Sequences with Low Cross Correlation

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. We find several classes of sequences that have low cross correlation with the m-sequence represented by $Tr(x)$. Firstly, we determine when a linear combination of Gold-terms is bent or Gold-like over $GF(p^n)$ by an efficient polynomial GCD computation. Using this GCD condition, we derive large classes of bent and Gold-like sequences over $GF(p^q)$, where q is prime. Secondly, we restrict ourselves to the binary case $p = 2$ and derive three large classes of Gold-like sequences which are certain sum of Gold terms. Thirdly, we generalise the construction of [13] to determine when a sum of cascaded GMW sequences is Gold-like. The proof is based on the theory of geometric sequence in [13] and our result on sum of binary Gold terms. These cascaded sequences also give rise to new non-quadratic almost optimal Boolean functions that have high nonlinearity and large linear span, suitable for cryptographic applications.

1 Introduction

In this paper, we find several classes of sequences that have low cross correlation with the m-sequence represented by $Tr(x)$. These sequences have useful applications in communications theory and cryptography. For example, they can be used to construct signal sets for deployment in CDMA systems [2, 4], or they can be converted to Boolean functions and S-boxes to be used in stream or block cipher systems [6, 16]. The sequences we will study are the bent and Gold-like sequences. The bent sequences achieve the lowest bound for cross correlation, while the Gold-like sequences have low cross correlation among sequences with odd length. For a survey of current literature, refer to [7, 8].

There are three main topics in this paper. Firstly, we determine when a linear combination of Gold terms over $GF(p^n)$ is bent or Gold-like by an efficient polynomial GCD computation. This is a p-ary generalisation of a recent result by Khoo, Gong and Stinson [11, 12] and can be derived using techniques from linear algebra and coding theory [15]. By analysing this polynomial GCD computation, we derive large classes of bent and Gold-like sequences over $GF(p^q)$ for primes $q \neq p$.

Secondly, we look at the case $p = 2$ more closely and derive three large classes of binary Gold-like sequences which can be obtained with minimal computation.

They consist of certain sum of Gold terms over $GF(2^p)$, p prime; the sum of Gold terms corresponding to an arithmetic progression; and the sum of all but one Gold-term. These sequences can be used for construction of generalised cascaded GMW sequences and non-quadratic almost optimal Boolean functions.

Thirdly, we generalise the cascaded GMW construction for sequences with low cross-correlation due to Klapper, Chan and Goresky [13]. We determine when a sum of cascaded GMW sequences is Gold-like. This is proven using the theory of geometric sequences in [13] and our result on sum of binary Gold terms. This also gives rise to a construction of new balanced non-quadratic almost optimal Boolean functions. These functions have high nonlinearity when the number of input bits is odd, which provides protection against linear approximation based attacks [14, 19]; and they have large linear span, which provides protection against interpolation attacks [10]. The balance and resiliency properties of our functions are shown to be better than general almost optimal Boolean functions, and the highly nonlinear Patterson-Wiedemann functions, for $n \geq 15$ [17, 18].

In Section 2, we give some definitions and preliminaries on sequences and Boolean functions. In Section 3, we analyse when a sum of Gold-terms is bent or Gold-like over $GF(p^n)$ and derive large classes of bent and Gold-like sequences over $GF(p^q)$, where $q \neq p$ is prime. In Section 4, we derive three large classes of binary Gold-like functions based on certain sum of Gold terms. In Section 5, we determine when a sum of cascaded GMW sequences is Gold-like, and use these sequences to construct new non-quadratic almost optimal Boolean functions with large linear span.

2 Definitions and Preliminaries

2.1 Sequences and Polynomial Representations

Let $GF(p^n)$ be the finite field with p^n elements, where p is prime, and let α be a primitive element in the field. We define the trace function on $GF(p^n)$ to be $Tr(x) = \sum_{i=0}^{n-1} x^{p^i}$. The trace function is linear over $GF(p)$.

Let $f : GF(p^n) \to GF(p)$. We say that $f(x)$ is the *trace representation* of the p-ary sequence $\underline{a} = \{a_i\}_{i=0}^{p^n-1}$ if $a_i = f(\alpha^i)$ for all i. In this paper, we will express all sequences in trace representation form as it makes analysis more convenient.

An m-sequence is a sequence whose trace representation is given by $Tr(x^r)$, $1 \leq r \leq p^n - 2$. Let $\underline{m}$ be the m-sequence represented by $Tr(x)$ and let $\omega = e^{2\pi i/p}$ be a complex pth root of unity. The *cross correlation* of a p-ary sequence $\underline{a} = \{a_i\}_{i=0}^{p^n-1}$ with $\underline{m}$ is

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

The *Hadamard Transform* of a polynomial function $f : GF(p^n) \to GF(p)$ is defined by

$$\hat{f}(\lambda) = \sum_{x \in GF(p^n)} \omega^{Tr(\lambda x) - f(x)}.$$

$\hat{f}$ maps $GF(p^n)$ to $\mathbf{Z}[\omega]$. Thus $\hat{f}(\lambda) = 1 + C_{\underline{a},\underline{m}}(\tau)$, where $\lambda = \alpha^\tau$ and $\underline{a}$ has trace representation $f(x)$. We make the following definition.

Definition 1. *Let $n \not\equiv 0 \mod p$. We say that $f : GF(p^n) \to GF(p)$ is* bent *if $|\hat{f}(\lambda)|$ takes on only the value $p^{n/2}$. We say it is* Gold-like *if $|\hat{f}(\lambda)|$ takes on only the values $0, p^{(n+1)/2}$. We will call the sequences they represent* bent *and* Gold-like *sequences respectively.*

When $p = 2$ and n is odd, f cannot be bent, but it can be Gold-like. The low cross correlation properties of bent and Gold-like sequences have useful applications in communications and cryptography. In [11, 12], we proved the following Theorem on binary Gold-like functions.

Theorem 1. *(Khoo, Gong and Stinson [11, 12]) For n odd, let*

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

Then f is Gold-like if and only if $g(x) = x + 1$ where $g(x) = \gcd(c(x), x^n + 1)$ $\mod 2$ and $c(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i(x^i + x^{n-i})$.

2.2 Boolean Functions

A Boolean function is a function $g : (GF(2))^n \to GF(2)$. There is a natural correspondence between Boolean functions g and polynomial functions $f : GF(2^n) \to GF(2)$. Let $\{\alpha_0, \ldots, \alpha_{n-1}\}$ be a basis for $GF(2^n)$. This correspondence is given by $g(x_0, \ldots, x_{n-1}) = f(\alpha_0 x_0 + \ldots + \alpha_{n-1} x_{n-1})$.

