Patterson–Wiedemann Type Functions on 21 Variables With Nonlinearity Greater Than Bent Concatenation Bound

Selçuk Kavut and Subhamoy Maitra

Abstract—**Nonlinearity is one of the most challenging combinatorial property in the domain of Boolean function research. Obtaining nonlinearity greater than the bent concatenation bound for odd number of variables continues to be one of the most sought after combinatorial research problems. The pioneering result in this direction has been discovered by Patterson and Wiedemann in 1983 (IEEE-IT), which considered Boolean functions on 5 x 3 = 15 variables that are invariant under the actions of the cyclic group $GF(2^5)^* \cdot GF(2^3)^*$ as well as the group of Frobenius automorphisms. Some of these Boolean functions possess nonlinearity greater than the bent concatenation bound. The next possible option for exploring such functions is on 7 x 3 = 21 variables. However, obtaining such functions remained elusive for more than three decades even after substantial efforts as evident in the literature. In this paper, we exploit combinatorial arguments together with heuristic search to demonstrate such functions for the first time.**

Index Terms—**Covering radius, first order reed-muller code, nonlinearity, Patterson-Wiedemann type functions.**

I. Introduction

Constructing Boolean functions on odd number of variables n having nonlinearity greater than the bent concatenation bound $2^{n-1}-2^{\frac{n-1}{2}}$ is one of the most difficult problems in the area of cryptography, coding theory, and combinatorics. In 1983, Patterson and Wiedemann discovered [15] for the first time such Boolean functions for $n = 15$ using some combinatorial techniques and search methods together. The search space could be reduced substantially in [15] by considering several group actions as described later in Section I-C. The crux of the observation was that 15 can be written as 5 × 3, product of two primes. The next attempt in this direction should have been for 21 = 7 × 3, but that could not be achieved till date. In this paper, for the first time, we demonstrate such functions for 21 variables which have remained unknown for more than 32 years. In this regard, one can computationally check that for 9 = 3 × 3, there is no Patterson-Wiedemann type Boolean functions having nonlinearity greater than the bent concatenation bound.

In cryptography, Boolean functions and S-boxes (multiple output Boolean functions) with high nonlinearity are important to resist against linear cryptanalysis. Given that such functions have certain kinds of invariance (one can group large number of inputs according to certain mathematical structures), they can be implemented efficiently in application domain. From coding theory viewpoint, the maximum nonlinearity is actually the covering radius of the first order Reed-Muller codes and thus have immediate relevance in this area of research.

At this point, let us refer to the most important results in the field of maximum nonlinearity of Boolean functions on odd number of variables with the time-line. The time-line is mentioned here to highlight that this problem is indeed challenging as only a few results appeared in a substantially long duration even after a lot of attention to these problems. The main challenge is to check whether it is possible to overcome the bent concatenation bound. The bent functions are also combinatorially challenging and well studied class with application in coding theory and cryptography. These functions exist for even number of variables m having the provably maximum possible nonlinearity $2^{m-1} - 2^{\frac{m}{2}-1}$. Consider two m-variable bent functions f_0, f_1 and then construct an $n = m+1$ variable Boolean function F as $(1 \oplus x_{m+1}) f_0 \oplus x_{m+1} f_1$. It can be easily checked that the nonlinearity of F is $2^{n-1} - 2^{\frac{n-1}{2}}$. Since the 2^n bit long truth table of F is concatenation of the two 2^m length truth tables of the bent functions f_0, f_1, this nonlinearity of F is called the bent concatenation nonlinearity.

- **1972:** In [2], it has been shown that for $n = 5$, the maximum nonlinearity of n-variable Boolean functions is the bent concatenation nonlinearity, which is 12.
- **1980:** In [14], the question for $n = 7$ could be solved and it has been noted that here also the maximum nonlinearity is the bent concatenation nonlinearity which is 56.
- **1983:** In [15], the seminal positive result has been presented by Patterson and Wiedemann showing that one can construct a 15-variable Boolean function f with nonlinearity $2^{15-1} - 2^{\frac{15-1}{2}} + 20 = 16276$. It is well known that using this function, one can construct any n-variable Boolean function F with nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 20 \cdot 2^{\frac{n-15}{2}}$ for $n > 15$. In fact, F can be written as $f \oplus g$, where g is an $(n-15)$-variable bent function.
- **2006-2010:** The 9-variable Boolean functions having nonlinearity 241 were identified [7] in the rotation-symmetric class and subsequently this result is improved [8] to 242 by considering the k-rotation-symmetric class. Thus, for $n = 9, 11, 13$, one can obtain Boolean functions having nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 2 \cdot 2^{\frac{n-9}{2}}$.

Manuscript received October 27, 2015; revised January 26, 2016; accepted February 12, 2016. Date of publication February 16, 2016; date of current version March 16, 2016.

S. Kavut is with the Computer Engineering Department, Balıkesir University, Balýkesir 10145, Turkey (e-mail: skavut@balikesir.edu.tr).

S. Maitra is with the Applied Statistics Unit, Indian Statistical Institute, Kolkata 700108, India (e-mail: subho@isical.ac.in).

Communicated by S. Mesnager, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2016.2530795

A. Our Contribution

The kind of constraints considered for constructing the 15-variable functions in [15] finally reduced to solving an integer programming problem on 11 binary variables, which was easy to solve using exhaustive search. However, the authors [15] pointed out the following in their paper[1]:

> "We have not succeeded in understanding algebraically the choice of orbits made in (6) and thus have not succeeded in generalizing our construction to other dimensions although we suspect there is a construction for all $\mathcal{R}_m$ when m is not a prime power."

In fact, the situation is significantly harder for the 21-variable case as in a similar manner of [15] it reduces to an integer programming problem with 115 binary variables. An attempt has been made towards studying this class almost a decade back in [5] without any success. In [5, p. 1551], it has been commented that:

> "The search space corresponding to this case is very large and exhaustive search is infeasible. It will be of interest to develop some heuristic methods to find solutions to this system of linear inequalities."

