Balanced Boolean Functions with Nonlinearity > $2^{n-1} - 2^{(n-1)/2}$

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. Furthermore, we have attained several balanced 13-variable Boolean functions with nonlinearity 4036, which improves the recent result of 4034.

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. Moreover, we have obtained several balanced 13-variable Boolean functions with nonlinearity $2^{13-1} - 2^{(13-1)/2} + 4 = 4036$, which exceeds the recent result [11] of 4034. Such functions could be constructed by using the unbalanced 9-variable Boolean functions with nonlinearity 242 [12].

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]. For the 15-variable case, 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]. For the 13-variable case, we adapt our search strategy to the idea in [7, 10, 11] described in Section 4 and improve the nonlinearity result from 4034 to 4036.

2 Background

Let f : GF(2^n) $\rightarrow$ 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 **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, **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 **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) $\rightarrow$ 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 λ = 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 $\zeta \in \mathrm{GF}(2^{15})$ 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 46,869$^{\text{th}}$ 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]. Choosing w as given above, the truth table of the balanced 15-variable Boolean function $f'(x) = f(x) \oplus w \cdot x$ with nonlinearity 16268 is given in Appendix A.

4 The 13-variable Function

Let f be the unbalanced 9-variable Boolean function with nonlinearity 242, for which the corresponding truth table is given as follows [12]:

```
125425D30A398F36508C06817BEE122E250D973314F976AED58A3EA9120DA4FE
0E4D4575C42DD0426365EBA7FC5F45BE9B2F336981B5E1863618F49474F6FE00
```

Following a similar construction to the one in [11], let $f_1(x) = f(x) \oplus w \cdot x$, where w = (0 , 0, 0, 0, 1, 1, 0, 1, 1) and $x \in \{0, 1\}^9$. Since the Walsh spectrum value of f corresponding to w = (0, 0, 0, 0, 1, 1, 0, 1, 1) is equal to 4, the 0^{th} component in the Walsh spectrum of f_1 becomes 4. Then, the 13-variable Boolean function $g = h(y_0, y_1, y_2, y_3) \oplus f_1(x_0, ..., x_8)$ has the nonlinearity of $2^{13-1} - 2^{(13-1)/2} + 8 = 4040$ where h is a 4-variable bent function. Besides, its Walsh spectrum value corresponding to w = (0, ..., 0) is either 16 or −16. In particular, we consider the bent function h = (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0).

Similar to the idea in [7, 10], the truth table of the 13-variable function is toggled from 0 to 1 at eight many random positions in [11], which provides a balanced function having nonlinearity ≥ 4032. So, the problem is to find those 8 positions, which would yield a nonlinearity > 4032. We have adapted our search strategy for this issue as follows. Initially we toggle eight bits of the unbalanced function $g = h(y_0, y_1, y_2, y_3) \oplus f_1(x_0, ..., x_8)$ randomly, to obtain a balanced g\`. Then, at each iteration of the algorithm, we make a systematic search within the intersection of two sets: balanced 2-bit neigborhood of $g$\` and 8-bit neigborhood of g. This intersection set contains 8×2^{12} many balanced functions and the function with the lowest cost is selected as the input of the next iteration. Setting the maximum iteration number to 30, a typical run of the algorithm takes around 10 minutes. At each run, we could obtain balanced 13-variable functions with nonlinearity 4036. As an example, the indices of g (with nonlinearity 4040) we toggle, to obtain the function g\` with nonlinearity 4036 are 4667, 4758, 4807, 4823, 4913, 5042, 8133, 8187 (where the truth table is indexed from 0 to 8191). The truth table of $g$\` is presented in Appendix B.

A more detailed explanation of the search strategies for the 13 and 15-variable cases will be provided in the full version of the paper.

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.

[11] S. Maitra. Balanced Boolean Function on 13-variables having Nonlinearity strictly greater than the Bent Concatenation Bound. Cryptology ePrint Archive, Report 2007/309, August 10, 2007, http://eprint.iacr.org/.

[12] S. Kavut and M. D. Yücel. Generalized Rotation Symmetric and Dihedral Symmetric Boolean Functions − 9 variable Boolean Functions with Nonlinearity 242. Cryptology ePrint Archive, Report 2007/308, August 8, 2007, http://eprint.iacr.org/.

