Ternary Ideal 2-level Autocorrelation Sequences

Michael Ludkovski and Guang Gong

Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, ON N2L 3G1, Canada
ggong@shannon1.uwaterloo.ca

Abstract. Ternary sequences with ideal 2-level autocorrelation are investigated. First, we prove that any p-ary sequence with 2-level autocorrelation is balanced for any prime p. We then present newly discovered 3-term sequences and conjecture the existence of two new infinite families of ternary ideal 2-level autocorrelation (AC) sequences of period $3^n - 1$. We also use the technique of applying Second Order Decimation-Hadamard Transform (DHT) operator, which was recently developed by Gong and Golomb [10] to these 3-term ternary sequences with ideal 2-level autocorrelation. Some variations of the Second Order DHT are also discussed. Furthermore, an exhaustive search for 3-term ternary AC sequences has been performed for $2 \leq n \leq 9$ and inequivalence classes of these sequences are determined. Last, a construction of infinite classes of ternary AC sequences is given by applying the Gordon-Mills-Welch method to the newly discovered ternary sequences.

Index words. 2-level autocorrelation, ternary sequences, Decimation-Hadamard Transform operator.

1 Introduction

Ideal 2-level autocorrelation sequences have found many applications in communications and cryptology, such as radar, global positioning systems, CDMA communication and stream cipher cryptosystems.

In the last three years great progress has been made in finding new families of binary 2-level autocorrelation sequences. It is now conjectured [10] that all infinite families of binary 2-level autocorrelation sequences of period $2^n - 1$ having no subfield factorization have been discovered for odd n. As opposed to the binary case, the situation for $p > 2$ is largely unknown. Beside the Singer and GMW constructions (or generalized GMW constructions), little else is known about p-ary two-level autocorrelation sequences. Recently, a few steps have been taken in this direction with investigations into $p = 3$, the ternary case. Helleseth *et. al.* [12] have found an infinite family of 2-term ternary two-level autocorrelation sequences and Lin, in his Ph.D. dissertation [16], has conjectured there is another family of 2-term ternary two-level autocorrelation sequences.

Gong and Golomb found that the Hadamard transform of three-term sequences is determined by one of the m-sequences [9] (a three term sequence $\{a_k\}$ is defined by $a_k = Tr(\alpha^k + \alpha^{rk} + \alpha^{r^{2k}})$, $k = 0, 1, \cdots, r = 2^{(n-1)/2} + 1$). It has been recently shown by Dillon and Dobbertin [1] that when n is odd, all the newly discovered classes of two-level autocorrelation sequences of period $2^n - 1$ have the same Hadamard transform as one of the m-sequences. Based on this observation, Gong and Golomb developed a new method to study and search for 2-level autocorrelation (AC) sequences over a finite field $GF(p)$ where p is a prime, called by them the *(iterative) decimation-Hadamard transform* [10] (the abstract of this work appeared in [8]).

In [17], we used the second-order Decimation-Hadamard Transform (DHT) operator to look for multi-term ternary AC sequences. Initially, we used m-sequences for our base, analogous to the binary situation which then gives all the known 2-level autocorrelation sequences of period $2^n - 1$ for $5 \leq n \leq 17$. As it turned out, this attempt was not successful as ternary m-sequences appear to form a closed equivalence class under DHT (i.e. only m-sequences could be realized). However, we had success applying the DHT operator to 2-term ternary AC sequences, obtaining several new multi-term ternary AC sequences with number of terms from 4 to 89. These latter sequences are computationally infeasible to find if we attempt exhaustive search. Based on our experimental results, we conjecture that for $n = 2m + 1$ odd there exist m or $m - 1$ infinite inequivalent families of ternary two-level autocorrelation sequences which are given by four constructions. We have verified this for $n = 5, 7, 9$ and 11. All these result can be found in [17].

In this paper we continue to investigate ternary sequences with 2-level autocorrelation. First, we prove that any p-ary 2-level auto-correlation sequence is balanced. This problem has been known for a while, but there seems to be no proof in the literature. We also discuss some variations of the second-order DHT operator. Helleseth and Martinsen performed an exhaustive search for ternary 3-term AC sequences for $2 \leq n \leq 8$. We confirmed their results and found that many of the sequences are equivalent. We also completed an exhaustive search for $n = 9$ and found no 3-term AC sequences for $n = 9$. We conjecture the existence of two new infinite families of ternary 3-term AC sequences and verified their validity for $3 \leq n \leq 16$. As well, we applied the second-order DHT operator to the newly obtained sequences. We had several non-trivial realizations, including new 9-term sequences. By using an AC sequence of period $3^n - 1$ that we obtained, we can construct infinite classes of AC sequences with period $3^{nm} - 1$ for any $m \geq 1$ by applying the Gordon-Mills-Welch method [11].

This paper is organized as follows. In Sections 2 and 3, we give a brief theoretical background on two-level autocorrelation sequences along with the definition of the DHT operator, the concepts of realizable pairs and realized sequences, and some special properties that apply to ternary sequences. In Section 4, we prove that any p-ary AC sequence is balanced. In Section 5, we give a generalization of the second-order DHT operator and discuss the realizations of ternary m-sequences. In Section 6, we present the conjectures on 3-term AC sequences and the realizations of 3-term AC sequences. Section 7 contains a construction of infinite classes of ternary AC sequences by applying the Gordon-Mills-Welch method to the newly discovered cases.

2 Preliminaries

Let

- p a prime number.
- $\mathbb{F} = GF(p),\ \mathbb{K} = GF(p^n),\ q = p^n$.
- α a primitive element of $\mathbb{K}$.
- $\omega = \mathrm{e}^{2\pi \mathrm{i}/p}$ complex primitive pth root of unity.
- $\chi(x) = \omega^x$ the canonical additive character [15] on $\mathbb{F}$.
- $\mathrm{Tr}_m^n(x)$ the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ where $n = l \cdot m$

$$\mathrm{Tr}_m^n(x) = x + x^q + x^{q^2} + \cdots + x^{q^{l-1}}, \quad x \in \mathbb{K},$$

$Tr(x)$ if the context is clear.