In this paper we revisit the problem with more disciplined effort and indeed obtain Patterson-Wiedemann type functions on 21 variables having nonlinearity strictly greater than the bent concatenation bound.

B. Caveat

The nonlinearity of the functions f_{21} that we achieve in this paper is $2^{21-1} - 2^{\frac{21-1}{2}} + 61$. Note that this nonlinearity is less than $2^{21-1} - 2^{\frac{21-1}{2}} + 20 \cdot 2^{\frac{21-15}{2}}$ as obtained by composing the Patterson-Wiedemann function f_{15} on 15 variables and a bent function g_6 on 6 variables, i.e., $f'_{21} = f_{15} \oplus b_6$, where the functions f_{15} and b_6 are on distinct variables. However, such functions f'_{21} are not of Patterson-Widemann type and it does not answer the challenge of obtaining such functions on 21 variables beating the bent concatenation bound as posed in [15]. We solve this problem for the first time. Further, we could not make exhaustive search as the integer programming problem in this case is on 115 binary variables. It may very well happen that with the dissemination of our results, the problem may be solved with better efficiency in obtaining solutions with higher nonlinearity. In case such a Patterson-Wiedemann type function on 21-variables with nonlinearity greater than $2^{21-1} - 2^{\frac{21-1}{2}} + 160$ could be obtained, that will provide the highest known nonlinearity for all the odd variable Boolean functions for 21 variables and more. That we leave as an open problem in this direction. For time to time updates related to search results in this direction as well as detailed codes and explanations, one may refer to [10] and [11] respectively.

Next we provide necessary background in this area. For this, we mostly follow to the explanations in [5] and [15]. One may also note that several modifications of Patterson-Wiedemann type functions have been studied in literature as evident from [4], [12], [16], and the references therein.

C. Background

By $\mathcal{B}_n$, let us denote the set of Boolean functions from $GF(2^n)$ to $GF(2)$ and consider $f \in \mathcal{B}_n$. The support of f is defined as $Supp(f) = \{x \in GF(2^n) | f(x) = 1\}$, and its weight is $wt(f) = |Supp(f)|$. Let a and b be two distinct odd primes such that $n = ab$. We use the usual notations, i.e., $\mathbb{F}_{2^n} = GF(2^n)$. Now consider the tower of subfields $\mathbb{F}_2 \hookrightarrow \mathbb{F}_{2^a} \hookrightarrow \mathbb{F}_{2^{ab}}$. The index of the multiplicative group $\mathbb{F}^*_{2^a}$ in $\mathbb{F}^*_{2^{ab}}$ is $m = \frac{2^{ab}-1}{2^a-1}$. One may note that $\mathbb{F}^*_{2^{ab}}$ can be written as $\mathbb{F}^*_{2^{ab}} = \cup_{i=1}^{m} \mathbb{F}^*_{2^a} x_i$ where $\{x_1, x_2, \ldots, x_m\}$ is the complete set of coset representatives of $\mathbb{F}^*_{2^a}$ in $\mathbb{F}^*_{2^{ab}}$. It is well known that one can characterize any function from $\mathbb{F}^*_{2^{ab}} \to \mathbb{F}_2$ by specifying its support. Let us consider functions in $\mathcal{B}_n$ whose supports are of the form $\cup_{i=1}^{\ell} \mathbb{F}^*_{2^a} x_i$ for some positive integer ℓ. Such functions have been considered by Dillon [3] towards the construction of bent functions and formal proofs could be devised using this idea to show that such functions provide the best known nonlinearity for even number of variables. Naturally, this idea was later exploited by Patterson and Wiedemann [15] to explore high nonlinearity for odd number of variables. Though there had been no clear proof of nonlinearity for odd number of variables as accepted in [15], such ideas along with some additional techniques produced functions with nonlinearity greater than bent concatenation bound.

Any linear function in $\mathcal{B}_n$ can be expressed as $l_\alpha(x) = Tr_1^n(\alpha x)$ where $\alpha \in \mathbb{F}_{2^n}$ and $Tr_1^n(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}}$ for all $x \in \mathbb{F}_{2^n}$. Given $n = ab$, the support of l_α is $Supp(l_\alpha) = \{x \in \mathbb{F}_{2^{ab}} | Tr_1^{ab}(\alpha x) = 1\}$, and the support of the affine function $h_\alpha(x) = l_\alpha(x) + 1$ is $Supp(h_\alpha) = \{x \in \mathbb{F}_{2^{ab}} | Tr_1^{ab}(\alpha x) = 0\}$. Let $H_\alpha = Supp(h_\alpha)$, which is a hyperplane in $\mathbb{F}_{2^{ab}}$ when considered as a vector space over $\mathbb{F}_2$.

As we have discussed, the nonlinearity of a Boolean function is defined as the minimum distance from the set of linear and affine functions. As a passing remark, we like to mention that nonlinearity can also be expressed in terms of Hadamard transform. The Hadamard transform of $f \in \mathcal{B}_n$ is defined as

$$\hat{f}(\lambda) = \sum_{x \in GF(2^n)} (-1)^{f(x)+Tr(\lambda x)}.$$

Given this, the nonlinearity of a Boolean function f can be described as

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in GF(2^n)} |\hat{f}(\lambda)|.$$

We can write the elements of $\mathbb{F}_{2^n}$ in some order, say $\{\alpha_0, \alpha_1, \ldots, \alpha_{2^n-1}\}$. For $f, g \in \mathcal{B}_n$, we define the distance $d(f, g)$ between f, g as the Hamming distance between the 2^n-dimensional vectors $(f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^n-1}))$ and $(g(\alpha_0), g(\alpha_1), \ldots, g(\alpha_{2^n-1}))$. It is easy to see that if $f, g \in \mathcal{B}_n$ then $d(f, g) = |Supp(f) \ominus Supp(g)|$ where $\ominus$ is the symmetric difference between the sets $Supp(f)$ and $Supp(g)$.

