Balanced 15-variable Boolean Functions with Nonlinearity 16268

Selçuk Kavut and Melek D. Yücel

Electrical & Electronics Engineering Dept., Middle East Technical University, Balgat, Ankara, 06531, Turkey,
{kavut, melekdy}@metu.edu.tr

Abstract. Recently, balanced 15-variable Boolean functions with nonlinearity 16266 were obtained by suitably modifying unbalanced Patterson-Wiedemann (PW) functions, which possess nonlinearity $2^{n-1}–2^{(n-1)/2} + 20 = 16276$. In this short paper, we present an idempotent (interpreted as rotation symmetric Boolean function) with nonlinearity 16268 having 15 many zeroes in the Walsh spectrum, within the neighborhood of PW functions. Clearly this function can be transformed to balanced functions keeping the nonlinearity and autocorrelation distribution unchanged. The nonlinearity value of 16268 is currently the best known for balanced 15-variable Boolean functions.

1 Introduction

The problem of constructing balanced Boolean functions on odd number of variables having nonlinearity greater than the bent concatenation bound of $2^{n-1} - 2^{(n-1)/2}$, is an important open question in the related literature [7, 9, 10] and the references therein. Recently, in [9], balanced 15-variable Boolean functions with nonlinearity $2^{15-1} - 2^{(15-1)/2} + 10 = 16266$ were obtained by systematically modifying the structure of the PW functions in the space of rotation symmetric Boolean functions (RSBFs). Notice that the idempotents can be seen as RSBFs with proper choice of basis [1, 2]. Before [9], the structure of the PW functions had been modified using heuristic search to get balanced Boolean functions having nonlinearity $2^{15-1} - 2^{(15-1)/2} + 6 = 16262$ on 15-variables [7, 10]. Here, we present a 15-variable Boolean function f : $GF(2^n) \rightarrow GF(2)$, which is idempotent (i.e., $f(\alpha^2) = f(\alpha)$ for any $\alpha \in GF(2^n)$) with nonlinearity $2^{15-1} - 2^{(15-1)/2} + 12 = 16268$ and 15 many zeroes in its Walsh spectrum.

We use the steepest-descent like search strategy that first appeared in [5] and later modified for a search in the class of RSBFs [6]. We initialize the algorithm with PW functions, and find the function with nonlinearity 16268 and 15 many Walsh zeroes in the neighborhood of PW functions. Clearly this function can be transformed to balanced functions keeping the nonlinearity and autocorrelation distribution unchanged. The nonlinearity value of 16268 is the best known till date for balanced 15-variable Boolean functions and improves the result in [9].

2 Background

Let $f : GF(2^n) \to GF(2)$ be a Boolean function and $\zeta \in GF(2^n)$ be a primitive element. The Patterson-Wiedemann construction [8] can be interpreted in terms of the interleaved sequence [3] obtained from the 2^n-1 elements of the truth table of f organized in a specific way. The ordered sequence $\{f(1), f(\zeta), f(\zeta^2), ..., f(\zeta^{2n-2})\}$ is called the sequence associated to f with respect to ζ. Conversely, if $\mathbf{A}=\{a_0, a_1, ..., a_{m-1}\}$ where $m=2^n-1$, the function f with $f(\zeta^i)=a_i$ for $i = 0, 1, ..., m-1$ and $f(0)=0$, is called the function corresponding to the sequence $\mathbf{A}$ with respect to the primitive element ζ [3].

Definition 1. Suppose m is a composite number such that $m = d.k$ where d and k are both positive integers greater than 1, $\mathbf{A}$ is a binary sequence $\{a_0, a_1, ..., a_{m-1}\}$ where $a_i \in \{0, 1\}$ for all i, then the (d, k)-interleaved sequence $\mathbf{A}_{d,k}$ corresponding to the binary sequence $\mathbf{A}$ is defined as

$$\mathbf{A}_{d,k} = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{(d-1)} \\ a_d & a_{1+d} & a_{2+d} & \cdots & a_{(d-1)+d} \\ a_{2d} & a_{1+2d} & a_{2+2d} & \cdots & a_{(d-1)+2d} \\ . & . & . & . & . \\ . & . & . & . & . \\ a_{(k-1)d} & a_{1+(k-1)d} & a_{2+(k-1)d} & \cdots & a_{(d-1)+(k-1)d} \end{bmatrix}$$

Let $m = 2^n-1 = d.k$, then for any function $f : GF(2^n) \to GF(2)$ and a primitive element $\zeta \in GF(2^n)$, an interleaved sequence $\mathbf{A}_{d,k}$ can be constructed such that $a_{i+\lambda d} = f(\zeta^{i+\lambda d})$ for all $i = 0, 1, 2, ..., d-1$ and $\lambda = 0, 1, 2, ..., k-1$. This interleaved sequence is called the (d, k)-interleaved sequence corresponding to f with respect to ζ. The Patterson-Wiedemann construction is formally described as follows [3, 4].