2.1 Cyclotomic Cosets and Trace Representation

Let $\mathbf{C} = \{1, p, p^2, \ldots, p^{n-1}\}$. Then $\mathbf{C}$ is a subgroup in $\mathbb{Z}^*_{p^n-1}$, and the set $g\mathbf{C} = \{g \cdot c \,|\, c \in \mathbf{C}\}$ is called a *(cyclotomic) coset* modulo $p^n - 1$. The smallest number in $g\mathbf{C}$ is called the *(cyclotomic) coset leader* modulo $p^n - 1$. Let Γ_{q-1} $(q = p^n)$, the set of all coset leaders modulo $q - 1$.

Any periodic sequence $\underline{\mathbf{a}}= \{a_i\}$ over $\mathbb{F}$ with period $v|q-1$ has trace representation:

$$a_i = \sum_{k=1}^{r} Tr_1^{n_k}(\beta_k\, \alpha^{i \cdot t_k}) \tag{1}$$

where $\beta \in \mathbb{F}^*_{p^{n_k}}$, $t_k \in \Gamma_{q-1}$, and n_k is the size of the cyclotomic coset containing t_k. Above we say that $\underline{\mathbf{a}}$ is a *r-term sequence.*

Thus, the trace representation is the main tool for classifying a given sequence into one of the known sequence classes (e.g. m-sequences, GMW sequences, etc.). Computationally, to obtain the trace representation of a given $\underline{\mathbf{a}}$ we use the Discrete Fourier Transform [6]

$$a_i = \frac{1}{q-1} \sum_{k \in \Gamma_{q-1}} Tr_1^{n_k}(A_k \alpha^{ki}) \tag{2}$$

where A_k are the discrete Fourier spectra of $\underline{\mathbf{a}}$: $A_k = \sum_{i=0}^{q-2} a_i\, \alpha^{-k\, i}$.

2.2 Autocorrelation

The autocorrelation of a periodic p-ary sequence $\underline{\mathbf{a}}$ is defined by

$$C_{\underline{\mathbf{a}}}(\tau) = \sum_{i=0}^{t-1} \chi(a_{i+\tau})\overline{\chi(a_i)}. \tag{3}$$

where τ is a phase shift of the sequence $\{a_i\}$ and the indexes are computed modulo t, the period of $\underline{\mathbf{a}}$. If $\underline{\mathbf{a}}$ has period $p^n - 1$ and

$$C_{\underline{\mathbf{a}}}(\tau) = \begin{cases} -1 & \text{if } \tau \not\equiv 0 \bmod q-1 \\ q-1 & \text{if } \tau \equiv 0 \bmod q-1 \end{cases} \tag{4}$$

(recall $q = p^n$) then we say that the sequence $\underline{\mathbf{a}}$ has *(ideal) 2-level autocorrelation.* This property is the third Randomness Postulate of Golomb [5]. We will use AC to denote the phrase of *2-level autocorrelation* in this paper. Let $f(x)$ be the trace representation of $\underline{\mathbf{a}}$. We also say that $f(x)$ has AC if $\underline{\mathbf{a}}$ is an AC sequence.

2.3 Decimation of AC Sequences

The elements of an m-sequence $\underline{\mathbf{a}}$ are defined by $a_i = Tr_1^n(\alpha^i)$. Recall that a proper decimation of an m-sequence yields another m-sequence. This is a general result based on the fact that if $\gcd(v, p^n - 1) = 1$, then $x \to x^v$ is a permutation of $\mathbb{K}$. Consequently,

Proposition 1. *([5]) Let* $\gcd(v, p^n - 1) = 1$. *If* $h(x)$ *has* AC*, then so does* $f(x) \triangleq h(x^v)$.

We call two sequences *non-equivalent* if they are not decimations of each other:

$$g(x) \neq f(x^c) \text{ for any } c \in \Gamma_{q-1} \text{ with } (c, q-1) = 1. \tag{5}$$

3 The Second-order DHT

In this section, we give a brief review for the second-order DHT operator introduced by Gong and Golomb in [10] and show some special properties which apply to ternary sequences.

3.1 Hadamard Transform

The Decimation-Hadamard Transform is a generalization of usual Hadamard transform where we first decimate f by v.

Definition 1. *For* $f(x) : \mathbb{K} \to \mathbb{F}$*, and an integer* $v \in \Gamma_{q-1}$ *define*

$$\widehat{f}(v)(\lambda) = \sum_{x \in \mathbb{K}} \chi(Tr(\lambda x))\overline{\chi(f(x^v))}, \quad \lambda \in \mathbb{K}. \tag{6}$$

$\widehat{f}(v)(\lambda)$ *is called* the first-order decimation-Hadamard transform (DHT) of $f(x)$ with respect to $Tr(x)$, *the first order DHT for short.*

Observe that $\widehat{f}(v)(\lambda)$ is essentially an inner product of $F(x^v) = \omega^{f(x^v)}$ with a dilation by λ of the trace function. The range of $\widehat{f}$ is in general $\mathbb{C}$, but in our case it is easy to establish

Lemma 1. *If* $f(-x) = -f(x)$ $\forall x$ *and* $p = 3$*, then* $\widehat{f}(v)(\lambda) \in \mathbb{Z}$ *for all* v, λ.

3.2 Second order DHT

The motivation for the second iteration stems from the inverse formula for Hadamard transform (compare with the classic Fourier expansion):

$$\omega^{f(\lambda)} = \frac{1}{q}\sum_{x\in\mathbb{K}} \chi(Tr(\lambda x))\overline{\widehat{f}(x)}, \qquad \lambda \in \mathbb{K} \tag{7}$$

Accordingly, with notation as above we define

Definition 2.

$$\widehat{f}(v,t)(\lambda) = \sum_{y\in\mathbb{K}} \chi(Tr(\lambda y))\,\overline{\widehat{f}(v)(y^t)}, \qquad t \in \Gamma_{q-1},\ \lambda \in \mathbb{K} \tag{8}$$

$\widehat{f}(v,t)(\lambda)$*is called the* second-order decimation-Hadamard transform of $f(x)$(with respect to $Tr(x)$), the second-order DHT *for short.*

Note that for $p = 3$, $\widehat{f}(v,t)(\lambda)$ is in $\mathbb{Z}[\omega]$. From the definitions the following result is immediate

Lemma 2.

$$\widehat{f}(v,t)(\lambda) = \sum_{x,y\in\mathbb{K}} \omega^{Tr(\lambda y)+Tr(y^t x)-f(x^v)}. \tag{9}$$

Remark 1. If $t = 1$, then the second order DHT reduces to the inverse Hadamard transform of $f(x^v)$.

