum distance* 5.

3.4. *The Niho Cases*

Let m be odd, and let $r \in \mathbf{Z}_m$ be such that $4r + 1 \equiv 0 \bmod m$. Here we consider the case where $t = \sigma^2 + \sigma - 1$, with $\sigma = 2^r$. Again, we will apply Theorem 4. It is not difficult to verify that the function

$$\Delta(x) = (x+1)^{\sigma^2+\sigma-1} + x^{\sigma^2+\sigma-1}$$

can be written in terms of the polynomial

$$q(y) = y^{2\sigma^2+2\sigma+1} + y^{2\sigma^2+2\sigma-1} + y^{2\sigma^2+1} + y^{2\sigma^2-1} + y$$

as

$$\Delta(x) = 1 + 1/q((x^{\sigma} + x)^{\sigma-1} + 1).$$

The preceding analysis as well as the following result can be found in [9].

THEOREM 9 [9]. *With the above definitions, the polynomial* $q(y)$ *is a permutation polynomial over* $\mathrm{GF}(2^m)$.

As a consequence, the number $v_{\sigma^2+\sigma-1}(x)$ of solutions y to $\Delta(x) = \Delta(y)$ equals 2 for all x; hence by Theorem 4, we have the following.

THEOREM 10. *Let m be odd, let $4r \equiv -1 \bmod m$, and let $t = \sigma^2 + \sigma - 1$, where $\sigma = 2^r$. Then the code $C_{1,\sigma^2+\sigma-1}$ has minimum distance* 5.

4. THE LARGEST POWER OF 2 DIVIDING THE WEIGHTS OF C

In this section, we use the following theorem of McEliece to obtain information on the largest power of 2 dividing the weights of $C_{1,t}^{\perp}$.

THEOREM 11 [16]. *Let C be a binary cyclic code, and let ℓ be the smallest positive integer such that ℓ nonzeros of C (with repetitions allowed) have product* 1. *Then the weight of every codeword in C in divisible by $2^{\ell-1}$, and there is at least one weight which is not divisible by 2^{ℓ}.*

Let $n = 2^m - 1$, and let $\mathbf{Z}_n$ be the ring of integers modulo n. We define the *weight* $w(a)$ of a given sequence $a = a_0, a_1, \ldots, a_{m-1}$ as

$$w(a) = \sum_{i=0}^{m-1} a_i.$$

We say that a number a has binary representation $a = a_{m-1} \cdots a_0$ if $a = \sum_{i=0}^{m-1} a_i 2^i$ with $a_i \in \{0, 1\}$ for all i. We will write $\bar{a}$ to denote the number with binary representation $\bar{a}_{m-1} \cdots \bar{a}_0$ (that is, $\bar{a} = 2^m - 1 - a$). By a slight abuse of notation, we also use $w(a)$ to denote the (*binary*) *weight* $\sum_{i=0}^{m-1} a_i$ of a number a with binary representation $a = a_{m-1} \cdots a_0$. Note that $w(\bar{a}) = m - w(a)$. Moreover, if $a \in \mathbf{Z}_n$ has a given binary representation $a \equiv \sum_{i=0}^{m-1} a_i 2^i \bmod 2^m - 1$, $a_i \in \{0, 1\}$, then we also use $w(a)$ to denote the weight of this representation. Note that an element $a \in \mathbf{Z}_n$ has a unique binary representation if $a \not\equiv 0 \bmod n$.

Next, for any integer $m > 1$ and $t \in \mathbf{Z}_n \backslash \{0\}$, we define

$$M(m, t) = \max^*(w(s) - w(a)), \tag{14}$$

where the maximum is over all integers a, s for which $0 \le a$, $s \le 2^m - 1$, $s \equiv ta \bmod 2^m - 1$, and $a \ne 0$ or $s \ne 2^m - 1$. For later use, we will write the above definition in a slightly different form. First we observe that the above maximum is never attained for $a \equiv 0 \bmod 2^m - 1$. Indeed, if $a = 2^m - 1$, then $w(s) - w(a) \le 0$ for all s, and if $a = 0$, then $s \equiv 0 \bmod 2^m - 1$, so $s = 0$ (the

case $a = 0$, $s = 2^m - 1$ is excluded) and $w(s) - w(a) = 0$. However, the choice $a = 1$, $s = t$ shows that $M(m, t) \geq w(t) - w(1) \geq 0$. Next, we note that $w(\bar{s}) - w(\bar{a}) = w(a) - w(s)$. As a consequence, we have that

$$M(m, t) = \max^*(w(a) - w(s)) = \max^*(w(s) - w(a))$$

$$= \max^*|w(a) - w(s)|, \tag{15}$$

where the maximum is now over all integers a, s for which $0 \leq a, s \leq 2^m - 1$, $s \equiv ta \bmod 2^m - 1$, and $a \not\equiv 0 \bmod 2^m - 1$, which will be the form used in this paper.

THEOREM 12. *Let $C_{1,t}$ be the binary cyclic code of length $n = 2^m - 1$ with defining zeros α and α^t, where α is a primitive element of $\mathrm{GF}(2^m)$ and $t \in \mathbf{Z}_n \backslash \{0\}$. Let $M(m, t)$ be defined as above. Then the weight of every codeword of $C_{1,t}^{\perp}$ is divisible by $2^{m - M(m,t) - 1}$, and there is at least one weight which is not divisible by $2^{m - M(m,t)}$.*

Proof. By definition, the zeros of $C_{1,t}$ are $\{\alpha^1, \alpha^2, \alpha^4, \ldots, \alpha^{2^{m-1}}, \alpha^t, \alpha^{2t}, \ldots, \alpha^{2^{m-1}t}\}$, so the nonzeros of $C_{1,t}^{\perp}$ are $\{\alpha^{-1}, \alpha^{-2}, \alpha^{-4}, \ldots, \alpha^{-2^{m-1}}, \alpha^{-t}, \alpha^{-2t}, \ldots, \alpha^{-2^{m-1}t}\}$. Let

$$N = \{-1, -2, -4, \ldots, -2^{m-1}, -t, -2t, \ldots, -2^{m-1}t\}.$$

We want to find the smallest $\ell \geq 1$ such that $i_1, i_2, \ldots, i_\ell$ come from the set N and

$$\alpha^{i_1 + i_2 + \cdots + i_\ell} = 1. \tag{16}$$

We remark that, since $N \subseteq \mathbf{Z}_{2^m - 1}$ is closed under multiplication by 2, we may assume without loss of generality that all i_j are distinct. Since $i_1, i_2, \ldots, i_\ell$ are from the set N, we may assume that some of them are $-2^{j_1}, -2^{j_2}, \ldots, -2^{j_c}$ and the rest are $-2^{h_1}t, -2^{h_2}t, \ldots, -2^{h_d}t$. Let $b = 2^{j_1} + 2^{j_2} + \cdots + 2^{j_c}$, and let $a = 2^{h_1} + 2^{h_2} + \cdots + 2^{h_d}$. Then we have $c + d = \ell$, $0 \leq a, b \leq 2^m - 1$, $w(a) = c$, $w(b) = d$, and since $\ell \geq 1$ we also have $a \neq 0$ or $b \neq 0$. Now $\alpha^{i_1 + i_2 + \cdots + i_\ell} = 1$ if and only if $\alpha^{-b - ta} = 1$, which is equivalent to

$$b + ta \equiv 0 \bmod 2^m - 1. \tag{17}$$

Write $s = 2^m - 1 - b$. Then (17) is equivalent to $s \equiv ta \bmod 2^m - 1$ and since $w(s) = w(\bar{b}) = m - w(b)$, we have $\ell = m - w(s) + w(a)$ and $a \neq 0$ or $s \neq 2^m - 1$. This tells us that the smallest ℓ such that (16) holds necessarily satisfies $\ell = m - M(m, t)$. The conclusion of the theorem now follows from Theorem 11. ■

5. THE DETERMINATION OF $M(m, t)$

In this section we will determine the number $M(m, t)$ as defined in (15) for various values of t. We treat successively the Gold case ($t = 2^r + 1$), the Kasami case ($t = 2^{2r} - 2^r + 1$), the Welch case ($t = 2^{(m-1)/2} + 3$, m odd), and the Niho cases (m odd, $4r \equiv -1 \bmod m$, $t = 2^{2r} + 2^r - 1$).

