Balanced Boolean Function on 13-variables having Nonlinearity strictly greater than the Bent Concatenation Bound

Subhamoy Maitra
Applied Statistics Unit, Indian Statistical Institute,
203 B T Road, Kolkata 700 108, India,
Email: subho@isical.ac.in

Abstract

Very recently, Kavut and Yucel identified 9-variable Boolean functions having nonlinearity 242, which is currently the best known. However, any of these functions do not contain any zero in the Walsh spectrum and that is why they cannot be made balanced. We use these functions to construct 13-variable balanced Boolean function having nonlinearity $2^{13-1} - 2^{\frac{13-1}{2}} + 2 = 4034$ which is strictly greater than the bent concatenation bound. This is the first demonstration of balanced Boolean functions on odd number of variables having nonlinearity strictly greater than the bent concatenation bound for number of input variables less than 15.

Keywords: Balancedness, Boolean Function, Nonlinearity.

1 Introduction

Very recently [3], 9-variable Boolean functions with nonlinearity 242 (greater than the bent concatenation nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$ for odd n) have been discovered. These functions are not balanced and there is no zero value in the Walsh spectrum of any of these 9-variable nonlinearity 242 functions. Thus these functions cannot be linearly transformed to 9-variable balanced functions with nonlinearity 242.

The current state of the art nonlinearity results for Boolean functions on odd number of variables is as follows.

1. In 1972 [1], it has been shown that the maximum nonlinearity of 5-variable Boolean functions is 12 and in 1980 [6] it has been shown that the maximum nonlinearity of 7-variable Boolean functions is 56. Thus for odd $n \leq 7$, the maximum nonlinearity of n-variable functions is $2^{n-1} - 2^{\frac{n-1}{2}}$.

2. In 1983 [7], it has been shown that one can get unbalanced Boolean functions on 15 variables having nonlinearity 16276 (we will refer these functions as PW functions as these function were found by Patterson and Wiedemann) and using this result one can show that for odd $n \geq 15$, it is possible to get Boolean functions having nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 20 \cdot 2^{\frac{n-15}{2}}$.

3. In 2006 [2], 9-variable unbalanced Boolean functions could be achieved with nonlinearity 241, and thus Boolean functions on 9, 11, and 13 variables could be constructed having nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 2^{\frac{n-9}{2}}$.

4. In 2007 [3], the result for 9-variables could be improved and unbalanced functions could be achieved with nonlinearity 242. Hence, Boolean functions on 9, 11, and 13 variables could be constructed having nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 2 \cdot 2^{\frac{n-9}{2}}$.

Balanced Boolean functions on odd number of variables having nonlinearity greater than the bent concatenation bound have received lot of attention in the literature. Balancedness is one of the important cryptographic and combinatorial properties of Boolean functions. Below we list the existing results in this area.

1. Using the PW functions as black box, in [9], balanced Boolean functions having nonlinearity greater than bent concatenation bound could be found for odd $n \geq 29$.

2. In [4, 5], the structure of the PW functions have beeen modified using heuristic search to get balanced Boolean functions having nonlinearity $2^{15-1} - 2^{\frac{15-1}{2}} + 6 = 16262$ on 15-variables.

3. In [8], the structure of the PW functions have been modified systematically in the space of rotation symmetric Boolean functions to achieve nonlinearity $2^{15-1} - 2^{\frac{15-1}{2}} + 10 = 16266$ on 15-variables.

4. So far no balanced Boolean function on odd number of variables n having nonlinearity greater than bent concatenation bound is known for $n = 9, 11, 13$. We use the functions presented in [3] to construct 13-variable balanced Boolean Functions having nonlinearity $2^{13-1} - 2^{\frac{13-1}{2}} + 2 = 4034$.

We refer to [2] for basic definitions of nonlinearity $nl(f)$ and Walsh spectrum $W_f(.)$ for a Boolean function f.

