[4] A. A. Davydov, "Constructions and families of covering codes and saturated sets of points in projective geometry," *IEEE Trans. Inform. Theory*, vol. 41, pp. 2071–2080, Nov. 1995.
[5] ——, "Constructions and families of nonbinary linear codes with covering radius 2," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1679–1686, July 1999.
[6] A. A. Davydov and P. R. J. Östergård, "New quaternary linear codes with covering radius 2," *Finite Fields Appl.*, vol. 6, pp. 164–174, 2000.
[7] ——, "On saturating sets in small projective geometries," *European J. Combin.*, vol. 21, pp. 563–570, 2000.
[8] J. W. P. Hirschfeld, *Projective Geometries Over Finite Fields*, 2nd ed. Oxford, U.K.: Clarendon, 1998.
[9] T. S. Baicheva and E. D. Velikova, "Correction to 'Covering radii of ternary linear codes of small dimensions and codimensions'," *IEEE Trans. Inform. Theory*, vol. 44, p. 2032, Sept. 1998.

On Binary Cyclic Codes with Codewords of Weight Three and Binary Sequences with the Trinomial Property

Pascale Charpin, Aimo Tietäväinen, and Victor Zinoviev

***Abstract*—Golomb and Gong ([8] and [9]) considered binary sequences with the trinomial property. In this correspondence we shall show that the sets of those sequences are (quite trivially) closely connected with binary-cyclic codes with codewords of weight three (which were already studied in [4] and [5]). This approach gives us another way to deal with trinomial property problems. After disproving one conjecture formulated by Golomb and Gong in [9], we exhibit an infinite class of sequences which do not have the trinomial property, corresponding to binary cyclic codes of length 2^m-1 with minimum distance exactly four.**

***Index Terms*—Binary cyclic code, factorization of polynomials, periodic binary sequence, trinomial, trinomial pair.**

I. Introduction

One of the interesting objects of algebraic coding theory is cyclic codes. Many problems connected with these codes are open. Even the simplest case—binary cyclic codes with minimal distance three—is still far from a complete classification (see [4] and [5]). In the recent papers [8] and [9], binary sequences with so-called trinomial properties were considered. We say that a binary sequence $\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1})$ of length $n = 2^m - 1$ has the trinomial property if there is (at least) one pair of positive integers, k and ℓ, where $0 < k, \ell < n$, such that

$$a_i + a_{i+k} + a_{i+\ell} = 0$$

for all i, $i \in \{0, 1, \ldots, n-1\}$, where the indices are taken modulo n. The purpose of this correspondence is to set a one-to-one relation between these two problems, i.e., between binary-cyclic codes with the minimal distance three and binary sequences with trinomial properties.

In Section II, we consider binary sequences with trinomial properties and characterize such sequences in terms of cyclic codes with minimal distance three. In Section III, we construct families of such sequences explicitly. Section IV is devoted to disproving the conjecture from [9] that any nonlinear binary sequence of period $n = 2^m - 1$, where m is prime, has no trinomial property. Finally, in Section V, we construct infinite families of binary nonlinear sequences which have no trinomial properties.

In this correspondence, a *codeword* is an element of the vector space F_2^n. A *code* is a subspace of F_2^n. The *distance* between two codewords will always be the Hamming distance. So the weight of any codeword $x = (x_1, \ldots, x_n)$ will be the Hamming weight $\mathrm{wt}\,(x) = \sum_{i=1}^n x_i$. The *dual* of any binary linear code C of length n is defined by means of the standard scalar product

$$C^\perp = \{\, y \in F_2^n \mid z \cdot y = 0, z \in C \,\} \tag{1}$$

where $z \cdot y = \sum_{i=1}^n z_i y_i$, $z = (z_1, \ldots, z_n)$, and $y = (y_1, \ldots, y_n)$.

II. On Binary Sequences with the Trinomial Property

Denote the finite field of order 2^m by F_{2^m}. Let $n = 2^m - 1$ and

$$R_n = F_2[x]/(x^n + 1).$$

In this correspondence, we consider elements of R_n and, as usual, we identify the sequence (or vector)

$$\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1}) \in F_2^n$$

and the polynomial

$$a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in R_n.$$

Definition 1 (cf. [8] and [9]): A sequence

$$\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1}) \in R_n$$

has the (k, ℓ) trinomial property (or (k, ℓ) is a trinomial pair of $\boldsymbol{a}$), if for any $i \in \{0, 1, \ldots, n-1\}$ we have

$$a_i + a_{i+k} + a_{i+\ell} = 0$$

where the indexes are taken modulo n and k, ℓ are positive integers.

Let us mention that in [8] and [9], Golomb and Gong further assumed that the (smallest) period of $\boldsymbol{a}$ is n.