In all these cases, we first obtain upper bounds on $M(m, t)$ through a detailed analysis of a suitable binary modular *add-with-carry algorithm* for the computation of $ta \bmod 2^m - 1$, where $a \in \mathbf{Z}_{2^m-1} \backslash \{0\}$ varies. The main idea is to express the quantity $w(ta) - w(a)$ as a sum $\sum_{i=0}^{m-1} \omega_i$, where each ω_i is an expression involving some of the digits of a and some of the carries that occur in the computation of $ta \bmod 2^m - 1$; then we show by a local analysis that this sum cannot grow beyond the desired bounds. In fact, a more detailed analysis of the arguments that we use to obtain these bounds is sufficient to construct examples where the bounds are actually attained.

It turns out that the Gold case is almost trivial and the Kasami case is only slightly more difficult. The Welch and Niho cases are much more involved. In the latter two cases, we essentially construct a weighted directed graph D (not depending on m) with the property that directed cycles in D of length m and total arc weight ω are in 1–1 correspondence with integers $a \in \mathbf{Z}_{2^m-1} \backslash \{0\}$ for which $w(a) - w(ta) = \omega$. We remark that a similar technique has been applied in [10] to count the number of solutions of certain equations involving the binary weight function w. Once we have constructed the weighted digraph D, proving the desired upper bounds on $M(m, t)$ is equivalent to showing that the weight of every directed cycle in D is not larger than its length, which is a finite problem. The Welch case can still be analysed by hand and we will present this analysis in full detail. In contrast, the Niho cases are perhaps best analysed by computer (although an analysis by hand seems feasible). We will give sufficient details to enable the interested readers to do such an analysis using a computer by themselves.

5.1. *Modular Add-with-Carry Algorithms in* $\mathbf{Z}_{2^m-1}$

We now discuss the add-with-carry algorithm for integers modulo $2^m - 1$ and describe some of its basic properties. The required results will follow

from a simple lemma given below. Before we state it, we introduce some notation.

Let $\{a_i\}_{i\in\mathbf{Z}}$ be a periodic integer sequence, with period m. Define

$$a^{[k]} = \sum_{i=0}^{m-1} a_{i+k} 2^i.$$

We write $a = a^{[0]}$.

LEMMA 3. *There exists a periodic integer sequence* $\{c_i\}_{i\in\mathbf{Z}}$ *with period* m *such that*

$$2c_i = a_i + c_{i-1} \tag{18}$$

holds for all i *if and only if* $a \equiv 0 \bmod 2^m - 1$. *If that is the case, then we have* $a^{[k]} \equiv 0 \bmod 2^m - 1$ *for all* k, *and*

$$c_{k-1} = a^{[k]}/(2^m - 1), \tag{19}$$

for all k; *in particular, the solution is* unique. *Also, if* (18) *holds, then*

$$\sum_{k=0}^{m-1} c_k = \sum_{k=0}^{m-1} a_k. \tag{20}$$

Proof. Suppose that (18) holds for all i. Write $c^{[k]} = \sum_{i=0}^{m-1} c_{i+k} 2^i$. Then, using (18), we have that

$$\begin{aligned} 2c^{[k]} &= a^{[k]} + \sum_{i=0}^{m-1} c_{i-1+k} 2^i \\ &= a^{[k]} + 2c^{[k]} + c_{k-1} - 2^m c_{k+m-1} \\ &= a^{[k]} + 2c^{[k]} - c_{k-1}(2^m - 1); \end{aligned}$$

hence $c_{k-1} = a^{[k]}/(2^m - 1)$. So $a^{[k]} \equiv 0 \bmod 2^m - 1$ for all k; in particular, we have that $a \equiv 0 \bmod 2^m - 1$.

Conversely, suppose that $a \equiv 0 \bmod 2^m - 1$. Then obviously $2^k a^{[k]} \equiv a^{[0]} \equiv 0 \bmod 2^m - 1$, hence $a^{[k]} \equiv 0 \bmod 2^m - 1$ for all k. Then the sequence $\{c_i\}_{i\in\mathbf{Z}}$ defined by (19) is an integer sequence with period m, and it is easily

verified that this sequence indeed satisfies (18). Finally, the equation (20) easily follows from (18) by summing (18) for $i = 0, \ldots, m-1$. ■

Now let $a^{(j)}$, $1 \le j \le k$, be nonnegative integers with $0 \le a^{(j)} \le 2^m - 1$, with binary representation $a^{(j)} = a_{m-1}^{(j)} \cdots a_0^{(j)}$ for all j. Furthermore, let $t_1, t_2, \ldots, t_k$ be nonzero integers. Define $t_+ = \sum_{i,t_i>0} t_i$ and $t_- = \sum_{i,t_i<0} t_i$ so that

$$\sum_{j=1}^{k} t_j = t_+ + t_-, \qquad t_+ \ge 0,\ t_- \le 0.$$

Let s be an integer with $0 \le s \le 2^m - 1$, with binary representation $s = s_{m-1} \cdots s_0$, say, and suppose that

$$s \equiv t_1 a^{(1)} + t_2 a^{(2)} + \cdots + t_k a^{(k)} \bmod 2^m - 1.$$

We will prove in the theorem below that there exists a unique integer sequence $c_{-1}, c_0, \ldots, c_{m-1}$ with $c_{-1} = c_{m-1}$ such that

$$2c_i + s_i = \sum_{j=1}^{k} t_j a_i^{(j)} + c_{i-1}, \qquad 0 \le i \le m-1. \tag{21}$$

The s_i and c_i will be called the *digits* and *carries* for the computation modulo $2^m - 1$ of the number s. We emphasize here that the non-obvious part is the existence of a carry sequence with $c_{m-1} = c_{-1}$ (otherwise (21) represents the ordinary add-with-carry algorithm). To stress the periodic nature of this *modular* add-with-carry algorithm, we will often consider all indices as indices from $\mathbf{Z}_m$.

THEOREM 13. (i) *There exists a unique integer sequence* $c_{-1}, c_0, \ldots, c_{m-1}$ *with* $c_{-1} = c_{m-1}$ *such that* (21) *holds. Moreover, if we define* $w(c) = \sum_{i=0}^{m-1} c_i$, *then we have that*

$$w(c) = \sum_{j=0}^{k} t_j w(a^{(j)}) - w(s). \tag{22}$$

Also, we have that $t_- - 1 \le c_i \le t_+$, *and furthermore*

$$t_- \le c_i < t_+ \tag{23}$$

for all i *if* $a^{(j)} \not\equiv 0 \bmod 2^m - 1$ *holds for some* j.

(ii) *If* $\bar{s}_i = 1 - s_i$, $\bar{a}_i^{(j)} = 1 - a_i^{(j)}$, *and* $\tilde{c}_i = t_+ + t_- - 1 - c_i$ *for all* i *and* j, *then the* $\bar{s}_i$ *and* $\tilde{c}_i$ *are the digits and carries for the modular computation of* $\bar{s} \equiv -s \equiv \sum_{j=1}^{k} t_j \bar{a}^{(j)} \bmod 2^m - 1$.

Proof. Define $a_i = -s_i + \sum_{j=1}^{k} t_j a_i^{(j)}$ for $i = 0, \ldots, m-1$ and extend the sequence to a sequence $\{a_i\}_{i \in \mathbf{Z}}$ by letting $a_{i+m} = a_i$ for all $i \in \mathbf{Z}$; now Lemma 3 applies. To obtain the bounds on the c_i, simply note that

$$(2^m - 1)t_- - (2^m - 1) \le a^{[k]} \le (2^m - 1)t_+$$

holds for all k, and if equality holds in either of these bounds then s and each $a^{(j)}$ equals either 0 or $2^m - 1$.

