A Modified Patterson-Wiedemann Construction Having Nonlinearity Greater Than Bent Concatenation Bound

Selçuk Kavut[0000−0002−9460−1418]

Department of Computer Engineering, Balıkesir University, Balıkesir 10145, Turkey
skavut@balikesir.edu.tr

Abstract. The Patterson-Wiedemann (PW) construction having odd number of variables n, where $n = pq$ such that p and q are distinct prime numbers, can be interpreted as idempotent functions which are represented by the (d, r)-interleaved sequences formed by all-zero and all-one columns, where $r = (2^p - 1)(2^q - 1)$, $d = \frac{(2^n-1)}{r}$. We here study a modified form of the PW construction, which only requires $2^n - 1$ $(= dr)$ be a composite number, by relaxing the constraint on the values of d and r. We then elaborate the case $n = 15$ and consider the functions corresponding to the (217, 151)-interleaved sequences. Taking into account the functions satisfying $f(\alpha) = f(\alpha^{2^k})$ for all $\alpha \in \mathbb{F}_{2^n}$ in this scenario, where k is a fixed divisor of n, we obtain new Boolean functions with nonlinearity 16268 exceeding the bent concatenation bound, which are not affine equivalent to the PW functions. Further, it has been recently shown that the maximum possible nonlinearity is 16276 for the functions corresponding to the (151, 217)-interleaved sequences; however, we find that in our case there is the possibility to achieve or exceed the best known nonlinearity 16276 of the PW functions.

Keywords: Nonlinearity · Patterson-Wiedemann (PW) construction · Bent concatenation bound.

1 Introduction

The maximum nonlinearity of n-variable Boolean functions – or, equivalently, the covering radius of the Reed-Muller $RM(1, 2^n)$ codes of order 1 and block length 2^n – is unknown for odd $n > 7$, as a long-standing open problem in cryptography and coding theory. The highest known nonlinearity had been the bent concatenation bound of $2^{n-1} - 2^{\frac{n-1}{2}}$, till Patterson and Wiedeman discovered [9] in 1983 the 15-variable Boolean functions with nonlinearity 16276 $(= 2^{15-1} - 2^{\frac{15-1}{2}} + 20)$, using a hybrid approach of combinatorial methods and heuristic search together. It is well-known that the direct sum of a bent function with one of these PW functions gives nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 20 \times 2^{\frac{n-15}{2}}$ for odd $n > 15$. For the smaller odd number of variables, the bent concatenation bound could be exceeded [7] over two decades later by attaining 9-variable

Boolean functions having nonlinearity 241 ($= 2^{9-1} - 2^{\frac{9-1}{2}} + 1$) in the rotation symmetric class. Shortly after that, this result is improved [8] to 242 by performing a search properly within the generalized rotation symmetric class (also known as the class of k-rotation symmetric Boolean functions (k-RSBFs)). Thus the highest known nonlinearity is $2^{n-1} + 2^{\frac{n-1}{2}} + 2^{\frac{n-7}{2}}$ for $n = 9, 11$, and 13. As evident from the above discussion, the lower bound of the maximum nonlinearity for odd n could be improved only by discovering Boolean functions having nonlinearity greater than the bent concatenation bound. For even n, the maximum nonlinearity is $2^{n-1} - 2^{\frac{n}{2}-1}$ and Boolean functions having this nonlinearity are called bent. It should also be noted that the generic upper bound on nonlinearity is $2\lfloor 2^{n-2} - 2^{\frac{n}{2}-2} \rfloor$ [3].

We now give a description of the PW construction. Let $n = pq$ such that p and q are distinct prime numbers. The invariance of a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ under the action of $\mathbb{F}_{2^p}^* \times \mathbb{F}_{2^q}^*$ implies that $f(\xi^i) = f(\xi^{i+jd})$ for all $i = 0, 1, \ldots, d-1$ and $j = 0, 1, \ldots, r-1$, where $r = (2^p - 1)(2^q - 1)$, $d = \frac{2^n-1}{r}$, and ξ is a primitive element of $\mathbb{F}_{2^n}$. In other words, f is invariant under the action of a cyclic subgroup of order r of $\mathbb{F}_{2^n}^*$. Then, the function f can be interpreted in terms of a (d, r)-interleaved sequence as follows [2]:

$$f^{d,r} = \begin{bmatrix} f(\xi^0) & f(\xi^1) & f(\xi^2) & \ldots & f(\xi^{d-1}) \\ f(\xi^d) & f(\xi^{d+1}) & f(\xi^{d+2}) & \ldots & f(\xi^{2d-1}) \\ f(\xi^{2d}) & f(\xi^{2d+1}) & f(\xi^{2d+2}) & \ldots & f(\xi^{3d-1}) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ f(\xi^{(r-1)d}) & f(\xi^{(r-1)d+1}) & f(\xi^{(r-1)d+2}) & \ldots & f(\xi^{rd-1}) \end{bmatrix}, \tag{1}$$

where each column is either all-zero or all-one column. The PW construction exploits the above structure and puts an additional condition of being invariant under the Frobenius automorphisms (i.e., $f(\alpha) = f(\alpha^2)$ for all $\alpha \in \mathbb{F}_{2^n}$ and such functions are called idempotent). Thus, a Boolean function f obtained from the PW construction is an idempotent in the form of a (d, r)-interleaved sequence consisting of all-one and all-zero columns. Let the rows and columns of the interleaved sequence be numbered from 0 to $r-1$ and 0 to $d-1$, respectively. Note that, thanks to the the idempotency property, the set of columns is partitioned into the equivalence classes with respect to the equivalence relation defined by $i \sim j$ if and only if $i \equiv j \times 2^s \mod d$ for some nonnegative integer s, and hence all the columns corresponding to the same equivalence class are either all-one columns or all-zero columns, where $i, j \in \{0, 1, \ldots d-1\}$.

Let us now consider n-variable Boolean functions for which $f(\alpha) = f(\alpha^{2^k})$ for all $\alpha \in \mathbb{F}_{2^n}$, where k is a fixed divisor of n. These functions can be interpreted [8] as (generalized) k-RSBFs by a proper choice of basis. It should be noted that when $k = 1$, we get idempotent functions which correspond to 1-RSBFs (simply called RSBFs) forming the rotation symmetric class [1]. In [4], the constraint imposed by the idempotency property of the PW construction is relaxed and the 15-variable functions satisfying $f(\alpha) = f(\alpha^{2^k})$ for all $\alpha \in \mathbb{F}_{2^{15}}$ are searched exhaustively for $k = 3$ and $k = 5$ (the case of $k = 1$ corresponds

to the PW construction). In both cases, new functions with nonlinearities 16268 and 16269, which are not affine equivalent to the PW functions, exceeding the bent concatenation bound are obtained. Recalling that the 9-variable Boolean functions having nonlinearity 242 are also obtained within the class of k-RSBFs, the result of [4] confirms that the class of generalized RSBFs contains highly nonlinear Boolean functions and it makes sense to search for them.

In this paper, we study a modified version of the PW construction in which n-variable Boolean functions with $2^n - 1$ being a composite number are considered and we obtain the necessary conditions, i.e., system of inequalities, to achieve nonlinearity greater than the bent concatenation bound for those corresponding to the interleaved sequences having each column either all-zero or all-one. Specifically, we elaborate the case of 15-variable Boolean functions which are represented in the form of (217, 151)-interleaved sequences consisting of all-one and all-zero columns, satisfying $f(\alpha) = f(\alpha^{2^k})$ for all $\alpha \in \mathbb{F}_{2^{15}}$ where $k = 1, 3$, and 5. Note that taking $k = 1$ and swapping the number of rows and the number of columns give the PW construction. We then obtain the system of inequalities for our case to exceed the bent concatenation bound and find that there exist some solutions. It is computed that the search spaces are of size 2^{21}, 2^{49}, and 2^{93} for $k = 1, 3$, and 5, respectively. After that, we perform an efficient exhaustive search for $k = 1$ and $k = 3$ by exploiting the system of inequalities and the functions having nonlinearity greater than the bent concatenation bound are enumerated. The nonlinearities we obtain are $16260, 16261, 16267$, and 16268. We have checked that the functions with these nonlinearities are not invariant under the action of $F_{2^3}^*$ or $\mathbb{F}_{2^5}^*$, and are not affine equivalent to the PW functions.