Define the following sets. For given k and ℓ, $0 < k, \ell < n$, let

$$S(k, \ell) = \{\boldsymbol{a} \in R_n \mid \boldsymbol{a} \text{ has the } (k, \ell) \text{ trinomial property}\}.$$

Since evidently $S(k, k) = \{\boldsymbol{0}\}$ and $S(\ell, k) = S(k, \ell)$, it is natural to define

$$\mathcal{S} = \bigcup \{S(k, \ell) \mid 0 < k < \ell < n\}. \tag{2}$$

Statement 1: $S(k, \ell)$ is a cyclic code (and thus also $S(k, \ell)^\perp$, the dual of $S(k, \ell)$, is cyclic).

Proof: If the vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ have the (k, ℓ) trinomial property, then also their sum $\boldsymbol{a} + \boldsymbol{b}$ has that property. Therefore, the set $S(k, \ell)$ is a linear space. By definition it is cyclic. Thus, $S(k, \ell)$ is a cyclic code. □

Theorem 1: We denote by $\langle h(x) \rangle$ the cyclic code generated by $h(x)$, i.e., the ideal of R_n generated by $h(x)$. Then

$$S(k, \ell) = \langle \gcd\,(1 + x^k + x^\ell, 1 + x^n) \rangle^\perp.$$

Manuscript received February 24, 2000; revised August 15, 2000. The work was supported by the Academy of Finland and by the Russian Fundamental Research Foundation under Project 99-01-00828. The material in this correspondence was presented at the 7th International Workshop on Algebraic and Combinatorial Coding Theory, Blagoevgrad, Bulgaria, June 18–19, 2000.

P. Charpin is with the INRIA-Rocquencourt, Domaine de Voluceau, BP 105, 78153 Le Chesnay, France (e-mail: Pascale.Charpin@inria.fr).

A. Tietäväinen is with the Department of Mathematics and TUCS, University of Turku, FIN-20014 Turku, Finland (e-mail: tietavai@lena.utu.fi).

V. Zinoviev is with the Institute for Problems of Information Transmission of the Russian Academy of Sciences, Bol'shoi Karetnyi 19, GSP-4, Moscow 101447, Russia (e-mail: zinovev@iitp.ru).

Communicated by P. Solé, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(01)00373-X.

Proof: This follows from the equivalence of the following four statements:

$$\begin{aligned}
&\boldsymbol{a} = (a_0, \ldots, a_{n-1}) \in S(k,\ell)\\
&\Leftrightarrow a_i + a_{i+k} + a_{i+\ell} = 0, \quad \text{for any } i \in \{0,1,\ldots,n-1\}\\
&\Leftrightarrow a(x) \in \langle 1 + x^k + x^\ell \rangle^\perp\\
&\Leftrightarrow a(x) \in \langle \gcd(1 + x^k + x^\ell, 1 + x^n) \rangle^\perp. \qquad \square
\end{aligned}$$

Thus we immediately find the size of the set $S(k,\ell)$.

Corollary 1:

$$|S(k,\ell)| = 2^{\deg \gcd(1+x^k+x^\ell, 1+x^n)}.$$

Since $1 + x^n$ does not have multiple factors

$$\begin{aligned}
\gcd\left(1 + x^{2^s k} + x^{2^s \ell}, 1 + x^n\right) &= \gcd\left((1 + x^k + x^\ell)^{2^s}, 1 + x^n\right)\\
&= \gcd(1 + x^k + x^\ell, 1 + x^n)
\end{aligned}$$

and so Theorem 1 has also the following corollary (see [9, Corollary 1]).

Corollary 2: For any nonnegative integer s

$$S(2^s k, 2^s \ell) = S(k,\ell).$$

For any integer s, $s \geq 0$, the trinomial pairs (k,ℓ) and $(2^s k, 2^s \ell)$ of a sequence $\boldsymbol{a}$ are called equivalent (see [9, Definition 1]). Two trinomial pairs, which are not equivalent, are called distinct. Now we can easily prove the following statement (cf. [9, Theorem 2]).

Statement 2: If for a sequence $\boldsymbol{a}$ there is $\boldsymbol{a}$ trinomial pair (k,ℓ), where $1 < k < \ell < n$ and $k \neq n/3$, then $\boldsymbol{a}$ has at least two distinct trinomial pairs.