3.3 Realizable pairs

Motivated by the formula for inverse Hadamard transform (7), we are interested in pairs (v,t), such that $\widehat{f}(v,t)(\lambda)$ is a character evaluation of another function.

Definition 3. *Let $\Omega = \{1, \omega, \ldots, \omega^{n-1}\} = \langle\omega\rangle$. If $\widehat{f}(v,t)(\lambda) \in q\cdot\Omega$ for all λ, then we call (v,t) a* realizable pair *and call g given by*

$$\omega^{g(\lambda)} = \frac{1}{q}\widehat{f}(v,t)(\lambda) \tag{10}$$

the realization *of $\widehat{f}(v,t)(\lambda)$.*

The following result is proven in [10]

Proposition 2. *With the above notation, let $a_i = f(\alpha^i)$ and $b_i = g(\alpha^i)$ where α is a primitive element of $GF(p^n)$, $i = 0,1,\ldots$. Then p-ary sequence $\{b_i\}$ has 2-level autocorrelation if and only if $\{a_i\}$ does.*

We wish to have the realization g to be an entirely new AC sequence, so that the second order DHT gives us a method to generate new sequences.

4 2-level Autocorrelation and Balanced Sequences

In this section we prove the result that if $\{a_i\}$ is AC then it is also balanced. The significance of the result is that it is a first step towards showing the equivalence of AC p-ary sequences and Hadamard difference sets with the Singer parameters. For the binary case, we have the following result.

Proposition 3. *Any binary AC sequence* $\underline{\mathbf{a}}$ *of period* $2^n - 1$ *has the following three properties.*

1. $\underline{\mathbf{a}}$ *is balanced. I.e., there are* 2^{n-1} *1's and* $2^{n-1} - 1$ *0's occurring in one period.*
2. *The discrete Fourier spectra* $\{A_k\}$ *of* $\underline{\mathbf{a}}$ *satisfy:*

$$A_k \in \{0, 1\} \text{ and } A_k A_{-k} = 0, \forall k.$$

The proof of the first result can be found in [5] and the second result appeared in [4].
In the following, we will show that any p-ary AC sequence satisfies the balance property.

Theorem 1. *If the p-ary sequence* $\underline{\mathbf{a}}$ *has two-level autocorrelation, then* $\underline{\mathbf{a}}$ *is balanced. I.e., each nonzero element in* $GF(p)$ *occurs precisely* p^{n-1} *times in one period of* $\underline{\mathbf{a}}$ *and zero element occurs* $p^{n-1} - 1$ *times in one period of* $\underline{\mathbf{a}}$.

Proof. : Let $h(x)$ be the trace representation of $\underline{\mathbf{a}}$. Since $\underline{\mathbf{a}}$ is AC, $h(x)$ is *orthogonal*, that is

$$\sum_{x \in \mathbb{K}} \chi(h(\lambda x))\overline{\chi(h(x))} = \begin{cases} 0 \text{ if } \lambda \neq 0, 1 \\ q \text{ if } \lambda = 1 \end{cases} \tag{11}$$

where we set $h(0) = 0$. Note that (11) is just a restatement of (4) in terms of functions.

To prove the theorem we need to show that $h(x)$ has p^{n-1} zeros in $\mathbb{F}_{p^n}$. Since $h(0) = 0$, it follows that $\underline{\mathbf{a}}$ will have exactly one zero less than $h(x)$ in one period ($a_i = h(\alpha^i)$). The former statement is equivalent to showing $\sum_{x \in \mathbb{K}} \chi(h(x)) = 0$, or that (11) holds for $\lambda = 0$. We utilize linear algebra.

For convenience, let $f(x) \triangleq \chi(h(x))$. Let V be the vector space of functions from $\mathbb{K}$ to $\mathbb{Q}[\omega]$ over $\mathbb{Q}[\omega]$. $V = \{f \mid f : \mathbb{K} \to \mathbb{Q}[\omega]\}$. Then $\dim(\mathrm{V}) = \mathrm{q}$, since any function in V naturally corresponds to a vector of length q with entries in $\mathbb{Q}[\omega]$. Furthermore, the sum in (11) then states that $< f(\lambda x), f(x) >= 0$ where the inner product on V naturally corresponds to the Euclidean inner product on $\mathbb{Q}[\omega]^q$. Since

$$\sum_x f(ax)\overline{f(bx)} = \sum_x f(\lambda x)\overline{f(x)} \qquad \text{where } \lambda = a \cdot b^{-1}, b \neq 0$$

, (11) gives us a set of $q - 1$ orthogonal (hence linearly independent) functions $g_\lambda(x) \equiv f(\lambda x)$. We can extend this to an orthogonal basis of V by adding one more implicit function $g(x)$, defined by

$$\sum_x g(x)\overline{f(\lambda x)} = 0 \qquad \forall \lambda \in \mathbb{K} \backslash \{0\}. \tag{12}$$

Suffices to show that $g(x)$ is constant, since this would imply that $f(0\cdot x)\equiv 1$ is a multiple of $g(x)$ and hence is orthogonal to all $f(\lambda x)$ which is what we are after. Observe

$$\begin{aligned}\sum_{\lambda\in\mathbb{K}} f(c\lambda))\overline{f(d\lambda))} &= \sum_{x} f(cd^{-1}x)\overline{f(x)}, \qquad x=\lambda\cdot d,\ c,d\neq 0\\ &= \begin{cases} 0 \text{ if } c\neq d\\ q \text{ if } c=d\end{cases}\end{aligned}$$

Using an inversion technique like the one for characters [15, p. 195] write for $c\neq 0$

$$\begin{aligned} g(c) &= \frac{1}{q}\sum_{d} g(d)\sum_{\lambda} f(\lambda c)\overline{f(\lambda d)}\\ &= \frac{1}{q}\sum_{\lambda} f(\lambda c)\sum_{d} g(d)\overline{f(\lambda d)}, \qquad \text{by (12) the inner sum is zero whenever } \lambda\neq 0\\ &= \frac{1}{q} f(0\cdot c)\sum_{d} g(d)\overline{f(0\cdot d)}\\ &= \frac{1}{q}\sum_{d} g(d) \end{aligned} \tag{13}$$

It follows that $g(x)$ is constant on $\mathbb{K}\backslash\{0\}$. Let $g(0)=a$, and $g(x)=b$ for all other x. Then by above $b=\frac{1}{q}(a+(q-1)b)$ implying $a=b$ or $g(x)$ is constant on all of $\mathbb{K}$.

