Designs, Codes and Cryptography, 38, 279–295, 2006

A New Characterization of Semi-bent and Bent Functions on Finite Fields*

KHOONGMING KHOO kkhoongm@dso.org.sg
DSO National Laboratories, 20 Science Park Dr, S118230, Singapore

GUANG GONG ggong@calliope.uwaterloo.ca
Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ont. N2L 3G1, Canada

DOUGLAS R. STINSON dstinson@uwaterloo.ca
School of Computer Science, University of Waterloo, Waterloo, Ont. N2L 3G1, Canada

Communicated by: T. Helleseth

Received November 14, 2002; Revised February 25, 2005; Accepted March 31, 2005

Abstract. We present a new characterization of semi-bent and bent quadratic functions on finite fields. First, we determine when a $GF(2)$-linear combination of Gold functions $Tr(x^{2^i+1})$ is semi-bent over $GF(2^n)$, n odd, by a polynomial GCD computation. By analyzing this GCD condition, we provide simpler characterizations of semi-bent functions. For example, we deduce that all linear combinations of Gold functions give rise to semi-bent functions over $GF(2^p)$ when p belongs to a certain class of primes. Second, we generalize our results to fields $GF(p^n)$ where p is an odd prime and n is odd. In that case, we can determine whether a $GF(p)$-linear combination of Gold functions $Tr(x^{p^i+1})$ is (generalized) semi-bent or bent by a polynomial GCD computation. Similar to the binary case, simple characterizations of these p-ary semi-bent and bent functions are provided.

Keywords: bent functions, semi-bent functions, cyclic matrix, cyclic codes, finite fields, Sophie-German princes

AMS Classification: 11T71

1. Introduction

A Boolean function is a mapping from the vector space $(GF(2))^n$ to $GF(2)$. Boolean functions taking on low Hadamard transform values have useful applications in cryptography and communications. In cryptography, such functions provide protection against linear cryptanalysis [14], while in

*Parts of this paper were presented at the 2002 IEEE International Symposium on Information Theory [10].

communications, they correspond to sequences that have low cross-correlation with the m-sequence represented by $Tr(x)$ [7,8].

By Parseval's equation, the maximum magnitude of the Hadamard transform is at least $2^{n/2}$. This lower bound is achieved only when n is even, and Boolean functions which achieve this bound are called bent functions [21]. It is well-known that the Hadamard transform of a bent function only takes on the values $\pm 2^{n/2}$. When n is odd, the lower bound for the maximum size of the Hadamard transform is not known in general. However, this lower bound has been shown to be $2^{(n+1)/2}$ when the function is quadratic [16] or when $n = 3, 5, 7$ [17]. Also, from [19,20], it is known that the lower bound for the maximum size of the Hadamard transform does not exceed $\frac{27}{32} \times 2^{(n+1)/2}$ when $n \geq 15$ is odd.

A useful class of functions which achieve this lower bound are the semi-bent functions, whose Hadamard transform only takes on the three values $0, \pm 2^{(n+1)/2}$ [4]. In the literature, semi-bent functions are also called 3-valued almost optimal Boolean functions [3], plateaued functions [23] and preferred functions [6,8]. These functions are widely studied in cryptography because, besides having low Hadamard transform which provides protection against linear cryptanalysis [14], they usually possess other desirable properties such as resiliency, propagation criteria, low additive autocorrelation and high algebraic degree [3,6,8,9,23].

In general, it is a hard problem to characterize all functions with low Hadamard transform values. But this problem has been solved for the quadratic Boolean functions $f: (GF(2))^n \to GF(2)$, defined by

$$f(x_0, \ldots, x_{n-1}) = \sum_{i<j} c_{ij} x_i x_j + \sum_i c_i x_i + c, \text{ where } c_{ij}, c_i, c \in \{0, 1\}.$$

All quadratic Boolean functions with the lowest Hadamard transform have been identified (see [16]) and they correspond to the semi-bent functions when n is odd and the bent functions when n is even.

