Title	On the balanced elementary symmetric Boolean functions
Author(s)	Qu, Longjiang; Dai, Qingping; Li, Chao
Citation	Qu, L., Dai, Q., & Li, C. (2013). On the Balanced Elementary Symmetric Boolean Functions. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E96.A(2), 663-665.
Date	2013
URL	http://hdl.handle.net/10220/18451
Rights	

LETTER

On the Balanced Elementary Symmetric Boolean Functions*

Longjiang QU[†,††a)], ***Member***, **Qingping DAI**[†], ***and*** **Chao LI**[†,†††], ***Nonmembers***

SUMMARY In this paper, we give some results towards the conjecture that $\sigma_{2^{t+1}l-1,2^t}$ are the only nonlinear balanced elementary symmetric Boolean functions where t and l are positive integers. At first, a unified and simple proof of some earlier results is shown. Then a property of balanced elementary symmetric Boolean functions is presented. With this property, we prove that the conjecture is true for $n = 2^m + 2^t - 1$ where $m, t(m > t)$ are two non-negative integers, which verified the conjecture for a large infinite class of integer n.

key words: *algebraic degree, Boolean functions, elementary symmetric, balanced*

1. Introduction

Symmetric Boolean functions are an interesting and fairly important class of Boolean functions. They have good cryptographic properties. The fact that an n-variable symmetric Boolean function can be entirely described by an $n + 1$-bit vector considerably reduces the amount of memory required for storing the function and is of great interest in software applications. On the other hand, as symmetric functions are the only functions having a known implementation with a number of gates which is linear in the number of input variables, they might be good candidates in term of implementation complexity. Therefore, it is of great importance to find symmetric Boolean functions with significant cryptographic properties such as high nonlinearity, high algebraic degree and high AI. Some cryptographically significant properties of symmetric Boolean functions have been studied in [1], [2], [10], [11], [15], [16]. It was proved that the maximum nonlinearity of n-variable symmetric Boolean functions can only be achieved by quadratic symmetric functions [15]. In [1], Canteaut and Videau established an interesting link between the periodicity of simplified value vector of a symmetric function and its degree, with which they gave some general results on the cryptographic properties of symmetric functions, such as balancedness, resiliency, propagation and nonlinearity. Recently, constructions of symmetric Boolean functions with high algebraic immunity have been studied by several researchers, see [11]–[13] etc.

Balancedness is a primary requirement for functions in cryptosystem. Enumeration of balanced symmetric Boolean functions has always been an important problem [10], [14], [16]. The conjecture [5] that balanced symmetric functions of fixed degree do not exist when the number of variables grows remains open. For elementary symmetric Boolean functions, Cusick et al. [4] proposed the following conjecture:

Conjecture 1. There are no nonlinear balanced elementary symmetric Boolean functions except for $\sigma_{2^{t+1}l-1,2^t}$, where t and l are positive integers, $\sigma_{n,d} = \bigoplus_{1\le i_1<\cdots<i_d\le n} x_{i_1}\cdots x_{i_d}$.

They also obtained many results towards the conjecture later in [5]. A major progress on this conjecture is made by Castro and Medina. They proved that if d is not a power of 2, then $\sigma_{n,d}$ is not balanced for all sufficiently large n [3]. Thus combining a result(see Lemma 3.3 in Sect. 3) by Cusick et al., only an (undetermined) finite number of cases of the conjecture remain unsolved. In a recent paper, G. Gao, W. Liu and X. Zhang [8] proved that for $n = 2^{t+1}l - 1$ with odd l, if $2^{t+1} \nmid d$, then $\sigma_{n,d}$ is balanced if and only if $d = 2^k, 1 \le k \le t$. More recently, Y. Guo, G. Gao and Y. Zhao [9] proved that there are no trivial balanced elementary symmetric Boolean functions except for $\sigma_{2^{t+1}l-1,2^t}$, where t and l are positive integers. That is, Conjecture 1 is correct for all trivial balanced elementary Boolean functions.