Let $T_i=\#\{x\,|\,h(x)=i\}$. From $\sum_{x\in\mathbb{K}} f(x)=0$ we get

$$T_0\,\omega^0+T_1\,\omega^1+\ldots T_{p-1}\,\omega^{p-1}=0 \tag{14}$$

Since the minimal polynomial of ω is $s(x)=1+x+x^2+\cdots+x^{p-1}$ and $T(\omega)=0$ where $T(x)=\sum_{i=0}^{p-1}T_i x^i$ we have $s\,|\,T$, or $T(x)=c\cdot s(x)$ since $deg(T)=deg(s)$. So we must have, $T_0=T_1=\cdots=T_{p-1}=p^{n-1}$ $\square$.

5 Realizations of m-Sequences and Signed Exponential Sums

At first, we used the m-sequence $\{a_i\}$ where $a_i=Tr(\alpha^i)$ for our base function f in the second order DHT. Unfortunately, only m-sequences were obtained as realizations.

With the hope of collapsing several equivalence classes into one, we tried a generalization of DHT. For m-sequences, we have $f(x)=Tr(x)$ and the second order DHT can be written as

$$\widehat{f}(v,t)(\lambda)=\sum_{x,y}\omega^{G(v,t,\lambda)}$$

where $G(v,t,\lambda)=Tr(\lambda y)+Tr(y^t x)-Tr(x^v)$. As a generalization, we replace the plus and minus signs above by any combination of (+, -), as well as replacing $Tr(x)$ by a general *orthogonal* function $h(x)$:

$$G_{a,b}(v,t,\lambda)=h(\lambda y)+a\,h(y^t x)+b\,h(x^v).\ \text{where } a,b\in\{1,-1\}. \tag{15}$$

We also write

$$\widehat{G}_{a,b}(v,t,\lambda)=\sum_{x,y}\omega^{G_{a,b}(v,t,\lambda)}.$$

Note 1. We can assume that the first sign in (15) is a plus (+), since changing all 3 signs at once doesn't do anything by the conjugation property $\omega^{-G} = \overline{\omega^G}$.

Lemma 3. *For all primes p, and for all $h(x)$ orthogonal and additive on $\mathbb{F}$, that is $h(cx) = c \cdot h(x)$ for all $c \in \mathbb{F}$, $x \in \mathbb{K}$, $\widehat{G}_{1,-1}(v,t,\lambda) = \widehat{G}_{-1,1}(v,t,\lambda)$ and $\widehat{G}_{1,1}(v,t,\lambda) = \widehat{G}_{-1,-1}(v,t,\lambda)$.*

Proof.

$$\begin{aligned}\widehat{G}_{1,-1}(v,t,\lambda) &= \sum_{x,y} \chi(h(\lambda y))\omega^{-h(y^t x)+h(x^v)} \\ &= \sum_{x,y} \chi(h(\lambda y))\overline{\omega^{h(y^t x)-h(x^v)}} \\ &= \sum_{x,y} \chi(h(\lambda y))\overline{\widehat{h}(v)(y^t)}\end{aligned}$$

Since by Lemma 1 $\widehat{h}(v)(y^t) \in \mathbb{R}$, the result follows. Similarly, $G_{1,1} \equiv G_{-1,-1}$.

Lemma 4. *For $h(x) = Tr(x)$ and all primes p, $\widehat{-G}_{1,1}(v,t,\lambda) = \widehat{G}_{1,-1}(v,t,\lambda)$.*

Proof.

$$\begin{aligned}\widehat{-G}_{1,1}(v,t,\lambda) &= \sum_{x,y} \omega^{-Tr(\lambda y + y^t x + x^v)} \\ &= \sum_{x} \omega^{Tr(-x^v)} \sum_{y} \omega^{-Tr(\lambda y + x y^t)} \\ &= \sum_{x} \omega^{Tr(-x^v)} \sum_{y} \overline{\omega^{Tr(\lambda y + x y^t)}}\end{aligned}$$

To finish the proof suffices to show that the inner sum is in $\mathbb{R}$, because then the last line above is exactly $\widehat{G}_{1,-1}(v,t,\lambda)$. But again, observe that in the conjugated sum, λ and x are constant, and hence $\lambda y + x y^t$ is an *odd* function of y, since $(t, p^n - 1) = 1$. Using same argument as in Lemma 1, the result is established.

Thus for $p = 3$ all four different sign exponential sums give the same realization (up to a constant multiple), and the generalization does not yield anything new.

6 Realizations of Two-term AC Sequences

As the second order DHT method failed on m-sequences, we tried applying it to 2-term ternary AC sequences $\{a_i\}$ where $a_i = Tr(\alpha^i + \alpha^{id})$. We obtained many non-trivial realizations, and the experimental results listed below suggested the following conjecture.

Let $n = 2m + 1$. In his PhD thesis Lin [16] conjectured that the 2-term sequence defined by $f(x) = Tr(x + x^d)$ where $d = 2 \cdot 3^m + 1$ is AC in $GF(3^n)$ (we verified that $f(x)$ is AC for all $n \leq 15$). It turns out that this is the most interesting case for applying the second order DHT on ternary sequences.