2 The 13-variable Function

We start with the following 9-variable function f having nonlinearity 242 [3]. The truth table is presented below in hexadecimal format.

```
3740B6A118A1E19642A85E2B7E2F3C3CB65FA0D95EC9DB1EA92BDB3666185AE0
087F5FE6E0757106A12FC918754C40E8A1BCCB7A714032A8961456E066E8A801
```

Let $x \in \{0,1\}^n$ be the input variables. Now we construct two 9-variable functions $f_1(x) = f(x) \oplus < \omega_1 \cdot x >$ and $f_2(x) = f(x) \oplus < \omega_2 \cdot x >$, where $\omega_1 = (0,0,0,0,0,0,0,1,0)$ and $\omega_2 = (0,0,1,0,0,1,1,0,0)$.

It is easy to see $nl(f_1) = nl(f_2) = 242$ and $W_{f_1}(0) = 4, W_{f_2}(0) = -4$. Also we denote $\overline{f}_1 = 1 \oplus f_1, \overline{f}_2 = 1 \oplus f_2$.

We construct a 13-variable function F whose truth table is the concatenation of sixteen many truth tables of 9-variable functions each having nonlinearity 242. The truth table of F is as follows.

$$f_2 f_1 f_1 \overline{f}_2 f_2 f_1 f_1 \overline{f}_2 f_2 f_1 f_1 \overline{f}_2 \overline{f}_2 \overline{f}_1 \overline{f}_1 f_2$$

It can be proved that $nl(F) = 2^{13-1} - 2^{\frac{13-1}{2}} + 8 = 4040$ and $W_F(0) = 16$.

Similar to the idea of [4, 5], we tried a heuristic search by modifying (toggling) the truth table of F from 0 to 1 at eight many random positions. This will provide a function G having $nl(G) \geq 4040 - 8 = 4032 = 2^{13-1} - 2^{\frac{13-1}{2}}$ and $W_G(0) = 0$. It implies that we will always get balanced function G on 13 variables. Thus the only important issue is to find a function G such that $nl(G) > 4040 - 8$. We searched 20,000 many functions by randomly choosing eight positions at the truth table of G where the values are zero and then toggling those positions to 1. We found one function G with nonlinearity $2^{13-1} - 2^{\frac{13-1}{2}} + 2 = 4034$. The locations where we needed to toggle the function are 183, 256, 671, 1025, 2231, 2662, 2948, 3298 (the locations of the truth table are indexed from 0 to $2^n - 1$).

The truth table of the function G is presented in Appendix A. This is the first time a balanced Boolean function having nonlinearity strictly greater than the bent concatenation bound is demonstrated for number of input variables less than 15.

After the first version of the paper, Kavut and Yucel tried further systematic searches on the function F and obtained the nonlinearity $2^{13-1} - 2^{\frac{13-1}{2}} + 4 = 4036$. As an example, the locations where they toggled the output of F are 4625, 4697, 4737, 4763, 4809, 5037, 5279, 5433.

We are currently working on further heuristic methods to find balanced Boolean functions on 9 and 11 variables with nonlinearity exceeding the bent concatenation bound.

References

[1] E. R. Berlekamp and L. R. Welch. Weight distributions of the cosets of the $(32, 6)$ Reed-Muller code. *IEEE Transactions on Information Theory*, IT-18(1):203–207, January 1972.

[2] S. Kavut, S. Maitra and M. D. Yücel. In *IEEE Transactions on Information Theory*, 53(5): 1743-1751, May 2007. See also "There exist Boolean functions on n (odd) variables having nonlinearity $> 2^{n-1} - 2^{\frac{n-1}{2}}$ if and only if $n > 7$" in IACR eprint server, http://eprint.iacr.org/2006/181, 28 May, 2006.

[3] S. Kavut and M. Yucel. 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/.

[4] 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.

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

[6] J. J. Mykkeltveit. The covering radius of the $(128, 8)$ Reed-Muller code is 56. *IEEE Transactions on Information Theory*, IT-26(3):359–362, 1980.

[7] 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.