In this paper, a theorem which unified all the results in [8] is given, a new and simple proof of this theorem is then presented. After that, a property of balanced elementary symmetric Boolean functions is presented. With this property, the conjecture is proved to be true for $n = 2^m+2^t-1$ where $m, t(m > t)$ are two non-negative integers. The first contribution of this work is that it proved the conjecture for a large infinite class of integer n. Also our results give a simple condition for an elementary symmetric Boolean function to be balanced, and may provide a different insight to this conjecture. The second contribution is the method used in this paper. It may also be helpful for some other problems on symmetric Boolean functions.

Manuscript received September 6, 2012.
Manuscript revised November 7, 2012.

[†]The authors are with the Department of Mathematics and System Science, College of Science, National University of Defense Technology, ChangSha, 410073, P.R. China.

[††]The author is with Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore.

[†††]The author is with Institute of Network and Information Security, School of Computer Science, National University of Defense Technology, Changsha, 410073, P.R. China.

*The work in this paper is supported by the National Natural Science Foundation of China (No. 61070215, 61272484), the Singapore National Research Foundation Competitive Research Program grant NRF-CRP2-2007-03 and the National Basic Research Program of China (Grant No. 2009CB32050003).

a) E-mail: 12054375@qq.com

DOI: 10.1587/transfun.E96.A.663

2. Preliminaries

Let $\mathbb{F}_2$ be the binary finite field, and the vector space of dimension n over $\mathbb{F}_2$ is denoted by $\mathbb{F}_2^n$. An n-variable Boolean function is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The set of all n-variable Boolean functions is denoted by $\mathbb{B}_n$. For any $f \in \mathbb{B}_n$, f can be uniquely represented as

$$f(X) = f(x_1, \cdots, x_n) = \bigoplus_{I \subseteq \{1,\cdots,n\}} a_I \prod_{i \in I} x_i (a_I \in \mathbb{F}_2) \quad (1)$$

which is called the algebraic normal form(ANF) of f. In this paper, "$\oplus$" and "+" denote the addition modulo 2 and the usual integer addition respectively. The algebraic degree of $f \neq 0$, denoted by $\deg(f)$, is the maximum degree of the monomials in (1) whose coefficients are nonzero. All the Boolean functions with algebraic degree no more than 1 are called affine functions. The set of all n-variable affine functions is denoted by $A(n)$. We call a function nonlinear if it is not in $A(n)$. The set $\mathrm{supp}(f)$ is the subset of $\mathbb{F}_2^n$ where f takes the value 1. The Hamming weight of f is $\mathrm{wt}(f) = |\mathrm{supp}(f)|$. A Boolean function $f \in \mathbb{B}_n$ is called balanced if $\mathrm{wt}(f) = 2^{n-1}$.

An n-variable Boolean function is called symmetric if its output is invariant under any permutation of its input bits. Equivalently, the output of f only depends on the weight of its input vector. Thus a symmetric function can be represented by a vector $(v_f(0), \cdots, v_f(n))$, where $v_f(i) = f(x)$ for $x \in \mathbb{F}_2^n$ with Hamming weight i. On the other hand, the ANF of a symmetric function can also be represented as $f(x_1, \cdots, x_n) = \bigoplus_{d=0}^{n} \lambda_d \sigma_{n,d}$, where $\lambda_d \in \mathbb{F}_2$ and $\sigma_{n,d} = \bigoplus_{1 \le i_1 < \cdots < i_d \le n} x_{i_1} \cdots x_{i_d}$ is the d-th elementary symmetric Boolean function with n variables. If $f(x) = \sigma_{n,d}$, then $v_f(i) \equiv C(i,d) \mod 2$, where $C(i,d)$ denotes the binomial coefficients. Define $C(i,d) = 0$ if $i < d$.

