Balanced Symmetric Functions over $GF(p)$

Thomas W. Cusick,Yuan Li, and Pantelimon Stănică*

***Abstract*—Under mild conditions on n, p, we give a lower bound on the number of n-variable balanced symmetric polynomials over finite fields $GF(p)$, where p is a prime number. The existence of nonlinear balanced symmetric polynomials is an immediate corollary of this bound. Furthermore, we prove that $X(2^t, 2^{t+1}\ell - 1)$ are balanced and conjecture that these are the only balanced symmetric polynomials over $GF(2)$, where $X(d,n) = \sum_{1\le i_1<i_2<\cdots<i_d\le n} x_{i_1}x_{i_2}\cdots x_{i_d}$.**

***Index Terms*—Cryptography, finite fields, balancedness, symmetric polynomials, multinomial coefficients.**

I. Introduction

Since symmetry guarantees that all of the input bits have equal status in a very strong sense, symmetric Boolean functions display some interesting properties. A lot of research about symmetry in characteristic 2 has been previously done, and we mention here the references [1], [2], [22], [4], [5], [6], [8], [14], [16], [17], [18], [20], [21]. On the other hand, it is natural to extend various cryptographic ideas from $GF(2)$ to other finite fields of characteristic > 2, $GF(p)$ or $GF(p^n)$, p being a prime number. For example, [15] and [10] studied the correlation immune and resilient functions on $GF(p)$. Also, [7] and [12] investigated the generalized bent functions on $GF(p^n)$. In [13], Li and Cusick first introduced the strict avalanche criterion over $GF(p)$. In [14], they generalized most results of [5] and determined all the linear structures of symmetric functions over $GF(p)$.

Balancedness is a desirable requirement of functions which will be used in cryptography. In this paper, by an enumerating method, we give a lower bound for the number of balanced symmetric polynomials over $GF(p)$, and as an immediate consequence, we show the existence of nonlinear balanced symmetric polynomials. We did not find (even conjecturally) any simple characterization of the algebraic normal form of nonlinear balanced symmetric polynomials even for $p = 2$. We prove that $X(2^t, 2^{t+1}\ell - 1)$ are balanced and conjecture that these polynomials are the *only* nonlinear balanced elementary symmetric polynomials, where $X(d,n) = \sum_{1\le i_1<i_2<\cdots<i_d\le n} x_{i_1}x_{i_2}\cdots x_{i_d}$.

II. Preliminaries

In this paper, p is a prime number. If f: $GF(p)^n \longrightarrow GF(p)$, then f can be uniquely expressed in the following form, called the *algebraic normal form* (ANF):

$$f(x_1, x_2, \ldots, x_n) = \sum_{k_1,k_2,\ldots,k_n=0}^{p-1} a_{k_1k_2\ldots k_n} {x_1}^{k_1} {x_2}^{k_2} \cdots {x_n}^{k_n},$$

where each coefficient $a_{k_1k_2\ldots k_n}$ is a constant in $GF(p)$.

The function $f(x)$ is called an *affine function* if $f(x) = a_1x_1 + \cdots + a_nx_n + a_0$. If $a_0 = 0$, $f(x)$ is also called a *linear function*. We will denote by F_n the set of all functions of n variables and by L_n the set of affine ones. We will call a function *nonlinear* if it is not in L_n.

If $f(x) \in F_n$, then $f(x)$ is a *symmetric function* if for any permutation π on $\{1, 2, \ldots, n\}$, we have $f(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$=$f(x_1, x_2, \ldots, x_n)$. The set of permutations on $\{1, 2, \ldots, n\}$ will be denoted by S_n.

We define the following equivalence relation on $GF(p)^n$: for any $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ in $GF(p)^n$, we say x and y are equivalent, and write $x \sim y$, if there exists a permutation $\pi \in S_n$ such that $(y_1, y_2, \ldots, y_n)$=$(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$ (by abuse of notation we write $y = \pi(x)$). Let $\widetilde{x} = \{y \,|\, \exists\, \pi \in S_n, \pi(x) = y\}$. Let $\overline{x} = (\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n})$ be the representative of $\widetilde{x}$, where $0 \le \overline{x_1} \le \overline{x_2} \le \cdots \le \overline{x_n} \le p - 1$. Obviously, we have $\widetilde{x} = \widetilde{y} \iff \overline{x} = \overline{y}$.