Proof: If (k,ℓ) is a trinomial pair for $\boldsymbol{a}$, so too are (ℓ, k) and $(\ell - k, n - k)$. These three pairs are equivalent only if there are integers i and j such that $\ell = 2^i k$ and $\ell = (2^j + 1)k$ and thus only if $i = 1, j = 0$, $\ell = 2k$, and $n = 3k$. $\square$

It should be noted that in Statement 2 the condition $k \neq n/3$ is not necessary; i.e., a sequence may have the trinomial pair $(n/3, 2n/3)$ and still a distinct trinomial pair. For example, in the case $n = 15$, the sequence

$$\begin{aligned}
\boldsymbol{a} &= (a_0, a_1, \ldots, a_{14}) = (x^{15} + 1)/(x^4 + x + 1)\\
&= 1 + x + x^2 + x^3 + x^5 + x^7 + x^8 + x^{11}\\
&= (1,1,1,1,0,1,0,1,1,0,0,1,0,0,0)
\end{aligned}$$

satisfies both the equation $a_i + a_{i+5} + a_{i+10} = 0$ and the equation $a_i + a_{i+3} + a_{i+4} = 0$. Thus, $(5, 10)$ and $(3, 4)$ are two distinct trinomial pairs of $\boldsymbol{a}$.

Theorem 2: Let $\mathcal{S}$ be the set previously defined by (2).

Then $\mathcal{S}$ is the union of all cyclic codes C in R_n such that $C^\perp$ contains at least one codeword of weight 3.

Proof: Let $\mathcal{E}$ denote the union of all cyclic codes C in R_n satisfying

$$\exists b(x) \in C^\perp : \mathrm{wt}\,(b(x)) = 3.$$

i) Assume first that $\boldsymbol{a}$ belongs to $\mathcal{E}$. Then there is a cyclic code C in R_n such that $\boldsymbol{a}$ is in C and so there is an element $b(x)$ of $C^\perp$ of weight three. If

$$b(x) = 1 + x^k + x^\ell$$

then for any i from $\{0, 1, \ldots, n-1\}$ we have

$$x^i b(x) = x^i + x^{k+i} + x^{\ell+i} \in C^\perp$$

and, therefore, for each i

$$a_i + a_{k+i} + a_{\ell+i} = 0 \tag{3}$$

which means that $\boldsymbol{a} \in S(k,\ell)$ and so $\boldsymbol{a} \in \mathcal{S}$.

ii) Assume now that $\boldsymbol{a} \in \mathcal{S}$. Then there are k and ℓ such that for each i the equality (3) is valid. Denote by $C(k,\ell)$ the linear subspace of R_n generated by all cyclic shifts of the trinomial $1 + x^k + x^\ell$. By construction, $C(k,\ell)$ is a cyclic code and in R_n each element of $C(k,\ell)$ is divisible by $1 + x^k + x^\ell$. Thus for any element $\boldsymbol{c}$ of $C(k,\ell)$ we have that

$$\boldsymbol{a} \cdot \boldsymbol{c} = \boldsymbol{0}$$

which means that $\boldsymbol{a}$ belongs to the code $C(k,\ell)^\perp$ (see (1) in Section I for the definition of the duality). By definition, $C(k,\ell)$ contains the codeword $1 + x^k + x^\ell$ of weight 3. Thus, $C(k,\ell)^\perp$ is an element of $\mathcal{E}$ and, therefore, $\boldsymbol{a} \in \mathcal{E}$. $\square$

III. On Binary-Cyclic Codes with Codewords of Weight Three

Because of Theorem 2, it is now important to study cyclic codes with codewords of weight 3. Let γ be a primitive element of the field F_{2^m} and $m_s(x)$ the minimal polynomial of γ^s over F_2. For a positive integer k, denote by I_k a set of representatives of all distinct 2-cyclotomic cosets modulo $2^k - 1$ and for an integer r by $K_k(r)$ the 2-cyclotomic coset modulo $2^k - 1$ determined by r; i.e.,

$$K_k(r) = \{r, 2r, \ldots, 2^{k-1} r\} \subseteq Z_{2^k - 1}.$$

If g is a divisor of m, define

$$I_m(g,r) = \{i \in I_m \mid \exists j = j(i) : i \equiv 2^j r (\mathrm{mod}\, 2^g - 1)\}.$$

If I is a subset of I_m, denote by C_I the binary-cyclic code of length $n = 2^m - 1$ generated by the polynomial

$$\prod_{i \in I} m_i(x).$$

The following theorem yields a large set of cyclic codes with codewords of weight three. It essentially was given in [4] and [5] and in case $r = 1$, in a different form, in [8] and [9].

Theorem 3: If there is a divisor g of m and an integer r such that $g > 1$, $\gcd(r, 2^g - 1) = 1$, and $I \subseteq I_m(g,r)$, then for every integer b in the interval $[1, 2^g - 2]$, the code C_I contains a word of the form

$$1 + x^{ub} + x^{uh}$$

where $u = (2^m - 1)/(2^g - 1)$ and h is an integer from the same interval.