The Hadamard Transform of a Boolean function $f : (GF(2))^n \to GF(2)$ is

$$\hat{f}(w) = \sum_{x \in GF(2)^n} (-1)^{w.x + f(x)}.$$

This is equivalent to the definition for the corresponding polynomial function over $GF(2^n)$, because the Boolean form of $Tr(\lambda x), \lambda \in GF(2^n)$ is $w \cdot x, w \in GF(2)^n$ [15].

The *nonlinearity* of a Boolean function f is defined by

$$N_f = \min\{d(f,a),\ a \text{ an affine function}\}.$$

where $d(f,a)$ is the number of x for which $f(x) \neq a(x)$. We want the nonlinearity of a function to be as high as possible, for protection against linear approximation. When n is odd, functions with $N_f = 2^{n-1} - 2^{(n-1)/2}$ are considered to have high nonlinearity. Functions with such nonlinearity are called *almost optimal* [3].

The following identity, which relates the Hadamard Transform and nonlinearity of $f : (GF(2))^n \to GF(2)$, can be proven easily:

$$N_f = 2^{n-1} - max_w |\hat{f}(w)|/2. \tag{2}$$

We can deduce from this identity that Gold-like functions correspond to almost optimal Boolean functions.

A polynomial function $f : GF(2^n) \to GF(2)$ such that $f(x) = f(x^2)$ is called a *cyclic invariant function*. These functions are basic to our construction for cascaded Gold-like functions in Section 5.

The *linear span* of a polynomial function $f(x) = \sum_i x^{s_i}$ is the number of monomials x^{s_i} in its polynomial representation. We want it to be high to defend against interpolation attacks [10]. The *algebraic degree* $deg(f)$ of the corresponding Boolean function is given by the maximum weight of the exponents $\max_i wt(s_i)$ (see [15]). We want it to be high so that algebraic analysis is complex.

3 *p*-ary Bent and Gold-like Functions

Theorem 1 characterizes when a linear combination of binary Gold terms is Gold-like. We generalize it to the p-ary case where we not only get Gold-like, but also bent, functions.

Lemma 1. *Let p be prime, let n be an odd integer which is not divisible by p and let*

$$f(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i Tr(x^{p^i+1}), \text{ where } c_i \in GF(p), x \in GF(p^n).$$

Then f is bent or Gold-like if and only if the cyclic matrix

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

has rank n or $n-1$ respectively modulo p, where we define $c_0 = 0$ and $c_{n-i} = c_i$ for $i = 1, \dots, \frac{n-1}{2}$.

Proof. By the Welch Squaring Formula, we can express $|\hat{f}(\lambda)|^2$ as follows:

$$\begin{aligned} |\hat{f}(\lambda)|^2 &= \sum_{x,y} \omega^{Tr(\lambda x) - f(x)} \omega^{f(y) - Tr(\lambda y)} \\ &= \sum_{x,z} \omega^{Tr(\lambda x) - f(x) + f(x+z) - Tr(\lambda(x+z))}, y = x + z \\ &= \sum_z \omega^{f(z) - Tr(\lambda z)} \sum_x \omega^{\Phi(x,z)} \end{aligned}$$

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

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

where $L(z) = \sum_{i=1}^{(n-1)/2} c_i (z^{p^i} + z^{p^{n-i}})$. Note that L is a linear function, and under a normal basis $\{\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}\}$ of $GF(p^n)$, the matrix representation of L is given by Equation (3). Also,

$$\sum_x \omega^{\Phi(x,z)} = \sum_x \omega^{Tr(xL(z))} = p^n$$

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

$$|\hat{f}(\lambda)|^2 = p^n \sum_{z \in ker(L)} \omega^{Tr(\lambda z) - f(z)}.$$

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

$$\sum_{z \in ker(L)} \omega^{Tr(\lambda z) - f(z)} = p^k \text{ or } 0,$$

depending on whether the exponent is the zero function or a non-zero linear function. This means that $|\hat{f}(\lambda)|$ is $0, p^{\frac{n+k}{2}}$ for all λ if and only if $dim(ker(L)) = k, k \geq 1$. $|\hat{f}(\lambda)| = p^{n/2}$ for all λ when $ker(L) = \{0\}$. As a special case, f is bent or Gold-like if and only if $dim(ker(L)) = 0$ or 1, i.e., when $rank(L) = n$ or $n-1$.

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 $(GF(p))^n$. In the study of cyclic codes, it is useful to represent the vectors of C by polynomials modulo $x^n - 1 \in \mathbf{Z}_p[x]$, where

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

and $c(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i(x^i + x^{n-i})$. Then we have the following well-known facts about the cyclic code C (see [15]):

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. $g(x) = \gcd(c(x), x^n - 1) \mod p$.

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

Theorem 2. *Let p be a prime, let n be an odd integer not divisible by p, and let*

$$f(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i Tr(x^{p^i+1}), \quad where\ c_i \in GF(p), \in GF(p^n).$$

Then f is bent or Gold-like if and only if $g(x) = 1$ or $x - 1$ respectively, where $g(x) = \gcd(c(x), x^n - 1) \mod p$ and $c(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i(x^i + x^{n-i})$.

We see that Theorem 1 is a special case of Theorem 2. Moreover, Theorem 2 can be used to give a short proof of some known results. We state them in the following proposition

Proposition 1. *1. Let p be an odd prime and let n be an odd integer not divisible by p. Then $Tr(x^{p^i+1})$, $x \in GF(p^n)$, is bent.*
2. Let n be odd and $f(x) = Tr(x^{2^i+1})$, $x \in GF(2^n)$. Then f is Gold-like if and only if $\gcd(i, n) = 1$.
3. Let n be odd. Then $f(x) = \sum_{i=1}^{(n-1)/2} Tr(x^{2^i+1})$, $x \in GF(2^n)$, is Gold-like.

Proof. 1. The corresponding polynomial $c(x)$ is $x^i(1 + x^{n-2i})$ and

$$\gcd(c(x), x^n - 1) = \gcd(x^{n-2i} + 1, x^n - 1) = 1$$

because if p is odd, $\gcd(x^k + 1, x^n - 1) \mod p = 1$ for all k whenever n is odd. Therefore $f(x)$ is bent by Theorem 2.
2. This is similar to the previous case but we are considering $\gcd(c(x), x^n + 1) = \gcd(x^{n-2i} + 1, x^n + 1)$ now. f is Gold-like when this GCD is $x + 1$, i.e. $\gcd(n - 2i, n) = \gcd(i, n) = 1$.
3. The corresponding polynomial $c(x)$ is $x + x^2 + \ldots + x^{n-1}$ and $1 + x = (xc(x) \bmod x^n + 1) + c(x)$. Therefore $\gcd(c(x), x^n + 1) = x + 1$ and f is Gold-like by Theorem 2.