III. Enumeration Results

Definition 1: f: $GF(p)^n \longrightarrow GF(p)$ is *balanced* if the probability $prob(f(x) = k) = \frac{1}{p}$ for any $k = 0, 1, \ldots, p - 1$. As an immediate consequence, f is balanced if and only if $\#\{x \in GF(p)^n | f(x) = k\} = p^{n-1}$.

Using the equivalence relation of the previous section, we get that f: $GF(p)^n \longrightarrow GF(p)$ is symmetric if $f(x) = f(y)$ whenever $\widetilde{x} = \widetilde{y}$. Let $C(n, k) = \frac{n!}{k!(n-k)!}$ if $0 \le k \le n$ and 0 otherwise be the usual binomial coefficients. Then we have

Lemma 1: The number of n-variable symmetric polynomials over $GF(p)$ is

$$p^{C(p+n-1,n)}.$$

Proof: The number of different vector classes $\widetilde{x}$ is the number of solutions of the linear equation $i_0+i_1+\cdots+i_{p-1} = n$, where i_k is the number of times k appears in $\overline{x}$. We know that the number of solutions to the previous linear diophantine equation is the same as the number of n-combinations of a set with p elements, that is $C(p+n-1, n)$ (see [3, p. 69]). Since a symmetric function $f(x)$ has the same value for any element of $\widetilde{x}$, the lemma is proved. ∎

Lemma 2: We have $\prod_{k=0}^{p-1} C((k+1)a, a) = \frac{(pa)!}{(a!)^p}$.

Manuscript received August, 2006.

*This work was supported by the Naval Postgraduate School RIP funding.

T.W. Cusick is with SUNY, Department of Mathematics, 244 Mathematics Building, Buffalo, NY 14260; Yuan Li is with Department of Mathematical Sciences, Alcorn State University, Alcorn State, MS 39096; P. Stănică is with Applied Mathematics Department, Naval Postgraduate School, Monterey, CA 93943

Proof: It is a straightforward computation

$$\prod_{k=0}^{p-1} C((k+1)a,a) = \frac{a!}{a!}\frac{(2a)!}{a!a!}\cdots\frac{(pa)!}{a!((p-1)a)!} = \frac{(pa)!}{(a!)^p}.$$

■

Lemma 3: The number of n-variable balanced polynomials over $GF(p)$ is

$$\frac{(p^n)!}{(p^{n-1}!)^p}.$$

Proof: The number we are looking for is

$$C(p^n,p^{n-1})C(p^n-p^{n-1},p^{n-1})\cdot \cdots C(p^n-(p-1)p^{n-1},p^{n-1}) = \frac{(p^n)!}{(p^{n-1}!)^p},$$

using Lemma 2, and the claim is proved. ■

Let $\overline{x} = (\underbrace{0,\ldots,0}_{i_0},\underbrace{1,\ldots,1}_{i_1},\ldots,\underbrace{p-1,\ldots,p-1}_{i_{p-1}})$, where $i_0+i_1+\cdots+i_{p-1}=n$, $0\leq i_j\leq n$, $j=0,1,\ldots,p-1$. The cardinality of the set $\widetilde{x}$ is the value of the multinomial coefficient $C(n,i_0,i_1,\ldots,i_{p-2}) = \frac{n!}{i_0!i_1!\cdots i_{p-1}!}$. We have the following widely known multinomial expansion lemma.

Lemma 4: [3, p. 123] We have the following formula

$$(t_0+t_1+\cdots+t_{p-1})^n = \sum_{i_0+i_1+\cdots+i_{p-1}=n} C(n,i_0,i_1,\ldots,i_{p-2})t_0^{i_0}t_1^{i_1}\cdots t_{p-1}^{i_{p-1}}.$$

By specializing $t_0=t_1=\cdots=t_{p-1}=1$, we get the following corollary.

Corollary 1: The n-th power of p satisfies

$$p^n = \sum_{i_0+i_1+\cdots+i_{p-1}=n} C(n,i_0,i_1,\ldots,i_{p-2}).$$

From the proof of Lemma 1, we know that the number of terms in the sum in Corollary 1 is $C(p+n-1,n)$. It is clear now, that to get balanced symmetric polynomials amounts to partitioning the set of $C(p+n-1,n)$ many multinomial coefficients $C(n,i_0,i_1,\ldots,i_{p-2})$ into p groups, the sum of each group being equal to p^{n-1}.

