# Patterson-Wiedemann Type Functions on 21 Variables 

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 $G F\left(2^{5}\right)^{*} \cdot G F\left(2^{3}\right)^{*}$ as well as the group of Frobenius authomorphisms. Such Boolean functions posses nonlinearity greater than the bent concatenation bound, namely $2^{n-1}-2^{\frac{n-1}{2}}$. The next possible option for obtaining 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. The crux of the observation was that 15 can be written as $5 \times 3$, 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 that. In this paper, for the first time, we demonstrate such functions for 21 variables that could not be achieved for more than 32 years.

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 $\left(1 \oplus x_{m+1}\right) f_{0} \oplus x_{m+1} f_{1}$. 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 [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
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
$2^{n-1}-2^{\frac{n-1}{2}}+20 \cdot 2^{\frac{n-15}{2}}$ 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 rotationsymmetric 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., $f_{21}^{\prime}=f_{15} \oplus b_{6}$, where the functions $f_{15}$ and $b_{6}$ are on distinct variables. However, such functions $f_{21}^{\prime}$ 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 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 $G F\left(2^{n}\right)$ to $G F(2)$ and consider $f \in \mathcal{F}_{n}$. The support of $f$ is defined as $\operatorname{Supp}(f)=\left\{x \in G F\left(2^{n}\right) \mid f(x)=1\right\}$, and its weight is $w t(f)=|S u p p(f)|$. Let $a$ and $b$ be two distinct odd primes such that $n=a b$. Let $M=G F\left(2^{a b}\right), L=G F\left(2^{a}\right), J=G F\left(2^{b}\right)$ and $K=G F(2)$. Now consider the tower of subfields $K \hookrightarrow L \hookrightarrow M$. The index of the multiplicative group $L^{*}$ in $M^{*}$ is $m=\frac{2^{a b}-1}{2^{a}-1}$. One may note that $M^{*}$ can be written as $M^{*}=\cup_{i=1}^{m} L^{*} x_{i}$ where $\left\{x_{1}, x_{2}, \ldots, x_{m}\right\}$ (the complete set of coset representatives of $L^{*}$ in $M^{*}$ ). It is well known that one can characterize any function from $M \rightarrow K$ 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 $\mathcal{F}_{a b}$ can be expressed as $l_{\alpha}(x)=\operatorname{Tr}_{1}^{a b}(\alpha x)$ where $\alpha \in M$ and $\operatorname{Tr}_{1}^{n}(x)=x+x^{2}+x^{2^{2}}+\ldots+x^{2^{n-1}}$ for all $x \in G F\left(2^{n}\right)$. The support of $l_{\alpha}$ is $\operatorname{Supp}\left(l_{\alpha}\right)=\{x \in$
$\left.M \mid \operatorname{Tr}_{1}^{a b}(\alpha x)=1\right\}$, and the support of the affine function $h_{\alpha}(x)=l_{\alpha}(x)+1$ is $\operatorname{Supp}\left(h_{\alpha}\right)=\left\{x \in M \mid \operatorname{Tr}_{1}^{a b}(\alpha x)=\right.$ $0\}$. Let $H_{\alpha}=\operatorname{Supp}\left(h_{\alpha}\right)$, 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

$$
\hat{f}(\lambda)=\sum_{x \in G F\left(2^{n}\right)}(-1)^{f(x)+\operatorname{Tr}(\lambda x)} .
$$

The nonlinearity of a Boolean function $f$ is defined as

$$
n l(f)=2^{n-1}-\frac{1}{2} \max _{\lambda \in G F\left(2^{n}\right)}|\hat{f}(\lambda)| .
$$

We can write the elements of $G F\left(2^{n}\right)$ in some order, say $\left\{\alpha_{0}, \alpha_{1}, \ldots, \alpha_{2^{n}-1}\right\}$. 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 $\left(f\left(\alpha_{0}\right), f\left(\alpha_{1}\right), \ldots, f\left(\alpha_{2^{n}-1}\right)\right)$ and $\left(g\left(\alpha_{0}\right), g\left(\alpha_{1}\right), \ldots, g\left(\alpha_{2^{n}-1}\right)\right)$. It is easy to see that if $f, g \in \mathcal{F}_{n}$ then $d(f, g)=|\operatorname{Supp}(f) \Delta \operatorname{Supp}(g)|$ where $\Delta$ is the symmetric difference between the sets $\operatorname{Supp}(f)$ and $\operatorname{Supp}(g)$. One may calculate that (see also [12]) if $\operatorname{Supp}(f)=\cup_{i=1}^{l} L^{*} x_{i}$ then