Based on Theorem 2, we can characterise large classes of bent and Gold-like functions over $GF(p^q)$ when $q \neq p$ is a prime. Before proceeding with our analysis, we need a lemma on the factorization of cyclotomic polynomials. We denote the order of p modulo q by $ord_q(p)$.

Lemma 2. *Let p, q be primes such that $p \neq q$. Over $\boldsymbol{Z}_p[x]$, the factorization of $x^q - 1$ into irreducible factors is of the form*

$$x^q - 1 = (x - 1)h_1(x)h_2(x)\ldots h_t(x)$$

where each $h_i(x)$ is a polynomial of degree $ord_q(p)$.

Proof. Let α be a primitive q-th root of unity in some extension field of characteristic p and let $H = \{p^s \mod q, s \in \mathbf{Z}\}$ be the subgroup of $\mathbf{Z}_q^*$ generated by p. The irreducible factors of $x^q - 1$ are given by $\prod_{i \in kH}(x - \alpha^i)$ where $k \in \mathbf{Z}_q$. Except for $k = 0$, kH is a coset of H in $\mathbf{Z}_q^*$. Thus, except for $k = 0$, which corresponds to the linear factor $x - 1$, the degree of each nonlinear irreducible factor is $|kH| = |H| = ord_q(p)$.

Now we can analyse the correlation properties of linear combinations of Gold terms over $GF(p^q)$, $q \neq p$ is prime. We call a polynomial $u(x)$ r-symmetric if

$$u(x) = x^r u(1/x).$$

The polynomial $c(x)$ which corresponds to the function $f(x) = \sum_{i=1}^{\frac{q-1}{2}} c_i Tr(x^{p^i+1})$ is a q-symmetric polynomial that has degree $\leq q - 1$.

Theorem 3. *Let p be a prime, let $q \neq p$ be an odd prime and let*

$$f(x) = \sum_{i=k}^{\frac{q-1}{2}} c_i Tr(x^{p^i+1}), \text{ where } c_i \in GF(p), x \in GF(p^q).$$

Then f is bent or Gold-like for all choices of coefficients c_i if and only if

1. $k \geq \frac{q - ord_q(p)+1}{2}$ *when $ord_q(p)$ is even, or*
2. $k \geq \frac{q-2ord_q(p)+1}{2}$ *when $ord_q(p)$ is odd.*

f is bent when $2\sum_{i=k}^{(n-1)/2} c_i \not\equiv 0 \mod p$, and f is Gold-like when $2\sum_{i=k}^{(n-1)/2} c_i \equiv 0 \mod p$.

Proof. We will apply Theorem 2. Suppose the above conditions are satisfied. The polynomial $c(x)$ corresponding to $f(x)$ has the form

$$\begin{aligned} c(x) &= x^k + x^l + \ldots + x^{q-l} + x^{q-k} \\ &= x^k d(x) \text{ where } d(x) \text{ has degree } q - 2k \end{aligned}$$

Consider the case when $ord_q(p)$ is even. $k \geq \frac{q-ord_q(p)+1}{2}$ means that

$$deg(d(x)) = q - 2k \leq ord_q(p) - 1.$$

But Lemma 2 says that all the factors of $x^q - 1$ not equal to $x - 1$ have degree at least $ord_q(p)$. So $\gcd(d(x), x^q - 1) = 1$ or $x - 1$.

When $ord_q(p)$ is odd, we have that

$$deg(d(x)) = q - 2k \leq 2ord_p(2) - 1.$$

Any common factor of $d(x)$ and $x^q - 1$ (not equal to $x - 1$) must have even degree. This is because if $\alpha \neq 0, 1$ is a root of

$$g(x) = \gcd(c(x), x^q - 1),$$

then $\alpha^{-1} \neq \alpha$ is also a root of $g(x)$, since $c(x)$ and $x^q - 1$ are both q-symmetric polynomials. Together with Lemma 2, this means that degree of any common factor of $d(x)$ and $x^q - 1$ (not equal to $x - 1$) has degree at least $2ord_q(p)$. Therefore, $\gcd(d(x), x^q - 1) = 1$ or $x - 1$ and f is bent or Gold-like by Theorem 2.

Next, we prove the converse by constructing a function $f(x)$ of degree k, where

$$k = \begin{cases} (q - ord_q(p))/2 & \text{when } ord_q(p) \text{ even}, \\ (q - 2ord_q(p))/2 & \text{when } ord_q(p) \text{ odd}, \end{cases}$$

which is not bent or Gold-like. Form the polynomial $u(x)$ whose roots are $\alpha^i, i \in \{\pm p^s \bmod q, s \in \mathbf{Z}\}$. Let the roots of $u(x)$ be $a_1, \ldots, a_r$. Then $u(x)$ is r-symmetric by the following computation.

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

because $a_1 a_2 \ldots a_r = 1$. We can reverse the order of subtraction in each linear factor because r is even. The top line of the above computation is $u(x)$ while the last line is $x^r u(1/x)$.

The algebraic degree r satisfies

$$r = \begin{cases} ord_q(p) \text{ when } ord_q(p) \text{ even}, \\ 2ord_q(p) \text{ when } ord_q(p) \text{ odd}. \end{cases}$$

This is because $\{\alpha^s \bmod q, s \in \mathbf{Z}\} = \{\alpha^{-s} \bmod q, s \in \mathbf{Z}\}$ if $-1 \in \{\alpha^s \bmod q, s \in \mathbf{Z}\}$, which happens only when $ord_q(p)$ is even. In a similar way, the two sets $\{\alpha^s \bmod q, s \in \mathbf{Z}\}$ and $\{\alpha^{-s} \bmod q, s \in \mathbf{Z}\}$ are disjoint when $ord_q(p)$ is odd.

The polynomial defined by

$$c(x) = x^{(q-r)/2} u(x)$$

can be seen to satisfy $c(x) = x^q c(1/x)$, i.e. it is q-symmetric and it corresponds to a sum of Gold terms starting from index $\frac{q-r}{2}$. This particular linear combination is not bent or Gold-like because $\gcd(c(x), x^q - 1) = u(x) \neq 1, x - 1$. Therefore, all linear combinations of Gold terms are bent or Gold-like only when we sum from index $(q - r + 1)/2$, which is the condition of our theorem.

If we only have bent or Gold-like functions, we can differentiate between them by seeing if $c(1) \neq 0$ (which implies $g(x) = 1$), or $c(1) = 0$ (which implies $g(x) = x - 1$).