Appendix A – Truth Table of the Balanced 15-variable Function with Nonlinearity 16268, Degree 13, and Absolute Indicator Value 208

```
A1C4C8B676F90D4103EF8351938EF32F93377A93B9D85E94057356D5C298242D50338D43030EBF9C1CEF30FC4F2AFEF279F053DDE011350E
DC9AAA13DF58CB8E0BC2238D469EF6663DCC396E1986119CC4CC3E8722C68666E6C7DBE4C37A97DFE8BE3D3C5ED98B256A3D942F32B0297B
9A72BF1F4BA0C023CA6D0B4777A607D57D5C88DB9E27538F48BAEB7E2855FE4198CE23D93301112BD1FA57012BC1EE36620832C9666EF9B8
DE256654B8EE44EB95AB8CE971F26A0D9C98070A140265D3D042B76E9CCF9DC80A2A9B4557F39B0BABF189DEBEE635299C61086D2155520C
41F0A970A3293B28E3A64E78C98631DC8C1A452093A6E35357E8B0EED203254EF8CFE58DA917CE5C0494DB571B98E83C4C03A64F3AF6FDD0
71570AA07D81B23AFB57CD3E9F3334FE368C2C91842F8AE2253E29A04BF82CD0CEA6273E957B77BBEA7087EC679F8901AF01AB85C641F752
9E2A65E0EA40A019F357C12EF25D6EB6EAE1A15813CC6EEB42C4968EEFB1D69F40CC14FD78ED7D4E8159D37541A18B886068F365F2FC153B
54DD3787AB2499067C0A611F05A3B31E4EEDC7C944A397A3A059D79447AF2591E62BC4BA981F8FFB5598FB2E2C0614208B6FF10E4EDA3C77
F23F6D2DE55103D61A62DEAB2618240781DCA4EBB684F8BDC851A8FB9D7B30C9F9727B4FB65ECB28AAD8E1AF2A37A177A0477EEDB297D53F
6535C62635E51D2EC7078C2D3A0E52DBE1056FA826D4E08C871D054CCB1D4BA980B601FC85137673B698C262B4AB582C8DA5694482608AD2
56950AADC2F40A380735F8805C34D8F1D60C4FB9679FD981FF28228C8C1C69808D5442DD2463FEC01609DB87AC5BD58BCE4E98D56411B0D7
F6A36DFC2173CF968D3AE1FECF539D94BAB0461DF91248B7810F568203576AC915B8BB2C13AE967F5AD7C32FE018ACB16700A23FD7B80B8E
41808BB451F4C1863FA5F778A0D26F0483D80EF9276A9E81C28E0F64AAD11941C40ED1D55A6EB5BD3BDC9D76FFD03FB6A2716249AAAEA96E
6BD70D7F8BABFE28A229279C2FF2D321BDB93B8E4674583EA8D54B506176F94E5CC1B1D542E246ACBA6DFBBC86DC00A428253CCC6EA07748
1FA2DE6598134312E40824B315AA86155667291EFE7BC18329E4B58819678485A3843FCEC8B8DD11E60C1B33BFB9F58D1B7DA4FBDFE9AEA3
F7575AD230E0EB95D1EF310C23495CF5FA137A38569729E24AA0BA0669A2CFC0212278AA814CCE3C13E3EB9283D12D6BF7C024B1263746E9
7D658DC6443025356F0EA16F28898ABF6E1E54DE30D00FA735FA2F429F4D8712F9958F624E0C6FB6E6FAE9F27CBC08DE77FDA13EF116831C
159EEDF376C6C9057CEAF93047595D6C1814A4C0C80D7512B40E9A432B3B5BC2700B77E81A7FF842E49658A9F8C52E9EF78AFEF8640E8986
AB0F885BC9EB35EE8D1A3E4A6A75257EC9E93DE917DD9F8A761A7C3EA47530E62E2F831E0538F4579A11650DD587BC27025684CE3DF05C22
72F7D0CE4959B441A886F3EFD37B6CC9ADF06E9CBC15EC77B2EFAB063731BF30B2B7A45DA0A9DA9C57DF4E1E415049B25231BA3DB84FDB8F
A444051E394EF13422243C19395B36176DEC23B539A9526D5B7726E330ED2D7ADAEA6C76A7971CBE45B9AB2D21BF572A2CD7CEA8749EB963
03CCC0DD4415FD8613CAB118498BCE318E49AE22D66B98D22BBA381525E34703F5674E09354B13A2C97E183E40F8344A01E73BC5187C2042
39140A26412087228E7EF832D829EBAE07CADCF1D0D5967B66D2E523FE61AEF6E71FE693A20581CAD7453EDEE2A84947567BC2835EBFFDDA
C763B456145E9D503EB4E7060DA78EC97AC9E42A0104B9C65F5ACEEC7322CBD2D0836B120E9C0C6FBE56C33DE18B777961461CE82C1DF87B