[1] Here $\mathcal{R}_m$ means the first-order Reed-Muller code of block length 2^m and (6) refers to certain description of orbits in [15, p. 355].

We are considering $f \in \mathcal{B}_n$ such that $Supp(f) = \cup_{i=1}^{\ell} \mathbb{F}_{2^a}^* x_i$. Let $\mathbf{0}$ and $\mathbf{1}$ be the constant functions with all 0 values and all 1 values respectively. Further, let $t(\alpha)$ be the number of cosets of the form $\mathbb{F}_{2^a}^* x_i$ that are totally contained in the hyperplane H_α, equivalently $t(\alpha)$ is the number of x_i's for which $Tr_a^{ab}(x_i\alpha) = 0$. Given this, one may calculate that (see also [15])

$$\begin{aligned} d(f, \mathbf{0}) &= \ell(2^a - 1), \\ d(f, \mathbf{1}) &= 2^{ab} - \ell(2^a - 1), \\ d(f, h_\alpha) &= 2^{ab-1} - 2^a \cdot t(\alpha) + \ell, \\ d(f, l_\alpha) &= 2^{ab-1} + 2^a \cdot t(\alpha) - \ell. \end{aligned} \quad (1)$$

Here the first two equations are clear, as there are l cosets in the support of f. Let us consider the restriction $H_\alpha \upharpoonright_{\mathbb{F}_{2^a}^* x_i}$ of H_α to the coset $\mathbb{F}_{2^a}^* x_i$. Then the other two equations follow from the fact that the weight of $H_\alpha \upharpoonright_{\mathbb{F}_{2^a}^* x_i}$ is either $2^{a-1} - 1$ or $2^a - 1$ and the number of those with weight $2^{a-1} - 1$ is 2^{ab-a}. Thus, the nonlinearity of f is given by the minimum of the above varying distances over all $\alpha \in \mathbb{F}_{2^{ab}}$, i.e.,

$$nl(f) = \min_{\alpha \in \mathbb{F}_{2^{ab}}^*} \{\ell(2^a - 1), 2^{ab} - \ell(2^a - 1), \\ 2^{ab-1} - 2^a \cdot t(\alpha) + \ell, 2^{ab-1} + 2^a \cdot t(\alpha) - \ell\}.$$

For such a function f with $nl(f) > 2^{ab-1} - 2^{(ab-1)/2}$, considering (1), we obtain that ℓ and $t(\alpha)$ must satisfy:

$$\psi^- < \ell < \psi^+, \quad (2)$$

$$\frac{\{\psi^- - 2^{(ab-1)/2}\}}{2^a} < t(\alpha) < \frac{\{\psi^+ + 2^{(ab-1)/2}\}}{2^a}, \quad (3)$$

where

$$\psi^- = \frac{2^{ab-1} - 2^{(ab-1)/2}}{2^a - 1} \text{ and } \psi^+ = \frac{2^{ab-1} + 2^{(ab-1)/2}}{2^a - 1}.$$

Consider the two subgroups $\mathbb{F}_{2^a}^*$ and $\mathbb{F}_{2^b}^*$ in $\mathbb{F}_{2^{ab}}^*$. The intersection of $\mathbb{F}_{2^a}^*$ and $\mathbb{F}_{2^b}^*$ contains only the identity element and the group $\mathbb{F}_{2^{ab}}^*$ is an abelian group. Hence the product $\mathbb{F}_{2^a}^* \cdot \mathbb{F}_{2^b}^*$ is direct. One can identify the group $\mathbb{F}_{2^{ab}}^*$ to the group $\Phi(\mathbb{F}_{2^{ab}}^*)$ of left multiplications by the elements of $\mathbb{F}_{2^{ab}}^*$ in $GL_{\mathbb{F}_2}(\mathbb{F}_{2^{ab}})$ and this correspondence is an isomorphism.

Let $\phi_2 \in GL_{\mathbb{F}_2}(\mathbb{F}_{2^{ab}})$ be the Frobenius automorphism of $\mathbb{F}_{2^{ab}}$. This is defined by $\phi_2(x) = x^2$ for all $x \in \mathbb{F}_{2^{ab}}$. The group $\langle\phi_2\rangle$ generated by ϕ_2 is a cyclic group of order ab, which is contained in $GL_{\mathbb{F}_2}(\mathbb{F}_{2^{ab}})$. To summarize, let us present the following definition.

Definition 1: Consider $n = ab$, the product of two distinct primes. Patterson and Wiedemann [15] considered the action of the group $G = [\Phi(\mathbb{F}_{2^a}^*) \cdot \Phi(\mathbb{F}_{2^b}^*)]\langle\phi_2\rangle/\Phi(\mathbb{F}_{2^a}^*)$, where $[\Phi(\mathbb{F}_{2^a}^*) \cdot \Phi(\mathbb{F}_{2^b}^*)]\langle\phi_2\rangle$ is the semidirect product of $\Phi(\mathbb{F}_{2^a}^*) \cdot \Phi(\mathbb{F}_{2^b}^*)$ by $\langle\phi_2\rangle$. Here, the functions $f \in \mathcal{B}_n$, which are invariant under this group action are referred to as Patterson-Wiedemann type functions.

