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 $5 \times 3 = 15$ 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 authomorphisms. Some of these Boolean functions posses nonlinearity greater than the bent concatenation bound. The next possible option for exploring such functions is on $7 \times 3 = 21$ 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 [12] 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 [12] by considering several group actions as described later in Section I-A. 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 $21 = 7 \times 3$, but that could not be achieved till date. In this paper, for the first time, we demonstrate such functions for 21 variables that could not be achieved for more than 32 years. In this regard, one can computationally check that for $9 = 3 \times 3$, 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 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 $2^{n-1} + 2^{\frac{n-1}{2}}$.

S. Kavut is with the Computer Engineering Department, Balıkesir University, Balıkesir, Turkey. Email: skavut@balikesir.edu.tr

S. Maitra is with the Applied Statistics Unit, Indian Statistical Institute, 203 B. T. Road, Kolkata 700108, India. E-mail: subho@isical.ac.in

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 [11], 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 [12], 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 $2^{n-1} - 2^{\frac{n-1}{2}} + 2 \cdot 2^{\frac{n-9}{2}}$.

OUR CONTRIBUTION: The kind of constraints considered for constructing the 15-variable functions in [12] finally reduced to solving an integer programming problem on 11 binary variables, which was easy to solve using exhaustive search. However, the authors [12] pointed out the following in their paper:

> "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 [12] 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, Page 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 obtained Patterson-Wiedemann type functions on 21 variables having nonlinearity strictly greater than the bent concatenation bound.

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 [12]. 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.

Next we provide necessary background in this area. For this, we mostly follow to the explanations in [12], [5]. One may also note that several modifications of Patterson-Wiedemann type functions have been studied in literature as evident from [4], [10], [13] and the references therein.

A. Background

By $\mathcal{F}_n$, let us denote the set of Boolean functions from $GF(2^n)$ to $GF(2)$ and consider $f \in \mathcal{F}_n$. 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 $n = ab$. Let $M = GF(2^{ab})$, $L = GF(2^a)$, $J = GF(2^b)$ and $K = GF(2)$. Now consider the tower of subfields $K \hookrightarrow L \hookrightarrow M$. The index of the multiplicative group L^* in M^* is $m = \frac{2^{ab}-1}{2^a-1}$. One may note that M^* can be written as $M^* = \cup_{i=1}^m L^* x_i$ where $\{x_1, x_2, \ldots, x_m\}$ (the complete set of coset representatives of L^* in M^*). It is well known that one can characterize any function from $M \to K$ by specifying

its support. Let us consider functions in $\mathcal{F}_n$ whose supports are of the form $\cup_{i=1}^{l} L^* x_i$ 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 [12] 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 [12], such ideas along with some additional techniques produced functions with nonlinearity greater than bent concatenation bound.

We denote the set of all such functions by $I_{a,b}$. Any linear function in $\mathcal{F}_{ab}$ can be expressed as $l_\alpha(x) = Tr_1^{ab}(\alpha x)$ where $\alpha \in M$ and $Tr_1^n(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}}$ for all $x \in GF(2^n)$. The support of l_α is $Supp(l_\alpha) = \{x \in M | Tr_1^{ab}(\alpha x) = 1\}$, and the support of the affine function $h_\alpha(x) = l_\alpha(x) + 1$ is $Supp(h_\alpha) = \{x \in M | Tr_1^{ab}(\alpha x) = 0\}$. Let $H_\alpha = Supp(h_\alpha)$, which is a hyperplane in M when considered as a vector space over K.