Next, we compute the possible nonlinearities for our case, i.e., the case of (217, 151)-interleaved sequences consisting of all-one and all-zero columns, by utilizing the method in [6] used to find some nontrival upper bounds and possible nonlinearities of a super-set of PW functions. It has been shown in [6] recently that for the 15-variable functions which are invariant under the action of $F_{2^3}^* \times \mathbb{F}_{2^5}^*$ (corresponding to the $(151, 217)$-interleaved sequences), the maximum possible nonlinearity is 16276 and all the possible nonlinearities are $16268, 16269, 16275$, and 16276 (which are achieved by the PW functions). However, in our case we find that all the possible nonlinearities are $[16259, 16261]$, $[16267, 16269]$, $[16275, 16277]$, $[16283, 16285]$, 16291, and 16292. Thus there is the possibility of an improved nonlinearity result with further search effort. We have also considered the cases $n = 11$ and 21 for which $2^n - 1$ is a composite number, which again indicates the existence of possible nonlinearities greater than the bent concatenation bound for both cases.

It is to be noted that the best known nonlinearity results in literature could be found merely by devising relatively small search spaces that are rich in terms of high nonlinearity. This is probably not an easy task, as evident from very few results in this direction. Therefore, identifying and canalizing search efforts to proper search spaces is of importance. The modified PW construction that we suggest basically provides more choices to look into for a suitable corpus of Boolean functions and our results for $n = 15$ indicate their existence. Further,

one can perform the search efficiently, since any solution of a system of linear inequalities (of size at most d) provides a Boolean function with nonlinearity greater than the bent concatenation bound, as shown in Section 2.

In the following section, we obtain the system of inequalities, for the case 2^n-1 is a composite number, to exceed the bent concatenation bound. In Section 3, we present the details of our exhaustive search and then we compute the possible nonlinearities for $n = 11$, 15 and 21 in Section 4.

2 Finding System of Inequalities

We start with the following proposition, which indicates that the linear functions, when considered in the form of interleaved sequences, are column-wise cyclic rotations of each other.

Proposition 1 *Let the function defined by $h(\xi^i) = Tr_1^n(\xi^i)$ for all $0 \leq i < 2^n-1$ be represented in the form of a (d,r)-interleaved sequence $h^{d,r}$, where ξ is a primitive element of $\mathbb{F}_{2^n}$ and $dr = 2^n - 1$. Then the j-th column of the (d,r)-interleaved sequence $g_t^{d,r}$ corresponding to the function $g_t(\xi^i) = h(\xi^{i+t})$ is a u-cyclic rotation of the v-th column of $h^{d,r}$ such that $v + ud \equiv j + t \mod 2^{n-1}$, where $0 \leq j, v < d$, $0 \leq u < r$, and $0 \leq t < 2^n - 1$.*

Proof. The v-th column of $h^{d,r}$ can be expressed as the following:

$$(Tr_1^n(\xi^v), Tr_1^n(\xi^{v+d}), Tr_1^n(\xi^{v+2d}), \ldots, Tr_1^n(\xi^{v+(r-1)d}))^T,$$

where $(.)^T$ stands for the transpose. On the other hand, the j-th column of $g_t^{d,r}$ can be written as follows:

$$\begin{aligned}
&(Tr_1^n(\xi^{j+t}), Tr_1^n(\xi^{j+t+d}), Tr_1^n(\xi^{j+t+2d}), \ldots, Tr_1^n(\xi^{j+t+(r-1)d}))^T \\
=&(Tr_1^n(\xi^{v+ud}), Tr_1^n(\xi^{v+(u+1)d}), Tr_1^n(\xi^{v+(u+2)d}), \ldots, Tr_1^n(\xi^{v+(r-1)d}), Tr_1^n(\xi^{v+rd}), \\
&Tr_1^n(\xi^{v+(r+1)d}), \ldots, Tr_1^n(\xi^{v+(r-1+u)d}))^T \\
=&(Tr_1^n(\xi^{v+ud}), Tr_1^n(\xi^{v+(u+1)d}), Tr_1^n(\xi^{v+(u+2)d}), \ldots, Tr_1^n(\xi^{v+(r-1)d}), Tr_1^n(\xi^{v}), \\
&Tr_1^n(\xi^{v+d}), \ldots, Tr_1^n(\xi^{v+(u-1)d}))^T,
\end{aligned}$$

where the last expression is the u-cyclic rotation of the v-th column of $h^{d,r}$. □

