Patterson-Wiedemann Construction Revisited*

S. Gangopadhyay, P. H. Keskar
Mathematics Group
Birla Institute of Technology and Science Pilani,
Rajasthan, 333 031,
INDIA
Email : {sugata, keskar}@bits-pilani.ac.in

S. Maitra
Applied Statistics Unit
Indian Statistical Institute
203, B. T. Road,
Calcutta 700 035, INDIA
Email : subho@isical.ac.in

Abstract

In 1983, Patterson and Wiedemann constructed Boolean functions on $n = 15$ input variables having nonlinearity strictly greater than $2^{n-1} - 2^{\frac{n-1}{2}}$. Construction of Boolean functions on odd number of variables with such high nonlinearity was not known earlier and also till date no other construction method of such functions are known. We note that the Patterson-Wiedemann construction can be understood in terms of interleaved sequences as introduced by Gong in 1995 and subsequently these functions can be described as repetitions of a particular binary string. As example we elaborate the cases for $n = 15, 21$. Under this framework, we map the problem of finding Patterson-Wiedemann functions into a problem of solving a system of linear inequalities over the set of integers and provide proper reasoning about the choice of the orbits. This, in turn, reduces the search space. Similar analysis also reduces the complexity of calculating autocorrelation and generalized nonlinearity for such functions. In an attempt to understand the above construction from the group theoretic view point, we characterize the group of all $GF(2)$-linear transformations of $GF(2^{ab})$ which acts on $PG(2, 2^a)$.

Keyword : Boolean Function, Algebraic Approach, Nonlinearity, Autocorrelation, Generalized Nonlinearity.

1 Introduction

Patterson and Wiedemann [7, 8] constructed Boolean functions on 15 variables with nonlinearity $> 2^{15-1} - 2^{(15-1)/2}$. In this paper we revisit this construction technique. First we describe the technique as in [7]. The supports of the functions, that Patterson and Wiedemann have considered, are unions of the cosets of the multiplicative group $GF(2^5)^*$ in $GF(2^{15})^*$. The cosets of the multiplicative group $GF(2^5)^*$ in $GF(2^{15})^*$ form a Desarguesian projective plane which is denoted by $PG(2, 2^5)$. The order of the multiplicative groups $GF(2^5)^*$ and $GF(2^3)^*$ are coprime to each other. The product $GF(2^5)^*.GF(2^3)^*$ in $GF(2^{15})^*$ is a direct product. Patterson and Wiedemann have considered the

*This is an extended version of the paper presented at R. C. Bose Centenary Symposium on Discrete Mathematics and Applications, Indian Statistical Institute, December 2002.

search space consisting of functions whose supports are invariant under the action of the semidirect product of $GF(2^3)^*.GF(2^5)^*$ by the group of Frobenius automorphisms along with some weight restrictions and obtained the functions with nonlinearity as high as $2^{15-1} - 2^{\frac{15-1}{2}} + 20$ by exhaustively searching this space.

In Section 2, we show that this construction can be understood by using interleaved sequence as introduced by Gong [3]. The functions whose supports are invariant under the above group action can be described as functions whose interleaved sequences are repetitions of a particular binary sequence as rows. This gives an alternative description of the construction technique explained by Patterson and Wiedemann. Exploiting this, we map the problem into a problem of solving a system of linear inequalities over the set of integers and reduce the search space considered by Patterson and Wiedemann. Our analysis also provides proper justification about the choice of the orbits which was not clearly explained under the framework of [7] (in particular see [7, Page 356]).

Moreover, our results can be used to reduce the complexity of calculating autocorrelation (Section 2.4) and generalized nonlinearity (Section 2.3) of such functions. We show that we need to calculate the autocorrelation values at only 10 distinct points instead of 32767 for the 15 variable case. Further our analysis helps in disproving a conjecture related to autocorrelation presented in [12]. This conjecture has earlier been disproved for 15-variable balanced Boolean function [6]. We disprove it for 21-variable balanced Boolean function too. It is also shown that while calculating the generalized nonlinearity [11] of such 15-variable functions, it is enough to evaluate the distances from bijective monomials corresponding to only 10 instead of all the 1800 cyclotomic coset leaders.

In Section 3 we give a complete description of the group of all $GF(2)$-linear transformations that act on the support of such functions.

1.1 Patterson-Wiedemann Construction

Let $\mathcal{F}_n$ be the set of functions from $GF(2^n)$ to $GF(2)$. Consider a function $f \in \mathcal{F}_n$. Support of f is defined as $Supp(f) = \{x \in GF(2^n) | f(x) = 1\}$. It is clear that a function in $\mathcal{F}_n$ is completely known once its support is specified. Weight of a function f is defined by $|Supp(f)|$ and it is said to be balanced if $|Supp(f)| = 2^{n-1}$.

Suppose a and b are two positive integers greater than 1 such that $n = ab$. Denote $GF(2^{ab})$ by M, $GF(2^a)$ by L, $GF(2^b)$ by J and $GF(2)$ by K. Consider the tower of subfields $K \hookrightarrow L \hookrightarrow M$. The index of the multiplicative group L^* in M^* is $m = \frac{2^{ab}-1}{2^a-1}$. The multiplicative group M^* can be written as $M^* = \cup_{i=1}^m L^* x_i$ where $\{x_1, x_2, \ldots, x_m\}$ is the complete set of coset representatives of L^* in M^*. We have already noted that one can characterize any function from $M \to K$ by specifying its support. Dillon [1] and later Patterson and Wiedemann [7] have considered functions in $\mathcal{F}_n$ whose supports are of the form $\cup_{i=1}^l L^* x_i$ for some positive integer l. Let us denote the set of all such functions by $I_{a,b}$. A linear function in $\mathcal{F}_{ab}$ is of the form $l_\alpha(x) = Tr_1^{ab}(\alpha x)$ where $\alpha \in M$ and $Tr_1^n(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}}$ for all $x \in GF(2^n)$. Clearly the support of l_α is $Supp(l_\alpha) = \{x \in M | Tr_1^{ab}(\alpha x) = 1\}$, whereas the support of the affine function $h_\alpha(x) = l_\alpha(x) + 1$ is $Supp(h_\alpha) = \{x \in M | Tr_1^{ab}(\alpha x) = 0\}$. Note that $Supp(h_\alpha)$, henceforth denoted by H_α, is a hyperplane in M when considered as a vector space over K.

The Hadamard transform of $f \in \mathcal{F}_n$ is defined by

$$\hat{f}(\lambda) = \sum_{x \in GF(2^n)} (-1)^{f(x)+Tr(\lambda x)}. \quad \text{Also,} \quad nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in GF(2^n)} |\hat{f}(\lambda)|$$

defines the nonlinearity of $f \in \mathcal{F}_n$.

Since $GF(2^n)$ contains finitely many elements it is possible to write them in some order. Let $\{\alpha_0, \alpha_1, \ldots, \alpha_{2^n-1}\}$ be the elements of $GF(2^n)$. For $f, g \in \mathcal{F}_n$, the Hamming distance between the 2^n-dimensional vectors $(f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^n-1}))$ and $(g(\alpha_0), g(\alpha_1), \ldots, g(\alpha_{2^n-1}))$ is defined as the distance between the functions f and g denoted $d(f,g)$. It is clear that if $f, g \in \mathcal{F}_n$ then $d(f,g) = |Supp(f) \oplus Supp(g)|$ where $\oplus$ is the symmetric difference between the sets $Supp(f)$ and $Supp(g)$. Patterson and Wiedemann [7] proved that if $Supp(f) = \cup_{i=1}^{l} L^* x_i$ then

$$d(f, \mathbf{0}) = l(2^a - 1), \quad d(f, \mathbf{1}) = 2^{ab} - l(2^a - 1),$$
$$d(f, h_\alpha) = 2^{ab-1} - 2^a \cdot t(\alpha) + l \text{ and } d(f, l_\alpha) = 2^{ab-1} + 2^a \cdot t(\alpha) - l,$$

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

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

For an $f \in I_{a,b}$ with $nl(f) > 2^{ab-1} - 2^{(ab-1)/2}$ each term within the parenthesis in the right hand side of the above equation is greater than $2^{ab-1} - 2^{(ab-1)/2}$. It implies that l and $t(\alpha)$ must satisfy:

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

When $b = 3$ then the cosets of L^* in M^* form the Desarguesian projective plane $PG(2, 2^a)$.

Suppose $n = 15, a = 5, b = 3$. Consider the two subgroups L^* and J^* in M^*. Intersection of these two subgroups is only the group containing the identity element and the group M^* is an abelian group. Thus in this case the product $L^*.J^*$ is direct. One can identify the group M^* to the group $\Phi(M^*)$ of left multiplications by the elements of M^* in $GL_K(M)$. Clearly this correspondence is an isomorphism. Let $\phi_2 \in GL_K(M)$ be the Frobenius automorphism of M 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 and is contained in $GL_K(M)$. The group $\langle\phi_2\rangle$ acts on the projective plane $PG(2, 2^a)$. Action of the group $\Phi(L^*)$ on $PG(2, 2^a)$ is trivial. For $n = 15$, Patterson and Wiedemann considered the action of the group $G = [\Phi(L^*).\Phi(J^*)]\langle\phi_2\rangle/\Phi(L^*)$, where $[\Phi(L^*).\Phi(J^*)]\langle\phi_2\rangle$ is the semidirect product of $\Phi(L^*).\Phi(J^*)$ by $\langle\phi_2\rangle$. This is in view of constructing supports of functions in $I_{5,3}$ which are invariant under the action of G and also satisfy the conditions (1) and (2). The group G acts on the projective plane in ten orbits of size 105 and one orbit of size 7. In the case of $n = 15$ one must choose 5 orbits out of the 10 orbits of size 105 so that the condition (1) is satisfied. Therefore, the total number of possible choices is $\binom{10}{5} = 252$. Exhausting all the possibilities they have obtained two solutions up to complementation which satisfy (2). The functions corresponding to these two solutions have nonlinearity 16276. Now on, we will refer the construction by Patterson and Wiedemann [7, 8] by PW construction.