As a corollary, we can deduce, for certain odd primes q, that all linear combinations of Gold terms are bent or Gold-like.

Corollary 1. *Let p, q be primes such that $p \neq q$ and let*

$$f(x) = \sum_{i=1}^{\frac{q-1}{2}} c_i Tr(x^{p^i+1}), \text{ where } c_i \in GF(p), x \in GF(p^q).$$

Then f is Bent or Gold-like for all choices of coefficients c_i if and only if

1. *$ord_q(p) = q - 1$ or*
2. *$ord_q(p) = (q-1)/2$ is an odd number.*

We can differentiate between the resulting bent and Gold-like functions as in Theorem 3.

Proof. We can apply Theorem 3 and see that $\sum_{i=k}^{\frac{n-1}{2}} c_i Tr(x^{p^i+1})$ is bent or Gold-like for all choices of coefficients c_i iff $k \geq 1$ when one of the two conditions in this corollary is satisfied. For other values of $ord_q(p)$, the lower bound for k is larger than 1.

Example: Let $p = 3$ and let $q \neq 3$ be an odd prime. By Corollary 1, the function $\sum_{i=1}^{\frac{q-1}{2}} c_i Tr(x^{3^i+1})$, $c_i \in GF(3)$, $x \in GF(3^q)$, is bent or Gold-like for all choices of coefficients if and only if q is in the list

$$5, 7, 11, 17, 19, 23, 29, 43, 47, 53, 59, 71, \ldots \tag{4}$$

It can be proven that there are an infinite number of such primes if the Riemann Hypothesis holds [20]. f is bent when $2\sum_{i=1}^{(q-1)/2} c_i \not\equiv 0 \mod 3$, and f is Gold-like when $2\sum_{i=1}^{(q-1)/2} c_i \equiv 0 \mod 3$.

4 Characterisation of Binary Gold-like Functions

In this section, we will restrict ourselves to the binary case. We present three classes of Gold-like functions based on the sum of Gold terms. Unlike Theorem 1, where we have to perform a polynomial GCD computation for each function, we can get large number of Gold-like functions with minimal computation. Firstly, we present the binary case of Theorem 3.

Theorem 4. *Let p be an odd prime and*

$$f(x) = \sum_{i=k}^{\frac{p-1}{2}} c_i Tr(x^{2^i+1}), \text{ where } c_i \in \{0, 1\}, x \in GF(2^p).$$

Then f is Gold-like for all choices of coefficients if and only if

1. *$k \geq \frac{p - ord_p(2) + 1}{2}$ when $ord_p(2)$ is even,*
2. *$k \geq \frac{p - 2ord_p(2) + 1}{2}$ when $ord_p(2)$ is odd.*

Proof. The proof is identical to the characteristic p case except that we can always factor $x+1$ from $c(x)$. Therefore we can only get Gold-like functions now, because $x+1$ always divides $\gcd(c(x), x^n+1)$.

Example: Let $p=7$ in Theorem 4. $ord_7(2)=3$ is odd, thus $k \geq (7-2\times 3+1)/2=1$. So $f(x)$ is Gold-like for all possible choices of coefficients c_i:

$$\begin{aligned} f(x) = Tr(x^3),\ &Tr(x^5),\ Tr(x^9), \\ &Tr(x^3+x^5),\ Tr(x^3+x^9),\ Tr(x^5+x^9), \\ &\text{or } Tr(x^3+x^5+x^9). \end{aligned}$$

Next, we characterize Gold-like functions whose trace representation is a sum of Gold terms corresponding to an arithmetic progression. These contain Gold-like functions which are a sum of two Gold terms as a special case.

Theorem 5. *Let n be odd. Then*

1. $f(x) = Tr(x^{2^i+1} + x^{2^j+1})$, $x \in GF(2^n)$ *is Gold-like if and only if* $\gcd(i+j, n) = 1 = \gcd(i-j, n)$.
2. *Consider the function*

$$f(x) = Tr(x^{2^a+1} + x^{2^{a+d}+1} + \ldots + x^{2^{a+(r-1)d}+1} + x^{2^{a+rd}+1})$$

over $GF(2^n)$, n odd, where

$$begin := a, a+d, \ldots, a+(r-1)d, end := a+rd$$

forms an arithmetic progression with common difference d. Then f is Gold-like if $\gcd(begin+end, n)=1=\gcd(end-begin+d, n)$. *Moreover, the converse is true if* $\gcd(d,n)=1$.

Proof. We analyse the two cases by applying Theorem 1.

1. Without loss of generality, assume $i>j$. The corresponding polynomial $c(x)$ is

$$\begin{aligned} c(x) &= x^i + x^j + x^{n-j} + x^{n-i} \\ &= (x^i + x^j)(1 + x^{n-(i+j)}) \\ &= x^j(1+x^{i-j})(1+x^{n-(i+j)}) \end{aligned}$$

Thus $\gcd(c(x), x^n+1) = x+1$ if and only if

$$\gcd(i-j) = 1 = \gcd(i+j)$$

2. The corresponding polynomial $c(x)$ is

$$\begin{aligned} c(x) &= x^a + \ldots + x^{a+rd} + x^{n-a-rd} + \ldots + x^{n-a} \\ &= (1 + x^{n-(2a+rd)})(x^a + \ldots + x^{a+rd}) \\ &= (1 + x^{n-(2a+rd)})x^a \left(\frac{1+x^{(r+1)d}}{1+x^d}\right) \end{aligned}$$

The gcd of the numerator with $x^n + 1$ is $x + 1$ if

$$\gcd(2a + rd, n) = 1 = \gcd((r + 1)d, n).$$

Moreover, we see that the converse is true if

$$\gcd(1 + x^d, 1 + x^n) = 1 + x, \text{ i.e. } \gcd(d, n) = 1.$$

When $n = p$ is prime in Theorem 5, all functions corresponding to arithmetic progressions are Gold-like. Therefore, we have a large number of Gold-like functions without any computation required to verify that they are Gold-like. Using Theorem 5, we show in the following corollary a way to construct infinitely many functions which are Gold-like for all odd n.

Corollary 2. *Let $f(x)$ be a function of the form in Theorem 5 part 2, where*

$$begin = 2^i - 2^j + r, end = 2^i + 2^j - r, d = 2r.$$

Then f is Gold-like on $GF(2^n)$ for all odd n.

Proof. We have that

$$\begin{aligned} begin + end &= 2^{i+1} \\ end - begin + d &= 2^{j+1} \end{aligned}$$

The above two quantities are always coprime to any odd n and thus f is Gold-like by Theorem 5.