6.1 Conjectures of 2-term AC Sequence Realizations

Conjecture 1 *Let $n = 2m+1$ and $f(x) = Tr(x+x^d)$ where $d = 2\cdot 3^m+1$. Then $(1,t)$ is a realizable pair of $f(x)$ where both t and the realization $g(\lambda)$ of $\widehat{f}(1,t)(\lambda)$ are given by the following four constructions where $g(x)$ is non-equivalent to $f(x)$ in the sense of (5). In other words, the realization $g(x)$ of $\widehat{f}(1,t)(\lambda)$ produces entirely new ternary AC sequences.*
Moreover, all such newly obtained ternary AC sequences are in one-to-one correspondence with cyclic Hadamard difference sets with parameters $(\frac{3^n-1}{2}, \frac{3^{n-1}-1}{2}, \frac{3^{n-2}-1}{2})$.

This Conjecture has been verified for $n = 5, 7, 9$, and 11.

Construction A Let $v = \frac{3^n-1}{2}$ and $u = \frac{3^m-1}{2}$. Then we have the following construction

$$t = \begin{cases} v+u & \text{if } n \equiv 1 \mod 4 \\ u & \text{if } n \equiv 3 \mod 4 \end{cases}$$

The ternary sequence obtained by this realization is a $(m+1)$-term AC sequence, whose trace representation $\mathrm{H}_n(x) = Tr(\sum_{j=1}^{m+1} b_j x^{c_j})$ is defined through

$$b_j = (-1)^{j+1}, \quad j = 1, 2, \ldots, m \qquad \text{with} \quad b_{m+1} = (-1)^{m+1},$$

and c_j are recursively given by

$$c_1 = 1, \quad c_{j+1} = c_j + 2\cdot 3^{2j-1}, \quad j = 1, \ldots, m.$$

This construction has also been verified probabilistically for $n = 13$ and 15 (computing several thousand random autocorrelation values).

Construction B We also have a conjectured infinite family of 5-term sequences for n odd. The construction is:

$$t = 3^m \left(\frac{3^r-1}{2}\right) - \frac{3^{r-1}-1}{2} \text{ where } n = 4r \pm 1.$$

The realization gives a 5-term sequence, whose trace representation for $n = 4r+1$ is defined by $\mathrm{J}_n(x) = Tr(-x^{c_{1,r}} - x^{c_{2,r}} - x^{c_{3,r}} + x^{c_{4,r}} + x^{c_{5,r}})$ where

$$c_{1,r} = 1 \qquad c_{3,r} = 3^{r+1}+2$$
$$c_{2,r} = 2\cdot 3^r + 1 \qquad c_{4,r} = 3^{2r+1} + 3^{r+1} + 1^*$$
$$c_{5,r} = 2\cdot 3^{3r} + 3^{2r} + 3^r + 1$$

For the case of $n = 4r-1$, we do not know the correct form for $c_{i,r}$.

* There is a "swinging" anomaly for $r = 1$: $c_{4,1} = 3^{2\cdot 1+1} + \mathbf{3^1} + 1$.

Construction C We have

$$t = \frac{3^{2m}+1}{2} - 2\cdot 3^{m-1}.$$

Let the sequence given by this realization have s_m terms. Then s_m is recursively defined by $s_{m+1} = 3 \cdot s_m - s_{m-1}$, with $s_0 = 1,\ s_1 = 2$.

Note. The actual values of s_m, which are $1, 2, 5, 13, 34, 89$, correspond to the even Fibonacci numbers F_{2m}. This resembles the hyper-oval construction for binary sequences, however at this point we do not know an appropriate generalization to $p = 3$.

Construction D In general, the second component $t = t_k$ of the realizable pairs $(1, t)$ can be explained by

$$t_k = 3^m \left(\frac{3^{k+1} - 1}{2}\right) - \frac{3^k - 1}{2} \tag{16}$$

where either $1 \le k \le m-1$ if $n \not\equiv 0 \bmod 3$ or $2 \le k \le m-1$ if $n \equiv 0 \bmod 3$. This construction includes Construction B for $k = 1$ or 2 depending on the value of n, and Construction C for $k = m - 1$.

Remark 2. The first order DHT $\widehat{f}(v)(\lambda)$ of $f(x)$ for $v = 1$ is 3-valued, as proven by Helleseth *et al.* [2]

Last we make a remark on Construction D.

Remark 3. The ternary AC sequences obtained from the realizable pair $(1, t_k)$ where t_k is defined by Construction D are analogous to the binary AC sequences obtained from the realizable pairs $(3, \frac{2^k+1}{3})$ where $(k, n) = 1$. The realizable pairs $(3, \frac{2^k+1}{3})$ give Dobbertin's Kasami power–function construction sequences [10, 1]. Here the 2-term ternary sequences play the same role in the second-order DHT over $GF(3)$, as the binary m-sequences in the second-order DHT over $GF(2)$. More precisely, let $n = 2m+1$.

1. For $p = 2$ and $f(x) = Tr(x)$, the function $g(x)$ defined by

$$\omega^{g(\lambda)} = \frac{1}{q}\widehat{f}(3, \frac{2^k + 1}{3})(\lambda) \tag{17}$$

   gives Dobbertin's Kasami power–function construction sequences where $1 \le k < m$ and $(k, n) = 1$. If $k = 2$, (17) gives the same class as the Segre hyper-oval construction [18].

2. For $p = 3$ and $f(x) = Tr(x + x^d)$ where $d = 2 \cdot 3^m + 1$, the function defined by

$$\omega^{g(\lambda)} = \frac{1}{q}\widehat{f}(1, t_k)(\lambda) \tag{18}$$

   gives $m - 1$ or $m - 2$ classes of ternary AC sequences where t_k is defined by (16). This has been verified for $n = 5, 7, 9$, and 11. For $k = m - 1$, it also has the special form as Construction C. Due to this resemblance, we consider the sequences from Construction C as the Segre hyper-oval sequences over $GF(3)$.

6.2 Experimental Results on 2-Term AC Sequence Realizations

In the following tables, we list all the non-equivalent realizations of 2-term sequences for $n = 5, 7, 9$, and 11. All such sequences are new ternary AC sequences which are in one-to-one correspondence with cyclic Hadamard difference sets with parameters $(\frac{3^n-1}{2}, \frac{3^{n-1}-1}{2}, \frac{3^{n-2}-1}{2})$. In each table, the first column lists the realizable pairs (v, t), the second column the number of terms in the realization, the third column the classification according to the conjectures above (for Construction D, the subscript gives the corresponding value of k), and the last column the spectrum obtained using DFT, i.e., the pair (k, A_k) defined in (2). For example, the second row of Table 2 means that if we start with $f(x) = Tr(x + x^{55})$, i.e. 2-term AC sequence, then we get the realizable pair $(1, t) = (1, 107)$. This pair gives the realization $g(x) = Tr(2x + 2x^7 + 2x^{11} + x^{37} + x^{277})$ which is a ternary 5-term AC sequence. This realization can be explained by Constructions B and D (with $k = 1$). We also list the primitive polynomial $h(x)$ of degree n over GF(3) which defines each finite field.