Next we define the Hadamard transform of $f \in \mathcal{F}_n$ as

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

The nonlinearity of a Boolean function f is defined as

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

We can write the elements of $GF(2^n)$ in some order, say $\{\alpha_0, \alpha_1, \ldots, \alpha_{2^n-1}\}$. For $f, g \in \mathcal{F}_n$, 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 $f, g \in \mathcal{F}_n$ then $d(f, g) = |Supp(f) \Delta Supp(g)|$ where Δ is the symmetric difference between the sets $Supp(f)$ and $Supp(g)$. One may calculate that (see also [12]) if $Supp(f) = \cup_{i=1}^{l} L^* x_i$ then

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

where $\mathbf{0}$ and $\mathbf{1}$ are constant functions with all 0 values and all 1 values respectively. Further, $t(\alpha)$ is the number of cosets of the form $L^* x_i$ that are totally contained in the hyperplane H_α, equivalently $t(\alpha)$ is the number of x_i for which $Tr_a^{ab}(x_i \alpha) = 0$. Thus, the nonlinearity of f is given by

$$nl(f) = \min_{\alpha \in M} \{l(2^a - 1), 2^{ab} - l(2^a - 1), 2^{ab-1} - 2^a \cdot t(\alpha) + l, 2^{ab-1} + 2^a \cdot t(\alpha) - l\}.$$

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

$$\frac{2^{ab-1} - 2^{(ab-1)/2}}{2^a - 1} < l < \frac{2^{ab-1} + 2^{(ab-1)/2}}{2^a - 1}, \tag{2}$$

$$\frac{1}{2^a} \left\{ \frac{2^{ab-1} - 2^{(ab-1)/2}}{2^a - 1} - 2^{(ab-1)/2} \right\} < t(\alpha) < \frac{1}{2^a} \left\{ \frac{2^{ab-1} + 2^{(ab-1)/2}}{2^a - 1} + 2^{(ab-1)/2} \right\}. \tag{3}$$

Consider the two subgroups L^* and J^* in M^*. The intersection of L^* and J^* contains only the identity element and the group M^* is an abelian group. Hence the product $L^* \cdot J^*$ is direct. One can identify the group M^* to the group $\Phi(M^*)$ of left multiplications by the elements of M^* in $GL_K(M)$ and this correspondence is an isomorphism.

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

Definition 1: Consider $n = ab$, the product of two primes. Let $L^* = GF(2^a)^*$ and $J^* = GF(2^b)^*$ and $\langle \phi_2 \rangle$ as above. Patterson and Wiedemann [12] considered the action of the group $G = [\Phi(L^*) \cdot \Phi(J^*)] \langle \phi_2 \rangle / \Phi(L^*)$, where $[\Phi(L^*) \cdot \Phi(J^*)] \langle \phi_2 \rangle$ is the semidirect product of $\Phi(L^*) \cdot \Phi(J^*)$ by $\langle \phi_2 \rangle$. Here, the functions $f \in \mathcal{F}_n$, which are invariant under this group action are referred to as Patterson-Wiedemann type functions.

The result of [12] was for $n = 15$. Here $L^* = GF(2^5)^*$ and $J^* = GF(2^3)^*$. The support of the function f is invariant under the action of L^* and J^*. That is, the support of f is invariant under the action of the product $L^* \cdot J^*$ which is also a cyclic subgroup of $M^* = GF(2^{15})^*$ of order $(2^5 - 1)(2^3 - 1) = (31)(7) = 217$. All the elements of $L^* \cdot J^*$ should have the same value and it is also true for the elements in each of its cosets in M^*. Note that $\frac{2^{15}-1}{217} = 151$. In the form of interleaved sequence [6], [5], 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. Generally 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 $x \in M^*$. 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 $\binom{10}{5} = 252$ many different Boolean functions on 15 variables. As described in [12], 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, Pages 1549-1550].

II. PATTERSON-WIEDEMANN TYPE CONSTRUCTION ON 21 VARIABLES

In this section, we consider the case for $n = 21 = 7 \cdot 3$. As explained in [5], we have $L^* = GF(2^7)^*$ and $J^* = GF(2^3)^*$ here. Now $L^* \cdot J^*$ is a cyclic subgroup of $M^* = GF(2^{21})^*$ 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 $x \in M^*$. Thus, 2359 elements are divided as 112 groups of size 21, 2 of size 3 and 1 of size 1. Thus, we have 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 $2\binom{112}{56}$ many 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, Section 2.1] for $n = 15$. We implement the strategy for $n = 21$ and generate the inequalities as completely described in Appendix A. 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 $57 \leq t(\alpha) \leq 72$. 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 A. 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 A. 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 below. All the solutions have nonlinearity $2^{21-1} - 2^{\frac{21-1}{2}} + 61 = 1047613$ and the minimum absolute values