The result of [15] was for $n = 15$, where the support of the function f is invariant under the action of $\mathbb{F}_{2^5}^*$ and $\mathbb{F}_{2^3}^*$. That is, the support of f is invariant under the action of the product $\mathbb{F}_{2^5}^* \cdot \mathbb{F}_{2^3}^*$ which is also a cyclic subgroup of $\mathbb{F}_{2^{15}}^*$ of order $(2^5-1)(2^3-1) = (31)(7) = 217$. All the elements of $\mathbb{F}_{2^5}^* \cdot \mathbb{F}_{2^3}^*$ should have the same value and it is also true for the elements in each of its cosets in $\mathbb{F}_{2^{15}}^*$. In other words, the functions which satisfy $f(\omega^i) = f(\omega^{i+151\kappa})$ for all $i = 0, 1, \ldots, 216$ and $\kappa = 0, 1, \ldots, 150$, where ω is a primitive element in $\mathbb{F}_{2^{15}}$, are considered in [15] (notice that $\frac{2^{15}-1}{217} = 151$). In the form of interleaved sequence [5], [6], this can be seen as 217 rows of length 151 each. The value in each column is the same. Thus one row of 151 elements will define the complete Boolean function at $2^{15} - 1$ inputs. Without loss of generality, we consider the output as zero for the all zero input point. Next comes the constraint that the function f is invariant under Frobenius automorphism, i.e., $f(x) = f(x^2)$ for all $x \in \mathbb{F}_{2^{15}}^*$. Due to this, the 151 elements are divided into 10 groups of size 15 each and one group of size 1. One can initially assign the output zero corresponding to the inputs of the group of size 1. Due to the weight conditions, it is evident that inputs corresponding to the 5 groups should have the output 0 and rest should have the output 1. Thus, we need to search $\binom{10}{5} = 252$ different Boolean functions on 15 variables. As described in [15], two distinct functions with nonlinearity 16276 could be obtained in this class up to affine equivalence. The problem could also be seen as solutions to certain specific inequalities as explained in [5, pp. 1549–1550].

II. Patterson-Wiedemann Type Construction on 21 Variables

In this section, we consider the case for $n = 21 = 7 \cdot 3$. Now $\mathbb{F}_{2^7}^* \cdot \mathbb{F}_{2^3}^*$ is a cyclic subgroup of $\mathbb{F}_{2^{21}}^*$ of order $(2^7-1)(2^3-1) = (127)(7) = 889$. Note that $\frac{2^{21}-1}{889} = 2359$. That is, we can consider the interleaved sequence, where we have 889 similar rows and each row has 2359 elements. Further, the function f is invariant under Frobenius automorphism, i.e., $f(x) = f(x^2)$ for all $x \in \mathbb{F}_{2^{21}}^*$. As a result, 2359 elements are divided as 112 groups of size 21, 2 of size 3 and 1 of size 1. Thus, we have at total 115 binary variables here. We consider the following preliminary things towards obtaining a solution.

- We consider that the outputs corresponding to the group of size 1 as zero.
- For satisfying the weight conditions, we need the following.
  - The inputs corresponding to the 56 groups of size 21 should have the output 0 and the rest 56 should have the output 1.
  - The inputs corresponding to one group of size 3 should have the output 0 and the other one should have the output 1.

With these constraints, we have $2\binom{112}{56}$ options to search which is computationally infeasible. For each option one may get back to the Boolean function of 21 variables and check the nonlinearity. However, this checking is time consuming and following [5, Remark 3] a much better strategy is to consider the concept of inequalities as explained in [5, Sec. 2.1] for $n = 15$. We implement the strategy for $n = 21$ and generate the inequalities as completely described in Appendix. We consider the degree 21 primitive polynomial $z^{21} + z^2 + 1$ over GF(2) for realization of the field. Following (3) and putting the values $a = 7, b = 3$, we obtain $57 \leq t(\alpha) \leq 72$.

TABLE I
THE FOUR SOLUTIONS THAT WE OBTAINED BY HEURISTIC SEARCH

0111000110111110011111101010010010111001110100001001100010100100101110001000001000100110100101110111011001111100000
0110010100111001010110000100001100111110011100111000000100010100000111111001110000111111001001011111100101001111000
0111010010100001111110010011001010111111000111001101001011001100101100110010000111110111011010000000000000101111001
0011000111100101111000100011011010100001101010101011011111111010001000001010111010100101000101100110010101110010100

Thus, the overall inequality is of the form $57 \leq \sum_{i=0}^{114} A_{i,j} x_i \leq 72$, where each i, j varies from 0 to 114 (total 115 elements) and there are 115 binary variables x_0 to x_{114}. The coefficient matrix $[A_{i,j}]$ is described in Appendix. So, we have the following technical result here.

Lemma 1: Let $x_i \in \{0, 1\}$ for $i \in [0, 114]$ and the coefficient matrix $[A_{i,j}]$ be as described in Appendix. If one obtains a solution to the set of inequalities $57 \leq \sum_{i=0}^{114} A_{i,j} x_i \leq 72$, for $i, j \in [0, 114]$, then that provides a 21-variable Patterson-Wiedemann type function having nonlinearity greater than the bent concatenation bound.

We like to present an observation here that if one leaves the rows and columns indexed by 0, 93 and 114, then the resulting 112×112 matrix becomes symmetric.

A. The Functions That We Obtained

As described above, we consider binary strings of length 115 such that the 0-th location is 0, one location (out of two locations corresponding to the groups of size 3) is 0 and the other is 1 and finally 56 locations (out of 112 locations corresponding to the groups of size 21) are 0 and the rest 56 are 1. This is clearly an integer programming problem, and seems to be a hard one given its dimension. Thus, we have attempted several heuristics and with one such heuristic, described in Section II-B, we obtain 4 solutions with an effort of more than a month. The solutions are as in Table I. For complete truth tables of these functions and relevant codes, one may refer to [11].