[8] S. Sarkar and S. Maitra. Idempotents in the Neighbourhood of Patterson-Wiedemann Functions having Walsh Spectra Zeros. In *WCC 2007, International Workshop on Coding and Cryptography*, April 16-20, 2007, Versailles (France).

[9] J. Seberry, X. M. Zhang, and Y. Zheng. Nonlinearly balanced Boolean functions and their propagation characteristics. In *Advances in Cryptology - CRYPTO'93*, LNCS 773, pages 49–60. Springer-Verlag, 1994.

Appendix A

38b0b9511751ee66b2a7ae248e20cc33b9afaf295139d5ee59242b399617aaef
878f5016ef857ef6512039178543b0e7ae4cc48a7eb03d58661ba6ef96e7580e
047385922b92d2a5719b6d184d1c0f0f856c93eb6dfae82d9a18e805552b69d3
3b4c6cd5d3464235921cfa2b467f73db928ff8494273019ba52765d355db9b32
447385922b92d2a5719b6d184d1c0f0f856c93ea6dfae82d9a18e805552b69d3
3b4c6cd5d3464235921cfa2b467f73db928ff8494273019ba52765d355db9b32
c74f46aee8ae11994d5851db71df33cc465050d6aec62b11a6dbd4c669e85510
f870afe9107a8109aedfc6e87abc4f1851b33b75814fc2a799e459106918a7f1
38b0b9511751ee66b2a7ae248e20cc33b9afaf295139d5ee59242b399617aaef
078f5016ef857ef6512039178543b0e7ae4cc48a7eb03d58661ba6ef96e7580e
047385922b92d2a5719b6d184f1c0f0f856c93ea6dfae82d9a18e805552b69d3
3b4c6cd5d3464235921cfa2b467f73db9a8ff8494273019ba52765d355db9b32
047385922b92d2a5719b6d184d1c0f0f856c93ea6dfae82d9a18e805752b69d3
3b4c6cd5d3464235921cfa2b467f73db928ff8494273019ba52765d355db9b32
c74f46aee8ae11994d5851db71df33cc465050d6aec62b11a6dbd4c669e85510
f870afe9107a8109aedfc6e87abc4f1851b33b75814fc2a799e459106918a7f1
38b0b9511751ee66b2a7ae248e20cc33b9afaf295139d4ee59242b399617aaef
078f5016ef857ef6512039178543b0e7ae4cc48a7eb03d58661ba6ef96e7580e
047385922b92d2a5719b6d184d1c0f0f856c93ea6dfae82d9a18e805552b69d3
3b4c6cd5d3464235921cfa2b467f73db928ff8494273019ba52765d355db9b32
047385922b92d2a5719b6d184d1c0f0f856c93ea6dfae82d9a18e805552b69d3
3b4c6cd5d3464235921cfa2b467f73db928ff8494273019ba52765d355db9b32
c74f46aee8ae11994d5851db71df33cc465050d6aec62b11a6dbd4c669e85510
f870afe9107a8109aedfc6e87abc4f1851b33b75814fc2a799e459106918a7f1
c74f46aee8ae11994d5851db71df33cc465050d6aec62b11a6dbd4c669e85510
f870afe9107a8109aedfc6e87abc4f1851b33b75814fc2a799e459106918a7f1
fb8c7a6dd46d2d5a8e6492e7b2e3f0f07a936c15920517d265e717faaad4962c
c4b3932a2cb9bdca6de305d4b9808c246d7007b6bd8cfe645ad89a2caa2464cd
fb8c7a6dd46d2d5a8e6492e7b2e3f0f07a936c15920517d265e717faaad4962c
c4b3932a2cb9bdca6de305d4b9808c246d7007b6bd8cfe645ad89a2caa2464cd
38b0b9511751ee66b2a7ae248e20cc33b9afaf295139d4ee59242b399617aaef
078f5016ef857ef6512039178543b0e7ae4cc48a7eb03d58661ba6ef96e7580e