For example, the following functions are Gold-like on $GF(2^n)$ for all odd n by Corollary 2.

$$Tr(x^3 + x^9), Tr(x^9 + x^{33}), Tr(x^5 + x^{65}), Tr(x^3 + x^9 + x^{33} + x^{127}).$$

Next, we present a result on Gold-like functions with all but one trace term. The result states that for two-third of all integers n, the sum of all but one Gold term is always Gold-like on $GF(2^n)$.

Theorem 6. *Consider the function*

$$f(x) = Tr(x^3 + \ldots + x^{2^{i-1}+1} + x^{2^{i+1}+1} + \ldots + x^{2^{(n-1)/2}+1})$$

on $GF(2^n)$, n odd, i.e., f consists of all but one trace term. Then

1. *If 3 does not divide n, f is always Gold-like.*
2. *If $n = 3^k$ for some k, f is never Gold-like.*
3. *If $n = 3^k m$, $m > 1$ and 3 does not divide m, f is Gold-like if and only if i is a multiple of 3^k.*

Proof. We analyse the corresponding polynomial $c(x)$:

$$c(x) = x + \ldots + x^{i-1} + x^{i+1} + \ldots + x^{n-(i+1)} + x^{n-(i-1)} + \ldots + x^{n-1}$$

The relation between $x^n + 1$ and $c(x)$ is

$$\begin{aligned} x^n + 1 &= (x+1)(1 + x + \ldots + x^{n-1}) \\ &= (x+1)(c(x) + 1 + x^i + x^{n-i}) \end{aligned}$$

Thus we have

$$x^n + 1 + (x+1)c(x) = (x+1)(1 + x^i + x^{n-i})$$

which enables us to simplify $g(x) := \gcd(c(x), x^n + 1)$ as

$$\begin{aligned} g(x) &= \gcd(c(x), (x+1)(1 + x^i + x^{n-i})) \\ &= (x+1)\gcd(c(x), 1 + x^i + x^{n-i}) \end{aligned}$$

The last equality is true because $c(1) = 0$ and $1 + 1^i + 1^{n-i} \neq 0$. By Theorem 1, we deduce that f is not Gold-like if and only if

$$\begin{aligned} g(x) \neq x + 1 \ &\text{iff there exists } a \neq 1 \text{ s.t. } g(a) = 0 \\ &\text{iff } 1 + a^i + a^{n-i} = 0 \text{ and } c(a) = 0 \\ &\text{iff } 1 + a^i + a^{n-i} = 0 \text{ and } a^n = 1 \\ &\text{iff } a^i + a^{2i} + 1 = 0 \text{ and } a^n = 1 \\ &\text{iff } a^{3i} = 1,\ a^i \neq 1 \text{ and } a^n = 1. \end{aligned}$$

Using this condition, we prove parts 1,2 and 3.

1. 3 does not divide n. Suppose there exists an i for which f is not Gold-like. This means that $g(x)$ has a root $a \neq 1$. By the conditions we derived, a satisfies $a^i \neq 1$ and $a^{3i} = 1$, which implies $ord(a) = 3$ or $3i$. Therefore 3 divides $ord(a)$ and $a^n = 1$ implies $ord(a)$ divides n which means that $3|n$. However, this is a contradiction to the hypothesis that 3 does not divide n.
2. $n = 3^s$. Since n is odd, there exists a primitive nth root of 1, say w (see [9]). We can write i as $i = 3^r d$, where $r < k$ and 3 does not divide d. Let $a = w^{3^{k-r-1}}$, then

   $$a^{3i} = w^{3^k d} = 1,\ a^i = w^{3^{k-1} d} \neq 1 \text{ and } a^n = 1.$$

   Thus f is never Gold-like.
3. $n = 3^k m$, 3 does not divide m. Let $i = 3^k d$, where 3 does not divide d and suppose f is not Gold-like, i.e. there exists an a such that

   $$a^{3i} = 1,\ a^i \neq 1 \text{ and } a^n = 1.$$

   $a^n = 1$ implies $ord(a)|3^k m$ and 3 does not divide m. So the maximum exponent of 3 in $ord(a)$ is 3^k. Now we have

   $$a^{3i} = 1 \implies a^{3^{k+1} d} = 1 \implies a^{3^k d} = 1 \implies a^i = 1,$$

a contradiction! Thus, f is Gold-like for $i = 3^k d$.
Let $i = 3^r d$, where $r < k$ and 3 does not divide d. Since n is odd, there exists a primitive nth root of 1, say w (see [9]). Let $a = w^{3^{k-r-1}m}$; then we can verify that

$$a^{3i} = 1,\ a^i \neq 1 \text{ and } a^n = 1.$$

as we have done in part (b) to show that f is not Gold-like.

5 A New Class of Cascaded GMW Sequences and Almost Optimal Boolean Functions

In this section, we generalise the construction for cascaded GMW sequences in [13]. We determine when a linear combination of cascaded GMW sequences is Gold-like. This lead to a construction for new classes of non-quadratic almost optimal Boolean functions with large linear span. We need to define the subfield trace functions for our next few constructions. Let $q = 2^n$. The subfield trace function from $GF(q^m)$ to $GF(q)$ is defined by

$$Tr_q^{q^m}(x) = \sum_{i=0}^{m-1} x^{q^i}.$$

Our starting point is Lemma 3 from [13], on geometric sequences. Let $I(f) = \sum_x (-1)^{f(x)}$ be the imbalance of f and let the correlation between polynomial functions f and g be defined as

$$C_{f,g}(\lambda) = \sum_{x \in GF(2^n)} (-1)^{f(\lambda x)+g(x)}.$$

Lemma 3 was stated in the language of sequences, but we state it in the language of polynomial functions.

Lemma 3. *(Klapper, Chan and Goresky [13]) Let $q = 2^n$, and let $g, h : GF(q) \to GF(2)$. The correlation between the pair of functions*

$$g(Tr_q^{q^m}(x)) \text{ and } h(Tr_q^{q^m}(x^{q^i+1}))$$

at $\lambda \neq 0$ takes on the values:

1. $q^{m-2} I(g) I(h)$ *and*
2. $(q^{m-2} - q^{m-(m-d)/2-2}) I(g) I(h) \pm q^{m-(m-d)/2-1} C_{g(x),h(x^2)}(\lambda)$,

where $d = \gcd(i, m)$.

Based on Lemma 3, we have an inductive construction for families of cascaded Gold-like functions with large linear span, starting from certain Gold-like functions f. We present this in our next Theorem.