Proof: If $u = (2^m - 1)/(2^g - 1)$ then $\beta = \gamma^u$ is a primitive element of the field F_{2^g} as well as β^r (because $\gcd(r, 2^g - 1) = 1$). Thus, for each b in the interval $[1, 2^g - 2]$ there is another integer h in this interval such that

$$1 + \beta^{rb} + \beta^{rh} = 0. \tag{4}$$

Define

$$a(x) = 1 + x^{ub} + x^{uh}.$$

If $i \in I$ then there are integers k and j such that

$$i = k(2^g - 1) + 2^j r.$$

Therefore

$$\begin{aligned} a(\gamma^i) &= 1 + \gamma^{uib} + \gamma^{uih} \\ &= 1 + \beta^{ib} + \beta^{ih} \\ &= 1 + \beta^{2^j rb} + \beta^{2^j rh} \\ &= (1 + \beta^{rb} + \beta^{rh})^{2^j} = 0 \end{aligned}$$

and so $a(x) \in C_I$. □

The following result is a reformulation of the previous theorem in terms of the factorization of $m_{ur}(x^u)$ (g, m, u and γ are defined as before).

Theorem 4: Let $r \in \{0, 1, \ldots, 2^g - 2\}$. Then i)

$$m_{ur}(x^u) = \prod_{i \in I_m(g,r)} m_i(x). \tag{5}$$

ii) The minimal polynomial $m_{ur}(x)$ divides the polynomial $f(x)$ if and only if for any $i \in I_m(g, r)$ the minimal polynomial $m_i(x)$ divides $f(x^u)$.

Proof:

i) First assume that $i \in I_m(g, r)$ and show that the polynomial $m_i(x)$ divides $m_{ur}(x^u)$. As $i = r2^j + v(2^g - 1)$ for some integer v, we have immediately

$$m_{ur}(\gamma^{ui}) = m_{ur}\left(\gamma^{u(2^g-1)v}\gamma^{ur2^j}\right) = (m_{ur}(\gamma^{ur}))^{2^j} = 0.$$

Thus, the right-hand side of (5) divides the left-hand side. Since both sides are monic polynomials, we only need to prove that the degrees are equal. The degree of $m_{ur}(x^u)$ is u times the degree of $m_{ur}(x)$, and the latter is the number of elements in the coset $K_g(r)$. On the other hand, the degree of the right-hand side is the number of elements i in the set $\{0, 1, \ldots, 2^m - 1\}$ such that $i \equiv r2^j \pmod{2^g - 1}$ for some j from $\{0, 1, \ldots, g-1\}$, and so it is also u times the number of elements in the set $K_g(r)$.

ii) First, assume that $m_{ur}(x)$ divides the polynomial $f(x)$. This means that $f(\gamma^{ur}) = 0$. Let $i \in I_m(g, r)$. We can write $i = r2^j + v(2^g - 1)$ where v is an integer. Thus, $ui = ur2^j + v(2^m - 1)$ and so

$$f(\gamma^{ui}) = f(\gamma^{ur2^j}) = (f(\gamma^{ur}))^{2^j} = 0.$$

The inverse statement follows easily from (5). □

Thus we have a complete description of all sequences with the (ub, uh) trinomial property.

Statement 3: Let g, m, u, and γ be defined as above. Assume that the sequence $\boldsymbol{a} \in F_2^n$ has the (k, ℓ) trinomial property.

i) There is an integer r such that

$$1 + \gamma^{rk} + \gamma^{r\ell} = 0. \tag{6}$$

ii) Assume that among all r for which (6) is valid, there is r' such that $\gcd(r', u) = 1$. Then, if u divides k then u divides ℓ.

Proof:

i) If $\boldsymbol{a}$ has the (k, ℓ) trinomial property then, according to Theorem 2, there is a cyclic code which contains a codeword $b(x)$ of weight three: $b(x) = 1 + x^k + x^\ell$. This means that there is an integer r such that γ^r is a root of $b(x)$.

ii) Assume that u divides k. Let $k = uk'$ and $\beta = \gamma^u$ be a primitive element of F_{2^g}. We suppose, moreover, that there is an integer $r', 0 < r' < n$, $\gcd(r', u) = 1$, such that

$$1 + \gamma^{r'uk'} + \gamma^{r'\ell} = 0. \tag{7}$$

Let $1 + \beta^{rk'} = \beta^{\ell'}$. As $\beta = \gamma^u$, we have that

$$1 + \gamma^{ur'k'} + \gamma^{u\ell'} = 0. \tag{8}$$

Comparing (7) and (8) we conclude that $r'\ell = u\ell'$. Since $\gcd(r', u) = 1$, ℓ is divisible by u. □

IV. Fourier Transform of Sequences

It is well known that the coordinates of any sequence $\boldsymbol{a} \in R_n$ can be expressed by the equations

$$a_i = f(\gamma^i), \qquad i = 0, \ldots, n-1$$

where $f(x)$ is a function from F_{2^m} to F_2 which is simply the Fourier transform of the sequence $\boldsymbol{a}$—in terminology of cyclic codes, it is the Mattson–Solomon polynomial of the corresponding codeword.