Definition 2. Let n be a positive odd integer such that $n = t.q$ where both t and q are primes and $t > q$. Let the product $\mathcal{K} = GF(2^t)^*.GF(2^q)^*$ be the cyclic group of order $k = (2^t-1)(2^q-1)$ in GF(2^n). Let $\langle \phi_2 \rangle$ be the group of Frobenius automorphisms where ϕ_2 : GF(2^n) $\rightarrow$ GF(2^n) is defined by $x \rightarrow x^2$. We call a function f "Patterson-Wiedemann type" if it is invariant under the action of both $\mathcal{K}$ and $\langle \phi_2 \rangle$.

Let {0, 1, 2, ..., d–1} be the set of column numbers of the (d, k)-interleaved sequence of a Boolean function. The equivalence relation between the columns i and j, denoted by ρ_d is defined as follows:

$$i \, \rho_d \, j \Leftrightarrow \text{there exists a positive integer } s \text{ such that } i \equiv j \cdot 2^s \bmod d.$$

From Definition 2, it is deduced that (d, k)-interleaved sequence of a PW function consists of either all 0 or all 1 columns, since it is invariant under the action of $\mathcal{K}$. Further, the columns in each equivalence class with respect to ρ_d have the same value because of the invariance of the PW function under the action of $\langle \phi_2 \rangle$.

For n=15, as the PW functions can be described by (151, 217)-interleaved sequences [3]; partitioning the columns (0, 1, 2, ..., 150) with respect to the equivalence relation ρ_d, one obtains 11 equivalence classes. In the search space of size 2^{11}, there are four PW functions achieving the nonlinearity values of 16268 and 16276. For each nonlinearity, there exist exactly two PW functions which are not affine equivalent.

3 The 15-variable Function

We refer to [6] for basic definitions of nonlinearity, Walsh spectrum, Rotation Symmetric Boolean Functions RSBFs and the search strategy.

We first apply change of bases to get RSBF forms of the PW functions as in [9], using the primitive polynomial $p(x) = x^{15} + x + 1$ over GF(2) and the normal basis of $\zeta^{(2^i \cdot 29) \bmod (2^{15}-1)}$ for i = 0, 1, ..., 14 where $\zeta \in$ GF(2^{15}) is a primitive element.

We use our steepest-descent like search strategy adapted for a search in the class of RSBFs [6]. By setting the maximum iteration number to 60,000, we make four runs of the algorithm initialized with each of the four PW functions mentioned above. One of these runs has yielded a 15-variable RSBF having nonlinearity 16268 and 15 many Walsh zeroes at the 46,869th iteration step. Now we present this function after describing the initial PW function:

Let us denote the smallest column number in the j^{th} equivalence class by l_j, where j = 0, 1, ..., 10. Then, l_j's are obtained as (0, 1, 3, 5, 7, 11, 15, 17, 23, 35, 37), for j = 0 to 10 as in [3]. Consider the PW function of nonlinearity 16268 with truth table values (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) corresponding to columns numbered (l_0, l_1, ..., l_{10}). Notice that the PW functions do not contain any zeroes in the Walsh spectrum. We transform this function to an RSBF and use it to initialize the algorithm. The search strategy toggles the truth table of the PW function corresponding to the following 20 orbits, ranked in the order of increasing orbit leaders:

(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) of size 1,
(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) of size 15,
(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) of size 15,
(0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) of size 15,
(0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) of size 15,
(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) of size 15,
(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) of size 15,
(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) of size 15,
(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) of size 15,
(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) of size 5,
(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) of size 15,
(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) of size 15,
(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) of size 5,
(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) of size 15,
(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) of size 15,
(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) of size 5,
(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) of size 15,
(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) of size 5,
(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) of size 5,
(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) of size 1.

The resulting 15-variable RSBF (say f) has nonlinearity 16268 and 15 many zeroes in its Walsh spectrum corresponding to the orbit represented by w = (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1). Then $f'(x) = f(x) \oplus u \cdot x$ will be balanced, if u is an element of the orbit represented by w. The nonlinearity value of 16268 is the best known till date for balanced 15-variable Boolean functions and improves the nonlinearity result in [9]. The rotation symmetric truth table (RSTT) of the function f is given in the appendix.