2 PW construction and Interleaved Sequence

In this section we interpret the Patterson Wiedemann construction in terms of interleaved sequence. By analysing their construction in this way we have understood algebraically the choice of orbits.

It was commented in [7, Page 356] that the choice of such orbits was not clearly understood and we provide a mathematical reasoning here which is related to the solution of a set of inequalities. We also characterize the Walsh spectra of such functions. Finally we show that the symmetry of the PW functions simplifies the calculation of autocorrelation and generalized nonlinearity.

A binary sequence of length m is denoted by $\mathbf{a} = \{a_0, a_1, a_2, \ldots, a_{m-1}\}$ where $a_i \in \{0, 1\}$ for all $i = 0, 1, 2, \ldots, (m-1)$. In case $m = 2^n - 1$ for some positive integer n we can choose a primitive element $\zeta \in GF(2^n)$ and construct a function such that $f(0) = 0$ and $f(\zeta^i) = a_i$ where $i = 0, 1, 2, \ldots, 2^n - 2$. This function f is called the function corresponding to the sequence $\mathbf{a}$ with respect to the primitive element ζ. If we change the primitive element then we obtain a different function. Again if f is a function from $GF(2^n)$ to $GF(2)$ with $f(0) = 0$ and $\zeta \in GF(2^n)$ is a primitive element then the sequence $\{f(1), f(\zeta), f(\zeta^2), \ldots, f(\zeta^{2^n-2})\}$ is referred to as the sequence associated to f with respect to ζ. When there is no chance of confusion the primitive element ζ is not mentioned. It is to be noted that restriction to the functions which take the value zero at zero does not restrict our search for high nonlinear functions since for any function g with $g(0) = 1$ there exists the complement of the function g' defined by $g'(x) = 1 + g(x)$ with $g'(0) = 0$, which has the same nonlinearity as g.

Definition 1 *Suppose m is a composite number such that $m = d.k$ where d and k are both positive integers greater than 1, $\mathbf{a}$ is a binary sequence $\{a_0, a_1, a_2, \ldots, a_{m-1}\}$ where $a_i \in \{0, 1\}$ for all i, then the (d, k)-interleaved sequence $\mathbf{a}_{d,k}$ corresponding to the binary sequence $\mathbf{a}$ is defined as*

$$\mathbf{a}_{d,k} = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{(d-1)} \\ a_d & a_{1+d} & a_{2+d} & \cdots & a_{(d-1)+d} \\ a_{2d} & a_{1+2d} & a_{2+2d} & \cdots & a_{(d-1)+2d} \\ . & . & . & . & . \\ . & . & . & . & . \\ a_{(k-1)d} & a_{1+(k-1)d} & a_{2+(k-1)d} & \cdots & a_{(d-1)+(k-1)d} \end{bmatrix}$$

Let $2^n - 1 = d.k$, $\mathbf{a}_{d,k}$ be an interleaved sequence and $\zeta \in GF(2^n)$ be a primitive element. Then a function $f : GF(2^n) \to GF(2)$ with $f(0) = 0$ and $f(\zeta^{i+\lambda d}) = a_{i+\lambda d}$ where $i = 0, 1, 2, \ldots, (d-1)$ and $\lambda = 0, 1, 2, \ldots, (k-1)$ is defined as the function corresponding to the interleaved sequence $\mathbf{a}_{d,k}$ with respect to the primitive element ζ. Conversely, for any function $f : GF(2^n) \to GF(2)$ and a primitive element $\zeta \in GF(2^n)$ an interleaved sequence $\mathbf{a}_{d,k}$ can be constructed such that $a_{i+\lambda d} = f(\zeta^{i+\lambda d})$ for all $i = 0, 1, 2, \ldots, (d-1)$ and $\lambda = 0, 1, 2, \ldots, (k-1)$. This interleaved sequence is called the interleaved sequence corresponding to f with respect to ζ. Again as in the case of binary sequences we drop the reference to ζ when there is no chance of confusion. The rows and columns of $\mathbf{a}_{d,k}$ are numbered from 0 to $(k-1)$ and 0 to $(d-1)$ respectively.

Recall that the support of a function $f \in \mathcal{F}_n$ is a subset of $GF(2^n)$. The general linear group $GL_{GF(2)}(GF(2^n))$ acts on the support of f. There exists a natural embedding of any subgroup $\mathcal{K}$ of $GF(2^n)^*$ into $GL_{GF(2)}(GF(2^n))$, which maps the elements of $\mathcal{K}$ to the left multiplications by the same elements. The action of this image of $\mathcal{K}$ on the support of f will be referred to as the action of $\mathcal{K}$. Instead of writing 'the action of $\mathcal{K}$ on the support of a function f' we write 'action of $\mathcal{K}$ on f', similarly when we write 'a function f is invariant under the action of $\mathcal{K}$' we imply that the support of the function f is invariant under the action of $\mathcal{K}$.

Lemma 1 *If the support of a function $f \in \mathcal{F}_n$ is invariant under the action of a cyclic subgroup $\mathcal{K}$ of order k of $GF(2^n)^*$ then the $(\frac{2^n-1}{k}, k)$-interleaved sequence of f with respect to any primitive* *element of $GF(2^n)$ has a fixed binary sequence of length $\frac{2^n-1}{k}$ as rows. Conversely, if the $(\frac{2^n-1}{k}, k)$-interleaved sequence of f with respect to a primitive element $\zeta \in GF(2^n)$ has a fixed binary sequence of length $\frac{2^n-1}{k}$ as rows, then the support of f is invariant under the action of $\mathcal{K}$.*

Proof : Let ζ be any primitive element of $GF(2^n)$. Let $\mathbf{a}_{d,k}$ where $d = \frac{2^n-1}{k}$ be the interleaved sequence of f with respect to ζ. Clearly ζ^d is a generator of a cyclic subgroup of order k in $GF(2^n)^*$. It is well known that if k is a divisor of the order of a cyclic group then there exists a unique subgroup of order k in that group. Thus $\mathcal{K} = \langle \zeta^d \rangle$, that is $\mathcal{K}$ is generated by ζ^d. If the support of f is invariant under the action of $\mathcal{K}$ then $f(\zeta^i) = f(\zeta^{i+\lambda d})$ for $\lambda = 0, 1, \ldots, (k-1)$ and $i = 0, 1, \ldots, (d-1)$. As a consequence the i-th column of $\mathbf{a}_{d,k}$ is constant for each i.

Conversely, if $\mathbf{a}_{d,k}$ has a fixed binary sequence of length d as rows then $a_i = a_{i+\lambda d}$ where $\lambda = 0, 1, \ldots, (k-1)$, for each $i = 0, 1, \ldots, (2^n-2)$, where the subscript of 'a' is always reduced modulo $2^n - 1$. If f is the function corresponding to $\mathbf{a}_{d,k}$ with respect to a primitive element ζ then $f(\zeta^i) = f(\zeta^{i+\lambda d})$ for $\lambda = 0, 1, 2, \ldots, (k-1)$ and $i = 0, 1, 2, \ldots, (2^n-2)$ which implies that the support of f is invariant under the action of the group generated by ζ^d. But we have already noted that for any primitive element ζ the subgroup of $GF(2^n)^*$ generated by ζ^d is equal to $\mathcal{K}$. Therefore the support of f is invariant under the action of $\mathcal{K}$. ■

Example 1 *Let $n = 15$, $L^* = GF(2^5)^*$ and $J^* = GF(2^3)^*$. The support of f is invariant under the action of L^* and J^* implies that the support of f is invariant under the action of the product $L^*.J^*$ which is also a cyclic subgroup of $M^* = GF(2^{15})^*$ of order $(2^5-1)(2^3-1) = (31)(7)$. Therefore by lemma 1 the support of the function f is invariant under the action of $L^*.J^*$ if and only if $(151, (31)(7))$-interleaved sequence of f has a fixed binary sequence of length 151 as rows. It is to be noted that this property is independent of the choice of the primitive element.*

Suppose $f \in \mathcal{F}_n$, apart from being invariant under the action of a cyclic subgroup $\mathcal{K}$ of order k, is also invariant under the action of the group of Frobenius automorphisms $\langle \phi_2 \rangle$.

Definition 2 *Define an equivalence relation ρ_d on $\{0, 1, 2, \ldots, (d-1)\}$ by $i_1 \ \rho_d \ i_2$ if and only if $i_1 \equiv 2^j i_2 \bmod d$ for some non-negative integer j where $i_1, i_2 \in \{0, 1, 2, \ldots, (d-1)\}$.*

The set $\{0, 1, 2, \ldots, (d-1)\}$ is the set of column numbers of the (d, k)-interleaved sequence of a Boolean function. Thus ρ_d partitions this set into equivalence classes.

Lemma 2 *A function f invariant under the action of $\mathcal{K}$ is also invariant under the action of $\langle \phi_2 \rangle$ if and only if the (d, k)-interleaved sequence of the function has a fixed binary sequence of length d as rows and the columns in the same equivalence class with respect to ρ_d are either 'all zero' columns or 'all one' columns.*

Proof : Any function f invariant under the action of $\mathcal{K}$ and $\langle \phi_2 \rangle$ is invariant under the action of $\mathcal{K}$ and hence by lemma 1 the (d, k)-interleaved sequence of this function has a fixed binary sequence of length d as rows. Consider the i-th column where $0 \le i \le (d-1)$. Under the Frobenius automorphism ϕ_2^j, the element ζ^i is mapped to $\zeta^{2^j \cdot i}$. If the support of f is invariant under the Frobenius automorphisms then $f(\zeta^i) = f(\zeta^{2^j \cdot i})$. Using division algorithm, we find $q_{i,j}$ and $r_{i,j}$ such that $2^j \cdot i = q_{i,j} d + r_{i,j}$, where $0 \le r_{i,j} < d$. The element $f(\zeta^{2^j \cdot i})$ will occur in the $q_{i,j}$-th row and $r_{i,j}$-th column in the (d, k)-interleaved sequence of f, the first row (column) being referred to as the 0-th row (column). Since the columns of this interleaved sequence corresponding to f are either 'all zero' or 'all one' columns, the $r_{i,j}$-th column of the interleaved sequence has the same value as

$f(\zeta^i)$, in particular $f(\zeta^{r_{i,j}}) = f(\zeta^i)$. Thus all the columns which are in the same equivalence class of ρ_d has the same value.