For a fixed solution $\{i_0,i_1,\ldots,i_{p-1}\}$ of $i_0+i_1+\cdots+i_{p-1}=n$, there are $\frac{p!}{m_0!m_1!\cdots m_n!}$ many ways to order it, where $i_j\in\{0,1,\ldots,n\}$, and m_l is the number of times that l appears in $\{i_0,\ldots,i_{p-1}\}$, $0\leq l\leq n$. Hence,

$$m_0+m_1+\cdots+m_n=p, \text{ and } 0m_0+1m_1+\cdots+nm_n=n. \quad (1)$$

Let us consider the following map:

$$F:\quad \{\{i_0,i_1,\ldots,i_{p-1}\}|\sum_{j=0}^{p-1} i_j = n\} \to \{(m_0,m_1,\ldots,m_n)|\sum_{l=0}^{n} m_l = p, \sum_{l=0}^{n} lm_l = n\}$$

defined by

$$F(\{i_0,i_1,\ldots,i_{p-1}\}) = (m_0,m_1,\ldots,m_n),$$

where m_l is as above. It is not hard to check that F is a bijection.

Now, we will partition the set of multinomial coefficients $C(n,i_0,\ldots,i_{p-2})$ using the following equivalence relation: $C(n,i_0,\ldots,i_{p-2})$ and $C(n,j_0,\ldots,j_{p-2})$ belong to the same class if and only if $j_0,\ldots,j_{p-1}$ is a permutation of $i_0,\ldots,i_{p-1}$. Of course, any element in the same class has the same value. So, we can think of F as a map that assigns to each class the value $\frac{p!}{m_0!m_1!\cdots m_n!}$.

Lemma 5: Let n,p be positive integers, with p a prime number. If $m_i<p$ for some i (and so for all i), or if $\gcd(n,p)=1$, then p divides $\frac{p!}{m_0!m_1!\cdots m_n!}$.

Proof: Assume $m_i<p$. By a known extension of Kummer's result that belongs to Dickson (see [11, Theorem D, p. 3860]) the power of p that divides the multinomial coefficient equals the number of carries when we add $m_0+m_1+\cdots+m_n$ in base p, but the mentioned sum is equal to p, therefore the number of carries is 1. (One can also prove the same assertion without using Dickson's result.)

Now, assume $\gcd(n,p)=1$. If $m_i<p$, the first part of the proof proves the claim. Assume $m_i\geq p$. Since $m_0+m_1+\cdots+m_n=p$, we can find j such that $m_j=p$ and $m_0=\cdots=m_{j-1}=m_{j+1}=\cdots m_n=0$. From the definition of the m_i's we obtain that $jp=n$, which is a contradiction. ■

Remark 1: The two conditions $m_i<p$, and $\gcd(n,p)=1$ are not equivalent (although, it is true that $\gcd(n,p)=1$ implies $m_i<p$). For instance, by taking $m_0=3, m_1=2, m_2=1, m_3=1, m_4=m_5=m_6=m_7=0$, we get $m_0+m_1+\cdots+m_7=p=7=n=0m_0+1m_1+\cdots+7m_7$, so $p=n$ in this case.

Since the cardinality of each multinomial coefficient class is a multiple of p, we can divide each class into p groups with an equal number of coefficients, hence, equal sum. Doing the same for each class, we finally partition all of the $C(p+n-1,n)$ coefficients into p groups with equal sum.

For a given $(m_0,m_1,\ldots,m_n)$, $m_0+m_1+\cdots+m_n=p$, $0m_0+1m_1+\cdots+nm_n=n$, the partition number is

$$C\left(\frac{p!}{m_0!m_1!\cdots m_n!},\frac{(p-1)!}{m_0!m_1!\cdots m_n!}\right)\cdot$$
$$C\left(\frac{p!}{m_0!m_1!\cdots m_n!}-\frac{(p-1)!}{m_0!m_1!\cdots m_n!},\frac{(p-1)!}{m_0!m_1!\cdots m_n!}\right)\cdots$$
$$C\left(\frac{p!}{m_0!m_1!\cdots m_n!}-\frac{k(p-1)!}{m_0!m_1!\cdots m_n!},\frac{(p-1)!}{m_0!m_1!\cdots m_n!}\right)\cdots$$
$$C\left(\frac{(p-1)!}{m_0!m_1!\cdots m_n!},\frac{(p-1)!}{m_0!m_1!\cdots m_n!}\right).$$

By Lemma 2, this product can be written as

$$\frac{(\frac{p!}{m_0!\cdots m_n!})!}{((\frac{(p-1)!}{m_0!\cdots m_n!})!)^p}.$$

In conclusion, we get our main result of this section.