E72E1779AD59A3E3E07A78588981B9AA266DA5F07953A8FDB497DB8AFFC69348BC899E12C28568BA65AC141B05C4536B66651380387D04F3
1EF1316F2F010CC5734C82C48EC5DAB4B5F1FFD1A3A5E735234C9A63519AF94087799FC68D825940B5CB52D1BE34E6ABE45AA53A1ABEBE81
FEF725167C31436C06A74EB3C23E71464A248EEA34F9FB738B966D208FDD2090B275B744D9B356944CEF06B3E4FCDD80F453CFF0F6E6F469
00D546FA69BFE6C4A1D8333BF7D49AA5F6656F215DBBF163B64F552169E65C89ACFE8A72D6385A5C8FFCCF4B7632D963FF840F2C07B91C02
D0D75A618A3A10B511A9D4674D8D6FDA85B73957DB4848726FF1E10B4610851F5EAE11FD9FAB90C5C32E070C623F02778EBE6F49B6E1F853
91AAEA07BCB2FCE51E77074C367D8D6B72AC09A98A743EC1D0AB296394F78872E369F3043C1A47CF7B5C42601B4C79F7DA7980504E954F63
3D13E4431B5EDADFDC796A2D951CFAE5656A6AD763C179729E27B7BF1B6787B5D65B7BC8E9F489BC5AEFBABC8FFE2B24080AE4D34DF4D310
1050E1DB66D327799E7E9A644613B01E427FB2DC8C7B3267D4762F72D049EA9B1733213E2421015DC6B9DC86CE185C7A70BB22ACB6106ABE
F9CEEB4AA961C8FEF218893C31B462E0007C797E1B2AFB863113E85516E44C82156F6A6EE01C619437D29BC3C6871A12D80B38B130785C9E
4586B29BE8AD6FDF69FF440EE928148FB68086DD1528E2FF80FAD21E6AFE6D201626E23787F8248106B892740A2ECDD4D7C42EEA5366D499
801E0590C47483CDFC1433518C5538B1A9983EA196146782F712B0AB1B3100236E567BB70B1D376998122C31AD4B9471E7F6382B45B4E262
2519620CB1B26270BD7997F206B9D44681A5BCC2D61258DE7B5845501B43F0017DB9324E317EBE2A92A8AC4E7D8569EC50B63C3F17AE0715
E54C683C53BCA4A6C814C44D885B6FD052DBC4A4636F0C0BFFF4FC4B70A5127E8C1084508D8B3BBA3EACCA70548612B5AC5084E00227267A
4A49EC1B729395FB8E85CF83ECCC3B3FC30A9CBCC2B30AE9EF1F7B85EE0AD28BDAE1F9E81D8D9B56689B0ABA120866802374C7C7B5988F30
E9203C428AC7DC3FE7BFB5EAF2A609D45EEC021196CD94387477FCE700628954F57587C6FBC504C8B2263BF46EDCA853A2DA81384FB6C210
37BD27954996982D49201C07F4B34A615F790ABACB5FEB63E5532187587A3F6AF62EE16C4904A6CF1F8A33C01CF4DC8EE3065D6C74B60786
E1B258E3861A84C47601583F3D2FC8189B60DA5C37322E549DBBB4F672BB3AF9AEDA2B882188B2B588BF0BAE1B9B14204A4D07F99A056E76
6282D161DECBEDE425B52BA4052647EB5E5301076F77A37B0DE1F7545AF39E9A7195E76DA1568FA47423DEB866944FF957E6BF7E08BABB67
C32633D988D78B20A208D41FD231BDEE857676E0E2C43B06A6FA12B3D96E6284F97F48041A959A248ABB510814AC64303449A31EC8E8951F
64E0948CF6568776685FAA471C3B3850990AF7B37FC9E1CB22BFB8946A03366EE67D2CFD36B3194E7D8084F88CE6324A7B131263CB3CE365
36446FB796A5DE014DC4708653528E7116D4F9D1865673CF30FD8BAF914CB13F925332A1DB7297913078255AEAAE125D41AECBDF3A0A8F67
967F40801FD47C0581BD2B6C2F411562F4DF7CB1576E26A13057A24F667ACB7B7A640FEC5D0119A80FEF1619727046234A7FA2792CDA65F5
6743EA76A6A30BFF944DB4C0AA300EC6DD841C1DD1B968AF96CF0A02AC2EDD45435FCC406B0CCBF12C8138A249BF22555E385E0F23857E99
46C970CF73E63164313D073340497FDA82D150D86D37103908D0E5018DCD27613F6B06A647AD5704518459FBC5D87FB821336A716DF8E9F2