In this paper, we study a related problem for finite fields. Every function $f: GF(2^n) \to GF(2)$ is equivalent to a Boolean function, by viewing each input $x = x_1\alpha_1 + \cdots + x_n\alpha_n \in GF(2^n)$ as a vector $(x_1, \ldots, x_n) \in (GF(2))^n$ where $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of $GF(2^n)$ over $GF(2)$. Under this correspondence, a quadratic Boolean function is equivalent to a function $f: GF(2^n) \to GF(2)$ defined as follows:

$$f(x) = \sum_{\{i:\text{weight}(e_i)\leq 2\}} Tr(\beta_i x^{e_i}),$$

where weight(e_i) is the number of 1's in the binary representation of e_i. Note that Tr is the usual trace function from $GF(2^n)$ to $GF(2)$. Our objective is to find the quadratic functions on $GF(2^n)$ with the lowest

Hadamard transform when n is odd, i.e., the semi-bent quadratic functions.

From the theory of sequences, it is known that the Gold function $Tr(x^{2^i+1})$ and the Boztas–Kumar function $\sum_{i=1}^{(n-1)/2} Tr(x^{2^i+1})$ are "Gold-like", i.e., they can be used to form a set of sequences with low cross correlation $-1, -1 \pm 2^{(n+1)/2}$ by XORing with the m-sequences represented by $Tr(\lambda x)$ [2, 5]. As a consequence, these quadratic functions based on one Gold function, as well as the sum of all Gold functions, are semi-bent.

In this paper, we investigate the problem of determining when a linear combination of the Gold functions, namely,

$$f(x) = \sum_{i=1}^{(n-1)/2} c_i \, Tr(x^{2^i+1}), \tag{1}$$

where $c_i \in \{0, 1\}$ for $1 \le i \le (n-1)/2$, is semi-bent. Let $\mathcal{Q}_2(n)$ denote the set off all functions described by equation (1). Using techniques from linear algebra and coding theory, we can determine whether a function $f \in \mathcal{Q}_2(n)$ is semi-bent by a simple polynomial GCD computation.

By analyzing this GCD condition, we obtain several nice characterizations of families of semi-bent quadratic functions on $GF(2^n)$. If n belongs to a certain class of primes, then we show that all functions $f \in \mathcal{Q}_2(n)$ are semi-bent. Furthermore, we prove theorems which describe when the sum of Gold functions corresponding to an arithmetic progression of indices i is semi-bent.

Finally, we generalize our construction to the fields $GF(p^n)$, where p and n are odd. We study the functions defined as follows:

$$f(x) = \sum_{i=1}^{(n-1)/2} c_i \, Tr(x^{p^i+1}), \tag{2}$$

where $c_i \in GF(p)$ for $1 \le i \le (n-1)/2$. The class of functions described by (2) is denoted $\mathcal{Q}_p(n)$. In this case, a function $f \in \mathcal{Q}_p(n)$ can be a generalized semi-bent or a bent function, which again can be identified by a polynomial GCD computation. (A generalized semi-bent function is one whose Hadamard transform has magnitude 0, $p^{(n+1)/2}$, while a generalized bent function is one whose Hadamard transform values all have magnitude $p^{n/2}$.) Similar to what we did for $GF(2^n)$, we analyze the polynomial GCD condition to prove that all functions $f \in \mathcal{Q}_p(n)$ are generalized semi-bent or bent when n belongs to a certain class of primes.

In Section 2, we give some definitions and preliminaries on semi-bent and bent functions. In Section 3, we show that the semi-bent functions in $\mathcal{Q}_2(n)$ can be identified by a polynomial GCD computation. In Section 4,

we study the polynomial GCD condition, and as a result, we characterize several classes of semi-bent functions in $\mathcal{Q}_2(n)$. In Section 5, we analyze when a function $f \in \mathcal{Q}_p(n)$ is bent or semi-bent and, as a result, we discover large classes of bent and semi-bent functions over $GF(p^n)$, when n is prime.

1.1. Related Work

Kim et al. [11] also investigated how to construct generalized bent functions of the form (2). They describe a construction for generalized bent functions of the form $f(x)$ as defined by (2), under the condition that all the coefficients $c_i \in \{0, 1\}$. See Section 5 for a more precise statement of their theorem.

Kim and No [12] present constructions for binary sequence families with four- and six-valued correlations. These constructions are based on the function

$$f(x) = \sum_{i=1}^{(n-1)/2} Tr(x^{2^{ki}+1}),$$

where k is an integer satisfying some suitable conditions.