Let us now briefly explain the autocorrelation spectrum of a Boolean function. Let $f \in \mathcal{B}_n$. The autocorrelation, $\Delta_f(\alpha)$ of f with respect to $\alpha \in GF(2^n)$ is

$$\Delta_f(\alpha) = \sum_{x \in GF(2^n)} (-1)^{f(x)+f(x+\alpha)}.$$

The absolute autocorrelation indicator Δ_f is defined as

$$\Delta_f = \max_{\alpha \in GF(2^n)^*} \left|\Delta_f(\alpha)\right|.$$

All the solutions have nonlinearity $2^{21-1} - 2^{\frac{21-1}{2}} + 61 = 1047613$ and the absolute autocorrelation indicator of these four functions are 2948, 3436, 3940, 5116. These different values show that the functions are not affine equivalent.

Thus, we have the following important theorem.

Theorem 1: For $n = 21$, one can construct Patterson-Wiedemann type functions (see Definition 1) having nonlinearity greater than bent concatenation bound $2^{n-1} - 2^{\frac{n-1}{2}}$. In particular, we construct functions having nonlinearity $2^{21-1} - 2^{\frac{21-1}{2}} + 61 = 1047613$.

B. Details of Our Heuristic

In order to attain our solutions, we utilize the steepest-descent-like iterative search algorithm [1], which was used in [7] and [8] to identify the 9-variable Boolean functions with nonlinearity greater than the bent concatenation bound. The search algorithm starts with an initial candidate solution, and at each iteration step the current candidate solution is replaced with the best neighbor solution (with respect to a cost function) within its predefined neighborhood. In other words, the best solution in the neighborhood, i.e., the one with the best cost value, is delivered to the next iteration step as the output of the preceding iteration, even if it is worse than the previously chosen iteration outputs. To prevent the algorithm from vicious loops, these best solutions are stored in memory.

The pseudocode for our heuristic search algorithm is given in Algorithm 1. The initial solution $s_{initial}$ is generated randomly such that it satisfies the weight condition as explained in the previous subsection. We have used the Mersenne Twister code [13] for producing the random numbers needed in our implementation. Here, we constitute the neighborhood by swapping two dissimilar bits (of the current solution s) at the locations corresponding to the groups of the same size. This implies that we will always get a neighbor solution $s_{swapped}$ keeping the weight condition satisfied. The entire neighborhood consists of in total $56^2 + 1 = 3137$ of them, which are obtained in lines 12 and 17 of Algorithm 1. For each $s_{swapped}$, we compute the cost function that we define as the sum of squared errors, which is a measure of its distance from the inequality bounds. Let $x = (x_0, x_1, \ldots, x_{114})$ be a solution, $A_i = (A_{i,0}, A_{i,1}, \ldots, A_{i,114})$ be the i-th row of the coefficient matrix, and $(x, A_i) = \sum_{j=0}^{114} A_{i,j} x_j$ be the inner product of x and A_i, where $i = 0, 1, \ldots, 114$. The cost function is then given by

$$Cost(x) = \sum_{i=0}^{114} C_i^2,$$

where

$$C_i = \begin{cases} |(x, A_i) - 72|^2 & \text{if } (x, A_i) > 72, \\ 0 & \text{if } 57 \leq (x, A_i) \leq 72, \\ |(x, A_i) - 57|^2 & \text{if } (x, A_i) < 57. \end{cases}$$

Thus, any solution x with zero cost value provides a 21-variable Patterson-Wiedemann type Boolean function having nonlinearity greater than the bent concatenation nonlinearity.

At each iteration, each $s_{swapped}$ out of the 3137 neighbor solutions and corresponding cost value $cost_{swapped}$ are stored in SET and $COST$ respectively. Then the algorithm finds within the neighborhood the best one, s_{min}, with the minimum cost value $cost_{min}$. To avoid the algorithm from being stuck to eternal loops, it is checked that whether the chosen solution s_{min} is already in $STORE$ which contains all the previous iteration outputs. If s_{min} is found in $STORE$, then it is

Algorithm 1 The Pseudocode of Our Heuristic Search

```
input : A randomly generated initial solution $s_{initial}$
output: A solution $s_{min}$ with zero cost value, otherwise
        the $N$-th iteration output
$s \leftarrow s_{initial}$;
for $K \leftarrow 0$ to $N-1$ do
{
    $k \leftarrow 0$;
    // Among the 112 locations corresp.
    // to the groups of size 21
    $B_0 \leftarrow$ the 56 locations of 0's in $s$;
    $B_1 \leftarrow$ the 56 locations of 1's in $s$;
    // Between the 2 locations corresp.
    // to the groups of size 3
    $b_0 \leftarrow$ the location of 0 in $s$;
    $b_1 \leftarrow$ the location of 1 in $s$;
    for $i \leftarrow 0$ to 55 do
        for $j \leftarrow 0$ to 55 do
        {
            Swap $s[B_0[i]]$ with $s[B_1[j]]$;
            $SET[k] \leftarrow s_{swapped}$;
            $COST[k] \leftarrow cost_{swapped}$;
            $k \leftarrow k+1$;
        }
    Swap $s[b_0]$ with $s[b_1]$;
    $SET[k] \leftarrow s_{swapped}$;
    $COST[k] \leftarrow cost_{swapped}$;
    $cost_{min} \leftarrow$ minimum $cost_{swapped}$ in COST;
    $s_{min} \leftarrow$ respective $s_{swapped}$ in SET;
    while $s_{min}$ is already in $STORE$ do
    {
        Remove $cost_{min}$ from $COST$;
        $cost_{min} \leftarrow$ minimum $cost_{swapped}$ in COST;
        $s_{min} \leftarrow$ respective $s_{swapped}$ in SET;
    }
    if $cost_{min} = 0$ then
        return $s_{min}$;
    $STORE[K] \leftarrow s_{min}$;
    $s \leftarrow s_{min}$;
}
return $s_{min}$;
```

replaced with the next best solution among the remaining neighbor solutions, which repeats until s_{min} is not in $STORE$. When this condition is satisfied, it passes to the input of the next iteration and it is the output of Algorithm 1 if the corresponding cost value is zero.