The relation between the digits and carries for the computation of s and $-s$ as given in the second part of the theorem is easily verified by substitution. ■

In the next part, we will be interested in the digits and carries for the modular computation of numbers s for which $s \equiv ta \bmod 2^m - 1$, where $t = \sum_{j=1}^{k} t_j 2^{e_j}$ with each $t_j \in \{-1, 1\}$. Note that if a has binary representation $a = a_{m-1} \ldots a_0$, then $a^{(j)} := 2^{e_j} a$ has binary representation $a_{m-1}^{(j)} \cdots a_1^{(j)} a_0^{(j)}$, where $a_i^{(j)} = a_{i-e_j}$ and the indices are considered modulo m. Now the existence of a carry sequence c and binary digits s_i satisfying

$$2c_i + s_i = \sum_{j=1}^{k} t_j a_{i-e_j} + c_{i-1} \tag{24}$$

for all $i \in \mathbf{Z}_m$ is guaranteed by Theorem 13.

5.2. *The Gold Case*

We now determine $M(m, t)$ for the case $t = 2^r + 1$. Let a and s be integers for which $0 \le a$, $s \le 2^m - 1$, $s \equiv ta \bmod 2^m - 1$, and $a \not\equiv 0 \bmod 2^m - 1$; suppose that s and a have binary representations $a = a_{m-1} \cdots a_0$ and $s = s_{m-1} \cdots s_0$. To determine $M(m, t)$, it is sufficient to derive a suitable upper bound on $w(a) - w(s)$. To this end, we will apply Theorem 13. According to this theorem, there are carries $c_i \in \{0, 1\}$ for $i \in \mathbf{Z}_m$ such that

$$2c_i + s_i = a_{i-r} + a_i + c_{i-1} \tag{25}$$

holds for all $i \in \mathbf{Z}_m$; moreover, $w(c) + w(s) = 2w(a)$. Now let

$$\omega_i = c_i - a_i.$$

Then $\omega_i \in \{-1, 0, 1\}$ and

$$w(\omega) := \sum_{i=0}^{m-1} \omega_i = w(a) - w(s).$$

LEMMA 4. *If* $\omega_i = 1$, *then* $\omega_{i-r} \le 0$.

Proof. "If" $\omega_i = 1$, then $c_i = 1$ and $a_i = 0$. Hence by (25), we have $a_{i-r} = 1$, therefore $\omega_{i-r} \le 0$. ■

THEOREM 14. *We have that*

$$M(m, 2^r + 1) = \begin{cases} m/2 & \text{if } m/(r, m) \text{ is even,} \\ (m - (m, r))/2, & \text{if } m/(r, m) \text{ is odd.} \end{cases}$$

Proof. Partition the m numbers $\omega_0, \ldots, \omega_{m-1}$ into groups

$$\{\omega_i, \omega_{i-r}, \omega_{i-2r}, \ldots\}.$$

There will be $e = (r, m)$ such groups, each consisting of $L = m/(r, m)$ elements. By Lemma 4, the sum of the elements from each group is at most $L/2$ if L is even or $(L-1)/2$ if L is odd. The upper bounds on $w(a) - w(s)$, and hence on $M(m, t)$, now follow.

It is easy to construct examples of $a \in \mathbf{Z}_{2^m-1} \backslash \{0\}$ for which the upper bounds are attained. For example, we may take $a = (2^e - 1) \cdot (2^{r(m/e-\varepsilon)} - 1)/(2^{2r} - 1) = (2^e - 1)(1 + 2^{2r} + 2^{4r} + \cdots + 2^{2r((m/e-\varepsilon)/2-1)})$, where $\varepsilon = 0$ if m/e is even and $\varepsilon = 1$ otherwise. Then $w(a) = (m - \varepsilon e)/2$ and $w((2^r + 1)a) = m - \varepsilon e$. Therefore $|w(a) - w((2^r + 1)a)| = (m - \varepsilon e)/2$. This completes the proof. ■

5.3. *The Kasami Case*

Next, we determine $M(m, t)$ for the case $t = 2^{2r} - 2^r + 1$. In fact, we will consider the more general case where $t = (2^{rk} + 1)/(2^r + 1) = 1 + 2^r + \cdots + 2^{(k-1)r}$, with $k \ge 3$ odd. Let a and s be integers for which $0 \le a$, $s \le 2^m - 1$, $s \equiv ta \bmod 2^m - 1$, and $a \not\equiv 0 \bmod 2^m - 1$; suppose that s and a have binary representations $a = a_{m-1} \cdots a_0$ and $s = s_{m-1} \cdots s_0$. Again, we apply Theorem 13 to derive a suitable upper bound on $w(a) - w(s)$. According to this theorem, there are carries $c_i \in \{-(k-1)/2, \ldots, (k-1)/2\}$ for $i \in \mathbf{Z}_m$ such that

$$2c_i + s_i = a_{i-(k-1)r} - a_{i-(k-2)r} + \cdots - a_{i-r} + a_i + c_{i-1} \tag{26}$$

holds for all $i \in \mathbf{Z}_m$; moreover, $w(c) + w(s) = w(a)$. In this case, we take $\omega_i = c_i + c_{i-r}$, so that $w(\omega) = \sum_{i=0}^{m-1} \omega_i = 2(w(a) - w(s))$.

LEMMA 5. *If $\omega_j \notin \{-1, 0, 1\}$ for some $j \in \mathbf{Z}_m$, then $a \equiv 0 \bmod 2^m - 1$.*

Proof. By adding the two equations (26) for i and $i-r$, we obtain that

$$2w_i + s_i + s_{i-r} = a_{i-kr} + a_i + w_{i-1} \tag{27}$$

for all $i \in \mathbf{Z}_m$. From (27), it is easily seen that

$$|w_i| \le (|w_{i-1}| + 1)/2, \tag{28}$$

for all $i \in \mathbf{Z}_m$. Due to the cyclic nature of (27), we may conclude that $|\omega_i| \le 2$ for all i; moreover, if $\omega_j \in \{-1, 0, 1\}$ for some $j \in \mathbf{Z}_m$, then the same will be true for all subsequent indices $i = j+1, j+2, \ldots,$ and hence for all $i \in \mathbf{Z}_m$. The only other possibilities are that either $w_i = 2, s_i = s_{i-r} = 0, a_{i-kr} = a_i = 1$ for all i, or $w_i = -2, s_i = s_{i-r} = 1, a_{i-kr} = a_i = 0$ for all i; in both these cases, we have that $a \equiv 0 \bmod 2^m - 1$. ■

THEOREM 15. *For $k \ge 3$ odd, we have that*

$$M(m, (2^{kr}+1)/(2^r+1)) = M(m, 2^r - 1) = \begin{cases} m/2, & \text{if } m/(r,m) \text{ is even;} \\ (m-(m,r))/2, & \text{if } m/(r,m) \text{ is odd.} \end{cases}$$

Proof. If $c_i = c_{i-r} = \pm 1$ for some i, then $|\omega_i| = 2$, hence $a \equiv 0 \bmod 2^m - 1$ by Lemma 5, which is excluded in the definition of $M(m, (2^{kr}+1)/(2^r+1))$. So we may assume that if $c_i = 1$, then $c_{i+r} = c_{i-r} = 0$. Again we partition the m numbers $c_0, c_1, \ldots, c_{m-1}$ into groups $\{c_i, c_{i-r}, c_{i-2r}, \ldots\}$. The remainder of the proof now proceeds similarly to the proof of Theorem 14. ■

5.4. *The Welch Case*

For the moment, let $m = 2r+1$ be odd. We now consider $M(m, t)$ for the case where $t = 2^r + 3$. Let a and s be integers for which $0 \le a, s \le 2^m - 1$, $s \equiv ta \bmod 2^m - 1$, and $a \not\equiv 0 \bmod 2^m - 1$; suppose that s and a have binary representations $a = a_{m-1} \cdots a_0$ and $s = s_{m-1} \cdots s_0$. Again, we apply Theorem 13 to derive a suitable upper bound on $w(a) - w(s)$. According to this theorem, there are carries $c_i \in \{0, 1, 2\}$ for $i \in \mathbf{Z}_m$ such that

$$2c_i + s_i = a_i + a_{i-1} + a_{i-r} + c_{i-1} \tag{29}$$

holds for all $i \in \mathbf{Z}_m$; moreover, $w(c) + w(s) = 3w(a)$.