Theorem 1: Let N be the number of n-variable balanced symmetric functions over $GF(p)$. If $m_i<p$, for all i (or $\gcd(n,p)=1$), then

$$N \geq \prod_{\substack{\sum_{j=0}^n m_j = p\\ \sum_{j=0}^n jm_j = n}} \frac{(\frac{p!}{m_0!\cdots m_n!})!}{((\frac{(p-1)!}{m_0!\cdots m_n!})!)^p}.$$

To illustrate the previous theorem, we take the following example, $p=3, n=4$. It is rather straightforward to check that the only solutions $(m_0, m_1, m_2, m_3, m_4)$ for (1) are $(2,0,0,0,1)$, $(1,1,0,1,0)$, $(0,2,1,0,0)$, $(1,0,2,0,0)$. Thus, the bound of Theorem 1 implies (we ignore the factors 1! or 0!) that the number of balanced symmetric functions on $GF(3)^4$ is

$$N \geq \frac{\left(\frac{3!}{2!}\right)!}{\left(\frac{2!}{2!}\right)!^3} \cdot \frac{(3!)!}{(2!)!^3} \cdot \frac{\left(\frac{3!}{2!}\right)!}{\left(\frac{2!}{2!}\right)!^3} \cdot \frac{\left(\frac{3!}{2!}\right)!}{\left(\frac{2!}{2!}\right)!^3} = 19440 \approx 3^{8.988}.$$

Next, since the linear balanced symmetric polynomials over $GF(p)$ have the form $a(x_1+\cdots+x_n)+b$, where $a \in GF(p)^*$ and $b \in GF(p)$, we get that the number of such functions is $p(p-1)$. Since $\frac{(pa)!}{(a!)^p} = \frac{a!}{a!}\frac{(2a)!}{a!a!}\cdots\frac{(pa)!}{a!((p-1)a)!} > 1\cdot 2\cdots p = p! \geq p(p-1)$, we have the next corollary.

Corollary 2: If n is not divisible by p, there exists a nonlinear n-variable balanced symmetric polynomial over $GF(p)$.

IV. The balancedness of elementary symmetric polynomials over $GF(2)$

In this section we consider the binary case, that is, $p = 2$. Here, we shall try to find all nonlinear balanced elementary symmetric polynomials. Throughout this section, $x = (x_1, \ldots, x_n)$.

Definition 2: For integers n and d, $1 \leq d \leq n$ we define the elementary symmetric polynomial by

$$X(d,n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_d \leq n} x_{i_1} x_{i_2} \cdots x_{i_d}. \tag{2}$$

By abuse of notation, we let $X(d,n)(j)$ be the value of $X(d,n)$ when $wt(x) = j$. Since $X(d,n)(j) \equiv C(j,d) \pmod 2$, we get

$$X(d,n)(j) = \frac{1-(-1)^{C(j,d)}}{2}.$$

Because there are $C(n,j)$ many vectors with weight j, we have the following result.

Lemma 6: The elementary symmetric polynomial $X(d,n)$ is balanced if and only if

$$\sum_{0 \leq j \leq n} C(n,j)(-1)^{C(j,d)} = 0.$$

Theorem 2: If $X(d,n)$ is balanced, then $d \leq \lceil n/2 \rceil$.