2. Definitions

Let $GF(p^n)$ be the finite field with p^n elements, where p is prime. The *trace function* on this field is the function $Tr: GF(p^n) \to GF(p)$ defined as

$$Tr(x) = \sum_{i=0}^{n-1} x^{p^i}.$$

The trace function is linear over $GF(p)$.

The *Hadamard transform* of a function $f: GF(p^n) \to GF(p)$ is the function $\hat{f}: GF(p^n) \to \mathbb{C}$ defined by

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

where $\omega = e^{2\Pi i/p}$ is a complex pth root of unity.

The special case $p = 2$ is most often studied in the literature. In that case, we have a function $f: GF(2^n) \to GF(2)$ and the Hadamard transform is defined as follows:

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

Here, $\hat{f}: GF(2^n) \to \mathbb{R}$.

Definition 2.1 [21]. Let n be even. The function $f: GF(2^n) \to GF(2)$ is bent if $|\hat{f}(\lambda)| = 2^{n/2}$ for all $\lambda \in GF(2^n)$.

Bent functions meet the lower bound on the maximum magnitude of the Hadamard transform of a function. Therefore, they offer the best possible protection against linear cryptanalysis [14]. Moreover, they are also *perfect nonlinear*, which means that the shift $f(x) + f(x+a)$ is balanced for all $a \in GF(2^n)$ [18]. This is desirable for protection against differential cryptanalysis [1]. However, one drawback of bent functions is that they are not balanced.

Bent functions for $p = 2$ can exist only when n is even. When n is odd, we have the following related concept.

Definition 2.2 [4, Definition 4]. Let n be odd. The function $f: GF(2^n) \to GF(2)$ is semi-bent if $|\hat{f}(\lambda)| \in \{0, 2^{(n+1)/2}\}$ for all $\lambda \in GF(2^n)$.

The semi-bent functions are widely studied in cryptography and have been investigated under various names, including 3-valued almost optimal Boolean functions, plateaued functions and preferred functions; (see [3, 4, 6, 23]).

The definition of bent and semi-bent functions can be generalized to arbitrary finite fields $GF(p^n)$, as follows.

Definition 2.3. The function $f: GF(p^n) \to GF(p)$ is a generalized bent function if $|\hat{f}(\lambda)| = p^{n/2}$ for all $\lambda \in GF(2^n)$. The function f is a generalized semi-bent function if $|\hat{f}(\lambda)| \in \{0, p^{(n+1)/2}\}$ for all $\lambda \in GF(2^n)$.

3. Linear Combination of Gold Functions

Assume that n is odd. In this section, we show how to determine whether the function $f(x) = \sum_{i=1}^{n-1/2} c_i \, Tr(x^{2^i+1}) \in \mathcal{Q}_2(n)$ is semi-bent using elementary algebraic techniques.

LEMMA 3.1. *Let n be odd and let $c_i \in \{0, 1\}$ for $1 \le i \le (n-1)/2$. Suppose the function f is defined as*

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

for all $x \in GF(2^n)$. *Then* f *is semi-bent 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 $n-1$ *over* $GF(2)$, *where we define* $c_0 = 0$ *and* $c_{n-i} = c_i$ *for* $i = 1, \dots, (n-1)/2$.

Proof. We use the Welch squaring method:

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

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

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

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 the matrix (3). Also, we have that

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

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

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

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

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

depending on whether the exponent is the zero function or a non-zero linear function, respectively. This means that $\hat{f}(\lambda) \in \{0, \pm 2^{n+k/2}\}$ for all λ if and only if $\dim(\ker(L))=k$. In particular, f is semi-bent if and only if $\dim(\ker(L))=1$, i.e., when $\operatorname{rank}(L)=n-1$. ■

Remark 3.1. The bilinear form $\Phi(x, w)$, defined in the above proof, corresponds to the symplectic of $f(x)$ under the Boolean representation. For results on quadratic Boolean functions, (see [16, 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 in the quotient ring $GF(2)[x]/(x^n+1)$, where

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

and

$$c(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i (x^i + x^{n-i}).$$

We will make use of the following well-known useful facts about the cyclic code C (see, e.g., [16]):