Conversely if the function f has the (d,k)-interleaved sequence with the above mentioned property then for any $j \geq 0$ and $i \in \{0,1,2,\ldots,(d-1)\}$, $f(\zeta^{i2^j})$ appears in the $q_{i,j}$-th row and $r_{i,j}$-th column. But $r_{i,j} \equiv 2^j i \bmod d$, therefore $r_{i,j}$ and i are in the same equivalence class of ρ_d. Hence $f(\zeta^i) = f(\zeta^{i2^j})$. Thus the function is invariant under the action of $\langle\phi_2\rangle$. Again since the interleaved sequence under consideration has a fixed binary sequence of length d as rows the corresponding function f is invariant under the action of the group $\mathcal{K}$. ■

Remark 1 *It is to be noted that the equivalence classes discussed above are the orbits of the group generated by $\langle\phi_2\rangle$ and $\mathcal{K}$ when it acts on $GF(2^n)^*/\mathcal{K}$.*

A function of the form $f(x) = Tr_1^n(\alpha x^c)$ where $\alpha \in GF(2^n)$ and $gcd(c, 2^n-1) = 1$ is called a bijective monomial [10, 11]. When $c = 1$, f is the linear function l_α. Thus linear functions can be thought of as special cases of bijective monomials. Suppose $t|n$ and $d = \frac{2^n-1}{2^t-1}$. The structure of $(d, 2^t-1)$-interleaved sequence corresponding to a bijective monomial has been stated without proof in [10, 11]. We give a complete proof below.

Lemma 3 *Let $f(x) = Tr_1^n(x^c)$, where $gcd(c, 2^n-1) = 1$. Then for all $t|n$ the $(d, 2^t-1)$-interleaved sequence of f with respect to a primitive element $\zeta \in GF(2^n)$ is such that*

1. *the columns are either 0-columns or cyclic shifts of the binary sequence corresponding to $Tr_1^t(x)$ when evaluated at $1, \zeta^{cd}, \zeta^{c2d}, \ldots, \zeta^{c(2^t-2)d}$ which contains 2^{t-1} ones,*
2. *the number of zero columns is $d - 2^{n-t}$.*

Proof : Let ζ be a primitive (2^n-1)-th root of unity. Then the entry in the i-th column and λ-th row of the $(d, 2^t-1)$- interleaved sequence of f is

$$\begin{aligned}
u_{i,\lambda} &= f(\zeta^{i+\lambda d}) \\
&= Tr_1^n(\zeta^{c(i+\lambda d)}) \\
&= Tr_1^t(Tr_t^n(\zeta^{c(i+\lambda d)})) \\
&= Tr_1^t(\zeta^{ci+c\lambda d} + \zeta^{ci2^t+c\lambda d2^t} + \zeta^{ci2^{2t}+c\lambda d2^{2t}} + \ldots + \zeta^{ci2^{(\frac{n}{t}-1)t}+c\lambda d2^{(\frac{n}{t}-1)t}}) \\
&= Tr_1^t((\zeta^{ci} + \zeta^{ci2^t} + \zeta^{ci2^{2t}} + \ldots + \zeta^{ci2^{(\frac{n}{t}-1)t}})\zeta^{c\lambda d}).
\end{aligned}$$

The sequence $\{u_{i,\lambda} | \lambda = 0,1,\ldots,2^t-2\}$ corresponds to the linear function of the form $Tr_1^t(\gamma_i x)$, where $\gamma_i = \zeta^{ci} + \zeta^{ci2^t} + \zeta^{ci2^{2t}} + \ldots + \zeta^{ci2^{(\frac{n}{t}-1)t}}$, when evaluated at the points $1, \zeta^{cd}, \zeta^{c2d}, \ldots, \zeta^{c(2^t-2)d}$. If $\gamma_i = 0$ for some i then the i-th column consists of only zeros. Otherwise it is cyclic shift of the binary sequence generated by $Tr_1^t(x)$ when evaluated at the points $1, \zeta^{cd}, \zeta^{c2d}, \ldots, \zeta^{c(2^t-2)d}$.

Since each non-zero column is a sequence corresponding to a linear function with respect to the element ζ^{cd}, the number of 'one's in each them is 2^{t-1}. Again the number of 'one's in the binary sequences corresponding to $f(x)$ and $Tr_1^n(x)$ are equal, therefore the total number of 'one's in the binary sequence corresponding to $f(x)$ is 2^{n-1}. Let the number of non-zero columns be r. Then $r(2^{t-1}) = 2^{n-1}$, i.e., $r = 2^{n-t}$. So, the number of zero columns is $d - r = d - 2^{n-t}$. ■

Example 2 *In case $n = 15$, let us consider the function $Tr_1^{15}(x)$. By the above result, the $(1057, 31)$-interleaved sequence corresponding to this function contains $1057 - 2^{15-5} = 1057 - 1024 = 33$ zero columns. The others columns are cyclic shifts of the sequence corresponding to the function $Tr_1^5(x)$.*

The way to construct the interleaved sequence corresponding to the function $Tr_1^n(\zeta^{i+1}x)$ from the interleaved sequence corresponding to the function $Tr_1^n(\zeta^i x)$ can be summarised in the following way.

The i-th column of the $(d, 2^t-1)$-interleaved sequence corresponding to $Tr_1^n(\zeta^i x)$ is the $(i-1)$-th column of the $(d, 2^t-1)$-interleaved sequence corresponding to the function $Tr_1^n(\zeta^{i+1}x)$ for $i = 1, 2, \ldots, (d-1)$. The zero-th column of the former sequence is to be given a cyclic shift in the upward direction and placed as the $(d-1)$-th column of the later sequence.

The support of the affine function $h_\alpha(x) = Tr_1^n(\alpha x) + 1$ is $Supp(h_\alpha) = \{x \in GF(2^n) | Tr_1^n(\alpha x) = 0\}$. Recall that $Supp(h_\alpha)$ (denoted by H_α) is a hyperplane in $GF(2^n)$ when considered as a vector space over $GF(2)$. Next we give an interpretation of $t(\alpha)$, that occur in condition (2) of Section 1, in the language of interleaved sequence. If $n = ab$ then we can write h_α as a $(\frac{2^{ab}-1}{2^a-1}, 2^a-1)$-interleaved sequence. Since $h_\alpha(x) = Tr_1^n(\alpha x)+1$, by lemma 3 the number of 'all one' columns in the interleaved sequence of h_α is $d - 2^{n-a}$. Let $f \in I_{a,b}$ i.e., the support of f is union of cosets of the type $L^* x_i$. By lemma 1 the $(\frac{2^{ab}-1}{2^a-1}, 2^a-1)$-interleaved sequence of f has a fixed binary sequence of length $\frac{2^{ab}-1}{2^a-1}$ as rows. In section 1 we defined $t(\alpha)$ as the number of cosets in the support of f that are contained in H_α. This is equivalent to the number of 'all one' columns of the $(\frac{2^{ab}-1}{2^a-1}, 2^a-1)$-interleaved sequence of f that correspond to the 'all one' columns of the $(\frac{2^{ab}-1}{2^a-1}, 2^a-1)$-interleaved sequence of h_α.

In case our aim is to search for a function $f \in I_{a,b}$ having nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ for any $\alpha \in GF(2^n)$, we need, $2^{n-1} - 2^{\frac{n-1}{2}} < d(f, h_\alpha) < 2^{n-1} + 2^{\frac{n-1}{2}}$. In particular for $\alpha = 0$, we obtain $2^{n-1} - 2^{\frac{n-1}{2}} < l(2^a-1) < 2^{n-1} + 2^{\frac{n-1}{2}}$ where l is the number of 'all one' columns in the $(\frac{2^{ab}-1}{2^a-1}, 2^a-1)$-interleaved sequence of f and consequently

$$\frac{2^{n-1} - 2^{\frac{n-1}{2}}}{2^a-1} < l < \frac{2^{n-1} + 2^{\frac{n-1}{2}}}{2^a-1}. \tag{3}$$

This is same as the condition (1) of Section 1. Consider $(\frac{2^{ab}-1}{2^a-1}, 2^a-1)$-interleaved sequences of f and h_α. In h_α, out of the $\frac{2^{ab}-1}{2^a-1}$ columns, number of 'all one' columns is $\frac{2^{ab}-1}{2^a-1} - 2^{ab-a}$ and among them $t(\alpha)$ number of 'all one' columns match with the 'all one' columns of f. This is same as saying that $t(\alpha)$ number of 'all zero' columns of l_α match with the 'all one' columns of f. From this we have

$$\begin{aligned} d(f, l_\alpha) &= t(\alpha)(2^a-1) + (l - t(\alpha))(2^{a-1}-1) + (2^{n-1} - l + t(\alpha))2^{a-1} \\ &= 2^{ab-1} + t(\alpha)2^a - l. \end{aligned}$$

Similarly we have $d(f, h_\alpha) = 2^{ab-1} - t(\alpha)2^a + l$. Again it is clear that if f is to have nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ then both $d(f, l_\alpha)$ and $d(f, h_\alpha)$ should be greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ for all $\alpha \in GF(2^n)^*$. Combining this with the bounds obtained above we obtain the following inequality

$$\frac{1}{2^a}\left\{\frac{2^{ab-1} - 2^{(ab-1)/2}}{2^a-1} - 2^{(ab-1)/2}\right\} < t(\alpha) < \frac{1}{2^a}\left\{\frac{2^{ab-1} + 2^{(ab-1)/2}}{2^a-1} + 2^{(ab-1)/2}\right\} \tag{4}$$

which is same as the condition (2) of section 1.