Definition 2: Let $a(x) \in R_n$ and define its Fourier coefficients

$$A_j = a(\gamma^j), \qquad 0 \le j \le n-1$$

and the function associated to the sequence $\boldsymbol{a}$

$$f_{\boldsymbol{a}}(x) = \sum_{j=0}^{n-1} A_j x^{n-j}. \tag{9}$$

Recall that I_m denotes a set of representatives of all distinct 2-cyclotomic cosets modulo $2^m - 1$. The next lemma is obtained from the basic theory of cyclic codes [3], see also ([10, p. 1165]).

Lemma 1: Let $\boldsymbol{a}$ be the sequence identified with $a(x) \in R_n$. Denote by $J(\boldsymbol{a})$ the subset of I_m composed of the j satisfying $a(\gamma^j) = 0$. On the other hand, consider the elements $h \in I_m$ such that $a(\gamma^{n-h}) \neq 0$. Denote by $H(\boldsymbol{a})$ the set of such h.

Then, the sequence $\boldsymbol{a}$ is produced by a function of the form (9) where the A_j are the Fourier coefficients of $a(x)$. More precisely, denoting by $\bar{H}$ the union of the 2-cyclotomic cosets of the elements of $H(\boldsymbol{a})$

$$f_{\boldsymbol{a}}(x) = \sum_{r \in \bar{H}} A_{n-r} x^r.$$

Moreover, $\boldsymbol{a}$ is a codeword of the code $C_{J(\boldsymbol{a})}$, which is the smallest binary-cyclic code containing $\boldsymbol{a}$.

The sequence $\boldsymbol{a}$ has the trinomial property if and only if the code $C_{H(\boldsymbol{a})}$ contains a codeword of weight 3.

Proof: As $f_{\boldsymbol{a}}(\gamma^i) = a_i$, $f_{\boldsymbol{a}}$ produces the sequence $\boldsymbol{a}$. Conversely, any function of the form (9), with $A_j \in F_{2^m}$ and such that $A_{2j} = A_j^2$, is the Fourier transform of a unique binary codeword of length n.

Let $J(\boldsymbol{a}) = \{j_1, \ldots, j_\ell\}$. By definition, $\boldsymbol{a}$ is a codeword of the binary-cyclic code $C_{J(\boldsymbol{a})}$, since it satisfies

$$a(\gamma^{j_1}) = 0, \ldots, a(\gamma^{j_\ell}) = 0.$$

Furthermore, it is well known that

$$C_{J(\boldsymbol{a})}^{\perp} = C_{H(\boldsymbol{a})}.$$

According to Theorem 2, the proof is completed. □

V. On Golomb's and Gong's Conjecture

In this section we assume that $a(\gamma^{n-1}) \neq 0$, i.e., $1 \in H(\boldsymbol{a})$. When, moreover, $H(\boldsymbol{a}) \neq \{1\}$, $\boldsymbol{a}$ is called *nonlinear*. When we define

$$U_i(x) = 1 + x^i + (1+x)^i$$

we see that $C_{H(\boldsymbol{a})}$ (the dual of $C_{J(\boldsymbol{a})}$) contains a word of weight 3 if and only if there are integers k and ℓ such that

$$\gamma^\ell = 1 + \gamma^k \quad \text{and} \quad \forall h \in H(\boldsymbol{a}) : U_h(\gamma^k) = 0 \tag{10}$$

(which means $\boldsymbol{a} \in S(k,\ell)$).

In [9], it is conjectured that *when m is prime, then any nonlinear binary sequence of period $2^m - 1$ has no trinomial pair*. By (10), this means that when m is prime and $i \in I_m \backslash \{0,1\}$ then the equation $U_i(x) = 0$ has no root in $F_{2^m} \backslash \{0,1\}$. One can easily check this property for $m \leq 13$. But we disprove this conjecture by showing that the following statement is true.

Statement 4: The polynomial $U_{281}(x)$ has a zero in $F_{2^{17}} \backslash \{0,1\}$. In other words, the binary-cyclic code $C_{1,281}$ of length $2^{17} - 1$ has minimum distance three. Moreover, it has exactly $17(2^{17} - 1)$ codewords of weight three.