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. $\operatorname{rank}(L) = \dim(C) = n - \deg(g(x))$.
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 $\operatorname{rank}(L) = \dim(C) = n-1$, which is the condition required in Lemma 3.1 to enusre that f is semi-bent. We summarize this discussion in the following theorem:

THEOREM 3.2. *Let n be odd and let $c_i \in \{0, 1\}$ for $1 \le i \le (n-1)/2$. Suppose the function f is defined as*

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

for all $x \in GF(2^n)$. Then f is semi-bent if and only if $\gcd(c(x), x^n + 1) = x + 1$, *where*

$$c(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i (x^i + x^{n-i}).$$

Here are a couple of small examples to demonstrate the application of Theorem 3.2.

1. $f(x) = Tr(x^3 + x^5)$ is semi-bent 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 semi-bent over $GF(2^{155})$ because $\gcd(x + x^4 + x^{151} + x^{154}, x^{155} + 1) = x^5 + 1$.

Using Theorem 3.2, we give short proofs of two known results regarding semi-bent functions.

COROLLARY 3.3 (Gold [5]). *Let n be odd. Then the function $f(x) = Tr(x^{2^i+1})$ from $GF(2^n)$ to $GF(2)$ is semi-bent if and only if* $\gcd(i, n) = 1$.

Proof. We have that

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

Because n is odd, this gcd equals $x + 1$ if and only if $\gcd(n, i) = 1$. ■

COROLLARY 3.4 (Boztas and Kumar [2]). *Let n be odd. Then the function $f(x) = \sum_{i=1}^{\frac{n-1}{2}} Tr(x^{2^i+1})$ from $GF(2^n)$ to $GF(2)$ is semi-bent.*

Proof. The associated cyclic code C is generated by the polynomial $c(x) = \sum_{i=1}^{n-1} x^i$ and

$$(x + 1)c(x) \bmod x^n + 1 = x + 1$$

is a vector in C. Hence, $\gcd(c(x), x^n + 1) = x + 1$. ■

For future use, we state a useful lemma regarding generator polynomials of cyclic codes.

LEMMA 3.5. *Let n be odd and let $g(x)$ be the generator polynomial of the cyclic code C generated by $c(x)=\sum_{i=1}^{(n-1)/2} c_i(x^i+x^{n-i})$, where $c_i \in \{0,1\}$ for $1 \le i \le (n-1)/2$. Then $g(x)=(x+1)h(x)$, where $\deg(h(x))$ is even.*

Proof. First, we have that one is a root of $c(x)$ and x^n+1, so $x+1$ is a factor of $g(x)=\gcd(c(x), x^n+1)$. Next, define $h(x)=g(x)/(x+1)$. It is easy to see that, if β is a root of $h(x)$ in some extension field of $GF(2)$, then β^{-1} is also a root of $h(x)$ (this follows because $\beta^n=1$ and $c(\beta)=c(\beta^{-1})$. Consider the irreducible factor of $h(x)$ of which β is a root; this is the minimal polynomial $m_\beta(x)$. If β^{-1} is a root of $m_\beta(x)$, then $\deg(m_\beta(x))$ is even. Otherwise, $m_{\beta^{-1}}(x)$ is also an irreducible factor of $h(x)$, and $\deg(m_\beta(x))+\deg(m_{\beta^{-1}}(x))$ is even. It follows that $h(x)$ has even degree. ■

4. Some Characterizations of Semi-bent Quadratic Functions

4.1. Semi-bent Functions for All Choices of Coefficients

In this section, we address the question of determining odd integers n such that all non-zero functions $f(x) \in \mathcal{Q}_2(n)$ are semi-bent.

LEMMA 4.1. *Let n be odd. If all non-zero functions $f(x) \in \mathcal{Q}_2(n)$ are semi-bent, then n is prime.*

Proof. This is an immediate consequence of Corollary 3.3. ■

Henceforth, we only consider the case where n is an odd prime. Since the generator polynomial $g(x)$ of a cyclic code is closely related to the factorization of the polynomial x^n+1, let us examine this factorization more closely. In the remainder of this paper, $\mathrm{ord}_p(a)$ will denote the order of a in the multiplicative group $GF(p)\backslash\{0\}$, where p is an odd prime and $a \neq 0$. The following result is well-known.

