A New Family of Gold-like Sequences

Khoongming Khoo [1], Guang Gong [2] and Douglas R. Stinson [3]

[1,3]Department of Combinatorics and Optimization
[2]Department of Electrical and Computer Engineering
University of Waterloo, Waterloo, Ont. N2L 3G1, Canada
Email: [1]kkhoo@math.uwaterloo.ca, [2]ggong@calliope.uwaterloo.ca
[3]dstinson@cacr.math.uwaterloo.ca

Abstract. For n odd, we characterize Gold-like sequences of period $2^n - 1$ represented by $\sum_{i=1}^{\frac{n-1}{2}} c_i Tr(x^{2^i+1})$, $c_i \in \{0,1\}$, $x \in GF(2^n)$ using techniques from linear algebra and coding theory. We find two new classes of primes p for which the above sequence of period $2^p - 1$ is Gold-like for all choices of coefficients. We also prove that these primes are the only odd integers n with this property. Finally, we prove that the two-term function $Tr(x^{2^i+1} + x^{2^j+1})$ gives Gold-like sequences of period $2^n - 1$ for all $1 \leq i \neq j \leq \frac{n-1}{2}$ if and only if n is prime.

1 Introduction

Families of sequences with low cross correlation have important applications in CDMA communications and cryptography. The first family of such sequences was found in 1968 by Gold[1]. The Gold sequences of period $2^n - 1$,n odd, have trace representation $Tr(x^{2^i+1})$ where $\gcd(i,n) = 1$ and $Tr(x) = x + x^2 + \ldots + x^{2^{n-1}}$ is the trace function from $GF(2^n)$ to $GF(2)$. They have 3-valued cross correlation, taking on the values $-1, -1 \pm 2^{(n+1)/2}$. Later, considerable research has been done to discover other sequences with similar cross correlation properties, e.g.[2],[3], also see Helleseth and Kumar's survey paper[4]. In [3], the authors considered sequences represented by $\sum_{i=1}^{\frac{n-1}{2}} Tr(x^{2^i+1})$ and proved that they have 3-valued cross correlation.

In this paper, we consider sequences represented by $\sum_{i=1}^{\frac{n-1}{2}} c_i Tr(x^{2^i+1})$, $c_i \in \{0,1\}$, $x \in GF(2^n)$, n odd. Following the terminology of [3], a sequence is called *Gold-like* if it has cross correlation values $-1, -1 \pm 2^{\frac{n+1}{2}}$. Using the Walsh squaring technique, we show that determining whether such a sequence is Gold-like is equivalent to doing a rank computation for an associated cyclic matrix. By the theory of cyclic codes, we can find the rank of this matrix by a polynomial gcd computation, and thus we devise an efficient polynomial time method for finding Gold-like sequences associated with arbitrarily large fields.

Using the tools we develop, we find two new classes of primes p for which the sequences represented by $\sum_{i=1}^{\frac{p-1}{2}} c_i Tr(x^{2^i+1}), c_i \in \{0,1\}$, $x \in GF(2^p)$ are Gold-like for all choices of c_i. One class consists of odd primes p for which 2 is a primitive element modulo p; while the other includes the Sophie-Germain primes of the form $p = 2q + 1$, p, q prime. Assuming the Riemann Hypothesis, the first class was proven to be infinite while it is a well-known conjecture that the second class of primes is infinite, too. Finally, we prove that these primes are the only odd integers n with this property.

For n odd, it is known that the sequence represented by $Tr(x^{2^i+1})$, $x \in GF(2^n)$ is Gold-like for all i if and only if n is prime. We prove a similar result for sequences represented by the sum of two trace terms: we show that $Tr(x^{2^i+1} + x^{2^j+1})$ is Gold-like on $GF(2^n)$ for all i, j if and only if n is prime.