Our aim is to prove that

$$|w(s) - w(a)| \le r. \tag{30}$$

In fact, we shall prove more. Let x, y, p, and q be integers for which $0 \leq x, y, p, q \leq 2^m - 1$,

$$p \equiv 3x + y, \qquad q \equiv 3y + 2^{m-1}x \bmod 2^m - 1, \tag{31}$$

and at least one of x, y is nonzero modulo $2^m - 1$; suppose that x, y, p, and q have binary representations $x = x_{m-1} \cdots x_0$, $y = y_{m-1} \cdots y_0$, $p = p_{m-1} \cdots p_0$, and $q = q_{m-1} \cdots q_0$. (The motivation for this will be discussed in a moment.) By Theorem 13, there are carries d_i, $e_i \in \{0, 1, 2\}$ such that

$$2d_i + p_i = x_i + x_{i-1} + y_i + d_{i-1} \tag{32}$$

and

$$2e_i + q_i = y_i + y_{i-1} + x_{i+1} + e_{i-1} \tag{33}$$

hold for all $i \in \mathbf{Z}_m$; furthermore, the carry sequences d and e satisfy

$$w(d) = 2w(x) + w(y) - w(p), \qquad w(e) = 2w(y) + w(x) - w(q). \tag{34}$$

We shall prove that

$$|w(x) + w(y) - w(p) - w(q)| \leq m. \tag{35}$$

Observe that if we let $x_i = a_i$, $d_i = c_i$, $p_i = s_i$, and $y_i = a_{i-r}$, $e_i = c_{i-r}$, $q_i = s_{i-r}$, for all i (so that $x = a$, $y \equiv 2^r a$, $p = s \equiv (2^r + 3)a$, and $q \equiv 2^r p$), then (32) follows from (29). Moreover, since $-2r \equiv 1 \bmod m$, (33) follows from (29) by replacing i by $i - r$. In that case $w(x) = w(y) = w(a)$ and $w(p) = w(q) = w(s)$, and (30) follows immediately from (35) because $m = 2r + 1$ is odd.

We now proceed to prove (35). Since the parity of m will no longer play a role in what follows, we will now drop our previous assumption that m is odd. In order to prove (35), we will follow a similar strategy as before. Let the numbers ξ_i ad η_i be defined by

$$\xi_i = x_i + x_{i-1} - d_i \tag{36}$$

and

$$\eta_i = y_i + y_{i-1} - e_i \tag{37}$$

and let us set

$$\omega_i = \xi_i + \eta_i. \tag{38}$$

Note that by (34), we have that $w(\xi) = w(p) - w(y)$ and $w(\eta) = w(q) - w(x)$; hence

$$w(\omega) := \sum_{i=0}^{m-1} \omega_i = w(p) + w(q) - w(x) - w(y). \tag{39}$$

We will prove (35) in a number of steps. In some of these, we will claim that certain expressions satisfy a lower and an upper bound. We will then only prove the upper bound; the corresponding lower bound will automatically follow from the symmetry stated in part (ii) of Theorem 13. (This remark also applies to the material in the Appendix.) Our first result gives a bound on ξ_i and η_i.

LEMMA 6. *We have that* $\xi_i, \eta_i \in \{-1, 0, 1\}$ *for all* i; *hence* $|\omega_i| \le 2$.

Proof. If $x_i = x_{i-1} = 1$, then by (32) we have that $d_i \ge 1$, hence $\xi_i \le 1$. Similarly, if $y_i = y_{i-1} = 1$, then $e_i \ge 1$, and hence $\eta_i \le 1$. Therefore $\omega_i = \xi_i + \eta_i \le 2$. ■

Next we will show that if ω takes the value 2 in some position, then the values taken by ω in subsequent positions are a limited number of 1s followed by a non-positive number. This result is stated more precisely in the following lemma.

LEMMA 7. *Suppose that* $\omega_h = 2$. *Then there is an integer* k *with* $0 \le k \le 3$ *such that* $\omega_{h+i} = 1$ *for* $i = 1, 2, \ldots, k$ *and* $\omega_{h+k+1} \le 0$.

By far the easiest way to verify this claim is by using a computer. To do so, for all choices of d_i, e_i, $x_i, \ldots, x_{i+7}$, and $y_i, \ldots, y_{i+6}$, we compute $\omega_{i+1}, \ldots, \omega_{i+6}$ using (32), (33), (36), (37), and (38). By inspecting all cases where $\omega_{i+2} = 2$, we see that Lemma 7 is true.

Alternatively, the claim in Lemma 7 can also be verified by a rigorous, but somewhat tedious analysis. The interested reader will find this analysis in the Appendix.

The next result follows directly from Lemma 7.

COROLLARY 4. *We have that*

$$|w(\omega)| \le m.$$

Proof. By Lemma 7, we can partition the m values ω_i, $i = 0, \ldots, m-1$, into blocks $B = \{\omega_h, \omega_{h+1}, \ldots, \omega_{h+j-1}\}$ of length $|B| = j \le 5$ such that the

sum S_B of the elements in B satisfies

$$|S_B| \leq |B|,$$

from which the desired conclusion follows immediately. ■

THEOREM 16. (i) *Let x, y, p and q be integers for which $0 \leq x, y, p, q \leq 2^m - 1$, $p \equiv 3x + y$, $q \equiv 3y + 2^{m-1}x \bmod 2^m - 1$, and at least one of x, y is nonzero modulo $2^m - 1$. Then we have that*

$$|w(x) + w(y) - w(p) - w(q)| \leq m.$$

(ii) *For odd m, we have that*

$$M(m, 2^{(m-1)/2} + 3) = (m-1)/2.$$

Proof. The first part of the theorem follows from Corollary 4 by using (39) and (31). If $m = 2r + 1$ is odd, then by taking $y = 2^r x$, we find that

$$|w(x) - w((2^r + 3)x)| \leq \lfloor m/2 \rfloor.$$

It is easy to see that the upper bound above is attained by the elements $1 + 2^2 + 2^4 + \cdots + 2^{2\lfloor (r-1)/2 \rfloor}$ from $\mathbf{Z}_{2^m-1}$. Therefore part (ii) follows. ■

5.5. *The Niho Cases*

Finally, we determine $M(m, t)$ for the cases where $m = 4r + 1$, $t = 2^{2r} + 2^r - 1$ or $m = 4r - 1$, $t = 2^{2r-1} + 2^{3r-1} - 1$. Our aim is to prove that $M(m, t) \leq (m-1)/2$ in these two cases. To motivate our approach, we will start treating the case where $m = 4r + 1$ and $t = 2^{2r} + 2^r - 1$. Let a and s be integers for which $0 \leq a, \; s \leq 2^m - 1, \; s \equiv ta \bmod 2^m - 1$, and $a \not\equiv 0 \bmod 2^m - 1$; suppose that s and a have binary representations $a = a_{m-1} \cdots a_0$ and $s = s_{m-1} \cdots s_0$. Again, we apply Theorem 13 to derive a suitable upper bound on $w(a) - w(s)$. According to this theorem, there are carries $c_i \in \{-1, 0, 1\}$ for $i \in \mathbf{Z}_m$ such that

$$2c_i + s_i = a_{i-2r} + a_{i-r} - a_i + c_{i-1} \tag{40}$$

holds for all $i \in \mathbf{Z}_m$; moreover, $w(c) = w(a) - w(s)$. We have to prove that

$$|w(c)| = |w(s) - w(a)| \leq 2r. \tag{41}$$

As in the Welch case, we shall prove more. Let $x^{(j)}$, $j = 0, 1, 2, 3$, be four integers, not all 0 modulo $2^m - 1$, with binary representation $x^{(j)} = x^{(j)}_{m-1} \cdots x^{(j)}_0$. Let the numbers $p^{(j)}$, $j = 0, 1, 2, 3$, satisfy