Theorem 7. *Let $q = 2^n$ and let n, n_j be odd for $j = 1 \ldots l$. Further, let $f : GF(q) \to GF(2)$ be cyclic invariant, i.e. $f(x^2) = f(x)$. Define recursively the functions f_i as follows:*

$$\begin{aligned} f_0(x) &= f(x) \\ f_j(x) &= f_{j-1}(Tr^{q_j}_{q_{j-1}}(x^{k_j})), j = 1, \ldots, l, \end{aligned}$$

where $q_0 = q$, $q_j = q_{j-1}^{n_j}$, $k_j = q_{j-1}^{r_j} + 1$ and $\gcd(r_j, n_j) = 1$. Then $f_l : GF(q_l) \to GF(2)$ is a balanced Gold-like function if and only if f is a balanced Gold-like function.

Proof. Let f be a balanced Gold-like function. We prove that f_j is balanced, Gold-like and cyclic invariant for all $j = 1, \ldots, l$. We proceed by induction on j. To prove the base case, $j = 1$, we apply Theorem 3, letting $g(x) = Tr^q_2(x)$ and $h(x) = f(x)$ in

$$g(Tr^{q^{n_1}}_q(x)) \text{ and } h(Tr^{q^{n_1}}_q(x^{q^{r_1}+1})) = f_1(x). \tag{5}$$

Note that $I(g) = I(Tr^q_2) = 0$, $\hat{f}(\lambda) = 0, \pm 2^{(n+1)/2}$ and

$$C_{g(x),h(x^2)}(\lambda) = C_{Tr^q_2(x),f(x^2)}(\lambda) = \hat{f}(\lambda),$$

because $f(x) = f(x^2)$. The Hadamard Transform $\widehat{f_1}(\lambda)$ at $\lambda \neq 0$ is the correlation between the pair of functions in Equation (5). By Theorem 3, this takes on the values 0 and

$$\pm q^{n_1-(n_1-1)/2-1} 2^{(n+1)/2} = \pm (2^n)^{(n_1-1)/2} 2^{(n+1)/2} = \pm 2^{(nn_1+1)/2}.$$

Furthermore, f_1 is balanced because it is a composition of a balanced function f. The subfield trace function and a permutation x^{k_1} over $GF(q_1)$. So $\widehat{f_1}(0) = 0$ and $f_1(x)$ is Gold-like. The fact that f is cyclic invariant implies that

$$f_1(x^2) = f(Tr^{q^{n_1}}_q((x^2)^{k_1})) = f(Tr^{q^{n_1}}_q(x^{k_1})^2) = f(Tr^{q^{n_1}}_q(x^{k_1})) = f_1(x).$$

Therefore f_1 is cyclic invariant.

Suppose that case $j-1$ is true, i.e., f_{j-1} is balanced, Gold-like and cyclic invariant. We can apply Theorem 3 by letting $g(x) = Tr^{q_{j-1}}_2(x)$ and $h(x) = f_{j-1}(x)$ in

$$g(Tr^{q_j}_{q_{j-1}}(x)) \text{ and } h(Tr^{q_j}_{q_{j-1}}(x^{q^{r_j}_{j-1}+1})) = f_j(x).$$

We see that $I(g) = I(Tr^{q_{j-1}}_2) = 0$ and

$$C_{g(x),h(x^2)}(\lambda) = C_{Tr^{q_{j-1}}_2(x),f_{j-1}(x^2)}(\lambda) = \hat{f}_{j-1}(x) = 0, \pm 2^{(nn_1\ldots n_{j-1}+1)/2},$$

because f_{j-1} is cyclic invariant and Gold-like. By Theorem 3, the Hadamard transform $\widehat{f_j}(\lambda)$ at $\lambda \neq 0$ takes on the values 0 and

$$\pm q_{j-1}^{n_j-(n_j-1)/2-1} 2^{(nn_1\ldots n_{j-1}+1)/2} = \pm 2^{(nn_1\ldots n_j+1)/2}.$$

Furthermore, f_j is balanced because it is a composition of a balanced function f_{j-1}, the subfield trace function and a permutation x^{k_j} on $GF(q_j)$. Therefore $\widehat{f_j}(0) = 0$ and f_j is Gold-like. The fact that f_{j-1} is cyclic invariant implies that

$$f_{j-1}(Tr^{q_j}_{q_{j-1}}((x^2)^{k_j})) = f_{j-1}(Tr^{q_j}_{q_{j-1}}(x^{k_j})^2) = f_{j-1}(Tr^{q_j}_{q_{j-1}}(x^{k_j}))$$

Therefore f_j is cyclic invariant.

Conversely, if f is not balanced and Gold-like, we can repeat the above computation to show that f_j is not balanced and Gold-like for $j = 1, \ldots, l$.

Since the function in Theorem 1 is cyclic invariant, we can apply Theorem 7 to get an extension of the cascaded GMW sequence construction in [13]. We state our result in the language of polynomial functions and show when a sum of cascaded GMW functions is Gold-like. These Gold-like functions also correspond to non-quadratic almost optimal Boolean functions, which are useful for applications in cryptography. This result is achieved by a basis conversion from polynomial form to Boolean form as shown in Section 2.2.

Theorem 8. *Let $q = 2^n$ and let n, n_j be odd for $j = 1, \ldots, l$. Define recursively the functions f_i as follows:*

$$f_0(x) = \sum_{i=1}^{(n-1)/2} c_i Tr^q_2(x^{2^i+1}) + \gamma Tr^q_2(x), \gamma, c_i \in \{0, 1\},$$
$$f_j(x) = f_{j-1}(Tr^{q_j}_{q_{j-1}}(x^{k_j})), j = 1, \ldots, l,$$

where $q_0 = q$, $q_j = q^{n_j}_{j-1}$, $k_j = q^{r_j}_{j-1} + 1$ and $\gcd(r_j, n_j) = 1$. f_l corresponds to a Boolean function with $N = nn_1 \ldots n_l$ input bits having the following properties:

1. *f_l is Gold-like and balanced if and only if*
   (a) $g(x) = x + 1$ where $g(x) = \gcd(c(x), x^n + 1)$ and $c(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i(x^i + x^{n-i})$ and
   (b) $\gamma \equiv wt(c) + 1$ modulo 2 where $wt(c)$ is the number of coefficients c_i that are equal to 1.