For an integer u, we denote by u_i the $(i+1)$-th least significant bit of the binary expression $(u_{m-1} \cdots u_1 u_0)_2$ of u. Let $\mathrm{supp}(u) = \{0 \le i \le m-1 | u_i = 1\}$, and denote by $wt(u)$ the cardinality of $\mathrm{supp}(u)$. Let u, v be positive integers and their binary expressions as $u = (u_{m-1} \cdots u_1 u_0)_2$, $v = (v_{m-1} \cdots v_1 v_0)_2$. If $u_i \le v_i$ holds for all $0 \le i \le m-1$, we say that u is covered by v, denoted by $u \preceq v$. Otherwise, we say that u is not covered by v, denoted by $u \not\preceq v$. For a binary sequence, k consecutive zeros(or ones) preceded by one(or zero) and followed by one(or zero) is called a run of zeros(or ones) of length k.

3. Main Results

The following theorem is a union of Theorems 1, 2 and 3 of [8] with a simple proof.

Theorem 3.1: ([8]) If $n = 2^{t+1}l - 1$, l is a positive integer and $2^{t+1} \nmid d$, then $f = \sigma_{n,d}$ is balanced if and only if $d = 2^k, 0 \le k \le t$.

Proof. It is easy to verify the sufficiency. We only prove the necessity.

Now assume that $f = \sigma_{n,d}$ is balanced. We have the following claim.

Claim 1. $v_f(i) + v_f(n-i) \le 1$ holds for any integer $0 \le i \le \frac{n-1}{2}$, that is, $d \preceq i$ and $d \preceq n-i$ can not hold simultaneously.

Since $2^{t+1} \nmid d$, there must exists an integer k such that $d_k = 1$ and $0 \le k \le t$. Let $0 \le i \le \frac{n-1}{2}$, it is easy to see that $i_j + (n-i)_j = 1$ holds for all $0 \le j \le t$ since $n = 2^{t+1}l - 1 = 2^{t+1}(l-1) + (\underbrace{11\cdots1}_{t+1})_2$. In particular, $i_k + (n-i)_k = 1$ holds for all $0 \le i \le \frac{n-1}{2}$. Thus Claim (1) is proved.

Recall that by the well-known Lucas' Theorem [10, p.79], $v_f(i) = 1$ if and only if $d \preceq i$. Thus we obtain

$$\begin{aligned} wt(f) &= \sum_{i=0}^{n} C(n,i) v_f(i) = \sum_{i=0}^{\frac{n-1}{2}} C(n,i)(v_f(i) + v_f(n-i)) \\ &\le \sum_{i=0}^{\frac{n-1}{2}} C(n,i) = 2^{n-1}. \end{aligned}$$

The above equality holds if and only if $v_f(i) + v_f(n-i) = 1$ holds for all $0 \le i \le \frac{n-1}{2}$. We conclude that $d = 2^k$ must then holds. Otherwise, assume that there exists an integer $p \neq k$ such that $d_p = d_k = 1$. Let $i = 2^k$, then we have $d \not\preceq i$ since $i < d$, and we also have $d \not\preceq n-i$ since $(n-i)_k = 0$. Thus $v_f(2^k) + v_f(n-2^k) = 0$. Contradicts! We are done. □

The above proof is much easier and unified, which simplified the proofs in [8]. We hope that this proof can give much insights to these results. It is easy to see that when $l = 1, 2$, the condition $2^{t+1} \nmid d$ in Theorem 3.1 can be removed, which then proved Conjecture 1 for a particular class of integers n. However, in general the condition $2^{t+1} \nmid d$ is indispensable. Now we want to prove Conjecture 1 for a large class of integers n. To do this, we introduce the following proposition, which is a necessary condition for an elementary symmetric Boolean function to be balanced.

Proposition 3.2: Let n, d be two positive integers, $n = (n_{m-1} \cdots n_1 n_0)_2$ be the binary expression of n, and let "$n_{t+l} \cdots n_{t+2} n_{t+1}$" be a run of zeros with length l. If $f = \sigma_{n,d}$ is balanced, then

$$|\mathrm{supp}(d) \cap \{t+1, t+2, \cdots, t+l\}| \le 1.$$

Proof. Assume that $|\mathrm{supp}(d) \cap \{t+1, t+2, \cdots, t+l\}| \ge 2$, then there exist two integers $1 \le u < v \le l$ such that $d_{t+u} = d_{t+v} = 1$. Since "$n_{t+l} \cdots n_{t+2} n_{t+1}$" is a run of zeros with length l, we know that $n_{t+v} = n_{t+v-1} = \cdots = n_{t+u} = 0$. We first prove the following claim.