$$p^{(0)} \equiv x^{(2)} + x^{(1)} - x^{(0)} \bmod 2^m - 1, \tag{42}$$

$$p^{(1)} \equiv x^{(3)} + x^{(2)} - x^{(1)} \bmod 2^m - 1, \tag{43}$$

$$p^{(2)} \equiv x^{(0)}/2 + x^{(3)} - x^{(2)} \bmod 2^m - 1, \tag{44}$$

$$p^{(3)} \equiv x^{(1)}/2 + x^{(0)}/2 - x^{(3)} \bmod 2^m - 1, \tag{45}$$

(The motivation for this will follow shortly.) Let the binary digits of the $p^{(j)}$ be $p^{(j)}_i$, for $i = 0, \ldots, m-1$. By Theorem 13, there are carries $e^{(j)}_i \in \{-1, 0, 1\}$ for all $i \in \mathbf{Z}$ such that

$$2e^{(0)}_i + p^{(0)}_i = x^{(2)}_i + x^{(1)}_i - x^{(0)}_i + e^{(0)}_{i-1}, \tag{46}$$

$$2e^{(1)}_i + p^{(1)}_i = x^{(3)}_i + x^{(2)}_i - x^{(1)}_i + e^{(1)}_{i-1}, \tag{47}$$

$$2e^{(2)}_i + p^{(2)}_i = x^{(0)}_{i+1} + x^{(3)}_i - x^{(2)}_i + e^{(2)}_{i-1}, \tag{48}$$

and

$$2e^{(3)}_i + p^{(3)}_i = x^{(1)}_{i+1} + x^{(0)}_{i+1} - x^{(3)}_i + e^{(3)}_{i-1}, \tag{49}$$

hold for all $i \in \mathbf{Z}_m$. We shall prove that if all $x^{(j)}$ are nonzero modulo $2^m - 1$, then

$$|w(x^{(0)}) + w(x^{(1)}) + w(x^{(2)}) + w(x^{(3)}) - w(p^{(0)}) - w(p^{(1)}) - w(p^{(2)}) - w(p^{(3)})| \le 2m. \tag{50}$$

Observe that if we let $x^{(j)}_i = a_{i-jr}$, $e^{(j)}_i = c_{i-jr}$, and $p^{(j)}_i = s_{i-jr}$, for $j = 0, 1, 2, 3$ and for all i so that $x^{(j)} = 2^j a$ and $p^{(j)} = 2^j(2^{2r} + 2^r - 1)a$, for $j = 0, 1, 2, 3$, then (46) follows from (40), and (47), (48), and since $-4r \equiv 1 \bmod m$, (49) follows from (40) by replacing i by $i - r$, $i - 2r$, and $i - 3r$, respectively. In that case $w(x^{(j)}) = w(a)$ and $w(p^{(j)}) = w(s)$, $j = 0, 1, 2, 3$, and since obviously all $x^{(j)}$ are nonzero modulo $2^m - 1$, (41) follows immediately from (50) because $m = 4r + 1$ is odd.

Very conveniently, the case where $m = 4r - 1$ and $t = 2^{2r-1} + 2^{3r-1} - 1$ can also be derived from (50). Indeed, if we let $x^{(0)} = 2^{3r}a$, $x^{(1)} = 2^{2r}a$,

$x^{(2)} = 2^r a$, and $x^{(3)} = a$, then (50) implies that $|w(ta) - w(a)| \leq m/2$, and since $m = 4r - 1$ is odd, we may conclude that $|w(ta) - w(a)| \leq (m-1)/2$.

In order to prove (50), we follow the same strategy as before. Let us define

$$\omega_i = e_i^{(0)} + e_i^{(1)} + e_i^{(2)} + e_i^{(3)}. \tag{51}$$

Now it follows easily from (46)–(49) that (50) is equivalent to

$$|w(\omega)| = \left| \sum_{i=0}^{m-1} \omega_i \right| \leq 2m. \tag{52}$$

We shall prove (52) by analysing a certain weighted directed graph D which we construct as follows. The set of vertices of D is the set of all vectors

$$(x, x', x'', x''', e, e', e'', e'''),$$

where $x, x', x'', x''' \in \{0, 1\}$ and $e, e', e'', e''' \in \{-1, 0, 1\}$. Corresponding to any solution $x^{(j)}$, $e^{(j)}$, $p^{(j)}$ for $j = 0, 1, 2, 3$ of (46)–(49), define the m vertices

$$v_i = (x_i^{(0)}, x_i^{(1)}, x_{i-1}^{(2)}, x_{i-1}^{(3)}, e_{i-1}^{(0)}, e_{i-1}^{(1)}, e_{i-1}^{(2)}, e_{i-1}^{(3)}), \qquad i = 0, 1, \ldots, m-1.$$

Our construction of the weighted directed edges of D will be motivated by the desire to obtain a 1–1 correspondence between solutions of (46)–(49) and directed cycles in D of length m so that a solution $x^{(j)}$, $e^{(j)}$, $p^{(j)}$ for $j = 0, 1, 2, 3$ will correspond to the directed cycle $v_0 \to v_1 \to \cdots \to v_{m-1} \to v_0$. We define a directed edge from a vertex $(x, x', x'', x''', e, e', e'', e''')$ to a vertex $(X, X', X'', X''', E, E', E'', E''')$, of weight $W = E + E' + E'' + E'''$, if and only if

$$X'' + x' - x + e - 2E \in \{0, 1\}; \tag{53}$$

$$X''' + X'' - x' + e' - 2E' \in \{0, 1\}; \tag{54}$$

$$X + X''' - X'' + e'' - 2E'' \in \{0, 1\}; \tag{55}$$

$$X' + X - X''' + e''' - 2E''' \in \{0, 1\}. \tag{56}$$

Here, the reader should think of the two vertices $(x, x', x'', x''', e, e', e'', e''')$ and $(X, X', X'', X''', E, E', E'', E''')$ as v_i and v_{i+1}, respectively, should think of W as ω_i, and should observe that (53)–(56) reflect (46)–(49).

Given these definitions, it is now easily verified that solutions of (46)–(49) with $w(\omega) = W$ are in 1–1 correspondence with directed cycles in D of length m and weight W. (Here, the weight $w(C)$ of a directed cycle C is defined as the sum of the weights of the edges that make up the cycle.) Let us call a directed cycle C in D a *null cycle* if the projection onto one of the first four coordinates of the vertices on the cycle is constant. (Observe that a null cycle corresponds to a solution of (46)–(49) for which one of $x^{(0)}$, $x^{(1)}$, $x^{(3)}$ is congruent to 0 modulo $2^m - 1$.) As a consequence, (52) is equivalent to the following.

THEOREM 17. *Let C be a non-null cycle of length m in D. Then we have that*

$$|w(C)| \leq 2m.$$

Proof. We investigated the weighted digraph D with the aid of a computer. It turns out that D, a digraph on $2^4 3^4 = 1296$ vertices, has 941 strongly connected components. Here, two vertices of a digraph are said to be *strongly connected* if they are contained together in a directed cycle. The relation of being strongly connected is an equivalence relation on the set of vertices; the equivalence classes of this relation are called the *the strongly connected components* of the directed graph.

One of these strongly connected components has size 320 (that is, contains 320 vertices) and all edge weights of directed edges in this component are contained in the set $\{-2, -1, 0, 1, 2\}$. So in this component, the theorem holds for *all directed* cycles.

The directed graph D has six further strongly connected components K_i, $i = 1, \ldots, 6$, each of size 6, two strongly connected components L_i, $i = 1, 2$, each of size 4, and further 932 strongly connected components M_i, $i = 1, \ldots, 932$, each of size 1.