in the autocorrelation spectra (see [5], [9] for details of autocorrelation spectra) of these four functions are 2948, 3436, 3940, 5116. These different values show that the functions are not affine equivalent.

```
011100011011111001111110101001001011100111010000100110001010010010011100010000010001001101001011101110110011111100000
011001010011100101011000010000110011111100111001110000001000101000001111100111000011111100100101111110010100101111000
011101001010000111111001001100101011111100011100110010010011001001100100100010001111101110110101000000000000000101111001
001100011110010111100010001101101010000110101010101011011111111101000100000101011101010010100010110011001010101110010100
```

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 bounds $2^{n-1} - 2^{\frac{n-1}{2}}$. In particular, we construct functions having nonlinearity $2^{21-1} - 2^{\frac{21-1}{2}} + 61 = 1047613$.

B. Details of our heuristic

We utilize the steepest-descent-like iterative search algorithm [1] to attain the solutions. In this search algorithm, the current solution is replaced by another solution from a predefined set of candidate solutions, called the neighborhood. Using a cost function, the entire neighborhood is evaluated in each step of the search algorithm. The best one, i.e., the one with the best cost value, is then delivered to the next step, even if it is worse than the previously selected best solutions. To prevent the algorithm from looping, these best solutions are stored in memory.

Here, we constitute the neighborhood by swapping two dissimilar bits (of the current solution) at the locations corresponding to the groups of the same size. This is required to satisfy the necessary condition on the weight of the Boolean function. Hence, the neighborhood consists of 6272 ($= 2 \times 56^2$) candidate solutions and for each of them we compute the cost function that we define as the sum of squared errors, which is a measure of the distance of a solution 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

$$
\begin{aligned}
Cost(x) &= \sum_{i=0}^{114} C_i^2, \text{ where} \\
C_i &= \begin{cases} |(x, A_i) - 72|^2 & \text{if } (x, A_i) > 72, \\ 0 & \text{if } 57 \leq (x, A_i) \leq 72, \\ |(x, A_i) - 57|^2 & \text{if } (x, A_i) < 57. \end{cases}
\end{aligned}
$$

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. The search algorithm stops after a fixed number of iterations, 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. Exploiting all the cores, it took more than a month to extract the aforementioned 4 solutions.

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.

REFERENCES

[1] M. Bartholomew-Biggs. Chapter 5: The Steepest Descent Method, pp. 51–64. Nonlinear Optimization with Financial Applications. Springer, 2005.

[2] 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.

[3] J. F. Dillon. Elementary Hadamard difference sets. In Proceedings of 6th S. E. Conference of Combinatorics, Graph Theory, and Computing. Utility Mathematics, Winnipeg, pp. 237-249, 1975.

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

[5] S. Gangopadhyay, P. H. Keskar and S. Maitra. Patterson-Wiedemann construction revisited. Discrete Mathematics, Volume 306, Issue 14, pp. 1540-1556 (2006)

[6] G. Gong. Theory and applications of q-ary interleaved sequences. IEEE Transactions on Information Theory, 41(2), pp. 400-411, (1995)

[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, Volume IT-53(5), pp. 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, Volume 208, No. 4, pp. 341-350 (2010)

[9] S. Kavut. Correction to the paper: Patterson-Wiedemann construction revisited. Discrete Applied Mathematics. Available online 1 September 2015.
http://www.sciencedirect.com/science/article/pii/S0166218X15004126

[10] S. Maitra and P. Sarkar. Modifications of Patterson-Wiedemann functions for cryptographic applications. IEEE Transactions on Information Theory, Volume 48(1), pp. 278-284, (2002)

[11] J. J. Mykkeltveit. The covering radius of the $(128, 8)$ Reed-Muller code is 56. IEEE Transactions on Information Theory, IT-26(3):358–362, (1983).