Remark 2 *It is to be noted that any $(\frac{2^{ab}-1}{2^a-1}, 2^a-1)$-interleaved sequence with a fixed binary sequence of length $\frac{2^{ab}-1}{2^a-1}$ as rows correspond to a function in $I_{a,b}$ and conversely. If we construct such an* *interleaved sequence with l non-zero columns satisfying (3) and (4) then by the above discussion the function corresponding to this sequence will have nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}$. However it is usually impossible to search all the possibilities. Because of this reason Patterson and Wiedemann have put extra restriction in the form of invariance with respect to J^* and $\langle \phi_2 \rangle$ and exhaustively searched the more restricted search space for $n = 15$. However the analogous search space even for $n = 21$ becomes too large to search exhaustively. Below we describe their technique in a generalized framework by using interleaved sequence.*

Suppose $\mathcal{K}$ be a proper subgroup of $GF(2^n)^*$ of order k and index d containing $GF(2^t)^*$ where $t|n$. Consider any $f \in \mathcal{F}_n$ which is invariant under the action of $\mathcal{K}$ and $\langle \phi_2 \rangle$. Also let us suppose that all the interleaved sequences considered are with respect to a particular primitive element $\zeta \in GF(2^n)$. The index of $GF(2^t)^*$ in $GF(2^n)^*$ is $d_1 = \frac{2^n-1}{2^t-1}$. Since $kd = 2^n - 1 = d_1(2^t - 1)$ and $(2^t - 1)|k$, $d|d_1$. *Please note that t is a different symbol form $t(\alpha)$.*

Since f is invariant with respect to $\mathcal{K}$ and $\langle \phi_2 \rangle$, by lemma 2 the (d, k)-interleaved sequence of f has a fixed binary sequence of length d as rows and the columns in the same equivalence class of ρ_d are either 'all zero' columns or 'all one' columns. Suppose l columns of the (d, k)-interleaved sequence of f are 'all one' columns. If we consider the $(d_1, 2^t - 1)$-interleaved sequence of f then each column of the (d, k)-interleaved sequence splits up into $\frac{d_1}{d}$ number of columns. Thus the total number of 'all one' columns in the $(d_1, 2^t - 1)$-interleaved sequence is $l\frac{d_1}{d}$. It should be noted that since f is invariant under the action of $\mathcal{K}$ and $\langle \phi_2 \rangle$, it is invariant under any subgroup of the group generated by $\mathcal{K}$ and $\langle \phi_2 \rangle$ in particular the group generated by $GF(2^t)^*$ and $\langle \phi_2 \rangle$. Therefore by lemma 2 the $(d_1, 2^t - 1)$-interleaved sequence of f is repetition of a fixed binary sequence of length d_1 as rows. From the conditions (3) and (4) it is known that the function f has nonlinearity greater than $2^{n-1} - 2^{\frac{(n-1)}{2}}$ if and only if

$$\frac{2^{n-1} - 2^{\frac{n-1}{2}}}{2^t - 1} < l\frac{d_1}{d} < \frac{2^{n-1} + 2^{\frac{n-1}{2}}}{2^t - 1} \tag{5}$$

$$\frac{1}{2^t}\left\{\frac{2^{n-1} - 2^{(n-1)/2}}{2^t - 1} - 2^{(n-1)/2}\right\} < t(\alpha) < \frac{1}{2^t}\left\{\frac{2^{n-1} + 2^{(n-1)/2}}{2^t - 1} + 2^{(n-1)/2}\right\}. \tag{6}$$

In case we are searching for a function with nonlinearity greater than $2^{n-1} - 2^{\frac{(n-1)}{2}}$ in the search space consisting of functions in $\mathcal{F}_n$ which are invariant under the action of $\mathcal{K}$ and $\langle \phi_2 \rangle$, if the condition (5) and (6) are not satisfied for any l then we conclude that there is no such function with such high nonlinearity in the given search space. Condition (5) is easy to check. Below we present a method to convert the condition (6) to a system of linear inequalities.

Definition 3 *Recall that ρ_d is an equivalence relation defined on the column numbers of (d, k)-interleaved sequence of f. Suppose that there are r equivalence classes. Define r distinct binary variables $l_0, l_1, \ldots, l_{r-1}$ such that $l_j = 1$ if the j-th equivalence class consists of 'all one' columns else $l_j = 0$. Let s_j be the size of the j-th equivalence class where $j = 0, \ldots, r - 1$.*

In the (d, k)-interleaved sequence of the function f if the j-th equivalence class has columns with entries $l_j \in \{0, 1\}$ then corresponding to these columns there are $s_j\frac{d_1}{d}$ columns in the $(d_1, 2^t - 1)$-interleaved sequence of f with entries l_j. Let $\mathcal{S}_j$ be the set of column numbers of these columns. Consider the $(d_1, 2^t - 1)$-interleaved sequence of $Tr_1^n(\zeta^i x)$. Let $\mathcal{T}_i$ be the set of column numbers of 'all zero' columns of this interleaved sequence. Let $c_{i,j} = |\mathcal{T}_i \cap \mathcal{S}_j|$. From this we obtain

$$t(\zeta^i) = \sum_{j=0}^{r-1} c_{i,j} l_j.$$

The number $c_{i,j}$ is the number of 'all zero' columns of the $(d_1, 2^t-1)$-interleaved sequence of $Tr_1^n(\zeta^i x)$ having the same column numbers as the columns corresponding to the j-th equivalence class in the $(d_1, 2^t-1)$-interleaved sequence of f. Thus the condition (6) can be written as

$$\frac{1}{2^t}\left\{\frac{2^{n-1}-2^{(n-1)/2}}{2^t-1} - 2^{(n-1)/2}\right\} < \textstyle\sum_{j=0}^{r-1} c_{i,j} l_j < \frac{1}{2^t}\left\{\frac{2^{n-1}+2^{(n-1)/2}}{2^t-1} + 2^{(n-1)/2}\right\}. \qquad (7)$$

for $i = 0, 1, \ldots 2^n - 2$. The number of inequalities in the above system is $2^n - 1$. Below we prove that it is enough to solve r inequalities among them, where r is the number of equivalence classes with respect to ρ_d.

Definition 4 *We define an equivalence relation $\hat{\rho}_d$ on $\{0, 1, 2, \ldots, 2^n - 2\}$ by $i, j \in \{0, 1, 2, \ldots, 2^n - 2\}$ are equivalent if and only if $i \equiv j2^k \bmod d$ for some $k \geq 0$. It is easy to see that the number of equivalence classes with respect to $\hat{\rho}_d$ is same as that of ρ_d.*

Theorem 1 *Let $f \in \mathcal{F}_n$ is invariant under the action of $\mathcal{K}$ and $\langle\phi_2\rangle$. If i and j are in the same equivalence class of $\hat{\rho}_d$, i.e., $j \equiv i2^k \bmod d$ for some $k \geq 0$, then (1) $\hat{f}(\zeta^i) = \hat{f}(\zeta^j)$, (2) $t(\zeta^i) = t(\zeta^j)$.*

Proof : If i and j are in the same equivalence class as defined above then $j \equiv i2^k \bmod d$ for some $0 \leq k \leq n-1$. Walsh transform of a function f is defined as $\hat{f}(\alpha) = \sum_{x \in GF(2^n)} (-1)^{Tr(\alpha x) + f(x)}$, where $\alpha \in GF(2^n)$. As i, j are in the same equivalence class of $\hat{\rho}_d$, $j = i2^k + qd$ for some integer q.

$$\begin{aligned}
\hat{f}(\zeta^j) &= \sum_{x \in GF(2^n)} (-1)^{Tr(\zeta^j x) + f(x)} \\
&= \sum_{x \in GF(2^n)} (-1)^{Tr(\zeta^j \zeta^{-qd} x) + f(\zeta^{-qd} x)} \text{ since } x \mapsto \zeta^{-qd} x \text{ is one-one onto} \\
&= \sum_{x \in GF(2^n)} (-1)^{Tr(\zeta^{i2^k} x) + f(\zeta^{-qd} x)} \\
&= \sum_{x \in GF(2^n)} (-1)^{Tr(\zeta^{i2^k} x) + f(x)} \text{ since } f \text{ is invariant under } \mathcal{K} \\
&= \hat{f}(\zeta^{i2^k}) = \sum_{x \in GF(2^n)} (-1)^{Tr(\zeta^{i2^k} x) + f(x)} \\
&= \sum_{x^{2^k} \in GF(2^n)} (-1)^{Tr(\zeta^{i2^k} x^{2^k}) + f(x^{2^k})} \text{ by replacing } x \text{ by } x^{2^k}, \text{ Frobenius automorphism} \\
&= \sum_{x \in GF(2^n)} (-1)^{Tr(\zeta^{i2^k} x^{2^k}) + f(x^{2^k})} \text{ since } x \to x^{2^k} \text{ is a field automorphism} \\
&= \sum_{x \in GF(2^n)} (-1)^{Tr(\zeta^i x) + f(x)} \text{ since } f(x^{2^k}) = f(x) \text{ and } Tr(\alpha^{2^k}) = Tr(\alpha) \text{ for all } \alpha \in GF(2^n) \\
&= \hat{f}(\zeta^i).
\end{aligned}$$

The $(d_1, 2^t - 1)$-interleaved sequence of $Tr(\zeta^i x)$ has $t(\zeta^i)$ zero columns corresponding to 'all one' columns of the $(d_1, 2^t - 1)$-interleaved sequence of $f(x)$. The total number of zero columns of the $(d_1, 2^t - 1)$-interleaved sequence of $Tr(\zeta^i x)$ is $d_1 - 2^{n-t}$ and the total number of 'all one' columns and 'all zero' columns of the $(d_1, 2^t - 1)$-interleaved sequence of $f(x)$ are l' and $d - l'$ respectively. The number of zero columns of $Tr(\zeta^i x)$ that correspond to 'all one' columns of $f(x)$ is $t(\zeta^i)$. The number of 'all one' columns of $f(x)$ that correspond to nonzero columns of $Tr(\zeta^i x)$ is $l' - t(\zeta^i)$ and the number of zero columns that correspond to the nonzero columns of $Tr(\zeta^i x)$ is $2^{n-t} - (l' - t(\zeta^i))$. Thus the Walsh transform

$$\hat{f}(\zeta^i) = (2^t - 1)t(\zeta^i) + (1)(l' - t(\zeta^i)) + (-1)(2^{n-t} - (l' - t(\zeta^i))).$$

Thus for any i, j if $\hat{f}(\zeta^i) = \hat{f}(\zeta^j)$ then $t(\zeta^i) = t(\zeta^j)$. ■

Remark 3 *Note that it is enough to solve the inequalities involving $t(\zeta^i) = \sum_{j=0}^{r-1} c_{i,j} l_j$, where i varies over a representative system of the equivalence classes of ρ_d. Once these inequalities are satisfied rest of the inequalities are automatically satisfied due to Theorem 1. Therefore we have to solve only r inequalities instead of $2^n - 1$ inequalities. Further, it is clear that the Walsh spectra will contain at most r different values at the nonzero points. Calculating $\hat{f}(\zeta^i)$ at a point ζ^i is enough for the complete equivalence class. This gives that the Walsh spectra may contain at most $1 + r$ values (the additional one is the Walsh transform value at the zero point).*

2.1 The case of $n = 15$

For $n = 15$ the functions invariant under the action of $\mathcal{K} = GF(2^3)^*.GF(2^5)^*$, the direct product of $GF(2^3)^*$ and $GF(2^5)^*$, and $\langle \phi_2 \rangle$ are considered. t is taken to be 5. The order of $\mathcal{K}$ in this case is $(31)(7)$. First we determine the number of equivalence classes with respect to ρ_{151}.