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

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 $H_{\alpha}$, equivalently $t(\alpha)$ is the number of $x_{i}$ for which $\operatorname{Tr}_{a}^{a b}\left(x_{i} \alpha\right)=0$. Thus, the nonlinearity of $f$ is given by

$$
n l(f)=\min _{\alpha \in M}\left\{l\left(2^{a}-1\right), 2^{a b}-l\left(2^{a}-1\right), 2^{a b-1}-2^{a} \cdot t(\alpha)+l, 2^{a b-1}+2^{a} \cdot t(\alpha)-l\right\} .
$$

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

$$
\begin{gather*}
\frac{2^{a b-1}-2^{(a b-1) / 2}}{2^{a}-1}<l<\frac{2^{a b-1}+2^{(a b-1) / 2}}{2^{a}-1}  \tag{2}\\
\frac{1}{2^{a}}\left\{\frac{2^{a b-1}-2^{(a b-1) / 2}}{2^{a}-1}-2^{(a b-1) / 2}\right\}<t(\alpha)<\frac{1}{2^{a}}\left\{\frac{2^{a b-1}+2^{(a b-1) / 2}}{2^{a}-1}+2^{(a b-1) / 2}\right\} . \tag{3}
\end{gather*}
$$

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 $\Phi\left(M^{*}\right)$ of left multiplications by the elements of $M^{*}$ in $G L_{K}(M)$ and this correspondence is an isomorphism.

Let $\phi_{2} \in G L_{K}(M)$ be the Frobenius automorphism of $M$. This is defined by $\phi_{2}(x)=x^{2}$ for all $x \in M$. The group $\left\langle\phi_{2}\right\rangle$ generated by $\phi_{2}$ is a cyclic group of order $a b$, which is contained in $G L_{K}(M)$. Patterson and Wiedemann [12] considered the action of the group $G=\left[\Phi\left(L^{*}\right) \cdot \Phi\left(J^{*}\right)\right]\left\langle\phi_{2}\right\rangle / \Phi\left(L^{*}\right)$, where $\left[\Phi\left(L^{*}\right) \cdot \Phi\left(J^{*}\right)\right]\left\langle\phi_{2}\right\rangle$ is the semidirect product of $\Phi\left(L^{*}\right) \cdot \Phi\left(J^{*}\right)$ by $\left\langle\phi_{2}\right\rangle$.

The result of [12] was for $n=15$. Here $L^{*}=G F\left(2^{5}\right)^{*}$ and $J^{*}=G F\left(2^{3}\right)^{*}$. 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 $M^{*}=G F\left(2^{15}\right)^{*}$ of order $\left(2^{5}-1\right)\left(2^{3}-1\right)=(31)(7)=217$. 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., $f(x)=f\left(x^{2}\right)$ 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 $L^{*}=G F\left(2^{7}\right)^{*}$ and $J^{*}=$ $G F\left(2^{3}\right)^{*}$ here. Now $L^{*} \cdot J^{*}$ is a cyclic subgroup of $M^{*}=G F\left(2^{21}\right)^{*}$ of order $\left(2^{7}-1\right)\left(2^{3}-1\right)=(127)(7)=889$. 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., $f(x)=f\left(x^{2}\right)$ 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 $\mathrm{GF}(2)$ 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 $\left[A_{i, j}\right]$ is described in Appendix A. We like to present an observation here that if one leaves the rows and columns indexed by 0,93 and 114 , then the resulting $112 \times 112$ 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.

## 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 $6272\left(=2 \times 56^{2}\right)$ 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 $x=\left(x_{0}, x_{1}, \ldots, x_{114}\right)$ be a solution, $A_{i}=\left(A_{i, 0}, A_{i, 1}, \ldots, A_{i, 114}\right)$
be the $i$-th row of the coefficient matrix, and $\left(x, A_{i}\right)=\sum_{j=0}^{114} A_{i, j} x_{j}$ be the inner product of $x$ and $A_{i}$, where $i=0,1, \ldots, 114$. The cost function is then given by

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

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, $3.50 \mathrm{GHz}, 6$ 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):358362, (1983).
[12] N. J. Patterson and D. H. Wiedemann. The covering radius of the $\left(2^{15}, 16\right)$ 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 $115 \times 115$ 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.