[12] 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, Volume IT-29(3), pp. 354-356 (1983) (See also correction in Volume IT-36(2), p. 443 (1990))

[13] S. Sarkar and S. Maitra. Idempotents in the neighbourhood of Patterson-Wiedemann functions having Walsh spectra zeros. Designs, Codes and Cryptography, Volume 49, Issue 1-3, pp. 95-103 (2008)

APPENDIX A: THE COEFFICIENT MATRIX A

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.

```
300000000000000v0000v0000000000000vv0000000000000000000000000000000000000000000000000000000000000000000000000vv0
0202012221212120330012500120010113112321013010000120023200010103120030121112311013021001012112111101300310001012
0000130011341121124131111101202101110121010010021100100310112112002012020040102210131110112220101226110111011040
0202110200101500011322030033232011111203010201101132301222202013111101201111040000131101212020020131110201010220
0011020312401100100110132202231121212102121110111402202122012200001120000311011011300430011230011011001030
0131243021020021111011212032031030010222104210113100212101220223202100111100133111100320022000000001300021120111201
0200032003002011103102000212211000130322322030021013002120212331111111111123113201000111220020120122400200100014100110
0202300032311140101022011311103010020204010020212111112012221200020010124312001101230120011013010101002211
0110120320122001021110112300122011220120410132100302022011211113110210040201012010311010140004022014111001020011
0210213200311030220210321232010111312021100013010101113221411221002125111001110000225201112010211011001001120021010
0131400313004001113133111100120211232021002300000101010023122122001143113021110030000111101201022120112110
0240020120010001111213222221300034021101111014021001310123021111112042120210110102210430020011011111212111101001100110
0111102121400112031001112211111110221202102401014032111110242000200101120201121111100111301012122021001220213112111100
0215120100011012221220022110131111111330220011121221001311010010022305212202013122010211020010004021200022210001100
0020011103011124010010020210040102213210311110100132212001221150120211201310011130311121041202023010101101200010110
0310011410112242011101101122031212002101122203201111210120111100121132031102000213010101122340001000110025100031110
0310111002110200213301212111111111210221121202021015103030001011111120114020212001100011121321002001210002120120043201
1021010012221232111133210010013011320122003000011221202021001010312221000230121112022015221111011011101101010112000
0011013011311101332011222120010210100001110150102304110121031122131021123102110141220001113210021013110003111100020
0141101110130211330002012200400212104112111010101011010103121110120120212202222010000011212112121232010000
0213110013320200021001113222301011132112102001101100312413001021212114512100011332010121011000311011110020011010
0532012202321001112121110002022120100010210331001210011113132123011001021111031321202030012002100101011122110500
1012120211121011202011121113010313123012321211101120212111011000221120021001140122001000100030030330031001
0110310012122201021112200000111025112312121121100313220311331202002000120132012002102010113051000101221114100110110
0213222123122201112230102030122102220001021101401010031021010033100012002110011001421121201101000011403112210140
0010201132112121232200001421002102101230203001312210010012312110011022122012101405110213141012000100
0010032300031112020201031012111010313100213414311210101012111031030211133110002111111020000011212200142201103002
0113222101001002110022300214001104330201101222022023200010210211300002310022001010311013011120231122310220120201100
0003201110101100110410300011200131211022132321211114012102200120000110000210123213000002121021250000212
0112331121001343131002112001042110400001021113300310201102110210210012111210021200002000311000002031200121210212312
0123110021031111120012012011320103112110011112111112201221110300510012110003211010010220346130221110011101111201
10010300302114010210210220131111111103210210210201021311100121112411253010303001213000001020400010
0120230103102121111112100400210320012110031011001141030310210231102210002211301013021101000011231421024021110
0111110101102212210110322214103204100020121111142001022101131010010120115111302012032203110100001102022010110031200
0201203012211110221211152103141101010314112122001030010040011200112110110211011201032200311221001000
0311110320021301001302120330001001212113121011101131110101001012021100114102303210001213001503111102204111110
1211110302220012200002031001020220001101020111202321011010101112122110132213110013111111015111103022112012210411000