The nonlinear sequence $\boldsymbol{a}$ which is produced by the function

$$f_{\boldsymbol{a}}(x) = \mathrm{Tr}\,(x + x^{281}), \quad x \in F_{2^{17}} \backslash \{0\}$$

where Tr, the trace function from $F_{2^{17}}$ to F_2, has the trinomial property.

Proof: By using Maple, one obtains the factorization of $U_{281}(x)$. There are exactly six minimal polynomials of degree 17 dividing $U_{281}(x)$. They are

$$(x^{17} + x^{16} + x^{13} + x^{12} + x^{11} + x^7 + x^5 + x^4 + 1)$$
$$(x^{17} + x^{16} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^6 + x^4 + 1)$$
$$(x^{17} + x^{13} + x^{11} + x^{10} + x^8 + x^7 + x^6 + x^5 + x^4 + x + 1)$$
$$(x^{17} + x^{13} + x^{12} + x^{10} + x^6 + x^5 + x^4 + x + 1)$$
$$(x^{17} + x^{13} + x^{11} + x^9 + x^8 + x^7 + x^4 + x + 1)$$
$$(x^{17} + x^{16} + x^{13} + x^{10} + x^9 + x^8 + x^6 + x^4 + 1).$$

Note that $2^{17} - 1$ is prime; moreover 281 is the smallest element of its 2-cyclotomic coset modulo $2^{17} - 1$. Let us denote by γ a primitive element of $F_{2^{17}}$ which is not a root of $U_{281}(x)$. Thus, there exists $\tau > 1$ such that γ^τ is a root of $U_{281}(x)$—for instance, the root of the first polynomial of degree 17 above. We know that the other polynomials have, respectively, as roots $1 + \gamma^\tau$, $\gamma^{-\tau}$, $1 + \gamma^{-\tau}$, $(1 + \gamma^\tau)^{-1}$, and $(1 + \gamma^{-\tau})^{-1}$.

Let τ' be defined by $\gamma^{\tau'} = 1 + \gamma^\tau$. Then (τ, τ') is a trinomial pair for $\boldsymbol{a}$ since $1 + \gamma^{281\tau} + \gamma^{281\tau'} = 0$.

In other words, the code $C_{1,281}$ of length $n = 2^{17}$–1 over F_2 has minimal distance 3. According to the factorization of $U_{281}(x)$, we know exactly the number B_3 of codewords of weight 3 in $C_{1,281}$. There are 6×17 distinct roots of $U_{281}(x)$ belonging to $F_n \backslash \{0,1\}$. Each root gives n codewords of weight 3—one codeword and their shifts. Each codeword appears six times in this enumeration. Finally, $B_3 = 17n$. □

VI. An Infinite Class of Sequences Which Do Not Have the Trinomial Property

According to Statement 4, nonlinear binary sequences of period $2^m - 1$ which have trinomial pairs should exist for any $m \geq 17$. On the other hand, it is known that the minimum distance of any code $C_{1,t}$ is in $\{2,3,4,5\}$ (see an overview in [2]). We focus here on the case m prime and will describe an infinite class of cyclic codes with minimum distance exactly 4—i.e., of sequences $\boldsymbol{a}$ which have a relation of the form $a_i + a_{i+j} + a_{i+k} + a_{i+\ell} = 0$, but have no such relation involving a smaller number of elements.

Now we want to notice a property, that we will use later, concerning the degree of the polynomial $U_t(x) = 1 + x^t + (1+x)^t$.

Lemma 2: Assume that m is odd and $m \not\equiv 0 \pmod 3$. Let t be such that

$$t \notin \{1, 2, \ldots, 2^{m-1}\} \quad \text{and} \quad 1 < t < 6m + 3.$$

Then the code $C_{1,t}$ of length $2^m - 1$ has minimum distance at least four if and only if $U_t(x)$ has no root in a proper subfield of F_{2^m} (except 0 and 1).

Proof: First, it is clear that if $C_{1,t}$ has no codeword of weight 3 then $U_t(x)$ has no root in F_{2^m} except 0 and 1. Let β be a root of $U_t(x)$ which is not in a proper subfield of F_{2^m}. Thus, one can construct a set S of roots of $U_t(x)$ whose cardinality is at most $6m$. It is composed of the elements of the orbit of β under the group generated by the permutations on F_{2^m}

$$\sigma; \alpha \longmapsto \alpha^{-1} \quad \text{and} \quad \rho; \alpha \longmapsto (\alpha + 1)$$

and of their conjugates (see [9, Lemma 2]). We have to examine the cases where the cardinality of S is strictly less than $6m$. We denote by $\mathrm{Conj}\,(\alpha)$ the set of the conjugates of α, for some α in F_{2^m}. Note that, by hypothesis, $\mathrm{Conj}\,(\beta)$ has m elements. Our conclusions are coming from the basic properties of the factorization of trinomials which can be found in [7, Ch. 5].