LEMMA 4.2 [15]. *Let p be an odd prime. The factorization of x^p+1 over $\mathbb{Z}_2[x]$ into irreducible factors is of the form*

$$x^p+1=(x+1)h_1(x)h_2(x)\ldots h_t(x),$$

where each $h_i(x)$ is a polynomial of degree $\mathrm{ord}_p(2)$ and $t=(p-1)/\mathrm{ord}_p(2)$.

We next look at the cases where x^p+1 has either two or three irreducible factors. First, suppose that p is an odd prime and $\mathrm{ord}_p(2)=p-1$.

Then x^p+1 has two irreducible factors by Lemma 4.2, and we can prove the following theorem.

THEOREM 4.3. *Suppose p is an odd prime such that* $\mathrm{ord}_p(2)=p-1$. *Then every non-zero function in $\mathcal{Q}_2(p)$ is semi-bent.*

Proof. By Lemma 4.2, x^p+1 has factorization

$$x^p+1=(x+1)(1+x+x^2+\cdots+x^{p-1})$$

into two irreducible factors. Because the generator polynomial $g(x)$ divides x^p+1 properly, it must be equal to $x+1$ or $1+x+\cdots+x^{p-1}$. But $(x+1)|g(x)$, which implies $g(x)=x+1$, and hence we are done by Theorem 3.2. ■

In view of the above theorem, it is natural to ask about the existence and distribution of primes p for which $\mathrm{ord}_p(2)=p-1$. The first ten such primes are 3, 5, 11, 13, 19, 29, 37, 53, 59 and 61.

A conjecture of Artin states that there exists an infinite number of such primes. The precise statement is as follows.

PROPOSITION 4.4 (*Artin's Conjecture* [13,22]). *Let $S(2)$ be the set of all primes for which two is a primitive root. Then Artin conjectured that the density of $S(2)$ relative to the set of all primes is given by C_{Artin} where*

$$C_{\mathrm{Artin}}=\prod_{k=1}^{\infty}\left[1-\frac{1}{p_k(p_k-1)}\right]=0.3739558136\ldots$$

where p_k is the kth prime.

This conjecture has been proven by Hooley in 1967, assuming that the Riemann Hypothesis holds [13,22].

The next case we consider is when $p=2s+1$ is prime, s is odd and $\mathrm{ord}_p(2)=s$. This is the situation where x^p+1 has three irreducible factors of odd degree. We have the following theorem.

THEOREM 4.5. *Suppose $p=2s+1$ is a prime such that s is odd and* $\mathrm{ord}_p(2)=s$. *Then every non-zero function in $\mathcal{Q}_2(p)$ is semi-bent.*

Proof. By Lemma 4.2, the factorization of x^p+1 into irreducible polynomials is

$$x^p+1=(x+1)h_1(x)h_2(x),$$

where $h_i(x)$ has degree s, $i = 1, 2$. The generator polynomial $g(x)$ is a proper divisor of $x^p + 1$ and has $x + 1$ as a factor. Hence, $g(x) = x + 1$ or $(x + 1)h_i(x)$, $i = 1, 2$. However, $g(x)$ is a product of $x + 1$ and an even degree polynomial, by Lemma 3.5. Therefore $g(x) = x + 1$ and we are done by Theorem 3.2. ■

The first ten primes of the form specified in Theorem 4.5 are as follows:

$$7, 23, 47, 71, 79, 103, 167, 191, 199, 239$$

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

As a corollary of Theorems 4.3 and 4.5, we prove a similar result holds for the Sophie Germain primes, which are the primes p of the form $p = 2q + 1$, where q is prime.

COROLLARY 4.6. *Suppose that $p = 2q + 1$ where p and q prime. Then every non-zero function in $\mathcal{Q}_2(p)$ is semi-bent.*

Proof. If $\text{ord}_p(2) = p - 1$, then we are done by Theorem 4.3. If not, then $\text{ord}_p(2)$ is a proper divisor of $p - 1 = 2q$, which implies $\text{ord}_p(2) = 2$ or q. But $\text{ord}_p(2) \neq 2$ because $p \geq 5$, so $\text{ord}_p(2) = q$, which is an odd prime, and we are done by Theorem 4.5. ■

The first ten Sophie-Germain primes are as follows:

$$5, 7, 11, 23, 47, 59, 83, 107, 167, 179.$$

The Sophie Germain primes are well studied in number theory and it is conjectured that there are an infinite number of such primes.