Claim 2. $v_f(i) + v_f(n-i) \le 1$ holds for any integer $0 \le i \le n$, $i \neq \frac{n}{2}$, that is, $d \preceq i$ and $d \preceq n-i$ can not hold simultaneously.

We prove this claim by contradiction. Assume that there exists an integer $j \neq \frac{n}{2}$ such that $d \preceq j$ and $d \preceq n-j$. Then we have

$$j_{t+u} = j_{t+v} = (n-j)_{t+u} = (n-j)_{t+v} = 1.$$

Now let us consider the binary expression of the equation $n = j + (n-j)$.

If $v = u + 1$, then we get

$$n_{t+v} \equiv j_{t+v} + (n-j)_{t+v} + 1 \equiv 1 + 1 + 1 \equiv 1 \mod 2,$$

where the third summation of the above equation is a carry. This contradicts with $n_{t+v} = 0$. Now we assume that $v \geq u + 2$. Since $n_{t+u+1} = 0$ and $j_{t+u} = (n-j)_{t+u} = 1$, we have $j_{t+u+1} + (n-j)_{t+u+1} = 1$ and it carries 1 to the $t + u + 2$ bit. Similarly, $j_{t+u+2} + (n-j)_{t+u+2} = 1$ and it carries 1 to the $t + u + 3$ bit since $n_{t+u+2} = 0$. And so on. Finally we get $j_{t+v-1} + (n-j)_{t+v-1} = 1$ and it carries 1 to the $t + v$ bit. Thus we have

$$n_{t+v} \equiv j_{t+v} + (n-j)_{t+v} + 1 \equiv 1 + 1 + 1 \equiv 1 \mod 2,$$

contradiction! Then we proved Claim (2).

Note that if n is even, then $d \not\leq \frac{n}{2}$ since $(\frac{n}{2})_{t+u} = 0$. Hence by Claim (1), we have

$$\begin{aligned} wt(f) &= \sum_{i=0}^{n} C(n,i) v_f(i) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} C(n,i)(v_f(i) + v_f(n-i)) \\ &\leq \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} C(n,i) \leq 2^{n-1}. \end{aligned}$$

Note that it is clear that $d \not\leq 2^{t+v}, n - 2^{t+v}$. Thus the above equality can not hold, which contradicts with the assumption that f is balanced. We finish the proof. □

The following lemma is a result of [5], which followed from Lemma 3.1, Corollary 3.10, Lemma 3.12 and Lemma 3.17 of [5].

Lemma 3.3: If $\sigma_{n,d}$ is balanced where $d = 2^t$, t is a positive integer, then there exists a positive integer l such that $n = 2^{t+1}l - 1$.

Combining Proposition 3.2 and Lemma 3.3, one can easily deduces the following result.

Corollary 3.4: If $n = 2^m$ where m is a positive integer. Then $\sigma_{n,d}$ is balanced if and only if $d = 1$.

Further, one can get the following theorem.

Theorem 3.5: Let $n = 2^m + 2^t - 1$, where m, t are positive integers such that $m > t$, and let d be a positive integer. Then $f = \sigma_{n,d}$ is balanced if and only if $d = 2^k, 0 \leq k \leq t - 1$.

Proof. It suffices to prove the necessity.