Lemma 4 *In a $(151, (31)(7))$-interleaved sequence there are 11 equivalence classes with respect to ρ_{151}. Among them 10 are of size 15 and 1 is of size 1.*

Proof : Suppose i is a representative of an equivalence class. If $i = 0$ then $i \cdot 2^k = 0$ for all k. Therefore the equivalence class containing $i = 0$ has only one element. Next suppose $i \neq 0$. Then any other member of the the same equivalence class can be written as $i \cdot 2^k$ modulo 151 where $0 \leq k \leq 14$. Thus we can have at most 15 elements in each such equivalence class. We can verify that modulo 151 each number $i \cdot 2^k$ is distinct when $0 \leq i \leq 150$ and $0 \leq k \leq 14$. Therefore each equivalence class for which the representative $i \neq 0$ contains exactly 15 elements. Thus there are exactly 10 such equivalence classes. ■

Remark 4 *From the above lemma, the number of equivalence classes with respect to $\hat{\rho}_{151}$ is 11. Note that $\hat{\rho}_{151}$ is an equivalence relation over $\{0, 1, \ldots, 2^{15} - 2\}$. It partitions the input points $\{\zeta^0, \zeta^1, \ldots, \zeta^{2^{15}-2}\}$ into 1 small class containing 217 elements and 10 large classes each containing 3255 elements. The other input point is the zero point. This counts to total 2^{15} input points which are basically elements of $GF(2^{15})$.*

By lemma 2 the $(151, (31)(7))$-interleaved sequence of of a function whose support is invariant under the action of $\mathcal{K}$ and $\langle \phi_2 \rangle$ must have a fixed binary sequence of length 151 as rows and columns belonging to the same equivalence class of ρ_{151} must have the same value. If a function f in this search space has to have nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ then the number of non-zero columns l in the $(151,(31)(7))$-interleaved sequence of f satisfies (5), where $d = 151$ and $d_1 = (151)(7)$, from which we obtain $74 < l \leq 76$. Thus in order to construct such a function we have to choose 5 among the 10 equivalence classes and we may or may not choose the equivalence class of size one. The columns belonging to these equivalence classes should be set to one while the remaining columns should be set of zero. The resulting $(151,(31)(7))$-interleaved sequence will satisfy the condition (5). Next by taking $t = 5$ we compare the $((151)(7),31)$-interleaved sequence with the $((151)(7),31)$-interleaved sequence of the trace function of the form $Tr_1^n(\zeta^i x)$ where i varies over some representative system of the equivalence classes of ρ_{151}. We obtain the system of inequalities by the algorithm described below.

Algorithm PrepareInequalties

Step 1 Take a primitive polynomial of degree 15 over $GF(2)$. As described in [7], we use the polynomial $x^{15} + x + 1$.

Step 2
- (i) Evaluate the sequence $\{Tr_1^{15}(\zeta^i)\}_{i=0}^{2^{15}-2}$ where ζ is a root of the polynomial $x^{15} + x + 1$.
- (ii) Write this sequence as a $(1057,31)$-interleaved sequence denoted by A. Note that the columns of A are numbered from 0 to 1056.
- (iii) The interleaved sequence A has 33 'all zero' columns. Store the column numbers in an array Z of length 33. The contents of $Z[j]$ are 1, 2, 4, 8, 16, 32, 55, 64, 110, 128, 139, 220, 256, 278, 299, 339, 349, 440, 453, 512, 529, 556, 598, 678, 698, 703, 755, 793, 880, 906, 925, 991, 1024 for $j = 0$ to 32.

Step 3
- (i) Partition the set $\{0,1,2,\ldots,150\}$ into equivalence classes corresponding to ρ_{151}. There are 11 such equivalence classes.
- (ii) Number them from 0 to 10 and store in an array E of length 11 such that $E[j]$ is the smallest integer in the j-th equivalence class where $j = 0,1,\ldots,10$. The contents of $E[j]$ in this case are 0, 1, 3, 5, 7, 11, 15, 17, 23, 35, 37 for $j = 0$ to 10.

Step 4 Construct an array L of length 151 such that $E[L[j]]$ is the representative of the equivalence class of ρ_{151} containing j.

Step 5 Set $i = 0$.

Step 6
- (i) Define an array C of length 11. Put $C[j] = 0$ for all $j = 0,1,\ldots,10$.
- (ii) Define an array K of length 33. Put $K[j] = 0$ for all $j = 0,1,\ldots,32$.

Step 7 For $j = 0,\ldots,32$ do
- (i) $K[j] = (Z[j] - E[i]) \bmod (1057)$
- (ii) $m = K[j] \bmod 151$
- (iii) $C[L[m]] = C[L[m]] + 1$

Step 8
- (i) Out put C. C is the 11-tuple $(c_{i,0}, c_{i,1}, \ldots, c_{i,10})$
- (ii) $i = i + 1$. Go to Step 6 till $i \leq 10$.

In this case, to have nonlinearity $> 2^{15-1} - 2^{\frac{15-1}{2}}$, one needs $13 \leq t(\zeta^i) \leq 20$. Running the Algorithm PrepareInequalties we get the following system of linear inequalities.

$$
\begin{array}{rcl}
13 \leq & 3l_0 + 15l_1 + 0l_2 + 0l_3 + 0l_4 + 0l_5 + 0l_6 + 0l_7 + 0l_8 + 0l_9 + 15l_{10} & \leq 20 \\
13 \leq & 1l_0 + 1l_1 + 2l_2 + 4l_3 + 2l_4 + 2l_5 + 4l_6 + 4l_7 + 6l_8 + 4l_9 + 3l_{10} & \leq 20 \\
13 \leq & 0l_0 + 2l_1 + 4l_2 + 1l_3 + 5l_4 + 3l_5 + 0l_6 + 4l_7 + 4l_8 + 5l_9 + 5l_{10} & \leq 20 \\
13 \leq & 0l_0 + 4l_1 + 1l_2 + 2l_3 + 6l_4 + 4l_5 + 5l_6 + 1l_7 + 5l_8 + 2l_9 + 3l_{10} & \leq 20 \\
13 \leq & 0l_0 + 2l_1 + 5l_2 + 6l_3 + 4l_4 + 2l_5 + 3l_6 + 3l_7 + 3l_8 + 0l_9 + 5l_{10} & \leq 20 \\
13 \leq & 0l_0 + 2l_1 + 3l_2 + 4l_3 + 2l_4 + 4l_5 + 5l_6 + 1l_7 + 1l_8 + 6l_9 + 5l_{10} & \leq 20 \\
13 \leq & 0l_0 + 4l_1 + 0l_2 + 5l_3 + 3l_4 + 5l_5 + 2l_6 + 6l_7 + 2l_8 + 3l_9 + 3l_{10} & \leq 20 \\
13 \leq & 0l_0 + 4l_1 + 4l_2 + 1l_3 + 3l_4 + 1l_5 + 6l_6 + 6l_7 + 2l_8 + 3l_9 + 3l_{10} & \leq 20 \\
13 \leq & 0l_0 + 6l_1 + 4l_2 + 5l_3 + 3l_4 + 1l_5 + 2l_6 + 2l_7 + 4l_8 + 5l_9 + 1l_{10} & \leq 20 \\
13 \leq & 0l_0 + 4l_1 + 5l_2 + 2l_3 + 0l_4 + 6l_5 + 3l_6 + 3l_7 + 5l_8 + 2l_9 + 3l_{10} & \leq 20 \\
13 \leq & 1l_0 + 3l_1 + 5l_2 + 3l_3 + 5l_4 + 5l_5 + 3l_6 + 3l_7 + 1l_8 + 3l_9 + 1l_{10} & \leq 20
\end{array}
$$

The solutions of the system of linear inequalities along with the restrictions provide the functions with nonlinearity greater than $2^{14} - 2^7$. We choose $l_0 = 1$. By observing the first inequality we note that if $l_1 = 0$ then $l_{10} = 1$. Once these two variables are fixed, we have only to search $\binom{8}{4} = 70$ possible cases of the remaining 8 variables, where exactly 4 variables have to be present. We obtained two solutions

$$l_0 = 1, l_1 = 0, l_2 = 0, l_3 = 1, l_4 = 0, l_5 = 1, l_6 = 1, l_7 = 0, l_8 = 1, l_9 = 0, l_{10} = 1 \text{ and}$$
$$l_0 = 1, l_1 = 0, l_2 = 1, l_3 = 1, l_4 = 0, l_5 = 0, l_6 = 0, l_7 = 0, l_8 = 1, l_9 = 1, l_{10} = 1,$$

which provide nonlinearity 16268. We obtain another two solutions by putting $l_1 = 1$ and $l_{10} = 0$. These solutions are

$$l_0 = 1, l_1 = 1, l_2 = 1, l_3 = 0, l_4 = 1, l_5 = 0, l_6 = 0, l_7 = 1, l_8 = 0, l_9 = 1, l_{10} = 0, \text{ and}$$
$$l_0 = 1, l_1 = 1, l_2 = 0, l_3 = 0, l_4 = 1, l_5 = 1, l_6 = 1, l_7 = 1, l_8 = 0, l_9 = 0, l_{10} = 0,$$

which provide the nonlinearity 16276. These two solutions were demonstrated in [7, 8]. Note that if we take the first two solutions (nonlinearity 16268), keep $l_0 = 1$ and complement $l_1, \ldots, l_{10}$, then we get the next two solutions (nonlinearity 16276). This basically implies that if one chooses $l_1 = 0$ and $l_{10} = 1$, then taking $l_0 = 1$ (respectively $l_0 = 0$) will provide nonlinearity 16268 (respectively 16276). Note that l_0 is related to the shorter equivalence class whose representative is the 0 element in the proof of Lemma 4. The nonlinearities of the functions corresponding to each of these solutions are greater than $2^{14} - 2^7$. This analysis provides a justification to the choice of the orbits which could not be clearly explained in [7, Page 356].