Since the g_t functions having $g_t(0) = 0$ for all $t = 0, 1, \ldots, 2^n - 2$ and the constant function with all 0's, denoted by $\mathbf{0}$, form all the linear functions, we need to find all the distances (of an n-variable Boolean function f) to these functions and their complements in order to compute nonlinearity (of f). Let $W_t = (W_{t,0}, W_{t,1}, \ldots, W_{t,d-1})$ such that $W_{t,j}$ is the weight of the j-th column of $g_t^{d,r}$ corresponding to the linear function defined by $g_t(\xi^i) = Tr_1^n(\xi^{i+t})$ for all $i = 0, 1, \ldots, 2^n - 2$ and $g_t(0) = 0$. Then, one can find the distance between the function f, for which $f(0) = 0$ and each column of $f^{d,r}$ is either all-zero or all-one, and the linear function g_t as given below:

$$d(f, g_t) = \sum_{i=0}^{d-1}(r - W_{t,i})l_i + \sum_{i=0}^{d-1} W_{t,i}(l_i \oplus 1) = 2^{n-1} + r\sum_{i=0}^{d-1} l_i - 2\sum_{i=0}^{d-1} W_{t,i}l_i, \quad (2)$$

where $l_i = 1$ if the i-th column of $f^{d,r}$ is all-one and $l_i = 0$ otherwise. Next, it follows from the definition of nonlinearity that the following inequalities must be satisfied to exceed the bent concatenation bound (given by μ):

$$d(f, \mathbf{0}) = r\sum_{i=0}^{d-1} l_i > \mu, \quad (3)$$

$$d(f, \mathbf{1}) = 2^n - r\sum_{i=0}^{d-1} l_i > \mu, \quad (4)$$

$$d(f, g_t) = 2^{n-1} + r\sum_{i=0}^{d-1} l_i - 2\sum_{i=0}^{d-1} W_{t,i}l_i > \mu, \quad (5)$$

$$d(f, \overline{g_t}) = 2^{n-1} - r\sum_{i=0}^{d-1} l_i + 2\sum_{i=0}^{d-1} W_{t,i}l_i > \mu, \quad (6)$$

where $\mu = 2^{n-1} - 2^{\frac{n-1}{2}}$, $\overline{g_t}(x) = g_t(x) \oplus 1$ for all $x \in \mathbb{F}_{2^n}$, and the constant function with all 1's (resp., all 0's) is denoted by $\mathbf{1}$ (resp., $\mathbf{0}$). These inequalities can be rearranged in a more compact form as follows:

$$\frac{\mu + 2^{\frac{n+1}{2}}}{r} > \sum_{i=0}^{d-1} l_i > \frac{\mu}{r}, \quad (7)$$

$$\frac{r}{2}\sum_{i=0}^{d-1} l_i + 2^{\frac{n-3}{2}} > \sum_{i=0}^{d-1} W_{t,i}l_i > \frac{r}{2}\sum_{i=0}^{d-1} l_i - 2^{\frac{n-3}{2}}. \quad (8)$$

Eq. (7) is called the weight condition as $r\sum_{i=0}^{d-1} l_i$ is the weight of the function f. Note that Eq. (8) should hold for all $t = 0, 1, \ldots, 2^n - 2$; however, thanks to Prop. 1, all the W_t vectors (of length d) are cyclic rotations of each other. Hence, there are only d inequalities provided by Eq. (8).