Proof: If n is even and $d \geq \frac{n}{2}+1$, then

$$\sum_{C(j,d)\equiv 0 \pmod 2} C(n,j) > C(n,0) + C(n,1) + \cdots + C(n,n/2) > 2^{n-1}.$$

If n is odd and $d \geq \frac{n+1}{2}+1$, then

$$\sum_{C(j,d)\equiv 0 \pmod 2} C(n,j) > C(n,0) + C(n,1) + \cdots + C(n,(n+1)/2) > 2^{n-1}.$$

In both cases, we have

$$\begin{aligned}
&\sum_{0 \leq j \leq n} C(n,j)(-1)^{C(j,d)} \\
&= \sum_{C(j,d)\equiv 0 \pmod 2} C(n,j) - \sum_{C(j,d)\equiv 1 \pmod 2} C(n,j) \\
&= \sum_{C(j,d)\equiv 0 \pmod 2} C(n,j) - \left(2^n - \sum_{C(j,d)\equiv 0 \pmod 2} C(n,j)\right) \\
&= 2\left(\sum_{C(j,d)\equiv 0 \pmod 2} C(n,j) - 2^{n-1}\right) > 0,
\end{aligned}$$

contradicting Lemma 6. ∎

Therefore, we see from Lemma 6 that the existence of balanced elementary symmetric polynomials is related to the problem of bisecting binomial coefficients (defined below). In [4], two of us found some computational results about such bisections, which results we shall describe below. (We mention here that the authors of [18] found the number of solutions but without the explicit solutions.) It was suspected that the existence of nontrivial binomial coefficient bisections (as in [4]) may cause difficulties in the study of the existence of balanced symmetric polynomials, but we conjecture that this is not true for the elementary symmetric case.

We begin with

Definition 3: [4] If $\sum_{i=0}^{n} \delta_i C(n,i) = 0$, $\delta_i \in \{-1,1\}$, $i = 0,1,\ldots,n$, we call $(\delta_0,\ldots,\delta_n)$ a solution of the equation

$$\sum_{i=0}^{n} x_i C(n,i) = 0, \quad x_i \in \{-1,1\}. \tag{3}$$

In fact, whenever we get a solution of (3), we get a bisection of binomial coefficients, that is, we find A, B such that $A \cup B = \{0,1,\ldots,n\}$, $A \cap B = \emptyset$, $\sum_{i\in A} C(n,i) = \sum_{i\in B} C(n,i) = 2^{n-1}$.

Obviously, if n is even, then $\pm(1,-1,1,-1,\ldots,1)$ are two solutions of (3). If n is odd, then $(\delta_0,\ldots,\delta_{\frac{n-1}{2}}, -\delta_{\frac{n-1}{2}-1},\ldots,-\delta_0)$ are $2^{\frac{n+1}{2}}$ solutions of (3). We call these trivial solutions.

Mitchell [17] mentioned the nontrivial solutions for $n = 8, 13$. In [4], two of us found all solutions of (3) when $n \leq 28$, and, it turns out, nontrivial solutions exist if and only if $n = 8, 13, 14, 20, 24, 26$ in this range. In [9], using a computer search, von zur Gathen and Roche found all nontrivial solutions for $n \leq 128$. It turns out that nontrivial solutions up to 128 exist for odd n if n belongs to $\{13, 29, 31, 33, 35, 41, 47, 61, 63, 73, 97, 103\}$ and for even n if n belongs to $\{24, 34, 48, 54\}$, plus the values $n = 6t+2, 1 \leq t \leq (n-4)/4$.

We note that the authors of [18], [19] also found lower bounds for the case $p = 2$ on the number of balanced symmetric Boolean functions. For n even, there was no improvement on the trivial bound, namely 2, but for n odd, the bound $1.125\cdot 2^{(n+1)/2}$ (strictly larger than the simple bound $2^{(n+1)/2}$) was determined. So, here we ask the question of determining necessary and sufficient conditions on the parameter n such that there exist nonlinear balanced symmetric polynomials on $GF(2)^n$.

First, we recall a known result that enables one to find residues of binomial coefficients modulo a prime p.

Lemma 7 (Lucas' Theorem): Let $n = a_m p^m + a_{m-1}p^{m-1} + \cdots + a_1 p + a_0$ with $0 \le a_i \le p-1$ and $k = b_m p^m + b_{m-1}p^{m-1} + \cdots + b_1 p + b_0$ with $0 \le b_i \le p-1$, then $C(n,k) \equiv C(a_m,b_m)\cdots C(a_1,b_1) \pmod p$

The next lemma can be derived from [1]. However, here we give a direct proof.