2 Definitions

Let $GF(2^n)$ be the finite field with 2^n elements and let α be a primitive element. Let $f : GF(2^n) \to GF(2)$, we say $f(x)$ is the *trace representation* of the binary sequence $\underline{a} = \{a_i\}_{i=0}^{2^n-1}$ if $a_i = f(\alpha^i)$ for all i. An m-sequence is a sequence whose trace representation is given by $Tr(x^r)$, $1 \le r \le 2^n - 2$. Let $\underline{m}$ be the m-sequence represented by $Tr(x)$. The *cross correlation* of a binary sequence $\underline{a} = \{a_i\}_{i=0}^{2^n-1}$ with $\underline{m}$ is

$$C_{\underline{a},\underline{m}}(\tau) = \sum_{k=0}^{2^n-2} (-1)^{a_k + m_{k+\tau}} \tag{1}$$

The *Hadamard transform* of a function $f : GF(2^n) \to GF(2)$ is defined to be

$$\hat{f}(\lambda) = \sum_{x \in GF(2^n)} (-1)^{Tr(\lambda x) + f(x)}, \lambda \in GF(2^n) \tag{2}$$

Thus $\hat{f}(\lambda) = 1 + C_{\underline{a},\underline{m}}(\tau)$ where $\lambda = \alpha^\tau$ and $\underline{a}$ has trace representation $f(x)$.

Definition 1. *Let n be odd. We say $\underline{a}$ is* Gold-like *if its cross correlation with m-sequence represented by $Tr(x)$ is -1 half of the time and $-1 \pm 2^{\frac{n+1}{2}}$ the other half of the time. This is equivalent to saying that the Hadamard Transform $\hat{f}$ has the following frequency distribution:*

$\hat{f}$	*frequency*
0	2^{n-1}
$\pm 2^{\frac{n+1}{2}}$	2^{n-1}

We also say that f is Gold-like if $\hat{f}$ has the above frequency distribution.

Let p be prime. We denote the multiplicative order of a modulo p by $ord_p(a)$.

3 Characterization of Gold-like Sequences

In this section, we prove that for n odd, we can determine very efficiently if the function $f(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i Tr(x^{2^i+1})$ is Gold-like using elementary algebraic techniques.

Lemma 1. *For n odd, let $f(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i Tr(x^{2^i+1})$, $c_i \in \{0,1\}$, $x \in GF(2^n)$. Then f is Gold-like if and only if the cyclic matrix*

$$L = \begin{pmatrix} c_0 & c_1 & c_2 & c_3 & \dots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & c_2 & \dots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & c_1 & \dots & c_{n-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & c_3 & c_4 & \dots & c_0 \end{pmatrix} \tag{3}$$

has rank $n-1$, where $c_0 = 0$ and $c_{n-i} = c_i$ for $i = 1, \dots, \frac{n-1}{2}$.

Proof. We use the Walsh squaring method:

$$\begin{aligned} \hat{f}(\lambda)^2 &= \sum_{x,y} (-1)^{Tr(\lambda x)+f(x)} (-1)^{Tr(\lambda y)+f(y)} \\ &= \sum_{w,x} (-1)^{Tr(\lambda x)+f(x)+Tr(\lambda(x+w))+f(x+w)} \\ &\quad \text{(where } y = x+w) \\ &= \sum_{w} (-1)^{Tr(\lambda w)+f(w)} \sum_{x} (-1)^{\Phi(x,w)} \end{aligned}$$

where $\Phi(x,w) = f(w) + f(x) + f(x+w)$. We simplify Φ as follows:

$$\begin{aligned} \Phi(x,w) &= \sum_{i=1}^{\frac{n-1}{2}} c_i \left[Tr(x^{2^i+1}) + Tr(w^{2^i+1}) + Tr((x+w)^{2^i+1}) \right] \\ &= \sum_{i=1}^{\frac{n-1}{2}} c_i Tr(x^{2^i} w + w^{2^i} x) \\ &= \sum_{i=1}^{\frac{n-1}{2}} c_i Tr(x(w^{2^{n-i}} + w^{2^i})) \\ &= Tr(xL(w)) \end{aligned}$$

where

$$L(w) = \sum_{i=1}^{\frac{n-1}{2}} c_i (w^{2^i} + w^{2^{n-i}}). \tag{4}$$

Note that L is a linear function, and under a normal basis $\{\alpha, \alpha^2, \alpha^4, \dots, \alpha^{2^{n-1}}\}$ of $GF(2^n)$, the matrix representation of L is given by matrix (3). Also,

$$\sum_{x} (-1)^{\Phi(x,w)} = \sum_{x} (-1)^{Tr(xL(w))} = 2^n \tag{5}$$

if and only if $L(w) = 0$, otherwise the sum is 0. Therefore

$$\hat{f}(\lambda)^2 = 2^n \sum_{w \in ker(L)} (-1)^{Tr(\lambda w)+f(w)}. \tag{6}$$