If a prime p is not of the form considered in Theorems 4.3 and 4.5, then we will show that there exists a non-zero function in $\mathcal{Q}_2(p)$ that is not semi-bent.

THEOREM 4.7. *The only odd integers n such that all non-zero functions in $\mathcal{Q}_2(n)$ are semi-bent are the primes mentioned in Theorems 4.3 and 4.5.*

Proof. Let p be a prime not of the form considered in Theorems 4.3 and 4.5 and let ζ be a primitive pth root of unity in $GF(2^p)$. The minimal polynomial of ζ, denoted $m_\zeta(x)$, is the polynomial in $GF(2)[x]$ whose roots are all the conjugates of ζ. $m_\zeta(x)$ is an irreducible factor of $x^p + 1$ whose degree is $s = \text{ord}_p(2)$.

Define a polynomial $u(x)$, depending on whether ζ^{-1} is a root of $m_\zeta(x)$, as follows:

Case 1. ζ^{-1} is a root of $m_\zeta(x)$. Define $u(x) = (x+1)m_\zeta(x)$. In this case, s is even and $\deg(u) = s+1$. Observe that $s < p-1$ because we are assuming that $\mathrm{ord}_p(2) \neq p-1$.

Case 2. ζ^{-1} is not a root of $m_\zeta(x)$. Define $u(x) = (x+1)m_\zeta(x)m_{\zeta^{-1}}(x)$. In this case, s is odd and $\deg(u) = 2s+1$. Observe that $s < (p-1)/2$ because we are assuming that $\mathrm{ord}_p(2) \neq (p-1)/2$ and we are not in case 1.

It is easy to see that $u(x) = x^r u(1/x)$, where $r = \deg(u) \leq p-1$, in both cases 1 and case 2. This implies that $u(x) = \sum_{i=1}^{r} u_i x^i$, where $u_i = u_{r-i}$ for all i. Now consider the polynomial $c(x) = x^{(p-r-1)/2}u(x)$. The following properties of $c(x)$ are easily verified:

- $\deg(c) \leq p-1$.
- $c(x) = \sum_{i=1}^{p-1} c_i x^i$, where $c_i \in \{0, 1\}$ and $c_i = c_{p-i}$ for all i.
- $\gcd(c(x), x^p + 1) = u(x) \neq x+1$.

It therefore follows from Theorem 3.2 that the function

$$f(x) = \sum_{i=1}^{(p-1)/2} c_i \, Tr(x^{2^i+1})$$

is not semi-bent. ■

EXAMPLE 4.1. *Consider the prime $p = 17$, which is not of the form considered in Theorems 4.3 and 4.5. Let ζ be a primitive 17th-root of unity in $GF(2^{17})$. It can be verified that*

$$m_\zeta(x) = m_{\zeta^{-1}}(x) = x^8 + x^7 + x^6 + x^4 + x^2 + x + 1$$

and we define

$$c(x) = x^{(17-8-1)/2}(1+x)m_\zeta(x) = x^{13} + x^{10} + x^9 + x^8 + x^7 + x^4.$$

Then $\gcd(c(x), x^{17} + 1) = (x+1)m_\zeta(x)$ *and hence*

$$f(x) = Tr(x^{17} + x^{129} + x^{257}),$$

$x \in GF(2^{17})$, *is not semi-bent.* ■

4.2. *Semi-bent Quadratic Functions from Arithmetic Progressions*

We now characterize semi-bent functions formed by a sum of Gold functions corresponding to an arithmetic progression. These contain semi-bent functions which are a sum of two Gold functions as a special case.

THEOREM 4.8. *Let n be odd. Consider the function $f(x) \in \mathcal{Q}_2(n)$ defined as*

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

Then f is semi-bent if $\gcd(2a+rd, n) = 1 = \gcd((r+1)d, n)$. *Further, if* $\gcd(d, n) = 1$, *then* $\gcd(2a+rd, n) \neq 1$ *or* $\gcd((r+1)d, n) \neq 1$ *implies f is not semi-bent.*

Proof. The polynomial $c(x)$ corresponding to $f(x)$ is

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

The gcd of the numerator and $x^n + 1$ is equal to $x + 1$ if $\gcd(2a+rd, n) = 1 = \gcd((r+1)d, n)$. In this case, $f(x)$ is bent by Theorem 3.2.