The search algorithm stops after a fixed number of iterations, N, which we set to 40000 in our experiments. The search is performed on a workstation with Intel Xeon CPU E5-1650v3 (15M Cache, 3.50 GHz, 6 cores) and 16 GB RAM under Windows 7 Professional 64-bit operating system. A typical run of the algorithm takes less than two minutes and exploiting all the cores, it took little more than a month to extract the aforementioned 4 solutions.

TABLE II

THE COEFFICIENT MATRIX $[A_{i,j}]$

3000000000000000v0000v0000000000000vv00000000000000000000000000000000000000000000000000000000000000000000000000vv0
0202012212121203300125012001011311232101301000011200232001010312003121112311013021001012111211110130031000101211310
0000130011341121121413111111012021011101211010012110010031112112202101201004102210131110112220101226110111101104020
0202110200101500011132203003323201111120301020110113230122222020131111012011110400001311012120200201311102010102200
0011020312401100100110132202231121211201211101114022212200214001212000011200023110111031011200343001123011101001030
0131243021020211111011212032031030010222104210113100212101220223202100111100133111100320022000000001300021120111201
0200032003002011103102002122110001303223220302101300212021233111111111123113201000111220020120122400200100014100110
0202300032311114010102201131110310030102020410020112210200122021111121012212100021012431200110123012001103010102211
0110120320122001021110112300122201122012041321003020220112111131102110042010120103110101140040220141110010200112200
0210213200311030221032123201011131202110001301010111132211411221002125111001110000225201112010211011001001120021010
0131400313004001113133111100100110202112320210023000001011102201100231221220011431130211103000111101201022120112110
0240020121000111121322222130003402110111101402100131012302111112042120210110102210430020011011111212111101001100110
0111102121400112031001112211111022120210240101403211111024200200101120201121111100111301012122021001220213112111100
0215120100011012221220022110131111111330220011121221001311010010022305212202103122010211020010040012100022212001100
0020011103011124010100120210041022132110311110100132212021221150120211201310011113031112104120202301010110120010110
0310011410112242011101101122031212002101122203201111210120111100121132031102002130101011223400010001100251000311110
0310111002110200213301211211111111210221121202021105103030001011111112011402021200110001131121202021002120120043201
1021010122123211113321001301132012200300011122120202110101031212221000230121112022015221111011011110111011010112000
0011013011311101332011222120010210100001110150102304110121031122131021123102110141220001113210021010311000311110020
0141101110130211330002012200400211210411211101011011301120241020301240000101201202122022220100001121211121213201000
0213110013320200021001113222301011132112102001101110031241300102121211451210001133201011210110003111101110020011010
0532012202321001111212110002022120100010121033100121001111313212301100102111110313212020300120021001010111122110500
1012120211121011202011121113010313123012322111112112111222110230012110110002211200210011401220010001003003033011001
0110310012121220102111220000011102511231121121100131220311331202002001201320120021020101130510001012211114100110110
0213222123122201112230102030122102220001021101401010031021010031300012002111001100142112120110100010114031122100140
0010201132112121231220100012100142100210201102111001021021311123042200013221020101100212201210140251102131012000100
0010032300031112102020103101211101031310201341431121101012111103103021113311000211111110200000112122001412011030020
0113222101001002110022300214001104330201101222022023200010210211300002310022001010311013011120231122310220120201100
0003201110101100110430001120013121102213232121111401210220312221201021120200112000210123213000002121012501201010200
0112331121001343131002112010142110400010211133003102011021101210012111210021200002200031100000203120012111210212312 0
0123110021031111120012012011320103112110011112111112012211103005100121100032111010010220346130221110011101111120110
0302100321140102102201311111111032102120120110221211111002111021010121210011121121411253010300300121300000102040010
0120230103102121111112100400210320012110013011001114031202111012100022113010113021110222000130000012231421024021110
0111101011022122120110322214103204100020212111111420010221011310101012011511130201203220311010000110202201011003120 0
0201203012211110221211152103141101010314112122010021102000000010002110221011010230221412211120100320031222002110010
0311110320012130100130212033001010121211312101110113111011010101210120211001141023032100012130015031111002204111110
1211103022200122000020310010202220011010201112023210110101112122211013221311001311111101151110302211120122104111000
1111222101112311230410020232201110320122111110201010211112101101101133003111020113200130002220221102011100110420000
0002022011111310200111130110111212111200142300141012051011023200110121302122231113401100311000111201100131101001210
0110123220210001101120211001300000410200143113111210221300000321341321101111201130000222102130101213011010021022120
0323212000312231101211310221220102132111021000022110010010123221135210010130121110031000001010020110201300112241010
0010102240204212211102222000311211110144201003421222110020122132000102110021023021211001110020111003000100021111210
0111140011010012110121211111211032221123110112012632021011101012110131010210330411113201200210020010021120000302020
0000123433241012211100111132111101111131001012011003020312111000212032310220121200021112011100020400001201311103300
0012010120100110025003120042231111201101001101111110310111012131200132412200221211012000101110230133132212011030200
0000102011021103220113111212132011212003032210120021202013201103141013010020111322002002021100012003204111104011200
0001111000014112011011111414010120101021104001101110300120151021111220021121203231110302111121030021203102112222 0120
0111110201200200220100100132101201112041221112101102005013012332303012010121211042013112211000210222210123000001020
0120431030303101102110201112131114003111212110110021111230110102211122001212301232101110100101401120020100412100100
0211013101012211123011110010411212012002126010110212101101301211110002111101111102140222210201142221100002100213020
0011200121031231000112131022001110211111123012002121312212023110110002021223001412202211011011020030100300241010040
0003200201011121524101210113122140130020022301321210011301331101111020010112001221010001111030202210130110111102120
0202222221001022111300120012200101111202010032001130022112231011011021112100014101002101502011302112502011211122110
0313111123011011011030123200111130011152112210001011200110030211321021111033110002101000202301220203123210001022120
0200022200212112030011110111001211221011100100215112120033210103110122005201122011201002210300122110222001301211023 0