Let $dim(ker(L)) = k$. By the definition of Φ, $Tr(\lambda w) + f(w)$ is a linear function on $ker(L)$. Therefore

$$\sum_{w \in ker(L)} (-1)^{Tr(\lambda w)+f(w)} = 2^k \text{ or } 0, \tag{7}$$

depending on whether the exponent is the zero function (2^{n-k} cases) or a non-zero linear function ($2^n - 2^{n-k}$ cases). That means that $\hat{f}$ is $0, \pm 2^{\frac{n+k}{2}}$ with frequency $2^n - 2^{n-k}, 2^{n-k}$ if and only if $dim(ker(L)) = k$. As a special case, f is Gold-like if and only if $dim(ker(L)) = 1$, i.e., $rank(L) = n - 1$.

Remark 1. The bilinear form $\Phi(x, w)$, defined in the above proof, corresponds to the symplectic form of $f(x)$ under the boolean representation. For results on quadratic boolean functions, see [6, Chapter 15].

Note that the rows of matrix (3) span a cyclic code C generated by the vector $(c_0, c_1, \ldots, c_{n-1})$. In the study of cyclic codes, it is useful to represent the vectors of C by polynomials modulo $x^n + 1$, where

$$C = span\{c(x), xc(x), \ldots, x^{n-1}c(x)\} \tag{8}$$

and $c(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i(x^i + x^{n-i})$. Then we have the following well-known useful facts about the cyclic code C (see [7]):

1. There exists a unique monic polynomial $g(x)$, called the generator polynomial, such that $g(x)|v(x)$ for all $v(x) \in C$.
2. $rank(L) = dim(C) = n - deg(g(x))$.
3. $g(x) = \gcd(c(x), x^n + 1)$.

Thus, if we can show that $g(x) = gcd(c(x), x^n + 1) = x + 1$, then we have proven that $rank(L) = dim(C) = n - 1$, the condition required in Lemma 1. We summarize our discussion in the following theorem:

Theorem 1. *For n odd, let $f(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i Tr(x^{2^i+1})$, $c_i \in \{0, 1\}$, $x \in GF(2^n)$. Then f is Gold-like if and only if $g(x) = x + 1$ where $g(x) = \gcd(c(x), x^n + 1)$ and $c(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i(x^i + x^{n-i})$.*

To demonstrate the application of Theorem 1, we can deduce that:

1. $f(x) = Tr(x^3 + x^5)$ is Gold-like over $GF(2^{155})$ because $\gcd(x + x^2 + x^{153} + x^{154}, x^{155} + 1) = x + 1$.
2. $f(x) = Tr(x^3 + x^{17})$ is not Gold-like over $GF(2^{155})$ because $\gcd(x + x^4 + x^{151} + x^{154}, x^{155} + 1) = x^5 + 1$.

The above computations can be done efficiently using the mathematical package MAPLE, while it would take a long time if we were to verify directly that $f(x)$ is Gold-like over a large field like $GF(2^{155})$.

Using Theorem 1, we give a short proof of two known results regarding Gold-like sequences. Let n be odd.

1. The function $f(x) = Tr(x^{2^i+1})$ is Gold-like if and only if $\gcd(i,n) = 1$[1]. This is because the generator polynomial $g(x) = \gcd(x^i + x^{n-i}, x^n + 1) = \gcd(x^{n-2i} + 1, x^n + 1) = x^{\gcd(n,n-2i)} + 1$. So $g(x) = x + 1$ if and only if $\gcd(n, i) = 1$.
2. The function $f(x) = \sum_{i=1}^{\frac{n-1}{2}} Tr(x^{2^i+1})$ is Gold-like[3]. This is because the associated cyclic code C is generated by the polynomial $c(x) = \sum_{i=1}^{n-1} x^i$ and $1+x = (xc(x) \bmod x^n+1)+c(x)$ is a vector in C. So $\gcd(c(x), x^n+1) = x+1$.

From Theorem 1, we see that it is useful to analyze the generator polynomial $g(x)$ of the associated cyclic code. Let us state a useful lemma regarding $g(x)$.