Now suppose that $\gcd(1 + x^d, 1 + x^n) = 1 + x$ (i.e., $\gcd(d, n) = 1$). Then $\gcd(c(x), x^n + 1) = x + 1$ if and only if $\gcd(2a+rd, n) = 1 = \gcd((r+1)d, n)$. ∎

COROLLARY 4.9. *Let n be odd. Consider the function $f(x) \in \mathcal{Q}_2(n)$ defined as $f(x) = Tr(x^{2^i+1}) + Tr(x^{2^j+1})$. Then $f(x)$ is semi-bent if and only if* $\gcd(i + j, n) = 1 = \gcd(i - j, n)$.

Proof. From the proof of Theorem 4.8 with $a = i$, $r = 1$ and $d = j - i$, we see that

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

Thus $\gcd(c(x), x^n + 1) = x + 1$ if and only if $\gcd(i + j, n) = 1 = \gcd(i - j, n)$. ∎

Remark 4.1. When $n = p$ is prime in Theorem 4.8, all functions corresponding to arithmetic progressions are semi-bent.

5. Generalized Bent and Semi-bent Functions over $GF(p^n)$

Theorem 3.2 characterizes when a linear combination of binary Gold functions is semi-bent. We now generalize this result to the p-ary case, where we can get both semi-bent and bent functions. We omit the proofs because they are similar to the binary case.

LEMMA 5.1. *Let p be an odd prime and let n be an odd integer which is not divisible by p. Suppose $c_i \in GF(p)$ for $1 \le i \le (n-1)/2$ and suppose the function f is defined as*

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

$x \in GF(p^n)$. Define the cyclic matrix

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

where $c_0 = 0$ and $c_{n-i} = c_i$ for $i = 1, \dots, (n-1)/2$. Then $f(x)$ is generalized bent if and only if L has rank n over $GF(p)$, and $f(x)$ is generalized semi-bent if and only if L has rank $n-1$ over $GF(p)$.

Remark 5.1. When $p = 2$, the matrix L cannot have rank n. This follows because the sum of all the rows is the 0-vector in $(GF(2))^n$.

Similar to the binary case, the rows of matrix L give rise to a cyclic code C in $GF(p)[x]/(x^n - 1)$ generated by the polynomial $c(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i(x^i + x^{n-i})$. The following result is analogous to Theorem 3.2.

THEOREM 5.2. *Let p be a prime and let n be an odd integer not divisible by p. Let $c_i \in GF(p)$ for $1 \le i \le (n-1)/2$, and define the function*

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

for all $x \in GF(p^n)$. *Then* f *is generalized bent or semi-bent if and only if* $\gcd(c(x), x^n - 1) = 1$ *or* $x - 1$ *respectively, where*

$$c(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i (x^i + x^{n-i}).$$

Using Theorem 5.2, we can characterize classes of bent and semi-bent functions over $GF(p^n)$ when $n \neq p$ is a prime.

THEOREM 5.3. *Let* p, n *be primes such that* $p \neq n$. *Suppose that* $\mathrm{ord}_n(p) = n - 1$, *or* $\mathrm{ord}_n(p) = (n-1)/2$ *is odd. Then every non-zero function in* $\mathcal{Q}_p(n)$ *is bent or semi-bent.*

Remark 5.2. A function $f(x)$ in Theorem 5.3 is bent if

$$\sum_{i=1}^{(n-1)/2} c_i \not\equiv 0 \mod p$$

and semi-bent, otherwise.

It is interesting to compare Theorem 5.3 to the following result, which is proven by Kim et al. [11].

THEOREM 5.4. *Let* $I \subseteq \{1, \ldots, (n-1)/2\}$ *and let* $f(x): GF(p^n) \to GF(p)$ *be defined as* $f(x) = \sum_{i \in I} Tr(x^{p^i+1})$. *If* $|I|$ *is relatively prime to both n and p, then* $f(x)$ *is generalized bent.*

This theorem has fewer conditions than our Theorem 5.3; however our result permits coefficients to take on arbitrary values in $GF(p)$.