Suppose that $(\beta + 1) \in \mathrm{Conj}(\beta)$—i.e. there is k such that $\beta^{2^k} + \beta + 1 = 0$. This is possible for even m only.

Suppose now that $\beta^{-1} \in \mathrm{Conj}\,(\beta)$. This means that there is k such that $\beta^{2^k} + \beta^{-1} = 0$ which is equivalent to $\beta^{2^k+1} + 1 = 0$. This is possible also for even m only.

If $(\beta + 1) \in \mathrm{Conj}\,(\beta^{-1})$ then there is k such that $\beta + 1 = \beta^{-2^k}$. We have

$$\beta^{2^k+1} + \beta^{2^k} + 1 = 0 \Longleftrightarrow \beta^{2^{m-k}+1} + \beta + 1 = 0.$$

So the degree of $m_\beta(x)$ divides $3(m-k)$ and is divisible by 3. So 3 divides m. Finally, we have proved that, in accordance with the hypothesis on m and β

$$\mathrm{Conj}\,(\beta) \neq \mathrm{Conj}\,(\beta^{-1}) \neq \mathrm{Conj}\,(\beta + 1).$$

Since the permutations σ and ρ, above defined, do not change the degree of minimal polynomials we conclude that S is the union of six distinct sets of conjugates; so the cardinality of S is exactly $6m$. Now the degree of $U_t(x)$, which is $t - 1$, must satisfy $t - 1 \geq 6m$. But 0 and 1 are roots of $U_t(x)$, so we obtain $t - 3 \geq 6m$ as a necessary condition for β to be a root of $U_t(x)$; this contradicts the hypothesis on t. We conclude that $C_{1,t}$ has no codeword of weight 3. □

Janwa, McGuire, and Wilson [11] studied the binary-cyclic codes $C_{1,t}$ of length $2^m - 1$ $(m > 5)$ by considering the curve defined by the polynomial

$$g_t(X,Y) = \frac{1 + X^t + Y^t + (X + Y + 1)^t}{(X+Y)(X+1)(Y+1)}$$

whose rational points correspond to codewords of weight less than or equal to 4. They used the following result (see [11, Theorem A]).

Theorem 5: If $g_t(X,Y)$ is absolutely irreducible then the code $C_{1,t}$ has minimum distance 5 for only a finite number of values of m.

Sketch of Proof: Suppose that $g_t(X,Y)$ is irreducible over the algebraic closure of F_2. Then a form of Weil's theorem, due to Schmidt [13], shows that the number N_m of rational points (X,Y) over F_{2^m} of $g_t(X,Y)$ satisfies

$$2^m + 1 - (t-4)(t-5)2^{m/2} - (t-3) \leq N_m \leq 2^m + 1 + (t-4)(t-5)2^{m/2}. \quad (11)$$

□

According to the lower bound above, if t is fixed and m increasing then the number of zeros will increase implying that the code $C_{1,t}$ of length $2^m - 1$, for a certain m, has codewords of weight 3 or 4. It is easy to check the following result which is given in [1]. If $t \leq 2^{m/4} + 4.5$, then the lower bound of N_m is greater than or equal to $2^{m/2-2} - 2^{m/4} + 1/2$; so there are solutions of the equation $g_t(X,Y) = 0$ for all $m \geq 7$.

Corollary 3: Assume that $g_t(X,Y)$ is absolutely irreducible. Then the minimum distance of $C_{1,t}$ is at most 4 when

$$t \leq 2^{m/4} + 4.5$$

where $m \geq 7$.

The next theorem is the main result given in [11].

Theorem 6: For fixed $t, t \equiv 3 \pmod 4, t > 3$, the curve $g_t(X,Y)$ is absolutely irreducible. So the code $C_{1,t}$ of length $2^m - 1$ has codewords of weight 3 or 4 for all but finitely many values of m.

By using the previous results, we are able to construct, as an example of application, a class of codes of type $C_{1,t}$ with minimum distance exactly 4. This leads to a large class of sequences which do not have the trinomial property.

Corollary 4: Suppose that m is prime. Let t be an integer such that

$$t \equiv 3 \pmod 4, \quad t > 3.$$

If m and t satisfy

$$t < \min(6m + 3, 2^{m/4} + 4.5)$$

then the minimum distance of the code $C_{1,t}$ is exactly 4. Therefore, any sequence $\boldsymbol{a}$ produced by a function of the form

$$f_{\boldsymbol{a}}(x) = \mathrm{Tr}\,(x + \alpha_0 x^t + \alpha_1 x^{k_1} + \cdots + \alpha_i x^{k_i})$$

where $\alpha_i \in F_{2^m} \backslash \{0\}$, does not have the trinomial property.