Table 1. $n = 5,\ f(x) = Tr(x + x^{19})$, and $h(x) = x^5 + 2x + 1$

(1, 125)	3-terms	A	(1, 1) (7, 2) (61, 2)
(1, 35)	5-terms	B, C, D_1	(1, 2) (7, 2) (11, 2) (31, 1) (67, 1)

Table 2. $n = 7,\ f(x) = Tr(x + x^{55})$, and $h(x) = x^7 + 2x^2 + 1$

(1, 13)	4-terms	A	(1, 1) (7, 2) (61, 1) (547, 1)
(1, 107)	5-terms	B, D_1	(1, 2) (7, 2) (11, 2) (37, 1) (277, 1)
(1, 347)	13-terms	C, D_2	(1, 1) (7, 1) (11, 1) (31, 2) (37, 2) (55, 1) (67, 2) (91, 2) (103, 2) (115, 2) (119, 2) (283, 1) (607, 1)

Table 3. $n = 9,\ f(x) = Tr(x + x^{163})$, and $h(x) = x^9 + 2x^6 + 2x^3 + x + 1$

(1, 9881)	5-terms	A	(1, 1) (7, 2) (61, 1) (547, 2) (4921, 2)
(1, 1049)	5-terms	B, D_2	(1, 2) (19, 2) (29, 2) (271, 1) (1549, 1)
(1, 3227)	34-terms	C, D_3	(1, 2) (7, 2) (11, 2) (31, 1) (37, 1) (55, 2) (67, 1) (83, 2) (91, 1) (103, 1) (115, 1) (119, 1) (247, 1) (253, 1) (271, 1) (283, 2) (361, 2) (499, 1) (571, 1) (595, 1) (607, 2)(763, 1)(767, 1) (823, 2) (895, 1) (931, 2) (1003, 2) (1039, 2) (1063, 2) (1075, 2) (1087, 2) (1091, 2) (2551, 1) (5467, 1)

Table 4. $n = 11$, $f(x) = Tr(x + x^{487})$, and $h(x) = x^{11} + 2x^{10} + x^9 + x^8 + 2x^2 + 2x + 1$

(1, 121)	6-terms	A	(1, 1) (7, 2) (61, 1) (547, 2) (4921, 1) (44287, 1)
(1, 3155)	5-terms	B, D_2	(1, 2) (19, 2) (29, 2) (271, 1) (6823, 1)
(1, 9707)	13-terms	D_3	(1, 1) (7, 1) (11, 1) (37, 2) (247, 2) (277, 2) (307, 2) (487, 1) (577, 2) (811, 2) (821, 2) (3007, 1) (22147, 1)
(1, 971)	34-terms	D_1	(1, 2) (7, 2) (11, 2) (37, 1) (85, 1) (163, 2) (245, 2)(271, 1) (733, 1) (739, 1) (811, 1) (1471, 1) (1549, 1) (1705, 1) (1783, 1) (2221, 1) (2225, 1) (2287, 1) (2299, 2) (2377, 1) (2443, 2) (2459, 1) (2521, 2)(2677, 1) (3001, 2) (7375, 2) (8113, 2) (8347, 2) (8863, 2) (9085, 1) (9565, 2)(16129, 2) (22151, 2) (28039, 1)
(1, 29363)	89-terms	C, D_4	(1, 1) (7, 1) (11, 1) (31, 2) (37, 2) (55, 1) (67, 2) (83, 1) (91, 2) (103, 2) (115, 2) (119, 2) (247, 2) (253, 2)(271, 2) (283, 1) (325, 2)(361, 1) (487, 1) (499, 2) (571, 2) (595, 2) (607, 1)(739, 2) (751, 2)(763, 2) (767, 2) (811, 2) (823, 1) (895, 2) (919, 2) (931, 1) (979, 2) (983, 2)(1003, 1) (1027, 2) (1039, 1) (1055, 2) (1063, 1) (1075, 1) (1087, 1) (1091, 1) (2215, 2) (2227, 1) (2305, 1) (2443, 1) (2515, 1) (2539, 1) (2551, 2) (2953, 1)(3169, 1) (3277, 2) (4459, 2) (4483, 2) (4495, 1) (5131, 2) (5143, 1) (5359, 1)(5431, 1)(5455, 1) (5467, 2) (6815, 2)(6835, 1) (6871, 1) (6895, 1) (6907, 1) (6919, 1) (6923, 1) (7375, 1) (7411, 2)(8059, 1) (8275, 1) (8347, 1) (8383, 2) (8863, 1)(8867, 1) (9031, 2) (9247, 1) (9355, 2) (9571, 2) (9679, 2) (9751, 2) (9787, 2) (9811, 2) (9823, 2) (9835, 2) (9839, 2)(22963, 1) (49207, 1)

7 3-term AC Sequences and the Realizations

For $4 \leq n \leq 9$ we performed a computer exhaustive search for 3-term sequences ($r = 3$ in (1)) in $\mathbb{F}_{3^n}$. Starting from an m-sequence $\underline{\mathbf{a}}$, we generated sequences which were a term-by-term sum of $\underline{\mathbf{a}}$ together with several of its decimations (using the additive property of Trace in (1)). The result was then checked for ideal autocorrelation. During our search we assumed without loss of generality (because of decimation property (1)) that one of the exponents is 1. That is, we only searched for sequences of the form

$$a_i + c_1 a_{d_1 i} + c_2 a_{d_2 i} \text{ where } \quad c_1, c_2 \in \{1, 2\}$$

and $d_1, d_2 \in \Gamma_{p^n-1}$. The trace representations of such sequences are then

$$h(x) = Tr(x + x^{d_1} + x^{d_2}).$$

Because of Proposition (1) in Section 2, the discovered 3-term sequences come in *equivalence classes* of two or three, depending upon whether the two non-trivial exponents are co-prime with $p^n - 1$ or not. So if $\gcd(d_1, p^n - 1) = 1$ and $Tr(x + x^{d_1} + x^{d_2})$ is AC, then by Proposition (1) $Tr(x^c + x + x^{c\,d_2})$ where $c = d_1^{-1} \mod p^n - 1$ is also AC. These equivalence classes are indicated in the figures with horizontal lines.