0001210212030301011121230000202022001103000310202123113431111420211201112111001020012110101010121110110121104432200
0032002011102122302241212211221001010110121111013010113324001031000111110101120020102110210500113221200300021202310
0112011021124110011011211120011220011210001213130121202142003411103122100100102202100313100340012200323010200111010
0012222114112021000233130312311111001100111102501303201100201010113221110111200113101000121110100232301002200110221
0112123211010121033401131111100111011020220110111023330100001315101410030012202201012103010200213100111212121100110
0022403211210011111103010110213113002130321121020131101113121113310213230020320000011100101200021200120200103100 31
0310021012212011021012220112220001011123210011231211020404031400011111001102110102121032023000202041113230020101100
0112021232010150112201303201210210102002231030130110113231111001311101101320010011312103012010120112131001011300101
0220131111120000122022021331105121012101122013122101111011051010011302101140011120000203201210313011001102111310110
0021221110101011121313003013201010022113101221132111031201113030221001100111100013111012011421011200010043311040110
0003101100040222123020100400010101011014301104101111120100103111223112102110230120211220111111203112221021231100210
0321221122021201111111220230120000201101500201231001111033111111301010210011110101021024201200201020403014101220 20
0111011111211321100221100200011101110113211010201000002211240113011031410001401311101203011130342110001131111131231
0201001212322013102410101020212222121322103331012002222012212100010302200010400111000000122000011021241011031210020
0111001105100512201010012012111120003311021223022220110112101112121120110012212011131101000120310023002112430310100
0120011001222220021041120013121211222031010340200100110111103011110421210211032010001024210011111112110120213102021
0101112141210103132050100111210111212000111111110121115110132000002101140114232202120021001120001102121222110220100
0212113221101211103012012330000035111321000020101110212200003111021000002100110223201013122030101112001213112204120
0300211200211231411121031230200001003111102220212121100111100131110000211452302200102131111130012011222020100001200
0101001110212010020011021212023111101121321202121021031100110024110011110502200012110121101010010211412102132533120
0141003201001202212101201112012101111121010000212132031110122200101102140220200101101420203210011134022010303111021
0011012111011100011201210000121113010022103121023100012011220100121442021322011011214030011250111011212204211001220
0101230021101010211001120200101210140230223221310100112020003111031001331000101200024131111330021002111111132231130 0
0320331000121312120110101001201132011011130111211111400102022001001102220200112030312000102120021520124012131012210
0024110010421111201213201120000100203111104223302142101002120101010310022201020002112202012100310301012121111211310 0
0210110200310213024031020011001221321113121012143012001220100012121111102010103004113210122210100310211300101100121
0100010130100230021233010110020112031330011012122221122002310210300111023021100240120021220100122301113000321121101
0010111012141001102122201113220410201240021000101120010011100130121101012111203111402101113010125110121222320032111 0
0030101112331130112201124011101113231000311210010401001100010210110003020010121112000220210020321202313331211210310
0111101205001011050212002011000102121010113122331020210220121120112101101201442230202210121110211010111200102123010
0013032412203210020000011210102222411112002100011220100113011012021201000114010220122211211100003221230121211030301
0111322300120111020212101111232520100302000100211210002111001300120000221322330012021102221320311101201200142001010
0201100111101121111210112203310323201002011202120211102003030233202301413110010201100120012200001001011211511103130
0110000211100012111122341122021300120103101201012120152112110000201401020111201101212122040102022110011114133210101 0
0111122041011202311210032001104101115010010102110111000010211210112120102100110122112121022210132011330321041013011
0122120002312043113000100101306000121212100111110011223100100321110120012113132220301112122110020111102102301011110
0221201100001014102111251201001311111201002111201200030053121002411101010102231121001132021010121311012113110121110
0122002141012120211012211102003030231203121010100013100104102011212302123311502010121020211120300100101221100111010
070000000007u00077000000000000000000000007770777000000000077000070000000000000000000000000000000700000000707000000003
0112301122110020200000001112022300103211010020324102322110120213020303101000120311132030210131012312111220000211110
0100402221112401012002100413002000010210212231010420022211010021102411100111112102221010232200141101122110012011120
0010302301111020211131010021231001052111010002001202201132032203130210111201101002511311120100210002131012111122210
0122004010120030010110000211111101302122100410221202121122211010211100111021005333120210101310310030022102021113210
0320000141010100211210011522221210231001101030122231100120302411010122101113122010101200011100100320101023122111230
0061110211121211100111120122100122011213030033220100232010200121022013222114110101020111011100212000241101001013210
0013132010212101013210021103000320011010200012020111512123310110020020110240211021131220131010111012001130102222230
0311200010012010011101011001111032312101002030312003022102011130124040120212112111211301130100123204021110131300210
0101300101110000211110314210221012110101101124100000230003112311010112011222214213131011102210121211110211102211112
0011001100012012100111010142511040201110311221011031020130020201003101122010210130232122131121210101112211111111321
0010120010201215210211013312010021202031002011220001111201012300420311221201011200230201420120211020311102001220220
0012110301213201010101341120121010222010000121130200103100220012311112023020412100310101112311002231001122032202100
0110110021101210103201011001211101021110100301104121200102210001324104211113231113221215303110001010111100012211320
0001021102201120211122302112001021000102120110201041101020021211131133111030123102010141340100011220030103140122110
0110104000012200001302302210121240244011210114202011112410010011110110302023121211012121211000021121212112200111000
0211011110111003011201011002011000111400213100201201101421113133011123122051030111321001100110201110232122211203011
0100010012101011411011110030122423111202410031200110221301101001402311020031011102212300011210112111201120121043110
0142110221201101320110100001030011011012112301010302220221000100002100204131112301103013131110112313201102121330030
1302021220111111200005011101211012010021020322101001112230210111120201011210232111130301001100112222221321310010130
1120301101110011002010014020021110110012112000220242123011213001112320202022201020111013111110121131311220210113310
0000070700000000700000700000000000000000000000000000000000707070000700700007000077000700070003000000000u700000700000