Lemma 2. *Let n be odd and $g(x)$ be the generator polynomial of the cyclic code C generated by $c(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i(x^i + x^{n-i})$. Then $g(x)$ has the form*

$$g(x) = (x+1)h(x) \text{ where } deg(h(x)) \text{ is even.} \tag{9}$$

Proof. If β is a root of $g(x) = \gcd(c(x), x^n + 1)$, then it is a root of both $x^n + 1$ and $c(x)$. $\beta^n = 1$ implies $(\beta^{-1})^i = \beta^{n-i}$ and thus $c(\beta^{-1}) = c(\beta) = 0$. Also, $(\beta^{-1})^n = (\beta^n)^{-1} = 1$. Therefore, β^{-1} is a root of $c(x)$ and $x^n + 1$, and thus of $g(x)$. So the roots of $g(x)$ come in pairs β, β^{-1}. If $\beta \neq 1$, then the assumption n odd and $\beta^n = 1$ imply $ord(\beta) \neq 2$ which means $\beta \neq \beta^{-1}$. Thus $\beta = 1$ gives the factor $x+1$, while the other pairs of roots give an even degree polynomial, $h(x)$.

4 Gold-like Functions for All Choices of Coefficients

For what n is $f(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i Tr(x^{2^i+1})$, $c_i \in \{0,1\}$, $x \in GF(2^n)$ Gold-like for all choices of coefficients? From the discussion following Theorem 1, we know that $Tr(x^{2^i+1})$ is not Gold-like when $\gcd(i,n) \neq 1$. So we have the following lemma.

Lemma 3. *Let n be odd. If $f(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i Tr(x^{2^i+1})$, $c_i \in \{0,1\}$, $x \in GF(2^n)$ is Gold-like for all choices of coefficients, then n is prime.*

By Lemma 3, we need only consider the case where n is prime. Since the generator polynomial $g(x)$ is closely related to the factorization of the polynomial $x^n + 1$, let us examine this factorization more clearly.

Lemma 4. *Let p be an odd prime. Over $\mathbf{Z}_2[x]$, the factorization of $x^p + 1$ into irreducible factors is of the form*

$$x^p + 1 = (x+1)h_1(x)h_2(x)\dots h_t(x) \tag{10}$$

where t is a divisor of $p-1$ and each $h_i(x)$ is a polynomial of degree $\frac{p-1}{t}$. There are $t+1$ irreducible factors, where $ord_p(2) = \frac{p-1}{t}$.

Proof. Let α be a primitive pth root of unity and let $H = \{2^s \bmod p\}$ be the subgroup of $\mathbf{Z}_p^*$ generated by 2. The irreducible factors of $x^p + 1$ are given by

$\prod_{i\in kH}(x-\alpha^i)$ where $k \in \mathbf{Z}_p$. Except for $k=0$, kH is a coset of H in $\mathbf{Z}_p^*$. Thus, except for $k=0$, which corresponds to the linear factor $x+1$, the degree of each nonlinear irreducible factor is $|kH| = |H| = ord_p(2)$, and the number of nonlinear factors is $t = \frac{p-1}{ord_p(2)}$.

If we want $f(x)$ to be Gold-like for all choices of coefficients, we might choose a prime p for which x^p+1 has as few irreducible factors as possible, for then it would be "harder" for $g(x) = \gcd(v(x), x^p+1)$ to contain any factor other than $x+1$. We look at the cases where x^p+1 has two and three factors in the following sections.

4.1 p is odd prime and $ord_p(2) = p-1$

This is the case where x^p+1 has two irreducible factors.

Theorem 2. *Let $f(x) = \sum_{i=1}^{\frac{p-1}{2}} c_i Tr(x^{2^i+1})$, $c_i \in \{0,1\}$, $x \in GF(2^p)$ where p is a prime such that $ord_p(2) = p-1$. Then f is Gold-like.*

Proof. By Lemma 4, x^p+1 has factorization

$$x^p+1 = (x+1)(1+x+x^2+\ldots+x^{p-1}). \tag{11}$$

Because the generator polynomial $g(x)$ divides x^p+1 properly, it must be $x+1$ or $1+x+\ldots+x^{p-1}$. By Lemma 2, $(x+1)|g(x)$, which implies $g(x)=x+1$, and hence we are done by Theorem 1.