Now let us impose the condition $f(\alpha) = f(\alpha^{2^k})$ for all $\alpha \in \mathbb{F}_{2^n}$, where k is a fixed divisor of n. As $f(\alpha) = f(\xi^{v+ud})$ for some values of u and v, it is clear that $f(\alpha^{2^k})$ should be within the $(v2^k \mod d)$-th column of $f^{d,r}$. Hence, the condition partitions the columns (numbered from 0 to $d-1$) with respect to the equivalence relation defined by $i\rho_d^k j$ if and only if $i \equiv j2^{ks} \mod d$ for some nonnegative integer s, such that those belonging to the same equivalence class are either all-one columns or all-zero columns. Then, Eqs. (7) and (8) can be expressed accordingly as follows:

$$\frac{\mu + \frac{2^{n+1}}{2}}{r} > \sum_{j=0}^{m-1} \mathcal{L}_j > \frac{\mu}{r}, \tag{9}$$

$$\frac{r}{2} \sum_{j=0}^{m-1} \mathcal{L}_j + 2^{\frac{n-3}{2}} > \sum_{j=0}^{m-1} \mathcal{W}_{t,j} \mathcal{L}_j > \frac{r}{2} \sum_{j=0}^{m-1} \mathcal{L}_j - 2^{\frac{n-3}{2}}, \tag{10}$$

where $\mathcal{L}_j$ and $\mathcal{W}_{t,j}$ are the sums of l_i's and $W_{t,i}$'s corresponding to the columns belonging to the same (i.e., the j-th) equivalence class, respectively, where m is the number of equivalence classes. It is well-known that in the case of the PW construction, the number of inequalities is equal to m. However, for the general case, i.e., when $2^n - 1$ is a composite number, it is at most d as we notice that after imposing the aforementioned condition, some of the inequalities obtained from Eq. (10) can be the same (in case of (217,151)-interleaved sequences) as we will see in the subsequent section.

It should be pointed out that Eqs. (7) and (8) apply to the case of any n whenever $2^n - 1$ is a composite number; however, Eqs. (9) and (10) additionally require that n is not a prime number.

3 Case $n = 15$

In the rest of this paper, we implement 15-variable Boolean functions using the primitive polynomial $x^{15} + x + 1$. Let f be a Boolean function represented as a $(217, 151)$-interleaved sequence which is made up of all-one and all-zero columns. From Eq. (7), we have $109 \geq \sum_{i=0}^{216} l_i \geq 108$. Substituting these two possible values into Eq. (8), we get

$$8218 \geq \sum_{i=0}^{216} W_{t,i} l_i \geq 8090 \quad \text{for} \quad \sum_{i=0}^{216} l_i = 108, \tag{11}$$

$$8293 \geq \sum_{i=0}^{216} W_{t,i} l_i \geq 8166 \quad \text{for} \quad \sum_{i=0}^{216} l_i = 109. \tag{12}$$

As aforementioned, the W_t vectors are cylic rotations of each other, and hence there are 217 of them which are different. One of them is computed as follows:

(76, 72, 72, 68, 72, 80, 68, 76, 72, 80, 80, 72, 68, 72, 76, 68, 72, 68, 80, 76, 80, 88, 72, 68, 68, 76, 72, 84, 76, 68, 68, 60, 72, 72, 68, 72, 80, 84, 76, 72, 80, 80, 88, 84, 72, 76, 68, 72, 68, 64, 76, 80, 72, 72, 84, 68, 76, 72, 68, 76, 68, 84, 60, 72, 72, 84, 72, 80, 68, 76, 72, 80, 80, 72, 84, 72, 76, 84, 72, 84, 80, 76, 80, 72, 88, 68, 84, 76, 72, 84, 76, 84, 68, 76, 72, 72, 68, 72, 64, 84, 76, 72, 80, 80, 72, 84, 72, 76, 84, 72, 68, 80, 76, 80, 72, 72, 68, 68, 76, 88, 68, 76, 84, 68, 60, 72, 72, 84, 72, 80, 84, 76, 72, 64, 80, 72, 68, 72, 76, 84, 72, 84, 80, 76, 80, 72, 72, 84, 84, 76, 72, 68, 76, 84, 84, 76, 72, 72, 84, 72, 80, 84, 76, 72, 80, 80, 72, 68, 88, 76, 68, 72, 84, 80, 76, 64, 72, 72, 84, 84, 76, 72, 84, 76, 68, 84, 76, 72, 72, 84, 72, 80, 68, 76, 72, 80, 64, 72, 84, 72, 76, 84, 72, 84, 80, 76, 80, 72, 72, 84, 84, 76, 72, 84, 76, 84, 84).