III. CONCLUSION

In this paper, for the first time, we could demonstrate Patterson-Wiedemann type Boolean functions on 21 variables that exceed the bent concatenation nonlinearity. This problem remained open for more than three decades even after significant effort as evident from the literature. We deploy heuristics to obtain such functions that can be seen as solutions to an integer programming problem with 115 binary variables. Indeed the problem is quite hard and exhaustive search seems to be elusive given the present computational power. The functions we obtain are of nonlinearity $2^{21-1} - 2^{\frac{21-1}{2}} + 61 = 1047613$ and we believe that further search effort may discover solutions with better nonlinearity. In this direction, we provide every details of the inequalities that need to be satisfied to obtain the solutions.

Appendix
The Coefficient Matrix A

In Table II, we have the 115×115 coefficient matrix, where each location contains an integer. The single digit integers 0 to 9 are written as they are. For brevity, the two digit values 14 and 21 are written as u and v respectively.

Acknowledgments

The authors like to acknowledge the anonymous reviewers and the Associate Editor for providing editorial as well as technical comments that improved this paper substantially. The second author likes to thank the Centre of Excellence in Cryptology, Indian Statistical Institute for support towards this research.

References

[1] M. Bartholomew-Biggs, "Chapter 5: The steepest descent method," in *Nonlinear Optimization With Financial Applications*. New York, NY, USA: Springer, 2005, pp. 51–64.

[2] E. Berlekamp and L. Welch, "Weight distributions of the cosets of the (32, 6) Reed–Muller code," *IEEE Trans. Inf. Theory*, vol. 18, no. 1, pp. 203–207, Jan. 1972.

[3] J. F. Dillon, "Elementary Hadamard difference sets," in *Proc. 6th S.E. Conf. Combinat., Graph Theory, Comput. Utility Math.*, Winnipeg, MB, Canada, 1975, pp. 237–249.

[4] C. Fontaine, "On some cosets of the first-order Reed–Muller code with high minimum weight," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1237–1243, May 1999.

[5] S. Gangopadhyay, P. H. Keskar, and S. Maitra, "Patterson–Wiedemann construction revisited," *Discrete Math.*, vol. 306, no. 14, pp. 1540–1556, Jul. 2006.

[6] G. Gong, "Theory and applications of q-ary interleaved sequences," *IEEE Trans. Inf. Theory*, vol. 41, no. 2, pp. 400–411, Mar. 1995.

[7] S. Kavut, S. Maitra, and M. D. Yücel, "Search for Boolean functions with excellent profiles in the rotation symmetric class," *IEEE Trans. Inf. Theory*, vol. 53, no. 5, pp. 1743–1751, May 2007.

[8] S. Kavut and M. D. Yücel, "9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class," *Inf. Comput.*, vol. 208, no. 4, pp. 341–350, Apr. 2010.

[9] S. Kavut, "Correction to the paper: Patterson–Wiedemann construction revisited," *Discrete Appl. Math.*, vol. 202, pp. 185–187, Mar. 2016.

[10] S. Kavut and S. Maitra. (2015). *Patterson–Wiedemann Type Functions on 21 Variables With Nonlinearity Greater Than Bent Concatenation Bound*. [Online]. Available: http://eprint.iacr.org/2015/1036.

[11] S. Kavut and S. Maitra. (2016). *Steepest-Descent-Like Search Algorithm: Heuristic Search to Find 21-Variable PW Type Functions With NL > 1047552*. [Online]. Available: https://sourceforge.net/projects/pw21/.

[12] S. Maitra and P. Sarkar, "Modifications of Patterson–Wiedemann functions for cryptographic applications," *IEEE Trans. Inf. Theory*, vol. 48, no. 1, pp. 278–284, Jan. 2002.

[13] M. Matsumoto and T. Nishimura, "Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator," *ACM Trans. Model. Comput. Simul.*, vol. 8, pp. 3–30, Jan. 1998.

[14] J. J. Mykkeltveit, "The covering radius of the (128,8) Reed–Muller code is 56 (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 26, no. 3, pp. 359–362, May 1983.

[15] N. Patterson and D. Wiedemann, "The covering radius of the $(2^{15}, 16)$ Reed–Muller code is at least 16276," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 354–356, May 1983.

[16] S. Sarkar and S. Maitra, "Idempotents in the neighbourhood of Patterson–Wiedemann functions having Walsh spectra zeros," *Designs, Codes Cryptogr.*, vol. 49, no. 1, pp. 95–103, Dec. 2008.

Selçuk Kavut received B.Sc. degree in Electronics Engineering from Ankara University in 1998. He received M.Sc. and Ph.D. degrees in Electrical and Electronics Engineering from the Middle East Technical University in 2002 and 2008, respectively. From 2009 to 2014 he was with the Department of Electronics Engineering at Gebze Technical University, now the Department of Computer Engineering at Balıkesir University, where he is an assistant professor. His research interests are in cryptology and coding theory.

Subhamoy Maitra received his Bachelor of Electronics and Telecommunication Engineering degree in the year 1992 from Jadavpur University, Calcutta and Master of Technology in Computer Science in the year 1996 from Indian Statistical Institute, Calcutta. He has completed Ph.D from Indian Statistical Institute in 2001. Currently he is a Professor at Indian Statistical Institute. His research interests are in Cryptology and Security.