   In this case, f_l has almost optimal nonlinearity $2^{N-1} - 2^{(N-1)/2}$.
2. *The algebraic degree of f_l is 2^{l+1}.*
3. *The linear span is $wt(c)nn_1^2n_2^4 \ldots n_l^{2^l} + \gamma nn_1n_2^2 \ldots n_l^{2^{l-1}}$.*

Proof. 1. By Theorem 7, f_l is balanced and Gold-like if and only if f_0 is balanced and Gold-like. By Theorem 1, f_0 is Gold-like if and only if $\gcd(c(x), x^n + 1) = x + 1$. Let us consider f_0 without the linear term $\gamma Tr(x)$, i.e. $f_0(x) = \sum_i c_i Tr(x^{2^i+1})$. From the proof of Lemma 1 for $p = 2$, we can deduce that

$$\hat{f}_0(\lambda)^2 = 2^n(1 + (-1)^{f_0(1)+Tr(\lambda)})$$

when f_0 is Gold-like. Therefore f_0 is balanced if and only if $\hat{f}_0(0) = 0$, i.e. $f_0(1) = 1$, which means $f_0(x)$ has an odd number of trace terms. Whenever

f_0 has an even number of trace terms, we can replace the function $f_0(x)$ by $Tr(x)+f_0(x)$ to get a balanced Gold-like function. This is what we have done by adding $\gamma Tr(x)$ in the definition of the basic function f_0. From Equation 2 of Section 2.2, we see that the Boolean forms of Gold-like functions have almost optimal nonlinearity.

2. By inductively expanding each trace terms of f_l and using the relation

$$(\sum_i x^{s_i})^{\sum_j 2^{a_j}} = \prod_j \sum_i x^{2^{a_j} s_i},$$

we see that

$$f_l(x) = \sum_i x^{t_i} + \sum_j x^{u_j},$$

where each t_i has Hamming weight 2^{l+1} and is expanded from the Gold terms $Tr(x^{2^i+1})$ in f_0. Each u_j has Hamming weight 2^l and is expanded from the linear term $\gamma Tr(x)$ in f_0. Since the algebraic degree of f_l is given by the maximum weight of the exponents, we see that $deg(f_l) = 2^{l+1}$.

3. Note that $f_l(x)$ can be written as

$$f_l(x) = \sum_{i=1}^{(n-1)/2} c_i Tr_2^q(g(x)^{2^i+1}) + \gamma Tr_2^q(g(x))$$

where $g(x)$ is a cascaded GMW function from $GF(2^N)$ to $GF(2^n)$ with known linear span $n_1 n_2^2 \cdots n_l^{2^{l-1}}$ [13]. Applying Lemma 2-(i) in [5] to each term $Tr_2^q(g(x)^{2^i+1})$, we obtain that, for each $i \neq j$, the monomial terms in $Tr_2^q(g(x)^{2^i+1})$ and $Tr_2^q(g(x)^{2^j+1})$ are distinct. By a similar reason, for each i, the monomial terms in $Tr_2^q(g(x)^{2^i+1})$ and $Tr_2^q(g(x))$ are also distinct. According to Theorem 1 and Lemma 2-(ii) in [5], the number of distinct monomials of $Tr_2^n(g(x)^{2^i+1})$ is $n(n_1 n_2^2 \cdots n_l^{2^{l-1}})^2$; and the number of distinct monomials of $Tr_2^n(g(x))$ is $n n_1 n_2^2 \cdots n_l^{2^{l-1}}$. Thus, the assertion is established.

By applying the results of Section 4, we can obtain large classes of generalised cascaded GMW sequences and, equivalently, balanced almost optimal Boolean functions, without any computation.

Corollary 3. *By substituting the quadratic part of the basic function f_0 of Theorem 8 by the Gold-like functions in Proposition 1 and Theorem 4, 5 and 6, we get large number of balanced non-quadratic almost optimal Boolean functions without any computations.*

Theorem 8 and Corollary 3 allow us to easily identify a large class of balanced almost optimal Boolean functions, which have high nonlinearity for protection against linear approximation based attacks [14, 19]. Our functions are linear combination of cascaded GMW functions, so they have larger linear span, for protection against interpolation attacks [10]. Our Boolean functions are non-quadratic, to make algebraic analysis more complex. The resiliency of our function is discussed in the next section.

5.1 Resiliency

We want a balanced Boolean function to be uncorrelated to as many linear functions as possible, so that linear approximation is difficult. We define the *zero spectrum set* of a Boolean function $f : GF(2)^n \to GF(2)$ by

$$Z_{\hat{f}} = \{w | \hat{f}(w) = 0\}.$$

$Z_{\hat{f}}$ represents the linear functions which are uncorrelated to f. We want this set to be as big as possible. Based on the following well known proposition, we see that Gold-like functions have better resiliency properties than almost optimal Boolean functions in general.

Proposition 2. *Let n be odd. If $f : GF(2)^n \to GF(2)$ is an almost optimal Boolean function, then the size of the zero spectrum set $Z_{\hat{f}} \leq 2^{n-1}$. Equality is achieved if and only if f is Gold-like.*

Proof. Let v be the size of the zero spectrum set $Z_{\hat{f}}$. Parseval's relation [15] says that

$$\sum_{w \in GF(2)^n} \hat{f}(w)^2 = 2^{2n}.$$

When f is almost optimal, $\hat{f}(w)^2 \leq 2^{n+1}$ for all w. Therefore

$$2^{2n} = \sum_{\hat{f}(w) \neq 0} \hat{f}(w)^2 \leq (2^n - v)2^{n+1},$$

which implies that $v \leq 2^{n-1}$. Equality is achieved if and only if $\hat{f}(w)^2 = 2^{n+1}$ for all $\hat{f}(w) \neq 0$, i.e., when f is Gold-like.

It is shown in [1] that when $n = 5$, the almost optimal Boolean function

$$f(x_1, \ldots, x_5) = x_3x_5 + x_2x_4 + x_1x_2x_3 + x_2x_3x_4x_5$$

has $\hat{f}(w)$ taking on the values $\{0, \pm 4, \pm 8\}$. So by the above proposition, f is uncorrelated to less than 16 linear functions while a Gold-like function will be uncorrelated to exactly 16 linear functions. So the function we constructed in Theorem 8 has better resiliency than almost optimal Boolean functions in this case.

Patterson and Wiedemann found examples of functions $f_{15} : GF(2)^{15} \to GF(2)$ with nonlinearity 16276 [17,18]. This is higher than the almost optimal nonlinearity $2^{14} - 2^7 = 16256$ for $n = 15$. In [17], they also defined the functions

$$f_{2k+15}(x_1, \ldots, x_{2k}, y_1, \ldots, y_{15}) = g(x_1, \ldots, x_{2k}) + f_{15}(y_1, \ldots, y_{15})$$

where g is a bent function and f_{15} is the Patterson-Wiedemann function for $n = 15$. We see that

$$\widehat{f_{2k+15}}(\lambda, \mu) = \hat{g}(\lambda)\widehat{f_{15}}(\mu) \leq 108/128 \times 2^k \tag{6}$$

and $N_{f_{2k+15}} = 2^{2k+14} - 108/128 \times 2^{k+7}$, which is slightly better than the almost optimal nonlinearity for $n = 2k + 15$; the linear bias is smaller by a factor of $108/128 = 0.84$. But it is shown in [17] that f_{15} has non-zero Hadamard Transform at all points. And Equation (6) shows that f_{2k+15} has non-zero Hadamard transform at all points too because $\hat{g}(\lambda)$ is $\pm 2^k$. We summarise our observations in the following proposition.