In view of the above theorem, it is natural to ask about the existence and distribution of primes p for which $ord_p(2) = p-1$. The first ten such primes are as follows:

$$3, 5, 11, 13, 19, 29, 37, 53, 59, 61. \tag{12}$$

A conjecture of Artin states that there exists an infinite number of such primes; this conjecture was proven, assuming that the Riemann Hypothesis holds [5].

4.2 $p = 2s+1$ is prime, s is odd and $ord_p(2) = s$

This is the case where x^p+1 has three irreducible factors of odd degree.

Theorem 3. *Let $f(x) = \sum_{i=1}^{\frac{p-1}{2}} c_i Tr(x^{2^i+1})$, $c_i \in \{0,1\}$, $x \in GF(2^p)$ where $p = 2s+1$ is a prime such that s is odd and $ord_p(2) = s$. Then f is Gold-like.*

Proof. By Lemma 4, the factorization of x^p+1 is

$$x^p+1 = (x+1)h_1(x)h_2(x), \tag{13}$$

where $h_i(x)$ has degree s, $i=1,2$. The generator polynomial is a proper divisor of x^p+1 and has $x+1$ as a factor by Lemma 2. So $g(x) = x+1$ or $(x+1)h_i(x)$, $i=1,2$. But Lemma 2 says that $g(x)$ is a product of $x+1$ and an even degree polynomial. Therefore $g(x) = x+1$ and we are done by Theorem 1.

The first ten primes of the form of Theorem 3 are as follows:

$$7, 23, 47, 71, 79, 103, 167, 191, 199, 239, \tag{14}$$

and computer simulations suggest that there are an infinite number of such primes.

As a corollary of Theorems 2 and 3, we prove a similar statement for the Sophie Germain primes, $p = 2q + 1$, p, q prime.

Corollary 1. *Let* $f(x) = \sum_{i=1}^{\frac{p-1}{2}} c_i Tr(x^{2^i+1})$, $c_i \in \{0, 1\}$, $x \in GF(2^p)$ *where* $p = 2q + 1$, p, q *prime. Then* f *is Gold-like.*

Proof. If $ord_p(2) = p-1$, then we are done by Theorem 2. If not, then $ord_p(2)$ is a proper divisor of $p - 1 = 2q$, which implies $ord_p(2) = 2$ or q. But $ord_p(2) \neq 2$ because $p \geq 5$, so $ord_p(2) = q$, which is an odd prime, and we are done by Theorem 3.

The first ten Sophie-Germain primes are as follows:

$$5, 7, 11, 23, 47, 59, 83, 107, 167, 179. \tag{15}$$

As shown in the proof of Corollary 1, it can be verified that the Sophie Germain primes are primes of the form mentioned in Theorem 2 and 3. The Sophie Germain primes are well studied in number theory and it is conjectured that there are an infinite number of such primes.

What about primes which are not of the form considered in Theorems 2 and 3? We show that non Gold-like functions exists in these cases.

Theorem 4. *The only odd integers* n *for which* $f(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i Tr(x^{2^i+1})$, $c_i \in \{0, 1\}$, $x \in GF(2^n)$ *is Gold-like for all choices of coefficients are the primes mentioned in Theorems 2 and 3.*

Proof. Let p be a prime not of the form considered in Theorems 2 and 3, and let α be a primitive pth-root of unity. Form the polynomial $u(x)$ whose roots are $\alpha^i, i \in \{\pm 2^s \bmod p, s \in \mathbf{Z}\}$. Then $r := deg(u)$ is even because $\alpha^{-1} \neq \alpha$ is a root of $u(x)$ whenever α is a root.

$u(x)$ is symmetric of degree r, i.e., $u(x) = x^r u(1/x)$. This can be shown by the following computation: Let $a_1, a_2, \ldots, a_r$ be the roots of u. Then $1/a_1, \ldots, 1/a_r$ are also the roots of u. Thus

$$\begin{aligned}
(x + a_1) \ldots (x + a_r) &= \left(x + \frac{1}{a_1}\right) \ldots \left(x + \frac{1}{a_r}\right) \\
&= \frac{x^r}{a_1 a_2 \ldots a_r} \left(\frac{a_1 x + 1}{x}\right) \ldots \left(\frac{a_r x + 1}{x}\right) \\
&= x^r \left(a_1 + \frac{1}{x}\right) \ldots \left(a_r + \frac{1}{x}\right)
\end{aligned}$$

because $a_1 a_2 \ldots a_r = 1$. The top line of the above computation is $u(x)$ while the last line is $x^r u(1/x)$. We see that $(x+1)u(x)$ is symmetric of degree $r+1$ by a similar reason.