30000000000000000 v 0000 v 0000000000000 vv 00000000000000000000000000000000000000000000000000000000000000000000000000 vv 0 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 0112331121001343131002112010142110400010211133003102011021101210012111210021200002200031100000203120012112102123120 0123110021031111120012012011320103112110011112111112012211103005100121100032111010010220346130221110011101111120110 0302100321140102102201311111111032102120120110221211111002111021010121210011121121411253010300300121300000102040010 0120230103102121111112100400210320012110013011001114031202111012100022113010113021110222000130000012231421024021110 0111101011022122120110322214103204100020212111114200102210113101010120115111302012032203110100001102022010110031200 0201203012211110221211152103141101010314112122010021102000000010002110221011010230221412211120100320031222002110010 0311110320012130100130212033001010121211312101110113111011010101210120211001141023032100012130015031111002204111110 1211103022200122000020310010202220011010201112023210110101112122211013221311001311111101151110302211120122104111000 1111222101112311230410020232201110320122111110201010211112101101101133003111020113200130002220221102011100110420000 0002022011111310200111130110111212111200142300141012051011023200110121302122231113401100311000111201100131101001210 0110123220210001101120211001300000410200143113111210221300000321341321101111201130000222102130101213011010021022120 0323212000312231101211310221220102132111021000022110010010123221135210010130121110031000001010020110201300112241010 0010102240204212211102222000311211110144201003421222110020122132000102110021023021211001110020111003000100021111210 0111140011010012110121211111211032221123110112012632021011101012110131010210330411113201200210020010021120000302020 0000123433241012211100111132111101111131001012011003020312111000212032310220121200021112011100020400001201311103300 0012010120100110025003120042231111201101001101111110310111012131200132412200221211012000101110230133132212011030200 0000102011021103220113111212132011212003032210120021202013201103141013010020111322002002021100012003204111104011200 0001111000014112011011114140101201010211040011011103001201510211112200211212032311103021111210300212031021122220120 0111110201200200220100100132101201112041221112101102005013012332303012010121211042013112211000210222210123000001020 0120431030303101102110201112131114003111212110110021111230110102211122001212301232101110100101401120020100412100100 0211013101012211123011110010411212012002126010110212101101301211110002111101111102140222210201142221100002100213020 0011200121031231000112131022001110211111123012002121312212023110110002021223001412202211011011020030100300241010040 0003200201011121524101210113122140130020022301321210011301331101111020010112001221010001111030202210130110111102120 0202222221001022111300120012200101111202010032001130022112231011011021112100014101002101502011302112502011211122110 0313111123011011011030123200111130011152112210001011200110030211321021111033110002101000202301220203123210001022120 0200222002121120300111101110012112210111001002151121200332101031101220052011220112010022103001221102220013012110230 0001210212030301011121230000202022001103000310202123113431111420211201112111001020012110101010121110110121104432200 0032002011102122302241212211221001010110121111013010113324001031000111110101120020102110210500113221200300021202310 0112011021124110011011211120011220011210001213130121202142003411103122100100102202100313100340012200323010200111010 0012222114112021000233130312311111001100111102501303201100201010113221110111200113101000121110100232301002200110221 0112123211010121033401131111100111011020220110111023330100001315101410030012202201012103010200213100111212121100110 0022403211210011111103010110213113002130321121020131101113112111331021323002032000001110010120002120012020010310031 0310021012212011021012220112220001011123210011231211020404031400011111001102110102121032023000202041113230020101100 0112021232010150112201303201210210102002231030130110113231111001311101101320010011312103012010120112131001011300101 0220131111120000122022021331105121012101122013122101111011051010011302101140011120000203201210313011001102111310110 0021221110101011121313003013201010022113101221132111031201113030221001100111100013111012011421011200010043311040110 0003101100040222123020100400010101011014301104101111120100103111223112102110230120211220111111203112221021231100210 0321221122021201111111220230120000201101500201231001111103311111130101021001111010102102420120020102040301410122020 0111011111211321100221100200011101110113211010201000002211240113011031410001401311101203011130342110001131111131231 0201001212322013102410101020212222121322103331012002222012212100010302200010400111000000122000011021241011031210020 0111001105100512201010012012111120003311021223022220110112101112121120110012212011131101000120310023002112430310100 0120011001222220021041120013121211222031010340200100110111103011110421210211032010001024210011111112110120213102021 010111214121010313205010011121011121200011111110121115110132000002101140114232202120021001120001102121222110220100 0212113221101211103012012330000035111321000020101110212200003111021000002100110223201013122030101112001213112204120 0300211200211231411121031230200001003111102220212121100111100131110000211452302200102131111130012011222020100001200 0101001110212010020011021212023111101121321202121021031100110024110011110502200012110121101010010211412102132533120 0141003201001202212101201112012101111121010000212132031110122200101102140220200101101420203210011134022010303111021 0011012111011100011201210000121113010022103121023100012011220100121442021322011011214030011250111011212204211001220 0101230021101010211001120200101210140230223221310100112020003111031001331000101200024131113300210021111111322311300 0320331000121312120110101001201132011011130111211111400102022001001102220200112030312000102120021520124012131012210 0024110010421111201213201120000100203111104223302142101002120101010310022201020002112202012100310301012121112113100 0210110200310213024031020011001221321113121012143012001220100012121111102010103004113210122210100310211300101100121 0100010130100230021233010110020112031330011012122221122002310210300111023021100240120021220100122301113000321121101 0010111012141001102122201113220410201240021000101120010011100130121101012111203111402101113010125110121223200321110 0030101112331130112201124011101113231000311210010401001100010210110003020010121112000220210020321202313331211210310 0111101205001011050212002011000102121010113122331020210220121120112101101201442230202210121110211010111200102123010 0013032412203210020000011210102222411112002100011220100113011012021201000114010220122211211100003221230121211030301 0111322300120111020212101111232520100302000100211210002111001300120000221322330012021102221320311101201200142001010 0201100111101121111210112203310323201002011202120211102003030233202301413110010201100120012200001001011211511103130 0110000211100012111223411220213001201031012010121201521121100002014010201112011012121220401020221100111141332101010 0111122041011202311210032001104101115010010102110111000010211210112120102100110122112121022210132011330321041013011 0122120002312043113000100101306000121212100111110011223100100321110120012113132220301112122110020111102102301011110 0221201100001014102111251201001311111201002111201200030053121002411101010102231121001132021010121311012113110121110