Remark 5 *Let us now present some observations regarding the above system of inequalities and its solutions. Consider the first solution namely,*

$$l_0 = 1, l_1 = 0, l_2 = 0, l_3 = 1, l_4 = 0, l_5 = 1, l_6 = 1, l_7 = 0, l_8 = 1, l_9 = 0, l_{10} = 1.$$

l_0 is chosen to be 1 in the beginning. Then l_1 is set to 0 which forces $l_{10} = 1$ by the first inequality. If we write the values of the remaining variables without changing the order as an 8-tuple we obtain

$$(0, 1, 0, 1, 1, 0, 1, 0)$$

which is a palindrome[1]*. Same holds for the other solutions too. If this palindromic symmetry is considered then the search for a solution reduces from $\binom{8}{4} = 70$ to $\binom{4}{2} = 6$ only. We also note that the matrix obtained by removing the first row and the first column from the coefficient matrix of the above system of inequalities is a symmetric one.*

[1] This observation has been pointed out by Prof. R. Balasubramanian of Institute of Mathematical Sciences, Chennai.

Item (1) of Theorem 1 identifies that for distinct i, j belonging to the same equivalence classes described in Lemma 4, $\hat{f}(\zeta^i) = \hat{f}(\zeta^j)$. Since from Lemma 4, we have 11 distinct equivalence classes, there can be at most 11 distinct values at the nonzero points of Walsh spectra. Further, considering the Walsh transform value at the zero point, the number of distinct values could be at most 12. Experimental results show that these 12 Walsh spectra values are indeed not distinct and in fact, there are only four distinct values (as given in the weight distribution table of [7]).

As described in Remark 4, the input points for the 15-variable function can be identified as $0, \zeta^0, \ldots, \zeta^{32766}$. Similarly, the Walsh spectra can be calculated at these points which are defined as $\hat{f}(0), \hat{f}(\zeta^0), \ldots, \hat{f}(\zeta^{32766})$. As we have described earlier, the equivalence relation $\hat{\rho}_{151}$ works on the integer set $\{0, \ldots, 2^{15} - 2\}$ and thus partitions the input points $\zeta^0, \ldots, \zeta^{32766}$ in 11 classes. One of these classes contains 217 elements (we refer this by S, i.e., small in the following table) and the 10 other classes contain 3255 elements each (we refer them by L, i.e., large in the following table). Also there is one more class just having the input point 0 (we refer this by Z). Now we relate the weight distribution given in [7] with this partition.

Weight w	Number of Vectors (number of input points)	Walsh Spectra Value $2^{15} - 2w$	How it comes (the classes)
16492	13021	-216	4 L, 1 Z
16428	217	-88	1 S
16364	3255	40	1 L
16300	16275	168	5 L

Table 1. Walsh spectra distribution for 15-variable PW function.

2.2 The case of $n = 21$

In case $n = 21$ we consider the functions whose $((337)(7), (127)(7))$-interleaved sequences are repetitions of a binary sequence of length $(337)(7)$ as rows. The columns are numbered from 0 to 2358. Among these column numbers we define an equivalence relation as above, i.e., i is equivalent to j if and only if there exists some k between 0 to 20 such that $i \equiv j2^k$ modulo 2359. It can be verified by direct computation that there are 115 equivalence classes corresponding to this equivalence relation. Among these equivalence classes 112 are of size 21, 2 are of size 3 and 1 of size 1. Because of the weight restriction of (3) we have to choose 56 equivalence classes among the 112 equivalence classes, any 1 among the two equivalence classes of size 3 and we may or may not choose the remaining 1 equivalence class. It is possible to construct 115 inequalities by considering the $t(\alpha)$'s involving 115 variables similar to what described in Subsection 2.1. 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.

Next we consider the functions whose $(337, (127)(49))$-interleaved sequences are repetitions of a binary sequence of length 337. It can be checked computationally that the number of equivalence classes with respect to the equivalence relation ρ_{337} is 17. However, it is not possible to choose the equivalence classes in such a way that the weight constraint arising from (5) is satisfied. Hence, there cannot be any function with nonlinearity $> 2^{20} - 2^{10}$ in this search space. However the functions found in this space are interesting in terms of autocorrelation properties and we will discuss that in more details in Subsection 2.4.

2.3 Generalized Nonlinearity

Generalized nonlinearity of a function $f \in \mathcal{F}_n$ is introduced by Gong and Golomb [4] and related results have been presented in [10, 11, 2]. Extended Hadamard Transformation is defined as [10]

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

where $gcd(c, 2^n - 1) = 1$, c is a cyclotomic coset leader modulo $2^n - 1$ and $\lambda \in GF(2^n)$. Using this, generalized nonlinearity can be defined by

$$nlg(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in GF(2^n), gcd(c, 2^{n-1})=1} |\sum_{x \in GF(2^n)} (-1)^{f(x)+Tr(\lambda x^c)}|.$$

In order to compute the generalized nonlinearity for any function $f \in \mathcal{F}_n$ we have to compute the extended Hadamard transformations $\hat{f}(\lambda, c)$ when λ varies over the whole of $GF(2^n)$ and c varies over the set of all cyclotomic coset leaders modulo $2^n - 1$ and coprime to $2^n - 1$. We prove below that this computation can be reduced to a large extent by considering the invariance of the support of the function f as discussed above. For any $d|2^n - 1$ define an equivalence relation over $\{0, 1, 2, \ldots, (2^n - 2)\}$ by i is equivalent to j if and only if $j \equiv i2^k$ modulo d for some $0 \leq k \leq n - 1$ (i.e., the equivalence relation $\hat{\rho}_d$). Recall that if we construct a functions whose (d, k)-interleaved sequence has a fixed binary sequence of length d as rows and if two columns numbers i and j are equivalent then they are either both 'all zero' columns or both all one columns then the support of the resulting function is invariant under the subgroup of order k in $GF(2^n)^*$ and the group of Frobenius automorphisms.

Theorem 2 *If the (d, s)-interleaved sequence of a function $f \in \mathcal{F}_n$ has a fixed binary sequence of size d as its rows and is invariant under the Frobenius automorphisms then the number of distinct elements in the extended Hadamard transformation spectra is less than or equal to $r(r - 1)$ where r is the number of equivalence classes with respect to $\hat{\rho}_d$.*

Proof : Suppose $\alpha \in GF(2^n)$ and $0 \leq k \leq (n - 1)$ and c be coprime to $2^n - 1$. Now,
$\hat{f}(\alpha^{2^k}, c) = \sum_{x \in GF(2^n)} (-1)^{Tr(\alpha^{2^k} x^c)+f(x)} = \sum_{x \in GF(2^n)} (-1)^{Tr(\alpha^{2^k} x^{c2^k})+f(x^{2^k})}$
$= \sum_{x \in GF(2^n)} (-1)^{Tr(\alpha x^c)+f(x)} = \hat{f}(\alpha, c)$.

Thus if i and j are equivalent then $\hat{f}(\zeta^i, c) = \hat{f}(\zeta^{i2^k}, c) = \hat{f}(\zeta^j, c)$. Next suppose c_1 and c_2 are coprime to $2^n - 1$ and c_1 is equivalent to c_2 that is there exists some k such that $c_1 \equiv c_2 2^k \bmod d$. Since both c_1 and c_2 are coprime to $2^n - 1$ there exists d_1 and d_2 such that $c_1 d_1 \equiv 1 \bmod (2^n - 1)$ and $c_2 d_2 \equiv 1 \bmod (2^n - 1)$. The relation $c_1 \equiv c_2 2^k \bmod d$ implies $d_2 \equiv d_1 2^k \bmod d$. Then $\hat{f}(\alpha, c_2)$
$= \sum_{x \in GF(2^n)} (-1)^{Tr(\alpha x^{c_2})+f(x)} = \sum_{x \in GF(2^n)} (-1)^{Tr(\alpha x)+f(x^{d_2})} = \sum_{x \in GF(2^n)} (-1)^{Tr(\alpha x)+f(x^{d_1 2^k + ld})}$.

Note that for any $x = \zeta^i$ where ζ is a primitive $2^n - 1$-th root of unity, we have $f(x^{d_1 2^k + ld}) = f(\zeta^{id_1 2^k + ild}) = f(\zeta^{ild} \zeta^{id_1 2^k}) = f(\zeta^{id_1 2^k}) = f(x^{d_1 2^k})$ since the (d, k)-interleaved sequence of the function has a fixed binary sequence of length d as rows. Therefore, $\hat{f}(\alpha, c_2) =$
$\sum_{x \in GF(2^n)} (-1)^{Tr(\alpha x)+f(x^{d_1 2^k})} = \sum_{x \in GF(2^n)} (-1)^{Tr(\alpha x)+f(x^{d_1})} = \sum_{x \in GF(2^n)} (-1)^{Tr(\alpha x^{c_1})+f(x)} = \hat{f}(\alpha, c_1)$.