We claim that $(x+1)u(x)$ has degree less than p. Let $m_1(x)$ and C_1 be the minimal polynomial and cyclotomic coset of α respectively, and let $m_{-1}(x)$ and C_{-1} be the minimal polynomial and cyclotomic coset of α^{-1} respectively. We split the proof of our claim into two cases:

Case $C_1 = C_{-1}$. Then $u(x) = m_1(x) = m_{-1}(x)$, $deg(u) = |C_1| = ord_p(2) < p-1$ because p is not from Theorem 2.

Case $C_1 \neq C_{-1}$. Then C_1, C_{-1} are disjoint and $s := ord_p(2)$ cannot be even. This is because otherwise $2^s = 1$ means $2^{s/2} = -1$ and this implies C_1 contains -1. Thus s must be odd and $s < (p-1)/2$ because p is not from Theorem 3. We have $u(x) = m_1(x)m_{-1}(x)$ and $deg(m_1(x)) = deg(m_{-1}(x)) = s$ implies $deg(u(x)) = 2s < p-1$.

Then $c(x) = x^{(p-(r+1))/2}(x+1)u(x)$ is a polynomial of degree

$$\frac{p-(r+1)}{2} + 1 + r = \frac{p+r+1}{2} < p \tag{16}$$

because $1 + r = deg((x+1)u(x)) < p$. We also have

$$\begin{aligned} x^p c(1/x) &= x^{(p+r+1)/2}(1+1/x)u(1/x) \\ &= x^{(p+r+1)/2}x^{-(r+1)}(1+x)u(x) \\ &= c(x). \end{aligned}$$

Thus $c(x)$ is a symmetric polynomial of degree p and the corresponding function $f(x)$ over $GF(2^p)$ will not be Gold-like by Theorem 1, because $\gcd(c(x), x^p+1) = (x+1)u(x) \neq x+1$.

As an example, we look at the prime 17 which is not of the form considered in Theorem 2 and 3. Let β be a primitive element of the finite field $GF(2^8)$. Then $\alpha = \beta^{15}$ is a primitive 17th-root of unity because $255 = 15 \times 17$. It can be verified that $C_1 = C_{-1} = \{1, 2, \ldots, 2^7\}$, and

$$\begin{aligned} u(x) &= (x+\alpha)(x+\alpha^2)\ldots(x+\alpha^{2^7}) \\ &= x^8 + x^7 + x^6 + x^4 + x^2 + x + 1. \end{aligned}$$

Then, following the procedure in the proof of Theorem 4, we get

$$c(x) = x^{13} + x^{10} + x^9 + x^8 + x^7 + x^4 \tag{17}$$

where $\gcd(c(x), x^{17}+1) = (x+1)u(x)$. Thus $f(x) = Tr(x^{17} + x^{129} + x^{257})$, $x \in GF(2^{17})$, is not Gold-like.

5 Gold-like Functions with Two Trace Terms

From the discussion on single trace term functions following Theorem 1, we deduce the following lemma:

Lemma 5. *Let n be odd, $f(x) = Tr(x^{2^i+1})$, $x \in GF(2^n)$, is Gold-like for all $1 \leq i \leq (n-1)/2$ if and only if n is prime.*

Can we say something similar for f when it has two or more trace terms? The following theorem says that we can do so for functions with two trace terms.

Theorem 5. *Let n be odd. Then $f(x) = Tr(x^{2^i+1} + x^{2^j+1})$, $x \in GF(2^n)$ is Gold-like for all $1 \leq i < j \leq (n-1)/2$ if and only if n is prime.*