7.1 Conjectures on 3-Term AC Sequences

We conjecture the existence of following infinite families of ternary AC sequences.

Conjecture 2 (E) *Let $n = 2k$ even, such that $3 \nmid n$ not a multiple of 3, and let*

$$d_1 = 3^k + 3^{k-1} - 1, \qquad d_2 = 3^{k+1} - 2.$$

Then $Tr(x + 2x^{d_1} + 2x^{d_2})$ gives an AC sequence.

Conjecture 2 has been verified for $n = 4, 8, 10, 14, 16$.

Conjecture 3 (F) *Let $n = 4r + 2$,*

$$d_1 = 2 \cdot 3^{2r+1} - 1, \qquad d_2 = 3^{2r+2} - 2.$$

Then $Tr(x + 2x^{d_1} + x^{d_2})$ gives an AC sequence. Or take

$$d_1 = 3^{2r+1} + 3^{r+1} - 1, \qquad d_2 = 3^{3r+1} - 3^r + 1.$$

Then $Tr(x + 2x^{d_1} + 2x^{d_2})$ also gives an AC sequence.

Conjecture 3 has been verified for $n = 6, 10, 14$.

Remark 4. For $n \geq 13$ we used the probabilistic method of computing random autocorrelation values. We don't have any theoretical results to bound the probability of the correct answer in this case, but empirically if $\underline{\mathbf{b}}$ doesn't have AC, then a large number (at least a third) of the autocorrelation values are non-zero.

7.2 Realizations of Three-term AC Sequences

In the following, we summarize the result on applying the second order DHT method to the found 3-term sequences.

If two AC sequences are equivalent with respect to decimation, their realizations will be also, so it makes sense to talk about the realization of an equivalence class. Below we view the AC sequences as objects in a set $\mathbf{S}$, with the second order DHT inducing an action on $\mathbf{S}$. So if AC sequence $\{b_i\}$ can be obtained by applying DHT to AC sequence $\{a_i\}$ and vice versa, we say that $\{a_i\}$ and $\{b_i\}$ belong to the same *DHT orbit*.

1. For $n = 4$ only trivial realizations were obtained. Note that for $n = 4$ both non-equivalent sequences have one exponent which wasn't co-prime with $p^n - 1$.
2. For $n = 5$ we have 2-term and 5-term sequences as realizations. These were already obtained in Section 6. We get a *DHT orbit* of size 3 consisting of a 2-term sequence, a 3-term sequence and a 5-term sequence (starting from any sequence in the orbit, we can realize all the other ones). We list these sequences in Table 5.
3. For $n = 6$ we have one orbit consisting of two 3-term sequences, with the third non-equivalent 3-term sequence being in a singleton orbit (i.e. the only realizations are decimations of the original base sequence).
4. For $n = 7$ we don't have any realizations whatsoever (not even trivial ones). Note that in this case we only had one equivalence class to begin with.
5. For $n = 8$ we have 2 orbits each consisting of a 3-term sequence and a 9-term sequence, whose trace representations are listed in Table 6. The third orbit is once again a singleton.
6. Applying the DHT operator for $n \geq 10$ is not computationally feasible at this point.

Note. Whenever one of the exponents was not co-prime with $p^n - 1$, we never obtained any non-trivial realizations. It appears that all the decimations of the original m-sequence must be *proper* in order to have realizable sequences.

Note. In Table 5, $g_2(x) = Tr(x + x^{19})$ refers to 2-term AC sequence and $g_5(x) = Tr(2x + 2x^7 + 2x^{11} + x^{31} + x^{67})$ refers to the 5-term AC sequence.

7.3 Experimental Results on Exhaustive Search for 3-term Sequences

The tables below give all the found 3-term AC sequences. For each n we also list $f(x)$ the defining primitive polynomial of degree n used to generate the finite field $GF(3^n)$. No three term sequences

Table 5. Realizations for $n = 5$, 3-term sequences

Starting Sequence	Realizable Pair	Realization
$x + 2x^{41} + x^5$	(5, 125)	$2 \cdot g_2(x^{13})$
	(41, 131)	$2 \cdot g_5(x^{31})$
	(61, 13)	$2 \cdot g_5(x)$
	(61, 31)	$2 \cdot g_2(x)$
$x + 2x^{19} + x^{53}$	-	-
$x + 2x^5 + x^{41}$	-	-

Table 6. Realized 9-term Sequences for $n = 8$

Seq 1:	(1, 2) (83, 1) (161, 1) (241, 2) (323, 1) (403, 2) (563, 2) (643, 1) (667, 1)
Seq 2:	(1, 1) (83, 2) (107, 2) (241, 2) (323, 2) (827, 1) (1043, 1) (643, 1) (667, 1)

were found for $n = 9$.

Remark 5. This confirms the results of Helleseth et al. [13] who performed similar search for $2 \leq n \leq 8$ a few months ago.

The first column gives the signs for the sequence (in GF(3) we have $-1 = 2$ so that for example the first row in figure 7 corresponds to $Tr(x + x^5 + 2x^{11})$. For even values of n we indicate which sequences belong to one of the conjectured families (^{E} refers to Conjecture 2 and ^{F} refers to Conjecture 3). We use the data from [13] for $4 \leq n \leq 8$ which are considered as inequivalence classes by Helleseth *et al.* and indicate true different equivalence classes in the tables by horizontal lines. For example, for $n = 5$, we only have three different inequivalent classes.