Thus if i is equivalent to j then $\hat{f}(\zeta^i, c) = \hat{f}(\zeta^j, c)$ and if c_1 is equivalent to c_2 then $\hat{f}(\zeta^i, c_1) = \hat{f}(\zeta^i, c_2)$. There is no c coprime to $2^n - 1$ in the equivalence class corresponding to 0. Hence the result. ∎

2.3.1 The case $n = 15$

Consider the the number of distinct cyclotomic coset leaders modulo $2^{15}-1$ and coprime to $2^{15}-1$. There are 1800 such distinct integers. Using the idea of Lemma 4, it is clear that these integers (nonzero) will be partitioned into 10 groups. It is interesting to note that we have computationally checked that each equivalence class contains exactly 180 elements, though we are yet to find any specific mathematical justification. Let these cyclotomic coset leaders representing each group be denoted by $\{c_1, c_2, \ldots, c_{10}\}$. Let the representative system for the equivalence classes be denoted by $\{k_0, k_1, \ldots, k_{10}\}$. Thus the extended Hadamard transformation values that we have to compute are $\hat{f}(\zeta^{k_i}, c_j)$ where $0 \le i \le 10$ and $1 \le j \le 10$. There are 1800 cyclotomic coset leaders modulo $2^{15}-1$ and coprime to $2^{15}-1$. Thus the extended Hadamard transformation spectra contains $(32767)(1800) = 58980600$ values. From Theorem 2 and the above discussion it is clear that among these at most $(11)(10) = 110$ values may be distinct for the functions under consideration. This reduces the computational cost of generalized nonlinearity for such functions to a large extent. Note that the generalized nonlinearity of the 15-variable PW functions is 15860 (see also [2]).

2.4 Autocorrelation

Apart from high nonlinearity, low autocorrelation is a desirable property of a Boolean function. The autocorrelation spectra of the PW functions were first investigated in [6] and it has been observed that the PW functions possess very low autocorrelation. The following autocorrelation spectra table has been presented in [6].

Number of input points	3255	6727	9765	3255	3255	6510
Autocorrelation values	160	64	0	-32	-64	-96
How it comes	1 L	2 L, 1 S	3 L	1 L	1 L	2 L

Table 2. Autocorrelation spectra distribution for 15-variable PW function.

The above table also highlights that the number of distinct values in autocorrelation spectra is very less, i.e., only 6. In this section we present some important characteristics of the autocorrelation spectra of PW construction and show that the maximum number of distinct values can be at most the number of equivalence classes with respect to ρ_d. The last row of Table 2 is similar to Table 1 in Section 2.1. We will describe this clearly later in this subsection. First we state the basic definitions.

Definition 5 *Let $f_1, f_2 \in \mathcal{F}_n$. We define $wd(f_1, f_2)$ as*

$$wd(f_1, f_2) = \sum_{x \in GF(2^n)} (-1)^{f_1(x)+f_2(x)}.$$

For any $f \in \mathcal{F}_n$ and $\alpha \in GF(2^n)$ the function $f_{(\alpha)} \in \mathcal{F}_n$ is defined as $f_{(\alpha)}(x) = f(x+\alpha)$.

Let $f \in GF(2^n)$. The autocorrelation, $\Delta_f(\alpha)$ of f with respect to $\alpha \in GF(2^n)$ is defined as

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

The absolute indicator Δ_f is defined as

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

Note that when $\alpha = 0$, $\Delta_f(\alpha) = 2^n$. That is why the value at input point zero is not considered in autocorrelation spectra. Now we present the main theorem related to autocorrelation.

Theorem 3 *Let $f \in \mathcal{F}_n$ be invariant under the action of a cyclic subgroup $\mathcal{K}$ of order k of $GF(2^n)^*$ and $\langle \phi_2 \rangle$. Let $\zeta \in GF(2^n)$ be a primitive element. For any two integers i and j, if $i\ \rho_d\ j$ then*

$$\Delta_f(\zeta^i) = \Delta_f(\zeta^j).$$

Proof : Since $i\ \rho_d\ j$ there exists integers m and s such that $i = 2^s j + md$. Then

$$\begin{aligned}
\Delta_f(\zeta^i) &= \sum_{x \in GF(2^n)} (-1)^{f(x)+f(x+\zeta^i)} \\
&= \sum_{x \in GF(2^n)} (-1)^{f(\zeta^{md}x)+f(\zeta^{md}x+\zeta^{2^s j+md})} \text{ since } x \mapsto \zeta^{md}x \text{ is an one-one, onto map} \\
&= \sum_{x \in GF(2^n)} (-1)^{f(\zeta^{md}x)+f(\zeta^{md}(x+\zeta^{2^s j}))} \\
&= \sum_{x \in GF(2^n)} (-1)^{f(x)+f(x+\zeta^{2^s j})} \text{ since } f \text{ is invariant under the action of } \mathcal{K} \\
&= \sum_{x \in GF(2^n)} (-1)^{f(x^{2^s})+f(x^{2^s}+\zeta^{2^s j})} \text{ since } x \mapsto x^{2^s} \text{ is a one-one, onto map} \\
&= \sum_{x \in GF(2^n)} (-1)^{f(x^{2^s})+f((x+\zeta^{j})^{2^s})} \text{ since } x \mapsto x^{2^s} \text{ is a field automorphism} \\
&= \sum_{x \in GF(2^n)} (-1)^{f(x)+f(x+\zeta^j)} \text{ since } f \text{ is invariant under the action of } \langle \phi_2 \rangle \\
&= \Delta_f(\zeta^j).
\end{aligned}$$

■

Remark 6 *From the Theorem 3 it is evident that if f is invariant under the action $\mathcal{K}$ and $\langle \phi_2 \rangle$ then the distinct autocorrelation values $\Delta_f(\alpha)$ when α varies over $GF(2^n)$ is at most the number of equivalence classes generated by the equivalence relation ρ_d.*

The last row of Table 2 gives how the 10 large (L) classes (of 3255 elements each) and one small (S) class (of 217 elements) are taking part in the autocorrelation spectra. Similar description has also been made for Walsh spectra before Table 1 in Section 2.1.

In [12], it has been conjectured that for balanced functions on odd number of variables n, $\Delta_f \geq 2^{\frac{n+1}{2}}$. This conjecture has been disproved in [6] by suitably modifying the PW functions. It has been shown in [6] that it is possible to construct balanced functions on 15 variables with $\Delta_f = 216 < 256 = 2^{\frac{15+1}{2}}$. In fact later experimentation revealed that it is also possible to get such functions with $\Delta_f = 208$.

However the conjecture has only been disproved for $n = 15$. We here disprove the conjecture of [12] for $n = 21$ too.

In Subsection 2.2 we have considered the functions whose $(337, (127)(49))$-interleaved sequences are repetitions of a binary sequence of length 337. We executed our experiments with the primitive polynomial $x^{21} + x^2 + 1$. It has been checked computationally that the number of equivalence classes with respect to the equivalence relation ρ_{337} is 17 and the representative elements of the equivalence classes are 0, 1, 3, 5, 7, 9, 11, 17, 19, 21, 23, 25, 35, 41, 51, 57, 113. The first equivalence class contains only 1 element and the other 16 classes contain 21 elements each. Note that $1 + 21 \times 16 = 337$.

Let us now consider the construction of a 21 variable function $f \in \mathcal{F}_{21}$ with $f(0) = 0$. The rest of the $2^{21} - 1$ input points $\zeta^0, \ldots, \zeta^{2^{21}-2}$ are divided into 17 classes. The class with representative element 0 contains 127×49 elements and the rest of the classes contain $21 \times 127 \times 49$ elements each. We choose 8 equivalence classes corresponding to the representative elements 11, 17, 23, 25, 35, 41, 51, 113 and put the value 1 in the function output corresponding to the input points of these classes. Rest of the points are assigned to the value zero. This function has weight $8 \times 21 \times 127 \times 49 = 1045464$ and we have checked that the nonlinearity of this function is 1045464 too. Note that from nonlinearity point of view this result is not of much interest since $1045464 < 2^{20} - 2^{10}$. However, the most important thing is to note that $\Delta_f = 920 < 2048 = 2^{\frac{21+1}{2}}$.

Now using the primitive polynomial $x^{21} + x^2 + 1$, it is possible to realize the function f as $f : \{0,1\}^{21} \rightarrow \{0,1\}$ (see [2, Section 2, 5] for more details of this realization). Consider the function f is on the input variables $X_1, \ldots, X_{21}$. Now it can be checked that the weight of the function $g(X_1, \ldots, X_{21}) = f(X_1, \ldots, X_{21}) + X_2 + X_3$ is $2^{20} - 40$, thus 40 away from balancedness. Moreover, since g is a linear transformation of f, $nl(g) = nl(f)$ and $\Delta_g = \Delta_f$ (see [6] for more details). The input points of the function g can be indexed by 0 to $2^{21} - 1$, where the input is the 21 bit binary representation of the integer value. Now we randomly select 40 input points where the function g takes the value 0 and change them to 1 (similar idea that has been used in [6, Algorithm 1, Section III]). Call this new function as $h(X_1, \ldots, X_{21})$. Clearly the weight of the function h is $2^{20} - 40 + 40 = 2^{20}$, i.e., the function h is balanced. We run this experiment many times and found interesting results in terms of autocorrelation. As one example consider 40 such input points of g as the indices 32422, 67033, 82243, 112941, 135033, 175078, 204181, 211252, 245710, 265678, 302766, 338036, 347423, 378814, 415814, 426246, 448514, 495425, 505305, 531185, 564270, 589462, 618096, 655062, 680971, 699797, 713104, 749641, 770943, 804760, 832387, 849856, 870619, 898330, 920904, 951680, 993640, 1010745, 1026031, 1069446. Changing the functional values at these points from 0 to 1 we get h and experimentally checked that $nl(h) = 1045482$ and $\Delta_h = 1024 < 2048 = 2^{\frac{21+1}{2}}$. Since h is balanced, this disproves the conjecture of [12] for $n = 21$.