Thus, one can restrict the weight of $l = (l_0, l_1, \ldots, l_{216})$ to either 108 or 109 and then perform some heuristic searches (e.g., [5]) exploiting the inequalities given by either Eq. (11) or Eq. (12), respectively. However, since the search space is of size 2^{217}, it is probable to not encounter with a solution easily yielding nonlinearity greater than the bent concatenation bound. Next, we consider the functions satisfying $f(\alpha) = f(\alpha^{2^k})$ for all $\alpha \in \mathbb{F}_{2^{15}}$ where $k = 1, 3$, and 5.

3.1 Idempotent Functions

Let the function f corresponding to the (217, 151)-interleaved sequence having a fixed binary sequence of length 217 as its rows be an idempotent function, i.e., $f(\alpha) = f(\alpha^2)$ for all $\alpha \in \mathbb{F}_{2^{15}}$. Thanks to the idempotency property, the columns (numbered from 0 to 216) are partitioned into 21 equivalence classes with respect to the equivalence relation ρ^1_{216}. Among these equivalence classes, 12 are of size 15, 6 are of size 5, 2 are of size 3, and 1 is of size 1. Let us represent an equivalence class by the smallest integer among its elements. We then have the following 21 representatives: 0, 1, 3, 5, 7, 9, 11, 13, 15, 19, 21, 25, 27, 31, 33, 35, 37, 49, 77, 93, 105. Then notice that the truth table of f can be obtained from the values of $(l_0, l_1, \ldots, l_{20}) = (f(1), f(\xi), f(\xi^3), \ldots, f(\xi^{93}), f(\xi^{105}))$ which we call the representative truth table (RTT). The representatives 7, 21, 35, 49, 77, 105 (resp., 31 and 93) belong to the equivalence classes of size 5 (resp., 3). All the other representatives except 0 (which corresponds to the equivalence class of size 1) represent the equivalence classes of size 15. By fixing $l_0 = 0$, it can be seen that there are only three possible combinations of the equivalence classes, such that $l_i = 1$ for each combination and $l_i = 0$ for the rest, because of the weight condition given by Eq. (7) (or Eq. (9)), which are

- 5 with size 15, 6 with size 5, and 1 with size 3,
- 6 with size 15, 3 with size 5, and 1 with size 3,
- 7 with size 15 and 1 with size 3,

Then we perform an exhaustive search only for these cases, which reduces the search space from 2^{21} to $2^{15.3}$, and found two functions having nonlinearity greater than the bent concatenation bound. The RTTs of these two functions are given in Table 1. By complementing their truth tables except $f(0)$, we obtain nonlinearities 16267 and 16261.

Table 1. The two RTTs among the idempotent functions with nonlinearity NL_f greater than the bent concatenation bound 16256.

#	$(f(1), f(\xi), f(\xi^3), \ldots, f(\xi^{93}), f(\xi^{105}))$	NL_f
1	$(0,1,0,0,1,1,1,0,1,0,0,1,0,0,0,0,1,1,0,1,1)$	16268
2	$(0,0,1,1,0,0,0,1,0,1,1,0,1,1,1,1,0,0,1,0,0)$	16260

3.2 Functions for which $f(\alpha) = f(\alpha^{2^3})$

Now we impose the condition $f(\alpha) = f(\alpha^{2^3})$ for all $\alpha \in \mathbb{F}_{2^{15}}$ on the function f which is represented by the (217, 151)-interleaved sequence having a fixed binary sequence of length 217 as its rows. In this case, the columns are partitioned into 49 equivalence classes with respect to the equivalence relation ρ_{216}^3 and thus there are 42 equivalence classes of size 5 and the rest are of size 1. We then have 49 representatives: 0, 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 15, 18, 19, 20, 21, 22, 23, 25, 26, 27, 31, 33, 35, 36, 37, 38, 43, 44, 46, 49, 50, 52, 54, 62, 66, 69, 74, 77, 93, 97, 100, 105, 108, 124, 155, 186. The representatives 0, 31, 62, 93, 124, 155, and 186 belong to the equivalence classes of size 1, and the rest of them belong to the equivalence classes of size 5. Because of the weight condition, there are two possible choices indicating that $l_i = 1$ for half of the equivalence classes of size 5, and 3 or 4 of the equivalence classes of size 1; and $l_i = 0$ for the rest. However, notice that the functions satisfying one choice and the complements of the functions satisfying the other choice are the same except their first bits. Therefore we select one of the two choices, which reduces the size of the search space from 2^{49} to $2^{44.1}$. Our exhaustive search finds 28 functions with nonlinearity 16268 and 7 functions with nonlinearity 16260. The RTT's of these functions are given in Table 2. Again, by complementing their truth tables except $f(0)$, we obtain nonlinearities 16267 and 16261.