Proposition 3. *The Patterson-Wiedemann (PW) functions for $n \geq 15$ have non-zero Hadamard transform at all points. Thus they are unbalanced and can be approximated by all linear functions.*

Therefore, although the PW functions have slightly higher nonlinearity, our Boolean functions have better resiliency properties.

5.2 Example

We use an example to illustrate the application of Theorem 8. Consider the function

$$f_l(x) = Tr_2^{2^5}(Tr_{2^5}^{2^{15}}(x^{33}) + Tr_{2^5}^{2^{15}}(x^{33})^3 + Tr_{2^5}^{2^{15}}(x^{33})^5),$$

which correspond to a balanced Boolean function with 15 input bits. We apply Theorem 8 with $n = 5, l = 1, n_1 = 3, k_1 = 2^5 + 1$ and $\gamma = c_1 = c_2 = 1$. The nonlinearity of f_l is $2^{14} - 2^7 = 16256$, because

$$\gcd(c(x), x^5 + 1) = \gcd(x + x^2 + x^3 + x^4, x^5 + 1) = x + 1.$$

The algebraic degree is $2^{l+1} = 4$ and the linear span is $wt(c)nn_1^2 + nn_1 = 2 \times 5 \times 3^2 + 3 \times 5 = 105$. By expanding the trace terms of f_l, we see that

$$f_l(x) = Tr_2^{2^{15}}(x^{33} + x^{99} + x^{165} + x^{297} + x^{561} + x^{1091} + x^{1157}).$$

Note that the exponents have maximum weight four, which confirms that $deg(f) = 4$. Also, f_l is a sum of seven trace terms, each of which expands into 15 monomials to give f_l a linear span of 105. A computer program shows that the nonlinearity of f_l is indeed 16256.

6 Conclusion

We have derived several classes of sequences that have low cross correlation with the m-sequence represented by $Tr(x)$, which is useful for communications and cryptographic applications. We showed that a linear combination of Gold-terms over $GF(p^n)$ can be determined to be Gold-like or bent by a polynomial GCD computation. Then we derived a large class of bent, Gold-like p-ary sequences and three large classes of Gold-like binary sequences by analysing this GCD condition. By applying the theory of geometric sequences from [13] to our binary sequences based on sum of Gold terms, we deduce when a sum of cascaded GMW sequences is Gold-like. By using a basis conversion from $GF(2^n)$ to $GF(2)^n$, we can convert the cascaded GMW sequences to new almost optimal Boolean functions. These functions have high nonlinearity when the number of input bits n, is odd, and they have useful applications in cryptography because they make linear approximation based attacks difficult. Moreover, our Boolean functions are non-quadratic, have large linear span and better resiliency properties than general almost optimal Boolean functions. These other good properties give added protection against various cryptographic attacks in certain applications.

References

1. E.R. Berlekamp and L.R. Welch, "Weight Distributions of the Cosets of the $(32, 6)$ Reed-Muller Code", *IEEE Transactions on Information Theory*, vol. 18, no. 1, pp. 203-207, 1972.
2. S. Boztas and P.V. Kumar, "Binary Sequences with Gold-Like Correlation but Larger Linear Span", *IEEE Transactions on Information Theory*, vol.40, no. 2, pp.532-537, 1994.
3. A. Canteaut, C. Carlet, P. Charpin and C. Fontaine, "On Cryptographic Properties of the Cosets of $R(1, m)$", *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1494-1513, 2001.
4. R. Gold, "Maximal Recursive Sequences with 3-valued Cross Correlation Functions", *IEEE Transactions on Information Theory*, vol. 14, pp. 154-156, 1968.
5. G. Gong, "Q-ary Cascaded GMW Sequences", *IEEE Transactions on Information Theory*, vol.42, no.1, Jan 1996.
6. G. Gong and A. Youssef, "On Welch-Gong Transformation Sequence Generators", LNCS 2012, *7th Selected Areas of Cryptography*, pp. 217-232, Springer Verlag, 2000.
7. T. Helleseth, "Correlation of m-sequences and Related Topics", *Sequences and Their Applications 98*, pp. 49-65, 1998.
8. T. Helleseth and P.V. Kumar, "Sequences with Low Correlation", Chapter in: *Handbook of Coding Theory*, North Holland, 1998.
9. T. Hungerford, *Graduate Text in Mathematics-Algebra*, Springer, 1974.
10. T. Jacobsen, L. Knudsen, "The Interpolation Attack on Block Ciphers", LNCS 1267, *Fast Software Encryption*, pp.28-40, Springer-Verlag, 1997.
11. K. Khoo, G. Gong and D.R. Stinson, "A New Family of Gold-like Sequences", *IEEE International Symposium on Information Theory 02*, p.181, 2002.
12. K. Khoo, G. Gong and D.R. Stinson, "A New Family of Gold-like Sequences", *CACR Technical Report*, CORR 2001-64, 2001.
13. A. Klapper, A.H. Chan and M. Goresky, "Cascaded GMW sequence", *IEEE Transactions on Information Theory*, vol. 39, no. 1, pp. 177-183, 1993.
14. M. Matsui, "Linear cryptanalysis method for DES cipher", LNCS 765, *Eurocrypt'93*, pp. 386-397, 1994.
15. F.J. McWilliams and N.J.A. Sloane, *Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.
16. K. Nyberg, "Differentially Uniform Mappings for Cryptography", LNCS 765, *Eurocrypt'93*, pp. 55-64, 1994.
17. N.J Patterson and D.H. Wiedemann, "The Covering Radius of the $(2^{15}, 16)$ Reed-Muller Code is at least 16276", *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 354-356, May 1983.

18. N.J Patterson and D.H. Wiedemann, "Correction to - The Covering Radius of the $(2^{15}, 16)$ Reed-Muller Code is at least 16276", *IEEE Transactions on Information Theory*, vol. 36, no. 2, pp. 443, Mar 1990.
19. T. Siegenthaler, "Decrypting a Class of Stream Ciphers using Ciphertexts only", *IEEE Transactions on Computers*, vol. C34, no. 1, pp. 81-85, 1985.
20. Song Y. Yan, *Number Theory for Computing*, Springer-Verlag, 2000.