84E8716AD007F8EAF0245A405F367B336A3CB9F557024F4207FE076BF301B15BDB14AB8FE5A587C6BDAAB466F1469331F7F2EAED24F353B0
C239D9BB0432A7BDB363BD50149485218CDFBDB1ABEC59B1EF5B0FC83AA22F08865F730C4ACC104CEB41FB4B7FD9A992D9ECBC8F3DB3C799
7B2A8380993AFEC3753C68D582D8634FFD67F388B89A8DA757D0724F9B5BA3F6A6A092D13882252AA1C9B1E52B07CD5E74C9182204A4EE66
4FD0FF5B39EAF27D0653F9AFAB7898FF578F06650F440DD2481E33B65B9ACED01CC0C85984EAE05DD1E60F4A0A1ECDA17B4EF77F5DD0577B
963BD7BDDA0BC454072333D0E627BBDD87555F131C7FB7893374CD8553940DEFB3F18F18AD7FC01E984839BBC31903C9ED1CEFFFEACFCA2D
A82CDA70DB2C1529F6CB06F50946E6199A50E7D9F4115548B2D86BD76CBEB38C6F5D388D8F34B9D37D08F0269D28C39738417E10D2B35004
28D7DFE1A3143DE51415B37C7A017258B5D5CF579C23C8F6D6BC9AF350F11B5E2C10BF4B103D64D5A4CB0DB7978055D8B2BA583DF41A8B2E
454195BAE0CC53EB4AD83CC1F90F139F2145C9A85F4E1A37139229C9882D1D5DF9019D71DE115488836CFDF286829E8869ACB241D4C8C764
9A82DFEDE1A1FF2AF90A731F946D090FD47A5AEE8BF304BDE6CE078B046C8F5B025F4D4377511AED31A7E2B81C0753DB457986D16E7BC3F6
1DAB2AC7164F80D35E7BA42F847A298BAF68A40D412D775B7772CFD46CE86D32FB349986698E53EC57811CC4452C4C1449142E2B93460BCD
FF80E11E3EF48757E662F3DA399C6F0F6E2F17FCC646F3CC66BA432143DFFFF2FC210A882C54B54407B4B84D267ACCC124284AE3255514D9
04092952F916178A818C5011797393482662 3A0BA35367C6ADF3A5C8199B45D6D0E7B789020192BC9B0E43150269B46D093EFBF4B7D6FE66
72757A8C3F5DB3333E5C1F6A64A521D365D8ADAF104B2564444BD59D831BD5F5BE4EAAA1545E9FBCEF36662E575047CBBF7A25AC19034CC3
6A1D44BD13434D5ECFEA0F58B9E373BCD451D6A646BB1CDCF0B06B82B30AE32346863D80601965F292B9D2A595A2CB88B6DB29598FCD7AD7
7FD64BC32A6B31A644BA8AD99A42ACAAEF3F423A01E4BE194CAE6FD84C699594F361A8C7A7CACA36569CF9E737DA40AD345DA910213C038F
2029E2EA945ABB187FB973CCDA2B8C9125F630C4D62AA0CB99ABE601208D5354996F7F12F1C8A8A5E92908E770DBA4374D10D139405EE66A
D2518D7B2FE2E3B0E50045C172F96CD13D7095E9B81473768C6A490904DF81D3D66DF8994641027A85A38BB1C358BCAB66D06BDD3AEDF54B
2BBBC4F7E79D02647BB54578AEB5FA9495D73E22BF3B044C98032430FF48CC8D660007563E4A3FDA35E8C3B33207F6958869B8EC5F22BA3F
49E0A9FB487540E68453B431BED774D35451C328A21897D0C40160028048178359541 63CF8EECA74D55ADFACC09E8369036878E0DFCB6A2F
EAA438C0113130D72EAA30BF7B74CC07ADF9C607CB19132A2CAAE6060474AD59680F603B329B21492112730C342AC01FB062AE108FB2EA15
067D808568E1FAC2634CA84CA8DC8960C7376AB7CD62B16AF8625BB1DDBC183E5BAB51FD262FA4C41510D04841F8B98B82AC3F9A587C0AF7
3A0922908339DE63412A4EAFE9F61C43284D6E35C957FEEA11FCD571602366D10E8BE6E3BBF306847B066D1537166118B70F5C18959B108F
71A16F15EB21C3D9B6D1B7CAAB35FC39B634475415132C707DBBF611214DA211466A1F5EF363988E2111D1315E439F2FB8B6B5BC1DA10AC7
94E2A766D7927C800635F7009D31F6813794173B48C0CBB4BBDEE0021A8DE3D54721F8F4FBEE7E8CF0281C456373726CC1174FD47CBC7FE5
2F1FE79D01536276B1661C88E0E3E1FFC8162AF62758B38BA9020B5CFED7706D5EDE8B1833091F0910985538868886A278823818D2624949
A92D5E0F7A8A567B
```