3 Group Action on $PG(2, 2^a)$

In this section we discuss what is a version of the fundamental theorem of projective geometry. For detailed discussion of this theorem, refer to [5, 9]. We give a short proof of this version which suits our purpose. It is expected that the functions with large nonlinearity would be invariant under certain subgroups of linear transformations and the PW construction supports this viewpoint. An important question arising in this direction is what possible subgroups can replace their group, which consists of linear transformations acting on a projective plane over a larger field. In this regard, we characterize the largest group of linear transformations acting on a projective plane over a larger field.

Recall that $GF(2) = K \subset L \subset M$ is a tower of field extension and assume $[M : L] = 3$. The set $\{xL : x \in M^*\}$ can be considered as $PG(2, 2^a)$ where for any $x \in M^*$, xL is the one dimensional L-subspace of M spanned by x. Let $GL_K(M)$ denotes the group of all invertible K-linear transformations of M. Then $GL_K(M)$ induces an action on the set of all K-subspaces of M.

Let H be the largest subgroup of $GL_K(M)$ which maps $PG(2, 2^a)$ to itself, i.e.,

$$H = \{g \in GL_K(M) : \text{ for any } x \in M^*, g(xL) = yL \text{ for some } y \in M^*\}.$$

Let $GL_L(M)$ be the group of all invertible L-linear transformations of M and $\phi_2 : M \to M$ be defined by $\phi_2(x) = x^2$ for all $x \in M$. Then $GL_L(M)$ is a subgroup of $GL_K(M)$ and $\phi_2 \in GL_K(M)$. Note that for any $g \in H$ if U and V are L-subspaces of M then $g(U \cap V) = g(U) \cap g(V)$ and $g(U + V) = g(U) + g(V)$ and if $x_1, x_2, y_1, y_2 \in M^*$ are such that $g(x_1L) = y_1L$ and $g(x_2L) = y_2L$ then $g(x_1L + x_2L) = y_1L + y_2L$.

Lemma 5 *Assume* $[M : L] \geq 2$. *If* $g \in H$, $x_1, x_2 \in M^*$ *then for any* $c \in L$, $\frac{g(cx_1)}{g(x_1)} = \frac{g(cx_2)}{g(x_2)}$.

Proof : We have two possible cases.
Case 1. Suppose x_1, x_2 are linearly independent over L. Let $y_1 = g(x_1)$ and $y_2 = g(x_2)$. Then $g(x_1L) = y_1L$ as $0 \neq y_1 \in g(x_1L)$ and $g(x_1L)$ is an 1-dimensional L-subspace. Similarly $g(x_2L) = y_2L$. Therefore, $g(cx_1) = \lambda_1 y_1$ and $g(cx_2) = \lambda_2 y_2$ for some $\lambda_1, \lambda_2 \in L$. Since g is additive $g(cx_1 + cx_2) = \lambda_1 y_1 + \lambda_2 y_2$. But $g(cx_1 + cx_2) \in g((x_1 + x_2)L)$ and $g((x_1 + x_2)L) = (y_1 + y_2)L$, since $(y_1 + y_2) \in g((x_1 + x_2)L)$ which is one dimensional. Thus there exists $\lambda_3 \in L$ such that $g(cx_1 + cx_2) = \lambda_3(y_1 + y_2)$.

Note that $g(x_1L + x_2L) = y_1L + y_2L$ and both are $GF(2)$-vector spaces. Comparing their dimensions over $GF(2)$, we see that y_1, y_2 are linearly independent over L, and hence $\lambda_1 = \lambda_2 = \lambda_3$. Therefore $\frac{g(cx_1)}{g(x_1)} = \frac{g(cx_2)}{g(x_2)}$.
Case 2. Suppose x_1, x_2 are linearly dependent over L. There exists $x_3 \in M^*$ such that x_1 and x_3 are linearly independent. Then x_2 and x_3 are also linearly independent. Then from case 1 we obtain

$$\frac{g(cx_1)}{g(x_1)} = \frac{g(cx_3)}{g(x_3)} = \frac{g(cx_2)}{g(x_2)}.$$

■

Definition 6 *Let* $x \in M^*$ *and* $g \in H$. *We define a map* $\phi : L \to L$ *by* $\phi(c) = \frac{g(cx)}{g(x)}$ *for any* $c \in L$.

Remark 7 *From lemma 5 it follows that* ϕ *as defined above does not depend on the choice of* x.

Lemma 6 *The map* ϕ *defined above is a field automorphism of* L.

Proof : Additivity of ϕ is obvious. Let $c_1, c_2 \in L$. Then

$$\phi(c_1c_2) = \frac{g(c_1c_2x)}{g(x)} = \frac{g(c_1c_2x)}{g(c_2x)}\frac{g(c_2x)}{g(x)} = \phi(c_1)\phi(c_2).$$

■

Theorem 4 *Let* $[M : L] = 3$. *As a subgroup of* $GL_K(M)$ *we have* $H = GL_L(M)\langle\phi_2\rangle$, *that is* $H = \{g_1\phi_2^i : g_1 \in GL_L(M)$ *and* $i \in \mathbf{Z}\}$.

Proof : Clearly for any $g_1 \in GL_L(M)$ and $i \in \mathbf{Z}$, $g_1\phi_2^i \in H$. To show the inclusion in the other direction, let $g \in H$. Let $c \in L$ and $x \in M$ then $\phi(c)g(x) = g(cx)$. Extend ϕ to a field automorphism $\hat{\phi}$ of M. Let $g_1 = g\hat{\phi}^{-1}$ then

$$g_1(cx) = g(\hat{\phi}^{-1}(cx)) = g(\phi^{-1}(c)\hat{\phi}^{-1}(x)) = \phi(\phi^{-1}(c))g(\hat{\phi}^{-1}(x)) = cg_1(x).$$

Moreover, the additivity of g_1 is obvious. Hence $g_1 \in GL_L(M)$. Thus $g = g_1\hat{\phi}$; and since $\hat{\phi}$ is a field automorphism of M, $\hat{\phi} = \phi_2^i$ for some $i \in \mathbf{Z}$. This proves that $H = GL_L(M)\langle\phi_2\rangle$. ■

In Section 2, support of the functions in $I_{a,b}$ with maximum reported nonlinearity were obtained by first defining an equivalence relation on the column numbers and then choosing some of the equivalence classes to give the support of such functions. In fact the equivalence classes of Section 2 were orbits under the action of a group generated by a subgroup of $\Phi(M^*)$ and ϕ_2 in $GL_K(M)$. From Theorem 4 it follows the the set of all elements of $GL_K(M)$ that act on the support of functions belonging to $I_{a,b}$ is H.

4 Conclusion

In this paper, we have interpreted the PW construction in terms of interleaved sequence. We have addressed the problem of choosing the orbits so that the constructed function attains high nonlinearity. It has been shown that this problem can be mapped to a problem of solving a system of linear inequalities. We have considered the case for $n = 21$ too and demonstrated the computational difficulty in this case. If some heuristic method of solving the corresponding system of inequalities (involving 115 binary variables) is developed then functions with nonlinearity higher than $2^{20} - 2^{10}$ can be constructed once a solution satisfying the inequalities is achieved. Also we have demonstrated that the computation of autocorrelation and generalized nonlinearity of such functions can be reduced because of the structure of their interleaved sequences. This highlights the utility of using the concept of interleaved sequences in this context. In the PW construction, the supports of the functions constructed are subsets of $PG(2, 2^a)$. The functions are chosen in such a way that their supports are invariant under the action of $[\Phi(L^*.J^*)]\langle\phi_2\rangle$. It is evident that if we want to study some alternative methods of construction then we must know the largest possible subgroup of $GF(2)$-linear transformations that acts on $PG(2, 2^a)$. This is precisely what we have mentioned in Section 3. The investigation of the effect on nonlinearity by replacing the above subgroup by other subgroups of H is a very interesting open question. For instance one can ask if the choice of the orbits which form the supports of functions with high nonlinearity can be characterized in terms of certain subgroup of H. In particular, can one find a subgroup of H such that the support itself becomes an orbit under the action of that subgroup on $PG(2, 2^a)$.

Acknowledgment : The authors like to thank Prof. R. Balasubramaniam of Institute of Mathematical Sciences, Chennai, Dr. P. Sarkar of Indian Statistical Institute, Calcutta and Mr. A. Venkateswarlu of Indian Institute of Technology, Madras for useful discussion and valuable comments during preparation of this draft.

References

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

[2] S. Gangopadhyay and S. Maitra. Further Results related to Generalized Nonlinearity. In *Proceedings of INDOCRYPT 2002*, volume 2551 in Lecture Notes in Computer Science, Pages 260–274, Springer-Verlag, 2002.

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

[4] G. Gong and S. W. Golomb. Transform domain analysis of DES. *IEEE Transactions on Information Theory*, 45(6):2065–2073, September 1999.

[5] D. R. Hughes, F. C. Piper. *Projective Planes.* Springer-Verlag, 1973

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

[7] N. J. Patterson and D. H. Wiedemann. The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. *IEEE Transactions on Information Theory*, IT-29(3):354–356, 1983.

[8] N. J. Patterson and D. H. Wiedemann. Correction to - the covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. *IEEE Transactions on Information Theory*, IT-36(2):443, 1990.

[9] A. Seidenberg. *Lectures in Projective Geometry.* Van Nostrand Reinhold co., New York and Affiliated East West Press, New Delhi, 1969.

[10] A. Youssef and G. Gong. Hyper-bent Functions. In *Advances in Cryptology, Eurocrypt 2001*, Lecture Notes in Computer Science, Number 2045, Pages 406–419, Springer-Verlag, 2001.

[11] A. Youssef and G. Gong. Boolean Functions with Large Distance to all Bijective Monomials: N odd case. In *Selected Areas in Cryptography, SAC 2001*, Lecture Notes in Computer Science, Number 2259, Springer-Verlag, 2001.

[12] X. M. Zhang and Y. Zheng. GAC - the criterion for global avalanche characteristics of cryptographic functions. *Journal of Universal Computer Science*, 1(5):316–333, 1995.