Obviously, all strongly connected components of size 1 contain only null cycles. A further inspection reveals that in each of the eight strongly connected components K_i and L_j, the vertices have a constant projection onto one of the first four coordinates. Hence, certainly all cycles in these strongly connected components are null cycles. ■

THEOREM 18. (i) *Let $x^{(j)}$, $j = 0, 1, 2, 3$, be four integers, all nonzero modulo $2^m - 1$. Let the numbers $p^{(j)}$, $j = 0, 1, 2, 3$, satisfy $p^{(0)} \equiv x^{(2)} + x^{(1)} - x^{(0)} \bmod 2^m - 1$, $p^{(1)} \equiv x^{(3)} + x^{(2)} - x^{(1)} \bmod 2^m - 1$, $p^{(2)} \equiv x^{(0)}/2 + x^{(3)} - x^{(2)} \bmod 2^m - 1$, and $p^{(3)} \equiv x^{(1)}/2 + x^{(0)}/2 - x^{(3)} \bmod 2^m - 1$. Then we have that*

$$|w(x^{(0)}) + w(x^{(1)}) + w(x^{(2)}) + w(x^{(3)}) - w(p^{(0)}) - w(p^{(1)})$$

$$- w(p^{(2)}) - w(p^{(3)})| \leq 2m.$$

(ii) *For* $m = 4r + 1$, *we have that*

$$M(m, 2^{2r} + 2^r - 1) = (m - 1)/2.$$

(iii) *For* $m = 4r - 1$, *we have that*

$$M(m, 2^{2r-1} + 2^{3r-1} - 1) = (m - 1)/2.$$

Proof. The first part of the theorem follows from Theorem 17. From part (i), we have $M(m, 2^{2r} + 2^r - 1) \leq (m - 1)/2$. It is easy to see that the upper bound in this case is attained by $a = 2^r + 1$. This finishes the proof of part (ii). Similarly, $M(m, 2^{2r-1} + 2^{3r-1} - 1) \leq (m - 1)/2$ and the upper bound here is attained by $a = 1$. ■

6. CONCLUSIONS

In this section, we use the methods developed in previous sections to prove the main results of this paper. Our first theorem concerns the Gold case. The result is of course well known and is cited in many places (see, for example, [2, 3, 18]).

THEOREM 19. *Let* $t = 2^r + 1$ *with* $0 < r < m$, *and let* $C_{1,t}$ *be the cyclic code of length* $2^m - 1$ *with defining zeros* α *and* α^t, *where* α *is a primitive element in* $\mathrm{GF}(2^m)$. *Let* $e = (r, m)$. *Then* $C_{1,t}^{\perp}$ *is a three-weight code* (*in fact, with nonzero weights* $2^{m-1} + \varepsilon 2^{(m-2+e)/2}$, $\varepsilon = -1, 0, 1$) *if and only if* m/e *is odd or* m *is even and* $r = m/2$.

Proof. We begin by noting that the dimension k of $C_{1,t}^{\perp}$ satisfies $k = 2m$ except when $m = 2r$, in which case $k = m + m/2$. (To see this, consider the binary representation of $2^i(2^r + 1)$ for $i = 1, \ldots, m - 1$.)

By Theorem 14, we know that $M(m, t) = (m - e')/2$, where $e' = e$ if m/e is odd and $e' = 0$ otherwise. Hence by Theorem 12, the weight of every codeword of $C_{1,t}^{\perp}$ is divisible by $2^{m-M(m,t)-1} = 2^{(m-2+e')/2}$.

First suppose that $m \neq 2r$. Then we apply Theorem 2 with $d^2 = 2^{m-2+e'}$. From Theorem 5, we know that the number of codewords of weight 3 or 4 of $C_{1,t}$ is $A_3 + A_4 = (2^{e-1} - 1)2^{m-2}(2^m - 1)/3$, hence by Theorem 2, the code $C_{1,t}^{\perp}$ has only three nonzero weights $2^{m-1} + \varepsilon 2^{(m-2+e)/2}$, $\varepsilon = -1, 0, 1$ if $e' = e$ and has at least four nonzero weights otherwise.

Next, suppose that $m = 2r$. From (5), now specialised to $n = 2^m - 1$ and $k = 3m/2$, we see that in this case $E = 0$ if $A_3 + A_4 = (2^{e-1} - 1) \cdot 2^{m-2}(2^m - 1)/3$, with $e = (r, m) = r$. So by Theorem 5, the code $C_{1,t}^{\perp}$ has only three nonzero weights. ■

Our next result concerns the Kasami case. The well-known "if" part in the theorem below was first obtained by Welch [22] and Kasami [14]. The "only if" part might be new.

THEOREM 20. *Let $t = 2^{2r} - 2^r + 1$ with $1 < r < m$, and let $C_{1,t}$ be the cyclic code of length $2^m - 1$ with defining zeros α and α^t, where α is a primitive element in* GF(2^m). *Let $e = (r, m)$. Then $C_{1,t}^{\perp}$ is a three-weight code (in fact, with nonzero weights $2^{m-1} + \varepsilon 2^{(m-2+e)/2}$, $\varepsilon = -1, 0, 1$) if and only if m/e is odd.*

Proof. The proof more or less follows the proof for the Gold case. Here, the dimension k of $C_{1,t}^{\perp}$ satisfies $k = 2m$ in all cases. (To see this, consider the binary representation of $2^i(2^{2r} - 2^r + 1)$ for $i = 1, \ldots, m-1$.)

By Theorem 15, we have that $M(m, t) = (m - e')/2$, where $e' = e$ if m/e is odd and $e' = 0$ otherwise. Hence by Theorem 12, the weight of every codeword of $C_{1,t}^{\perp}$ is divisible by $2^{m-M(m,t)-1} = 2^{(m-2+e')/2}$.

Now we apply Theorem 2 with $d^2 = 2^{m-2+e'}$. If m/e is even, then $e' = 0$ and we immediately see from Theorem 2 that $C_{1,t}^{\perp}$ cannot be a three-weight code. (Indeed, the number $A_3 + A_4$ of codewords of weight 3 or 4 would have to be negative, which is absurd.) Conversely, if m/e is odd, then from Theorem 6 and Theorem 2, the code $C_{1,t}^{\perp}$ is a three-weight code, with weights as indicated in the theorem. ■

The weight distribution of a three-weight code $C_{1,t}^{\perp}$ with known weights can easily be determined, for example by using the power moments. The results for the codes from Theorems 19 and 20 are as follows. If $t = 2^r + 1$ or $t = 2^{2r} + 2^r + 1$, if $e = (m, r)$, and if m/e is odd, then

$$B_{2^{m-1}-2^{(m-2+e)/2}} = (2^m - 1)(2^{m-e-1} + 2^{(m-e-2)/2})$$

$$B_{2^{m-1}} = (2^m - 1)(2^m - 2^{m-e} + 1)$$

$$B_{2^{m-1}+2^{(m-2+e)/2}} = (2^m - 1)(2^{m-e-1} - 2^{(m-e-2)/2}). \tag{57}$$

The following two results concern the Welch and Niho conjectures.

THEOREM 21. *Let $m = 2r + 1$, $t = 2^r + 3$, and let $C_{1,t}$ be the cyclic code of length $2^m - 1$ with defining zeros α and α^t, where α is a primitive element in* GF(2^m). *Then $C_{1,t}^{\perp}$ is a three-weight code with weights $2^{m-1} + \varepsilon 2^{(m-1)/2}$, $\varepsilon = -1, 0, 1$, and weight-distribution given by* (57) *with $e = 1$.*

Proof. Since $(t, 2^m - 1) = 1$, the code $C_{1,t}^{\perp}$ has dimension $2m$. By Theorem 16, we know that $M(m, t) = (m - 1)/2$. Hence by Theorem 12, the weight of every codeword of $C_{1,t}^{\perp}$ is divisible by $2^{m-M(m,t)-1} = 2^{(m-1)/2}$.

Now we apply Theorem 2 with $d^2 = 2^{m-2+e}$, where $e = 1$. From Theorem 8, we know that the number of codewords of weight 3 or 4 of $C_{1,t}$ is $A_3 + A_4 = 0$, hence by Theorem 2, the code $C_{1,t}^{\perp}$ has only three weights $2^{m-1} + \varepsilon 2^{(m-1)/2}$, $\varepsilon = -1, 0, 1$. ■

THEOREM 22. *Let m be odd, $t = 2^{(m-1)/2} + 2^{(m-1)/4} - 1$ if $m \equiv 1 \pmod 4$ and $t = 2^{(m-1)/2} + 2^{(3m-1)/4} - 1$ if $m \equiv 3 \pmod 4$. Let $C_{1,t}$ be the cyclic code of length $2^m - 1$ with defining zeros α and α^t, where α is a primitive element in $\mathrm{GF}(2^m)$. Then $C_{1,t}^{\perp}$ is a three-weight code with weights $2^{m-1} + \varepsilon 2^{(m-1)/2}$, $\varepsilon = -1, 0, 1$, and weight-distribution given by (57) with $e = 1$.*

Proof. The proof proceeds exactly in the same way as in the Welch case except that we use Theorem 18 to get the value of $M(m, t)$ and Theorem 10 to get $A_3 + A_4 = 0$. ■

The last two theorems state that both the Welch and Niho cases give rise to pairs of preferred m-sequences. Concerning preferred pairs in general, we have the following.