Lemma 8: For any integer $d \ge 2$, the sequence $\{(-1)^{C(j,d)}\}_{j=0}^{\infty}$ is periodic of least period $2^{\lfloor \log_2 d \rfloor + 1}$.

Proof: First, recall that d has at most $\lfloor \log_2 d \rfloor + 1$ bits. For $0 \le i \le 2^{\lfloor \log_2 d \rfloor + 1} - 1$, according to Lemma 7, we have $C(i + 2^{\lfloor \log_2 d \rfloor + 1}, d) \equiv C(1,0)C(i,d) \equiv C(i,d) \pmod 2$, so the least period is a divisor of $2^{\lfloor \log_2 d \rfloor + 1}$. On the other hand, $1 = C(d,d)$ and $C(d + 2^{\lfloor \log_2 d \rfloor}, d) \equiv C(1,0)C(0,1)\cdots \equiv 0 \pmod 2$, which implies that $2^{\lfloor \log_2 d \rfloor}$ cannot be a period. The lemma is proved. ∎

With the help of Lemma 8, we get the following computational results. The list could easily be extended. The notation $\overline{abc\ldots}$ stands for an infinite sequence with period $abc\ldots$.

Lemma 9: We have

$\{\frac{1-(-1)^{C(j,2)}}{2}\}_{j=0}^{\infty} = \overline{0011}$

$\{\frac{1-(-1)^{C(j,3)}}{2}\}_{j=0}^{\infty} = \overline{0001}$

$\{\frac{1-(-1)^{C(j,4)}}{2}\}_{j=0}^{\infty} = \overline{00001111}$

$\{\frac{1-(-1)^{C(j,5)}}{2}\}_{j=0}^{\infty} = \overline{00000101}$

$\{\frac{1-(-1)^{C(j,6)}}{2}\}_{j=0}^{\infty} = \overline{00000011}$

$\{\frac{1-(-1)^{C(j,7)}}{2}\}_{j=0}^{\infty} = \overline{00000001}$

$\{\frac{1-(-1)^{C(j,8)}}{2}\}_{j=0}^{\infty} = \overline{0000000011111111}$

$\{\frac{1-(-1)^{C(j,9)}}{2}\}_{j=0}^{\infty} = \overline{0000000001010101}$

$\{\frac{1-(-1)^{C(j,10)}}{2}\}_{j=0}^{\infty} = \overline{0000000000110011}$

$\{\frac{1-(-1)^{C(j,11)}}{2}\}_{j=0}^{\infty} = \overline{0000000000010001}$

$\{\frac{1-(-1)^{C(j,12)}}{2}\}_{j=0}^{\infty} = \overline{0000000000001111}$

$\{\frac{1-(-1)^{C(j,13)}}{2}\}_{j=0}^{\infty} = \overline{0000000000000101}$

$\{\frac{1-(-1)^{C(j,14)}}{2}\}_{j=0}^{\infty} = \overline{0000000000000011}$

Theorem 3: If t, ℓ are positive integers, then $X(2^t, 2^{t+1}\ell - 1)$ is balanced.

Proof: First, $C(j, 2^t) = 0$ when $0 \le j \le 2^t - 1$. By Lucas' Theorem, we have

$$C(j,2^t) \equiv 1 \pmod 2 \text{ when } 2^t \le j \le 2^{t+1} - 1.$$

By Lemma 8, the period of $\{(-1)^{C(j,2^t)}\}_{j=0}^{\infty}$ is 2^{t+1}. Hence, we get the sequence $\{(-1)^{C(j,2^t)}\}_{j=0}^{2^{t+1}\ell-1}$ by repeating $\underbrace{++\cdots+}_{2^t}\underbrace{--\cdots-}_{2^t}$ exactly ℓ times. Obviously $\{(-1)^{C(j,2^t)}\}_{j=0}^{2^{t+1}\ell-1}$ is a (trivial) solution of the equation $\sum_{i=0}^{n} x_i C(n,i) = 0$ when $n = 2^{t+1}\ell - 1$. Using Lemma 6 we obtain our result. ∎

Finally, we conjecture that the functions in Theorem 3 are the only balanced ones.

Conjecture 1. *There are no nonlinear balanced elementary symmetric polynomials except for $X(2^t, 2^{t+1}\ell - 1)$, where t and ℓ are any positive integers.*

Acknowledgment

The authors would like to thank the referees who made some much appreciated suggestions.