1112221011123112304100202322011103201221111020201211003100030002220221110011011040420
0002022011111310200111130110111212111200142300141012051011023200110121302122311134011003110001112011001311010011210
0110123320210001101120211001300000410200143113111210221300000321341321101111201130000222102130101213011010021022120
0323212000312231101211310221220010213211102101012332213521001013012111003100002010102110203100301223410010
0010102240204212211102220003121111010442010034212221100201221320001021100210230212110011100201100300010002111210
0111140011010012110121211111211103222112311011201263202101110101211013101021033041111320120021002001002112000300302020
0000123433241012211100111132111101111151111100021203231022012120002111201110020040000120131110330
0012010120100110025003120042231111201101000110111111030101110121312001324122002121011012000101112033133132201130302200
0000010201102110322011311121213011212000303322100120021200201320110314101301002011132200020021100012003204111040011200
0001111000014112011101114101012010010120101010410401011010300211031030021221030122022120
0111110201200200222010010013210120111204122111121011010200501301233230301201012121104201311222110000210222201230000001020
0120431030303101102110201112213111440031112121110110021111230110102211220012122301232101011101001014011200201004121001 00
0211013101012112112301111000101041121201200212602110012101101301211100021111000111011110112140222210201142221100002100213020
0011200121031231000112310220011102111111230120021211232122023110110002021122300141220221101101020030100300241010040
0003200201011121524101210011312214013002002230132121001130133110111110200101120012210100011110302200213130110111102120
0202222210010221113001200122001011112020100320013002212231011010211211000141010021015020011302112502011211122110
0313111123011011011030123200111130011152112210000101120011000302113210211110331100002010000202301220203123210001022120
```

```
0200222002121120300111101110012112201011100100215112120033210103110122005201122011201002210300122110222001301211  0230
0001210212030301011121230000202022001103000310202123113431111420211201112111001020012110101010121110110121104432200
0032002011102122302241212211221001010110121111013010113324001031000111110101120020102110210500113221200300021202310
0112011021124110011011211120011220011210001213130121202142003411103122100100102202100313100340012200323010200111010
0012222114112021000233130312311110011001111025013032011002010101132211101112001131010001211101002323010022001 10221
0112123211010121033401131111100111011102022011011102333010000013151041003001220220101201030102002131001112121211  00110
0022403211210011111103010110213113002130321121020131101113112111331021323002032000001110010120002120012020010310031
0310021012212011021012220112220001011123210011231211020404031400011111000110211010212103202300020204111323002010  1100
0112021232010150112201303201210210020022310313010011323111100131101101320010011312103012010120112131001011300101
0220131111120000122022021331105121012101122013122101111011051010011302101140011120000203201210313011001102111310110
0021221110101011121313003013201010022113101221132111031201113030221001100111100013111012011421011200010043311040110
0003101100040222123020100400010101011043011041011111201001031112231121021102301202112201111112031122210212311  00210
0321221122021201111111122023012000020110150020123100111110033111111301010210011101010210242012002010204030141012  2020
0111011111211321100221100200011101110113211010201000002211240113011031410001401311101203011130342110001131111131231
0201001212322013102410101020212222121322103331012000222012212100010302200010400111000000122000011021241011031210020
0111001105100512201010012012111120003310212230222201101121011212112011001221201113110100012031002300211243031 0100
0120011001222220021041120013121211222031010340200100110111030111104212102110320100010242100111111121110120213102021
0101112141210103132050100111210111212000111111110121115110132000002101140114232201200210011200011021212221102  20100
0212113221101211103012012330000035111321000020101110212200003110210000021001102232010131220301011120012131122  04120
0300211200211231411121031230200001003111102220212121100111100131110000211452302200102131111130012011222020100001200
0101001110212010020011021212023111101121321202121021031100110024110011111050220001211012110101001021141210212532  3120
0141003201001202212101201112012101111121010000212132031110122001011021402202000101101420203210011340220 10303111021