6. Conclusion

Functions with low Hadamard transform, such as (generalized) semi-bent and bent functions, have useful applications in cryptography and communications. We showed that the semi-bent quadratic functions over finite fields of characteristic two correspond to cyclic binary matrices with rank $n-1$. By studying the connection between cyclic matrices and cyclic codes, this allowed us to characterize several large classes of semi-bent functions on $GF(2^n)$. We also observed that this technique can be naturally extended to the finite fields $GF(p^n)$, where p is odd. In this case, we obtain both generalized bent and semi-bent functions.

Acknowledgments

Research of the authors is supported as follows: NSERC Grant RGPIN 227700-00 (GG) and NSERC Grant RGPIN 203114-02 (DRS).

References

1. E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, *Journal of Cryptology*, Vol. 4 (1991) pp. 3–72.
2. S. Boztas and P. V. Kumar, Binary sequences with Gold-like correlation but larger linear span, *IEEE Transactions on Information Theory*, Vol. 40 (1994) pp. 532–537.
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 (2001) pp. 1494–1513.
4. J. H. Cheon and S. Chee, Elliptic curves and resilient functions, *Lecture Notes in Computer Science*, Vol. 2015 (2000) pp. 386–397.
5. R. Gold, Maximal recursive sequences with 3-valued cross correlation functions, *IEEE Transactions on Information Theory*, Vol. 14 (1968) pp. 154–156.
6. G. Gong and K. Khoo, Additive autocorrelation of resilient boolean functions, *Lecture Notes in Computer Science*, Vol. 3006 (2004) pp. 275–290.
7. T. Helleseth, Correlation of m-sequences and related topics, In *Sequences and Their Applications*, Springer, Berlin, (1998) pp. 49–66.
8. T. Helleseth and P. V. Kumar, Sequences with low correlation, In *Handbook of Coding Theory*, North-Holland, Amsterdam, (1998) pp. 1765–1853.
9. K. Khoo and G. Gong, New constructions for resilient and highly nonlinear boolean functions, *Lecture Notes in Computer Science*, Vol. 2727 (2003) pp. 498–509.
10. K. Khoo, G. Gong and D. R. Stinson, A new family of Gold-like sequences, *Proceedings of IEEE International Symposium on Information Theory* (2002) p. 181.
11. Y. S. Kim, J. W. Jang, J. S. No and T. Helleseth, On p-ary bent functions defined on finite fields, In *Mathematical Properties of Sequences and Other Combinatorial Structures*, Kluwer, Dordrecht, (2002) pp. 65–76.
12. Y. S. Kim and J. S. No, New families of binary sequences with low correlation, *IEEE Transactions on Information Theory*, Vol. 49 (2003) pp. 3059–3065.
13. Mathworld: Artin's Conjecture, http://mathworld.wolfram.com/ArtinsConstant.html.
14. M. Matsui, Linear cryptanalysis method for DES cipher, *Lecture Notes in Computer Science*, Vol. 765 (1994) pp. 386–397.
15. R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, Cambridge, (1994).
16. F. J. McWilliams and N. J. A. Sloane, *Theory of Error-Correcting Codes*, North-Holland, Amsterdam, (1977).
17. J. Mykkeltveit, The covering radius of the $(128, 8)$ Reed Muller code is 56, *IEEE Transactions on Information Theory*, Vol. 26 (1980) pp. 359–362.
18. K. Nyberg, Perfect nonlinear S-boxes, *Lecture Notes in Computer Science*, Vol. 547 (1992) pp. 378–386.
19. 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 (1983) pp. 354–356.
20. 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 Information Theory*, Vol. 36 (1990) pp. 443.

21. O. S. Rothaus, On bent functions, *Journal of Combinatorial Theory A*, Vol. 20 (1976) pp. 300–305.
22. Song Y. Yan, *Number Theory for Computing*, Springer-Verlag, Berlin, (2000).
23. Y. Zheng and X. M. Zhang, Relationships between bent functions and complementary plateaued functions, *Lecture Notes in Computer Science*, Vol. 1787 (1999) pp. 60–75.