We have checked that the functions in Table 1 and 2 are not affine equivalent to the PW functions. Further, note that there exist some functions which are invariant under the action of $\mathbb{F}_{2^3}^*$ or $\mathbb{F}_{2^5}^*$ among those that we here consider. However, we find that none of them exceeds the bent concatenation bound.

As mentioned previously, there are at most $d = 217$ inequalities provided by Eq. (10). In our case, we observe that 16 (resp., 30 and 54) inequalities are the same for $k = 1$ (resp., $k = 3$ and $k = 5$), which reduces the number of inequalities from 217 to 202 (resp., 188 and 164). For $k = 5$, the search space is of size 2^{93} and the weight condition reduces it to $2^{88.1}$, which is still huge and an exhaustive search is not possible; however, some other search strategies can be applied and we are in the process of performing a heuristic search.

4 Possible Nonlinearities

We compute the possible nonlinearities following the method used in [6] for any function f corresponding to the (217, 151)-interleaved sequences having each column either all-zero or all-one. Since the maximum nonlinearity of an 15-variable Boolean function can be at most 16292 ($= \mu + 36$) [3], where $\mu = 2^{15-1} - 2^{\frac{15-1}{2}} = 16256$, one of the distances defined by Eqs. (3)-(6) should be an integer within the interval $[\mu+1, \mu+36]$ to exceed the bent concatenation bound. From the weight condition, the possible values of $\sum_{i=0}^{216} l_i$ are 108 and 109. Then, the corresponding values of the distances $d(f, \mathbf{0})$ and $d(f, \mathbf{1})$, defined by Eqs. (3) and (4), respectively, are found as 16308, 16459, 16460, and 16309, which are greater than the upper bound (16292) of the maximum nonlinearity. Thus we

Table 2. The 35 RTTs with nonlinearity $NL_f > 16256$, among the functions satisfying $f(\alpha) = f(\alpha^{2^3})$ for all $\alpha \in \mathbb{F}_{2^{15}}$.

#	$(f(1), f(\xi), f(\xi^2), \ldots, f(\xi^{155}), f(\xi^{186}))$	NL_f
1	(111100010001000111000011101010111100110010110000)	16268
2	(110010110101001101111001100000001100011010101100)	16268
3	(110100110100010011100001011011001110011010011010)	16268
4	(101001010111011110000100111010001000001110011111001)	16268
5	(101001111001100111010010010100101000101011110000)	16268
6	(101111111010010001001000100010001001111010111010100)	16268
7	(100010010100010111011111011101100010011010010010010)	16268
8	(110001011000000010010000110111110111011001111010100)	16268
9	(110010001001101100011000110101101100001011101010)	16268
10	(111100000010001100001110111110011100010111010000 1)	16268
11	(100111010111001101001100110010011001000110001010 1)	16268
12	(101010101000010000101000011011001111011110110001 1)	16268
13	(011110101100001100011101100011000110101011100 1000)	16268
14	(011110010110000010001011010111001111100000110101 0)	16268
15	(000110101110101010001011000110010010111100110100 1)	16268
16	(001101001101000100010101101111100111010001010 1100)	16268
17	(011101110100010101000001111110010010001001110101 0)	16268
18	(011100011010001010111001010010010101011011010001)	16268
19	(011111001001110100001101001010000001011110110011 0)	16268
20	(011011010101000100001111010001101101010100010110 1)	16268
21	(011011110000100010101010110100001101101101010110 0)	16268
22	(001010111101110111011010110010000000111101000000 1)	16268
23	(010001100001111110101110101001000101101100100011 0)	16268
24	(011010100001101110000010101110010110111010010010 1)	16268
25	(001011110000011100100000111001110100101000111101 1)	16268
26	(010010011111010100011010111110100000010001011011 0)	16268
27	(011010011010011000111000001101111100000101011001 1)	16268
28	(010111010001001111010100010011010101011000100011 1)	16268
29	(101110011110000001010001010110111010010011011 1000)	16260
30	(110010110010111011101010010000011000101110101000 1)	16260
31	(111001010001010101110100111001101101000010001011 0)	16260
32	(000101100101100111000111110010000011111010100110 0)	16260
33	(010110000110011000101101101011010111010100000101 1)	16260
34	(011000101000110010110010001101100110111001101101 0)	16260
35	(001011001011101100011110100100110001000101110010 1)	16260