Table 7. $n = 4, \qquad f(x) = x^4 + x + 2$

$+-$	5	11
$--$	5	17
E $--$	11	25
$+-$	25	17

8 Infinite Classes of Ternary AC Sequences

Theorem 2. *For any $m > 1$ and $n \in \{4, 5, \ldots, 14\}$, let $h(x)$ be the trace representation of a ternary AC sequence of period $3^n - 1$ taken from the set consisting of all AC sequences listed in Tables 1-13.*

Table 8. $n = 5, \qquad f(x) = x^5 + 2x + 1$

$+-$	5	41
$--$	7	61
$--$	35	49
$+-$	41	5
$+-$	61	7
$+-$	49	35
$--$	17	41
$+-$	23	61
$+-$	53	19

Table 9. $n = 6, \qquad f(x) = x^6 + x + 2$

F_1	$+-$	79	53
	$--$	29	107
	$+-$	157	211
F_2	$--$	35	79
	$+-$	133	157

Table 10. $n = 7, \qquad f(x) = x^7 + 2x^2 + 1$

$+-$	17	89
$--$	41	131
$+-$	643	391

Table 11. $n = 8, \qquad f(x) = x^8 + x^7 + x^5 + 2x + 2$

$--$	89	721
$+-$	347	1769
$+-$	643	1201
$--^E$	107	241
$+-$	907	1361
$+-$	1049	1043
$--$	131	365
$+-$	485	217

Table 12. $n = 10, \qquad f(x) = x^{10} + x^9 + x^8 + 2x^7 + 2x^2 + 2x + 2$

E $--$	323	727
F_1 $+-$	727	485
F_2 $--$	269	2179

Table 13. $n = 14$, verified probabilistically

E $--$	2915	6559
F_1 $+-$	6559	4373
F_2 $--$	2267	59023

Let $\sigma(x)$ be a GMW function of length r [3] related to a field chain $\mathbb{F}_{3^n} = F_0 \subset F_1 \subset \cdots \subset F_r = \mathbb{F}_{3^{nm}}$ where r is a positive integer. I.e.,

$$\sigma(x) = Tr_{F_1/F_0}(x^{s_1}) \circ Tr_{F_2/F_1}(x^{s_2}) \circ \cdots \circ Tr_{F_{r-1}/F_r}(x^{s_r}), x \in F_r$$

where $\circ$ is a function composition operator and s_i's satisfy $gcd(s_i, |F_i| - 1) = 1$. Let $g(x) = h(x) \circ \sigma(x)$, a composition of $\sigma(x)$ and $h(x)$, which is a function from $\mathbb{F}_{3^{nm}}$ to $\mathbb{F}_3$. Then $g(x)$ gives a ternary AC sequence of period $3^{mn} - 1$.

A proof of this result can be derived from the work of Gordon, Mills and Welch in [11] as early as in 1962, and it also explicitly follows from repeatedly using the result of Klapper, Chan and Goresky in [14] in 1993.

Remark 6. Here $g(x)$ can be replaced by any ternary AC sequence of period $3^n - 1$, the resulting sequence is still a new AC sequence of period $3^{nm} - 1$. The general case of Theorem 2 is presented in [7].

Acknowledgment. The authors wish to thank Tor Helleseth for his many valuable discussions on ternary sequences and for providing them with his exhaustive search results for 3-term ternary sequences.

References

1. J. Dillon and H. Dobbertin. New cyclic difference sets with singer parameters, 12 August, 1999. preprint.
2. H. Dobbertin, T. Helleseth, V. Kumar, and H. Martinsen. Ternary m-sequences with three-valued crosscorrelation function: Two new decimations. Abstract in *Proceedings of 2000 IEEE International Symposium on Inform. Theory*, June 2000, p. 329.
3. G.Gong. On $q-$ary cascaded gmw sequences. *IEEE Trans. on Inform. Theory*, vol. 42, No. 1:263–267, January 1996.

4. G.Gong and S. W. Golomb. Binary sequences with two-level autocorrelation. *IEEE Trans. on Inform. Theory*, vol. 45, No.2:692–693, March 1999.
5. S. Golomb. *Shift Register Sequences.* Aegean Park Press, Laguna Hills, CA, second revised edition, 1982.
6. G. Gong. Sequence analysis, lecture notes for course co739x. University of Waterloo, http://www.cacr.math.uwaterloo.ca/∼ggong.
7. G. Gong. New designs for signal sets with low cross-correlation, balance property-and large linear span: $gf(p)$ case. Technical Report, University of Waterloo, CORR 2000-32, May 2000, May 2000.
8. G. Gong and S. Golomb. Inverse hadamard transforms of two-level autocorrelation sequences. In *Proceedings of 2000 IEEE International Symposium on Inform. Theory*, page 300, 2000.
9. G. Gong and S. Golomb. Hadamard transforms of three term sequences. *IEEE Trans. on Inform. Theory*, vol. 45, No.6:2059–2059, September 1999.
10. G. Gong and S. W. Golomb. Second iteration of the decimation-hadamard transform of two-level autocorrelation sequences. *IEEE Trans. on Inform. Theory*, submitted August 2000.
11. B. Gordon, W. Mill, and L. Welch. Some new differnce sets. *Canadian J. Math.*, vol. 14, no. 4:614–625, 1962.
12. T. Helleseth, V. Kumar, and H. Martinsen. A new family of ternary sequences with ideal two-level autocorrelation function. Abstract in *Proceedings of 2000 IEEE International Symposium on Inform. Theory*, June 2000, p. 328.
13. T. Helleseth and H. Martinsen. Ternary sequences with ideal autocorrelation, June 2000. private communication.
14. A. Klapper, A. Chan, and M. Goresky. Cross-correlations of linearly and quadratically related geometric sequences and gmw sequences. *Discrete Appl. Math.*, **46**, No.1:1–20, 1993.
15. R. Lidl and H. Niederreiter. *Finite Fields.* Encyclopedia of Mathematics and its Applications, Volume 20. Addison-Wesley, Reading, MA, 1983.
16. A. Lin. *From Cyclic Hadamard Difference Sets to Perfectly Balanced Sequences.* PhD thesis, University of Southern California, Los-Angeles, 1998.
17. M. Ludkovski and G. Gong. New families of ideal 2-level autocorrelation ternary sequences from second order dht. preprint, September 2000.
18. A. Maschietti. Difference sets and hyperovals. *Designs, Codes and Cryptography*, **14**:89–98, 1998.