References

[1] A. Canteaut and M. Videau, "Symmetric Boolean Functions", *IEEE Trans. on Information Theory* 51 (2005), 2791–2811.

[2] C. Carlet, "On the degree, nonlinearity, algebraic thickness, and nonnormally of Boolean functions, with developements on symmetric functions", *IEEE Trans. on Information Theory* 50 (2004), 2178–2185.

[3] C.A. Charalambides, "Enumerative Combinatorics", New York, *CRC Press,* 2002.

[4] T.W. Cusick and Yuan Li "k-th Order Symmetric SAC Boolean Functions and Bisecting Binomial Coefficients", *Discrete Applied Mathematics* 149 (2005), 73–86.

[5] Ed Dawson and Chuan-kun Wu, "On the Linear Structure of Symmetric Boolean Functions", *Australasian Journal of Combinatorics* 16 (1997), 239–243.

[6] C. Ding, G. Xiao and W. Shan, "The Stability Theory of Stream Ciphers", Springer-Verlag LNCS 561, Section 4.5, 1991.

[7] Keqin Feng and Fengmei Liu, "New Results On The Nonexistence of Generalized Bent Functions", *IEEE Trans.on Information Theory* 49 (2003), 3066–3071.

[8] K. Gopalakrishnan, D.G. Hoffman and D.R. Stinson, "A Note on a Conjecture Concerning Symmetric Resilient Functions", *Information Processing Letters* 47 (1993), 139–143.

[9] J. von zur Gathen and J. Roche, "Polynomials wih two values", *Combinatorica* 17, no. 3 (1997), 345–362.

[10] Yupu Hu and Guozhen Xiao "Resilient Functions Over Finite Fields", *IEEE Trans. on Information Theory* 49 (2003), 2040–2046.

[11] J.M. Holte, "Asymptotic prime-power divisibility of binomial, generalized binomial, and multinomial coefficients", *Trans. Amer. Math. Soc.* 349 (1997), no. 10, 3837–3873.

[12] P.V. Kumar, R.A. Scholtz, and L.R. Welch, "Generalized Bent Functions and Their Properties", *J. Combinatorial Theory (A)* 40 (1985), 90–107.

[13] Yuan Li and T.W. Cusick, "Strict Avalanche Criterion over Finite Fields", *Journal of Mathematical Cryptology* 1 (2007), 65–78.

[14] Yuan Li and T.W. Cusick, "Linear Structures of Symmetric Functions over Finite Fields", *Information Processing Letters* 97 (2006), 124–127.

[15] Mulan Liu, Peizhong Lu and G.L. Mullen, "Correlation-Immune Functions over Finite Fields", *IEEE Trans. on Information Theory* 44 (1998), 1273–1276.

[16] S. Maitra and P. Sarkar, "Maximum Nonlinearity of Symmetric Boolean Functions on Odd Number of Variables", *IEEE Trans. on Information Theory* 48 (2002), 2626–2630.

[17] C. Mitchell, "Enumerating Boolean Functions of Cryptographic Significance", *Journal of Cryptology* 2 (1990), 155–170.

[18] P. Sarkar and S. Maitra, "Balancedness and Correlation Immunity of Symmetric Boolean Functions", *Proceedings of the R.C. Bose Centenary Symposium, Electronic Notes in Discrete Mathmatics*, 15 (2003), 178–183.

[19] P. Sarkar and S. Maitra, "Balancedness and Correlation Immunity of Symmetric Boolean Functions", Cryptology Research Group, Indian Statistical Institute, Technical Report Number CRG/2002/09, Nov 18, 2002. *http://www.isical.ac.in/~crg/tech_reports/tech9.ps*

[20] P. Savicky, "On the Bent Boolean Functions That Are Symmetric", *Europ. J. Comb.* 15 (1994), 407–410.

[21] Y.X. Yang and B. Guo, "Futher Enumerating Boolean Functions of Cryptographic Significance", *Journal of Cryptology* 8 (3), 1995, 115–122.

[22] Chuan-kun Wu and Ed Dawson, "Correlation Immunity and Resiliency of Symmetric Boolean Functions", *Theoretical Computer Science* 312 (2004), 321–335.