Appendix B – Truth Table of the Balanced 13-variable Function with Nonlinearity 4036, Degree 11, and Absolute Indicator Value 536

```
74CDBCB56CA0165036159FE71D778B4843940E557260EFC8B313A7CF74943D9868D4DC13A2B44924
05FC72C19AC6DCD8FDB6AA0FE72C78E050816DF2126F676674CDBCB56CA0165036159FE71D778B48
43940E557260EFC8B313A7CF74943D9868D4DC13A2B4492405FC72C19AC6DCD8FDB6AA0FE72C78E0
50816DF2126F676674CDBCB56CA0165036159FE71D778B4843940E557260EFC8B313A7CF74943D98
68D4DC13A2B4492405FC72C19AC6DCD8FDB6AA0FE72C78E050816DF2126F676674CDBCB56CA01650
36159FE71D778B4843940E557260EFC8B313A7CF74943D9868D4DC13A2B4492405FC72C19AC6DCD8
FDB6AA0FE72C78E050816DF2126F676674CDBCB56CA0165036159FE71D778B4843940E557260EFC8
B313A7CF74943D9868D4DC13A2B4492405FC72C19AC6DCD8FDB6AA0FE72C78E050816DF2126F6766
74CDBCB56CA0165036159FE71D778B4843940E557260EFC8B313A7CF74943D9868D4DC13A2B44924
05FC72C19AC6DCD8FDB6AA0FE72C78E050816DF2126F67668B32434A935FE9AFC9EA6018E28874B7
BC6BF1AA8D9F10374CEC58308B6BC267972B23EC5D4BB6DBFA038D3E65392327024955F018D3871F
AF7E920DED9098998B32434A935FE9AFC9EA6018E28874B7BC6BF1AA8D9F10374CEC58308B6BC267
972B23EC5D4BB6DBFA038D3E65392327024955F018D3871FAF7E920DED90989974CDBCB56CA01650
36159FE71D778B4843940E557260EFC8B313A7CF74943D9868D4DC13A2B4492405FC72C19AC6DCD8
FDB6AA0FE72C78E050816DF2126F67668B32434A935FE9BFC9EA6018E28874B7BC6BF3AA8D9F1037
4DEC59308B6BC267972B23EC5D4BF6DBFA038D3E65392327024955F018D3A71FAF7E920DED909899
74CDBCB56CA0165036159FE71D778B4843940E557260EFC8B313A7CF74943D9868D4DC13A2B44924
05FC72C19AC6DCD8FDB6AA0FE72C78E050816DF2126F67668B32434A935FE9AFC9EA6018E28874B7
BC6BF1AA8D9F10374CEC58308B6BC267972B23EC5D4BB6DBFA038D3E65392327024955F018D3871F
AF7E920DED90989974CDBCB56CA0165036159FE71D778B4843940E557260EFC8B313A7CF74943D98
68D4DC13A2B4492405FC72C19AC6DCD8FDB6AA0FE72C78E050816DF2126F67668B32434A935FE9AF
C9EA6018E28874B7BC6BF1AA8D9F10374CEC58308B6BC267972B23EC5D4BB6DBFA038D3E65392327
024955F018D3871FAF7E920DED9098998B32434A935FE9AFC9EA6018E28874B7BC6BF1AA8D9F1037
4CEC58308B6BC267972B23EC5D4BB6DBFA038D3E65392327024955F018D3871FAF7E920DED909899
74CDBCB56CA0165036159FE71D778B4843940E557260EFC8B313A7CF74943D9868D4DC13A2B44924
05FC72C19AC6DCD8FDB6AA0FE72C78E054816DF2126F6776
```