Now assume that f is balanced. By Theorem 3.1, the theorem is true if $2^t \nmid d$. We then assume that $2^t \mid d$. By Proposition 3.2, we have $|\text{supp}\,(d) \cap \{t, t+1, \cdots, m-1\}| \leq 1$. Thus we just need to prove that $f = \sigma_{n,d}$ is not balanced for any $d = 2^k, t \leq k \leq m - 1$. Hence the desired result follows from Lemma 3.3. □

Unlike the former results of [5], [8] which proved Conjecture 1 under some conditions on d, Theorem 3.5 proves the conjecture for a large infinite class of integer n.

4. Conclusion

Symmetric Boolean functions are of importance in cryptographic applications. This paper presents some results about the nonexistence of balanced elementary symmetric Boolean functions. We would hope that our method will provide further progress on the conjecture and may be helpful to other problems on symmetric Boolean functions.

Acknowledgments

The authors would like to thank Prof. Thomas Cusick for his interests and encouragements on this work, and for bringing [3] to their attention.

References

[1] A. Canteaut and M. Videau, "Symmetric Boolean functions," IEEE Trans. Inf. Theory, vol.51, no.8, pp.2791–2811, 2005.
[2] C. Carlet, "On the degree, nonlinearity, algebraic thickness and nonormality of Boolean function, with developments on symmetric functions," IEEE Trans. Inf. Theory, vol.50, no.9, pp.2178–2185, 2004.
[3] F. Castro and L. Medina, "Linear recurrences and asymptotic behavior of exponential sums of symmetric boolean functions," Electronic J. Combinatorics, vol.18, no.2, ♯P8, 2011.
[4] T. Cusick, Y. Li, and P. Stanica, "Balanced symmetric Boolean functions over $GF(p)$," IEEE Trans. Inf. Theory, vol.3, no.54, pp.1304–1307, 2008.
[5] T. Cusick, Y. Li, and P. Stanica, "On a conjecture for balanced symmetric Boolean functions," J. Math. Crypt., vol.3, no.4, pp.273–290, 2009.
[6] S. Fu, L. Qu, C. Li, and B. Sun, "Balanced rotation symmetric Boolean functions with maximum algebraic immunity," IET Inform. Secur., vol.5, no.2, pp.93–99, 2011.
[7] S. Fu, C. Li, K. Matsuura, and L. Qu, "Construction of even-variable rotation symmetric Boolean functions with maximum algebraic immunity," SCIENCE CHINA Information Sciences, DOI: 10.1007/s11432-011-4350,2012.
[8] G. Gao, W. Liu, and X. Zhang, "The degree of balanced elementary symmetric Boolean functions of $4k + 3$ variables," IEEE Trans. Inf. Theory, vol.57, no.7, pp.4822–4825, 2011.
[9] Y. Guo, G. Gap, and Y. Zhao, "Recent results on balanced symmetric Boolean functions," eprint.iacr.org/2012/093.
[10] C.J. Mitchell, "Enumerating Boolean functions of cryptographic significance," J. Cryptol., vol.2, no.3, pp.155–170, 1990.
[11] J. Peng, Q. Wu, and H. Kan, "On symmetric Boolean functions with high algebraic immunity on even number of variables," IEEE Trans. Inf. Theory, vol.57, no.10, pp.7205–7220, 2011.
[12] L. Qu and C. Li, "On the 2^m-variable symmetric Boolean functions with maximum algebraic immunity," SCIENCE CHINA Information Sciences, vol.51, no.2, pp.120–127, 2008.
[13] L. Qu, K. Feng, F. Liu, et al., "Constructing symmetric Boolean functions with maximum algebraic immunity," IEEE Trans. Inf. Theory, vol.55, no.5, pp.2406–2412, 2009.
[14] P. Sarkar and S. Maitra, "Balancedness and correlation immunity of symmetric Boolean functions," Proc. R.C. Bose Centenary Symp. Electron. Notes Discr. Math., vol.15, pp.178–183, 2003.
[15] P. Savicky, "On the bent Boolean functions that are symmetric," Eur. J. Combin., vol.15, pp.407–410, 1994.
[16] Y.X. Yang and B. Guo, "Further enumerating Boolean functions of cryptographic significance," J. Cryptol., vol.8, no.3, pp.115–122, 1995.