Proof. Suppose n is prime, say $n = p$. The corresponding cyclic code is generated by the polynomial $c(x) = x^i + x^j + x^{p-j} + x^{p-i}$. We will show that the only root of the generator polynomial $g(x) = \gcd(c(x), x^p + 1)$ is x=1. Any root of $g(x)$ is a root of $x^p + 1$, so let a root be α^s where α is a primitive pth-root of unity. We have

$$\alpha^{si} + \alpha^{sj} + \alpha^{s(p-j)} + \alpha^{s(p-i)} = 0. \tag{18}$$

Multiplying the equation by $\alpha^{s(i+j)}$ and applying the relation $\alpha^p = 1$, we have

$$(\alpha^{s(i+j)} + 1)(\alpha^{si} + \alpha^{sj}) = 0. \tag{19}$$

Suppose $s \neq 0$. Then α^s is also a primitive pth-root of unity. So $\alpha^{si} \neq \alpha^{sj}$ because $i \neq j$ and $0 < i, j < p$. Also, $0 < i, j \leq (p-1)/2$ implies $0 < i + j < p$, and then $\alpha^{s(i+j)} \neq 1$. We have a contradiction when $s \neq 0$ because equation (19) cannot be zero. Therefore, the only root of $g(x)$ is $x = 1$, i.e. $g(x) = x + 1$.

Conversely, suppose n is composite, say $n = st$, $s, t > 1$. Then the above function with $i = (s-1)/2$, $j = (s+1)/2$ is not Gold-like. This is because the generator polynomial $g(x)$ is

$$\begin{aligned}
&\gcd(x^{(s-1)/2} + x^{(s+1)/2} + x^{n-(s+1)/2} + x^{n-(s-1)/2}, x^n + 1) \\
&= \gcd(1 + x + x^{n-s} + x^{n-(s-1)}, x^n + 1) \\
&= \gcd((1 + x)(1 + x^{n-s}), x^n + 1) \\
&= \gcd((1 + x)(1 + x^{s(t-1)}), x^{st} + 1).
\end{aligned}$$

Then we can see that $x^s + 1$ divides g because it divides $x^{s(t-1)} + 1$ and $x^{st} + 1$. This means that $g(x) \neq x + 1$.

What about functions with more than two trace terms? We suggest the following generalization of Theorem 5 as an open problem:

Open Question 1. *For what odd integers n are all functions*

$$f(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i Tr(x^{2^i+1}), c_i \in \{0, 1\}, x \in GF(2^n) \tag{20}$$

with $3, 4, 5, \ldots$ trace terms Gold-like?

6 Conclusion

We constructed a new class of Gold-like sequences represented by functions having domain $GF(2^n)$, n odd. We also gave an efficient method to identify such functions over arbitrarily large fields.

Using the tools we developed, we identified those fields for which the function we defined is Gold-like for all choice of coefficients. It turned out the fields were of the form $GF(2^p)$ for certain primes p such that $x^p + 1$ has a simple factorization over $GF(2)$. There are conjectured to be an infinite number of such primes. Next we noticed that the function we defined with any single trace term is Gold-like if and only if the field is $GF(2^p)$, p prime. We investigated if this is true when f has two or more trace terms and found out that it is true for functions with two trace terms. We make the conjecture that this is not true when f has three or more trace terms.

In conclusion, we have found a new class of Gold-like sequences with useful applications in communications and cryptography. These functions are easily identified by an efficient polynomial gcd computation. We also characterize those finite fields for which these functions can be identified without any computation.

7 Acknowledgement

D.R. Stinson's research is supported by NSERC grants IRC #216431-96 and RGPIN #203114-98. G. Gong's research is supported by NSERC grants RGPIN #227700-00. K. Khoo's research is supported by a scholarship from DSO National Labs in Singapore.

References

1. R. Gold, "Maximal Recursive sequences with 3-valued cross correlation functions", *IEEE Trans. Inform. Theory*, vol. 14, pp. 154-156, 1968.
2. T. Helleseth, "Correlation of m-Sequences and Related Topics", In *Sequences and their Applications SETA 98*, pp. 49-66, 1999.
3. S. Boztas and P.V. Kumar, "Binary Sequences with Gold-Like Correlation but Larger Linear Span", *IEEE Trans. on Information Theory*, vol. 40 no. 2, pp.532-537, 1994.
4. T. Helleseth and P.V. Kumar, "Sequences with Low Correlation", In *Handbook of Coding Theory*, edited by V. Pless and C. Huffman, Elsevier Science Publishers, 1998.
5. Song Y. Yan, "Number Theory for Computing", Springer-Verlag, 2000.
6. F.J. MacWilliams and N.J.A. Sloane, "Theory of Error-Correcting Codes", North-Holland, Amsterdam, 1977.
7. D.G. Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger, J.R. Wall, "Coding Theory: The Essentials", Dekker, 1991.