cannot get any possible nonlinearity $NL_f > \mu$ using the distances $d(f, \mathbf{0})$ and $d(f, \mathbf{1})$, and now we look at the other distances defined by Eqs. (5) and (6).

Let us consider the distance $d(f, g_t) = 2^{14} + 151 \sum_{i=0}^{216} l_i - 2 \sum_{i=0}^{216} W_{t,i} l_i$, obtained from Eq. (5). It can be easily computed that the greatest common divisor of the values (given in the Section 3) of the vector W_t is 4. Hence, it should be noted that if $(2^{14} + 151 \sum_{i=0}^{216} l_i - d(f, g_t))/8$ is an integer for any $d(f, g_t) \in [\mu+1, \mu+36]$, then the corresponding distance $d(f, g_t)$ is a possible nonlinearity. Substituting 108 and 109 for $\sum_{i=0}^{216} l_i$, we obtain the possible nonlinearities as 16259, 16260, 16267, 16268, 16275, 16276, 16283, 16284, 16291, 16292. Following the same argument for Eq. (6), we get more values of the possible nonlinearities which are 16261, 16269, 16277, 16285.

Similarly, we have computed the possible nonlinearities for $n = 11$ and 21, too (notice that $2^n - 1$ is prime for $n = 13$, 17, and 19). For $n = 11$, we find that these are 995, 996, and 997 (which is greater than the best known value) for the $(89, 23)$-interleaved sequences. We have checked that the idempotents in this case do not have nonlinearity greater than the bent concatenation bound. In case $n = 21$, we find that for the $(6223, 337)$-interleaved sequences, all the nonlinearities up to the upper bound of 1047850 are possible except the nonlinearities $\{2^{20} - 2^{10} + 4 + 8i \mid i = 0, 1, \ldots, 36\}$. For the latter case, the search space is of size 2^{311} for the idempotent functions in the form of $(6223, 337)$-interleaved sequences.

References

1. E. Filiol and C. Fontaine. Highly nonlinear balanced Boolean functions with a good correlation-immunity. In: Eurocrypt 1998, LNCS, vol. 1403, pp.475–488, Springer, 1998.
2. S. Gangopadhyay, P. H. Keskar and S. Maitra. Patterson-Wiedemann construction revisited. *Discrete Mathematics*, 306(14):1540–1556, 2006.
3. X.-D. Hou. On the norm and covering radius of first-order Reed-Muller codes. *IEEE Transactions on Information Theory*, 43(3):1025–1027, 1997.
4. S. Kavut. New Patterson-Wiedemann type functions with 15 variables in the generalized rotation-symmetric class. *Turkish Journal of Electrical Engineering and Computer Science*, 25(6):4901–4906, 2017.
5. S. Kavut and S. Maitra. Patterson–Wiedemann type functions on 21 Variables with nonlinearity greater than bent concatenation bound. *IEEE Transactions on Information Theory*, 62(4):2277–2282, 2016.
6. S. Kavut, S. Maitra and F. Özbudak. A super-set of Patterson–Wiedemann sunctions: Upper bounds and possible nonlinearities. *SIAM J. Discrete Math.*, 32(1):106–122, 2018.
7. 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*, 53(5):1743–1751, 2007.
8. S. Kavut and M. D. Yücel. 9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class. *Information and Computation*, 208(4):341–350, 2010.
9. 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.