THEOREM 23. *Let $C_{1,t}$ be the binary cyclic code of length $2^m - 1$ with defining zeros α and α^t, where α is a primitive element of $\mathrm{GF}(2^m)$ and $\gcd(t, 2^m - 1) = 1$. Let A_w denote the number of codewords of weight w in $C_{1,t}$. The code $C_{1,t}^{\perp}$ is a three-weight code with nonzero weights 2^{m-1}, $2^{m-1} \pm 2^{\lfloor (m+2)/2 \rfloor - 1}$, or, equivalently, the pair of m-sequences obtained from an m-sequence of length $2^m - 1$ and the decimation of that sequence by the integer t constitute a preferred pair, if and only if either*

(i) *m odd, $A_3 + A_4 = 0$, and all weights in $C_{1,t}^{\perp}$ are divisible by $2^{(m-1)/2}$, or*

(ii) *m even, $A_3 + A_4 = 2^{m-2}(2^m - 1)/3$, and all weights in $C_{1,t}^{\perp}$ are divisible by $2^{m/2}$.*

Proof. As explained in the introduction, the cross-correlation of a pair of m-sequences takes on values -1 and $-1 \pm 2D$ if and only if the code $C_{1,t}^{\perp}$ has only nonzero weights 2^{m-1} and $2^{m-1} \pm D$. By definition, the pair is preferred if $D = 2^{\lfloor (m+2)/2 \rfloor - 1}$. Now the theorem follows directly from Theorem 2 with $e = 1, 2$. ■

APPENDIX

In this Appendix, we shall give a rigorous proof of Lemma 7. The notation used here is the same as in Section 5.4. In what follows, we will repeatedly use (32), (33), (36), and (37) with different values i. To help the reader follow the somewhat detailed arguments, we will refer to these equations as

$D_i(x_i, x_{i-1}, y_i, d_{i-1})$, $E_i(y_i, y_{i-1}, x_{i+1}, e_{i-1})$, $X_i(x_i, x_{i-1}, d_i)$, and $Y_i(y_i, y_{i-1}, e_i)$, respectively.

LEMMA 8. *If* $\omega_j = 2$, *then* $y_j = 1$, $x_{j+1} = 0$, *and* $d_{j+1} \geq 1$.

Proof. If $\omega_j = 2$, by Lemma 6, we have $\xi_j = 1$ and $\eta_j = 1$. Assume to the contrary that $y_j = 0$, then from $\eta_j = 1$ and $Y_j(y_j = 0, y_{j-1}, e_j)$, we have that $y_{j-1} = 1$ and $e_j = 0$, which together with $E_j(y_j, y_{j-1} = 1, x_{j+1}, e_{j-1})$ implies that $e_{j-1} = 0$. Now from $E_{j-1}(y_{j-1} = 1, y_{j-2}, x_j, e_{j-2})$, we find that $x_j = 0$, so from $\xi_j = 1$ and $X_j(x_j, x_{j-1}, d_j)$ we conclude that $x_{j-1} = 1$ and $d_j = 0$. Hence by $D_j(x_j, x_{j-1} = 1, y_j, d_{j-1})$, we have $d_{j-1} = 0$. However by $D_{j-1}(x_{j-1} = 1, x_{j-2}, y_{j-1} = 1, d_{j-2})$, we must have $d_{j-1} = 1$. This is a contradiction. Therefore we conclude that $y_j = 1$.

From $\xi_j = 1$ and $X_j(x_j, x_{j-1}, d_j)$, we see that $x_j + x_{j-1} \geq 1$. Hence by $D_j(x_j, x_{j-1}, y_j = 1, d_{j-1})$, we have $d_j \geq 1$. Then by $\xi_j = 1$ and $X_j(x_j, x_{j-1}, d_j \geq 1)$, we see that $x_j = x_{j-1} = 1$ and $d_j = 1$. Now $d_{j+1} \geq 1$ follows from $D_{j+1}(x_{j+1}, x_j = 1, y_{j+1}, d_j = 1)$.

Finally, if $x_{j+1} = 1$, then first from $\eta_j = 1$ and $Y_j(y_j, y_{j-1}, e_j)$, we conclude that $y_j + y_{j-1} \geq 1$; so by $E_j(y_j, y_{j-1}, x_{j+1} = 1, e_{j-1})$, we have $e_j \geq 1$. Now from $\eta_j = 1$ and $Y_j(y_j, y_{j-1}, e_j \geq 1)$, we see that $y_j = y_{j-1} = 1$ and $e_j = 1$. Hence from $E_j(y_j = 1, y_{j-1} = 1, x_{j+1} = 1, e_{j-1})$ again, we obtain that $e_{j-1} = 0$. Also, from $\xi_j = 1$ and $X_j(x_j, x_{j-1}, d_j)$, we see that $x_j + x_{j-1} \geq 1$, and by $D_j(x_j, x_{j-1}, y_j = 1, d_{j-1})$, we have $d_j \geq 1$. Therefore we conclude that $x_j = x_{j-1} = 1$ and $d_j = 1$. However, from $E_{j-1}(y_{j-1} = 1, y_{j-2}, x_j = 1, e_{j-2})$, we obtain that $e_{j-1} \geq 1$, contradicting the conclusion $e_{j-1} = 0$ obtained earlier. So we conclude that $x_{j+1} = 0$. ■

LEMMA 9. *Let* $y_j = 1$, $x_{j+1} = 0$, *and* $d_{j+1} \geq 1$. *If* $\omega_{j+1} \geq 1$, *then* $\omega_{j+1} = 1$. *If furthermore* $\omega_{j+2} \geq 1$, *then* $y_{j+1} = 1$ *and* $e_{j+1} \geq 1$.

Proof. If $\omega_{j+1} \geq 1$, then $\xi_{j+1} \geq 0$. so by $X_{j+1}(x_{j+1} = 0, x_j, d_{j+1} \geq 1)$, we have that $x_j = 1$, $\xi_{j+1} = 0$. So $\omega_{j+1} = \eta_{j+1} = 1$. If $y_{j+1} = 1$, then $e_{j+1} \geq 1$ follows from $E_{j+1}(y_{j+1} = 1, y_j = 1, x_{j+2}, e_j)$. In the following, we will show that if $y_{j+1} = 0$, then $\omega_{j+2} \leq 0$. The proof goes as follows. if $y_{j+1} = 0$, then from $\eta_{j+1} = 1$ and $Y_{j+1}(y_{j+1} = 0, y_j = 1, e_{j+1})$, we see that $e_{j+1} = 0$. Then by $E_{j+1}(y_{j+1} = 0, y_j = 1, x_{j+2}, e_j)$, we have $x_{j+2} = e_j = 0$, hence by $X_{j+2}(x_{j+2} = 0, x_{j+1} = 0, d_{j+2})$, we obtain $\xi_{j+2} = -d_{j+2} \leq 0$. Therefore if $d_{j+2} \geq 1$, then $\omega_{i+2} \leq 0$. If $d_{j+2} = 0$, then by $D_{j+2}(x_{j+2} = 0, x_{j+1} = 0, y_{j+2}, d_{j+1} = 1)$, we have $y_{j+2} = 0$. Hence by $Y_{j+2}(y_{j+2} = 0, y_{j+1} = 0, e_{j+2})$, we see that $\eta_{j+2} = -e_{j+2} \leq 0$. So in both cases ($d_{j+2} \geq 1$ or $d_{j+2} = 0$), we have $\omega_{i+2} \leq 0$.