0122002141012120211012211102003030231203121010100013100104102011212302123311502010121020211120300100101221100111010 070000000007 u 000770000000000000000000000000000007770777000000000770000700000000000000000000000700000000707000000003 0112301122110020200000001112022300103211010020324102322110120213020303101000120311132030210131012312111220000211110 0100402221112401012002100413002000010210212231010420022211010021102411100111112102221010232200141101122110012011120 0010302301111020211131010021231001052111010002001202201132032203130210111201101002511311120100210002131012111122210 0122004010120030010110000211111101302122100410221202121122211010211100111021005333120210101310310030022102021113210 0320000141010100211210011522221210231001101030122231100120302411010122101113122010101200011100100320101023122111230 0061110211121211100111120122100122011213030033220100232010200121022013222114110101020111011100212000241101001013210 0013132010212101013210021103000320011010200012020111512123310110020020110240211021131220131010111012001130102222230 0311200010012010011101011001111032312101002030312003022102011130124040120212112111211301130100123204021110131300210 0101300101110000211110314210221012110101101124100000230003112311010112011222214213131011102210121211110211102211112 0011001100012012100111010142511040201110311221011031020130020201003101122010210130232122131121210101112211111111321 0010120010201215210211013312010021202031002011220001111201012300420311221201011200230201420120211020311102001220220 0012110301213201010101341120121010222010000121130200103100220012311112023020412100310101112311002231001122032202100 0110110021101210103201011001211101021110100301104121200102210001324104211113231113221215303110001010111100012211320 0001021102201120211122302112001021000102120110201041101020021211131133111030123102010141340100011220030103140122110 0110104000012200001302302210121240244011210114202011112410010011110110302023121211012121211000021121212112200111000 0211011110111003011201011002011000111400213100201201101421113133011123122051030111321001100110201110232122211203011 0100010012101011411011110030122423111202410031200110221301101001402311020031011102212300011210112111201120121043110 0142110221201101320110100001030011011012112301010302220221000100002100204131112301103013131110112313201102121330030 1302021220111111200005011101211012010021020322101001112230210111120201011210232111130301001100112222221321310010130 120301101110011002010014020021110110012112000220242123011213001112320202022201020111013111110121131311220210113310 000007070000000070000070000000000000000000000000000000000070707000070070000700007700070007000300000000 u 700000700000