References

[1] E. Filiol and C. Fontaine. Highly nonlinear balanced Boolean functions with a good correlation-immunity. In *Advances in Cryptology - EUROCRYPT'98*, Springer-Verlag, pp. 475-488, 1998.

[2] C. Fontaine. On some cosets of the First-Order Reed-Muller code with high minimum weight. *IEEE Transactions on Information Theory*, 45(4):1237–1243, 1999.

[3] S. Gangopadhyay, P. H. Keskar, and S. Maitra. Patterson–Wiedemann construction revisited. *Discrete Mathematics*, Volume 306, Issue 14, 28 July 2006, pp. 1540-1556.

[4] S. Gangopadhyay, and S. Maitra. Crosscorrelation Spectra of Dillon and Patterson-Wiedemann type Boolean Functions. IACR eprint server, http://eprint.iacr.org/2004/014, 2004.

[5] S. Kavut and M. D. Yücel. A new algorithm for the design of strong Boolean functions (in Turkish). In *First National Cryptology Symposium*, pp. 95–105, METU, Ankara, Turkey, November 18-20, 2005.

[6] S. Kavut, S. Maitra and M. D. Yücel. Search for Boolean Functions with Excellent Profiles in the Rotation Symmetric Class. *IEEE Transactions on Information Theory*, Volume IT-53(5), 1743-1751, May 2007 (an earlier version of this paper is available under the title "There exist Boolean functions on n (odd) variables having nonlinearity > $2^{n-1}-2^{(n-1)/2}$ if and only if n>7" at IACR eprint server, http://eprint. iacr.org/2006/181, May 28, 2006).

[7] S. Maitra and P. Sarkar. Modifications of Patterson-Wiedemann functions for cryptographic applications. *IEEE Transactions on Information Theory*, 48(1):278–284, January 2002.

[8] 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*, IT-29(3):354–356, 1983. See also correction in IT-36(2):443, 1990.

[9] S. Sarkar and S. Maitra. Idempotents in the neighbourhood of Patterson-Wiedemann functions having Walsh spectra zeros. *International Workshop on Coding and Cryptogrpahy*, France, 2007.

[10] P. Sarkar and S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. In *Advances in Cryptology – EUROCRYPT 2000*, LNCS 1807, pages 485–506. Springer Verlag, 2000.

Appendix
Rotation Symmetric Truth Table (RSTT) of the 15-variable Function with Nonlinearity 16268 and 15 many Walsh Zeroes

```
1110101100100101011011110000010100010100000101110100111100001111
1100110110000100101101111110101010000111011011100010010001110111
1111011000001010110111101011101010100111100000101000001111011111
1101111111011000100100110111110001010001100100111001111101000011
0110010000000110101000100110011011010010110011000010110010100110
1010100000110001101110011011001110001011010101111010011000101010
1101011011110001000000110100010100001000100011010001000000101110
1110100011101100100111000001010000011111011110011101011110001111
1100100001010010011110011011010111001001011100011101100111010010
0000011110101010101001010110010000101001100111100111101000010011
1010000110011001011110111100101110111110110000101011100000011010
1100011100010110101100001001011110011011010000110001100111011000
1110100101011001010000100110100011100010100110000111010010111110
1110110011100011110011000000010000101101101011110000011001111001
1000111010010000110111001000000100111011100111111110110011111011
0011001101111010001000000001010111001010001010111011010010010000
1110111010100011101000011000001011101111010100111010001101011101
1101111011011111001101010011110110001011100010010010011001110111
1011111000010101100001101001001101011001101000111110010101011100
1000111111000100100101110110110010111011011100010000111000011101
0010011110100110100011111101010100101000010010000000000011010010
0010111001011111000100011110010001101001101000110000110000001000
1111011011101001010100011011110110010101000111101001110011111011
0001000001010100010101110000000101111111010001011001011000000101
1101110111101110001000100000111001001100110101001101110010101010
1001010011110111010001011101111000100001010100111101001010001101
0010111100110001000100011000001100011001000110111010001101010001
0001001110000111110000100111010100010000010001001101101100001101
0010110010100010000010011010101000001101010011101101111101111101
0001110010010111011001001001000011001100100101100000001110100001
1101100111000001100100110011111011111010010000110000101011100011
1010100000011110111011101000010010110101100110110011110001110100
1100011011001000100000011000110111110101001000010101001110010011
1010111011000011011000110001110011011100110001010111100001110100
0001110011001110
```