LEMMA 10. *If* $y_{j-1} = 1$, $d_{j-1} \geq 1$, $e_{j-1} \geq 1$, $x_j + x_{j-1} \leq 1$ *and* $\omega_j \geq 1$, *then* $\omega_j = 1$, $x_j + x_{j-1} = 1$, $x_{j+1} = 0$, *and* $y_j = d_j = e_j = 1$.

Proof. Since $y_{j-1} = 1$ and $e_{j-1} \geq 1$, by $E_j(y_j, y_{j-1}, x_{j+1}, e_{j-1})$, we have $e_j \geq 1$. We will prove that $e_j = 1$. Assume to the contrary that $e_j = 2$, then $\eta_j = y_j + y_{j-1} - e_j = y_j - 1 \leq 0$. Now $\xi_j = x_j + x_{j-1} - d_j \leq 1 - d_j$, $1 \leq \omega_j = \xi_j + \eta_j \leq 1 - d_j$, we must have $d_j = 0$, $\eta_j = 0$ and $y_j = 1$. Then from $D_j(x_j, x_{j-1}, y_j = 1, d_{j-1} \geq 1)$, we see that $d_j \geq 1$. This is a contradiction. Therefore $e_j = 1$, and $\eta_j = y_j + y_{j-1} - e_j = y_j$. We proceed to prove that $y_j = 1$ by way of contradiction. If $y_j = 0$, then $\eta_j = 0$. Hence $\omega_j = \xi_j = 1$. By (36), we have $\xi_j = x_j + x_{j-1} - d_j$, hence $x_j + x_{j-1} = 1$ and $d_j = 0$, which is impossible because $d_{j-1} = 1$. So we conclude that $y_j = \eta_j = 1$. From $E_j(y_j = 1, y_{j-1} = 1, x_{j+1}, e_{j-1} \geq 1)$ and $e_j = 1$, we see that $x_{j+1} = 0$. By (32), we have $d_j = \lfloor x_j + x_{j-1} + y_j + 1 \rfloor / 2 \geq 1$. Since $\xi_j \geq 0$ and $x_j + x_{j-1} \leq 1$, by (36) we see that $x_j + x_{j-1} = 1$, $d_j = 1$, $\xi_j = 0$. Therefore $\omega_j = \eta_j = 1$. ■

Now we are in position to prove our earlier Lemma 7 concerning the values taken by ω_i following a value of 2.

Proof. Suppose that $\omega_h = 2$. By Lemma 8 for $j = h$, we have that $y_h = 1$, $x_{h+1} = 0$, and $d_{h+1} \geq 1$. Then by Lemma 9 for $j = h$, either $\omega_{h+1} \leq 0$, or $\omega_{h+1} = 1$ and $\omega_{h+2} \leq 0$, or $\omega_{h+1} = 1$, $y_{h+1} = 1$, $e_{h+1} \geq 1$. In the last case, we will repeatedly apply Lemma 10. First, we have $y_{h+1} = 1$, $d_{h+1} \geq 1$, $e_{h+1} \geq 1$, and $x_{h+1} = 0$. Hence by Lemma 10 for $j = h + 2$, we have either $\omega_{h+1} \leq 0$ or $\omega_{h+2} = 1$, $x_{h+2} + x_{h+1} = 1$, $x_{h+3} = 0$, and $y_{h+2} = d_{h+2} = e_{h+2} = 1$. Hence again by Lemma 10, now for $j = h + 3$, we conclude that either $\omega_{h+3} \leq 0$, or $\omega_{h+3} = 1$, $x_{h+3} + x_{h+2} = 1$, $x_{h+4} = 0$, and $y_{h+3} = d_{h+3} = e_{h+3} = 1$. Now since $x_{h+3} = x_{h+4} = 0$, a third application of Lemma 10, this time with $j = h + 4$, shows that now $\omega_{h+4} \leq 0$. ■

ACKNOWLEDGMENTS

The second author thanks Hans Dobbertin for a conversation in March 1998 in which Hans Dobbertin mentioned that under the assumption of the truth of the inequality (30), Pascale Charpin could possibly show that the Welch conjecture is true. After we completed a proof of the Welch and Niho conjectures in July 1998, Hans Dobbertin informed the second author that he also has a proof of the inequality (30), and using this, Canteaut *et al.* [4] can also give a proof of the Welch conjecture.

REFERENCES

1. A. E. Brouwer and L. M. G. M. Tolhuizen, A sharpening of the Johnson bound for binary linear codes, *Des. Codes and Cryptogr.* **3** (1991), 95–98.
2. A. R. Calderbank and J.-M. Goethals, Three-weight codes and association schemes, *Philips J. Res.* **39** (1984), 143–152.

3. A. R. Calderbank, G. McGuire, B. Poonen, and M. Rubinstein, On a conjecture of Helleseth regarding pairs of binary m-sequences, *IEEE Trans. Inform. Theory* **42** (1996), 988–990.
4. A. Canteaut, P. Charpin, and H. Dobbertin, Binary m-sequences with three-valued cross-correlation: A proof of Welch's conjecture, submitted for publication.
5. A. Carlet, P. Charpin, and V. Zinoviev, Codes, bent functions, and permutations suitable for DES-like cryptosystems, *Des. Codes Cryptogr.* **15** (1998), 125–156.
6. A. Chang, P. Gaal, S. W. Golomb, G. Gong, and P. V. Kumar, "On a Sequence Conjectured to Have Ideal 2-level Autocorrelation Function," ISIT, Cambridge, MA, 1998.
7. T. Cusick and H. Dobbertin, Some new three-valued cross-correlation functions for binary m-sequences, *IEEE Trans. Inform. Theory* **42** (1996), 1238–1240.
8. H. Dobbertin, Almost perfect nonlinear power functions on GF(2^n): The Welch case, *IEEE Trans. Inform. Theory* **45** (1999) 1271–1275.
9. H. Dobbertin, Almost Perfect nonlinear power functions on GF(2^n): The Niho case, *Inform. and Comput.* **151** (1999), 57–72.
10. R. Evans, H. D. L. Hollmann, C. Krattenthaler, and Q. Xiang, Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets, *J. Combin. Theory Ser. A* **87** (1999), 74–119.
11. R. Gold, Maximal recursive sequences with 3-valued cross-correlation functions, *IEEE Trans. Inform. Theory* **14** (1968), 154–156.
12. T. Helleseth, Some results about the cross-correlation function between two maximal linear sequences, *Discrete Math.* **16** (1976), 209–232.
13. T. Kasami, Weight distribution of Bose–Chaudhuri–Hocquenghem codes, *in* "Proceedings Conference Combinatorial Mathematics and Its Applications," (R. C. Bose and T. A. Dowling, Eds.), pp. 335–357, Univ. of North Carolina Press, Chapel Hill, 1969.
14. T. Kasami, The weight enumerator for several classes of subcodes of the 2nd order binary Reed–Muller codes, *Inform. and Control* **18** (1971), 369–394.
15. J. H. van Lint and R. M. Wilson, On the minimum distance of cyclic codes, *IEEE Trans. Inform. Theory* **32** (1986), 23–40.
16. R. J. McEliece, On periodic sequences from GF(q), *J. Combin. Theory Ser. A* **10** (1971), 80–91.
17. G. McGuire and A. R. Calderbank, Proof of a conjecture of Sarwate and Pursley regarding pairs of binary m-sequences, *IEEE Trans. Inform. Theory* **41** (1995), 1153–1155.
18. F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.
19. Y. Niho, "Multi-valued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequences," Ph.D. thesis, Univ. of Southern California, Los Angeles, 1972.
20. V. Pless, Power moment identities on weight distributions in error correcting codes, *Inform. and Control* **6** (1963), 147–152.
21. D. V. Sarwate and M. B. Pursley, Cross-correlation properties of pseudorandom and related sequences, *Proc. IEEE* **68** (1980), 593–619.
22. L. R. Welch, "Trace Mappings in Finite Fields and Shift Register Cross-Correlation Properties," Electrical Engineering Department Report, Univ. Southern California, 1969.