0011012111011100011201210000121113010022103121023100012011220100121442021322011011214030011250111011212204211001220
0101230021101010211001120200101210140230223223131010011202000311031001331000101200024131113300210021111113223  11300
0320331000121312120110101001201132011011130111211111400102022000100110222020011203031200010212002152012401213  1012210
0024110010421111201213201120000100203111042233021421010021201010310022021020000211220201210031030101212111211  13100
0210110200310213024031020011001221321113120121243012001220010041100011212111121010101030041132101221202100130210211  30011  00120
0100010130100230021233010110020112031330011012122221122002310210300111023021100240120021220100122301113000321121101
0010111012141001102122201113220410201240021000101120010011100130121101012111203111402101113010125110121232003211  10
0030101112331130112201124011101113231000311210010401001100012101100030200010121120002202100203212002313331211203  10
0111101205001011050212002011000102121010113122331020210220121120112101101201442230202210121111021101011120010212  3010
0013032412203210020000011210102222411120021000112201001130110202120100011401022012221121110000322123012121  11030301
0111322300120111020212101111232520100302000100211211000210124110013000120000221322300120211022213203111012012  00142001010
0201100111101121111210112203310323010020011202120211102003030233202301413110010201100120012200001001011211511  1103130
0110000211100012111223411220213001201031012010121201521121100002014010201120110121212204010202211001111413  32101010
0111122041012023112100320011041011150100101021011110000102112101121201021001012211212102220103201133032104101  3011
0122120002312043113000100101306000121212100111110011223100100321110120012113132220301112122110020111102102301  011110
0221201100001014102111251201001311111201002111201200030053121002411101010102231121001132021010121311012113110  121110
0122002141012120211012211102003030231200312101010001310010410201121230212331150201012102021112030010010122110  01210
0700000000007u0007700000000000000000000000000000000000000000000000007770777000000000077000070000000000000000000000  000700000007070000000003
0112301122110020020000000111202230010321101002032410232211012021302030310100012031113203023101310123121112200  00211110
0100402221112401012002100413002000010210212231010002000231001003211012001211313220301112122110020111102102301  011120
0010302301111020211311010021231001052110100020012022011320322031302101112011010025131112010021000213101211  1122210
0122004010120030010110000211111101302122100410221202121122211010211100111021005331120210101310310030022102021113210
0320000141010100211210011522221210231001101030122231101203024110101200011100100320100141340100001122003010314012  2110
0061110211121211100111120122100120011213030033220100232010200121022013222114110101020111011100212000241101001013210
0013132010212101013210021103000320011010200012020111512123310110020020110240211021131220131010111012001130102222230
0311200010012100111011103231210100040200130124040120121211211011312304023110201011022123000112101120112012004  2001010
0101300101110000211110314210221012110101101124100000230003112311010112011222214213131011022101212111102110221  1112
0011001100012012100111010142511040201110311122101103102013002020100310122010210130232122131121210101112211111  11321
0010120010201215210211013312010021202031002011220001111201012300420311221201011200230202014201202001110200  1220220
0012110301213201010101341120121010222010000121130200103100220012311112023020412100310101112311002231001122  032202100
0110110021101210103201011001211101021110100301104212001022100013241042111132311132212153031100010101110  0022113  20
0001021102201120211122302112001021000102011010200412111311331110301231020101413401000114134010001122003010314  01222110
0110104000012200001302302210212240244011210114202011112410010011110110302023121211012121211000021121212112  2001110
0211011110110110030112010110020110001114002131002012011014211131330111231220510301113210011001100211102321222  11203011
0100010012101011411011100301224231112024100312001102213011010014023110200310111022212300011210112011201210121  043110
0142110221201101320110100001030011011012112301010302202210001000210020413111230110301313111012313201102121  330030
1302021220011111120000501110121101201002102032210100111223021011112020101121023211113030100110011222222132131001  0130
1120301101110011002010014200211101100121120002202421230112130011232020202220102011101311111012113131122021011  3310
0000070700000000700007000000000000000000000000000000000000070700000700700007000077000700070003000000000u70000070  0000
```