Proof: According to Corollary 3 and Theorem 6, the code $C_{1,t}$ has minimum distance at most 4. Moreover, since we assume that $t < 6m + 3$ with m prime, we can apply Lemma 2. We conclude that $C_{1,t}$ has no codeword of weight 3; its minimum distance is exactly 4.

Now consider a sequence $\boldsymbol{a}$ produced by $f_{\boldsymbol{a}}(x)$. Then $\boldsymbol{a}$ is a codeword of the cyclic code $C^{\perp}_{1,t,k_1,\ldots,k_i}$ (see Lemma 1). If the sequence $\boldsymbol{a}$ has trinomial property then $C_{1,t,k_1,\ldots,k_i}$ contains codewords of weight 3; this is impossible because this code is contained in the code $C_{1,t}$. □

TABLE I
CODES $C_{1,t}$ OF LENGTH $2^m - 1$, $m \geq m_0$ AND m PRIME, WITH MINIMUM DISTANCE 4 (SEE EXPLANATION BELOW)

t	m_0	Λ
7	7	7.8
11	11	11.2
15, 19, 23	17	23.5
27, 31	19	31.4
35, 39, 43, 47, 51, 55	23	58.3
59, 63, ..., 63+4i, ..., 155	29	156.7
159, ..., 159+4i, ..., 187	31	189

Explanation of Table I: For any fixed t of the form $4i + 3$ we computed the smallest prime number m, denoted m_0, such that $t < \Lambda$, where

$$\Lambda = \min(6m + 3, 2^{m/4} + 4.5).$$

According to the previous corollary, the binary-cyclic code $C_{1,t}$ of length $2^{m_0} - 1$ has minimum distance 4. Moreover, this property holds for any prime m such that $m \geq m_0$. Note that from $m_0 = 31$ we have $\Lambda = 6m_0 + 3$.

ACKNOWLEDGMENT

The authors wish to thank Anne Canteaut for valuable discussions concerning her paper [1]. She notably indicated the counterexample $m = 17$ and $t = 281$, and also other examples for $m = 17$ and for m greater than 17.

REFERENCES

[1] A. Canteaut, "Differential cryptanalysis of Feistel ciphers and differentially uniform mappings," in *Proc. Conf. Selected Areas on Cryptography, SAC'97*, Ottawa, ON, Canada, Aug. 1997, pp. 172–184.

[2] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," *Des., Codes Cryptogr.*, vol. 15, pp. 125–156, 1998.

[3] P. Charpin, "Open problems on cyclic codes," in *Handbook of Coding Theory*, V. S. Pless, W. C. Huffman, and R. A. Brualdi, Eds. Amsterdam, The Netherlands: Elsevier, 1998, pt. 1, ch. 11.

[4] P. Charpin, A. Tietäväinen, and V. Zinoviev, "On binary cyclic codes with minimum distance three," in *Proc. 5th Int. Workshop on Algebraic and Combinatorial Coding Theory*, Sozopol, Bulgaria, 1996, pp. 93–97.

[5] ——, "On binary cyclic codes with minimum distance three," in *Probl. Inform. Transm.*, 1997, vol. 33, pp. 287–296.

[6] M. D. Fried and M. Jarden, *Field Arithmetic*. New York: Springer-Verlag.

[7] S. W. Golomb, *Shift Register Sequences*. Laguna Hills, CA: Aegean Park , 1982.

[8] S. W. Golomb and G. Gong, "Periodic binary sequences with the "trinomial property"," in *Proc. 1997 IEEE Int. Symp. Inform. Theory*, Ulm, Germany, June 29–July 4 1997, p. 41.

[9] ——, "Periodic binary sequences with the "trinomial property"," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1276–1279, May 1999.

[10] I. Honkala and A. Tietäväinen, "Codes and number theory," in *Handbook of Coding Theory*, V. S. Pless, W. C. Huffman, and R. A. Brualdi, Eds. Amsterdam, The Netherlands: Elsevier, 1998, pt. 2, ch. 16. .

[11] H. Janwa, G. McGuire, and R. M. Wilson, "Double-error-correcting codes and absolutely irreducible polynomials over GF (2)," *J. Algebra*, vol. 178, pp. 665–676, 1995.

[12] R. Lidl and H. Niederreiter, "Finite fields," in *Encyclopedia of Mathematics and Its Applications*. Sydney, NSW, Australia: Addison-Wesley, 1983.

[13] W. M. Schmidt, "Equations over finite fields. An elementary approach," in *Lecture Notes in Mathematics*. Berlin, Germany: Springer-Verlag, 1976, vol. 536.