Crosscorrelation Spectra of Dillon and Patterson-Wiedemann type Boolean Functions

Sugata Gangopadhyay and Subhamoy Maitra
Applied Statistics Unit, Indian Statistical Institute
203 B. T. Road, Kolkata 700 108, INDIA
Communicating email : subho@isical.ac.in

Abstract

In this paper we study the additive crosscorrelation spectra between two Boolean functions whose supports are union of certain cosets. These functions on even number of input variables have been introduced by Dillon and we refer to them as Dillon type functions. Our general result shows that the crosscorrelation spectra between any two Dillon type functions are at most 5-valued. As a consequence we find that the crosscorrelation spectra between two Dillon type bent functions on n-variables are at most 3-valued with maximum possible absolute value at the nonzero points being $\leq 2^{\frac{n}{2}+1}$. Moreover, in the same line, the autocorrelation spectra of Dillon type bent functions at different decimations is studied. Further we demonstrate that these results can be used to show the existence of a class of polynomials for which the absolute value of the Weil sum has a sharper upper bound than the Weil bound. Patterson and Wiedemann extended the idea of Dillon for functions on odd number of variables. We study the crosscorrelation spectra between two such functions and then use the results for calculating the autocorrelation spectra too.

Keywords: Boolean Functions, Nonlinearity, Crosscorrelation, Autocorrelation, Character Sums.

1 Introduction

Analysis of crosscorrelation between sequences has received a lot of attention in literature. The crosscorrelation can be multiplicative or additive. Analysis of multiplicative (shift) crosscorrelation has important role in several fields such as digital signal processing, coding and cryptology. Similarly study on additive crosscorrelation (specifically for Boolean functions, that can also be seen as sequences) has immediate effect in design and crtptanalysis of symmetric key cryptosystems. Boolean functions have frequent applications in both stream and block ciphers and different kinds of correlation analysis has found application in this field. Nonlinearity is one of the most important properties of Boolean functions (or vector

valued Boolean functions) for cryptographic applications. For functions on even number of variables n, the maximum nonlinearity is $2^{n-1} - 2^{\frac{n}{2}-1}$ and the most well known (oldest too) construction has been provided by Dillon [4, 5]. Considering the Boolean functions as mappings from $GF(2^n) \to GF(2)$, the Dillon type ones are the functions whose supports are union of cosets of $GF(2^{\frac{n}{2}})^*$ in $GF(2^n)^*$. Under some weight constraints, these Dillon type functions provide maximum nonlinearity to give rise to (Dillon type) bent functions. Though these functions have been introduced almost thirty years ago and there are many other different constructions of bent functions [2], till date these Dillon type functions receive serious attention in literature [22, 1]. When functions on odd number of variables are considered, then also Dillon's strategy comes into play to achieve very high nonlinearity. Patterson and Wiedemann [13, 14] exploited similar idea to obtain functions with nonlinearity strictly greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ for odd number of input variables $n \geq 15$. This result is pioneering as this is the first instance when such a high nonlinearity has been demonstrated and further till date (even after twenty years) there is no other strategy to get such functions. Later in [16, 11] these functions have been changed heuristically to get highly nonlinear balanced functions.

In this paper we systematically analyse the additive crosscorrelation spectra between two Dillon type (respectively Patterson-Wiedemann type) functions for n even (respectively n odd). We first present a technical result to show that the crosscorrelation (from now on crosscorrelation will imply additive crosscorrelation in the rest of the paper) spectra between any two bent functions (may not be Dillon type) are the same as the Walsh spectra of sum of their duals. This result follows directly from the well known relationship between the crosscorrelation spectra between two functions and the Walsh spectra of the respective functions. However, this technique does not suffice to completely characterize the crosscorrelation spectra between any two Dillon type (may not be bent) functions. Thus we need to take a different route using the interleaved sequence of Dillon type functions and show that the crosscorrelation spectra between two Dillon type (may not be bent) functions are at most 5-valued. Roughly speaking, the technique uses counting the points of intersections between the cosets of $\frac{n}{2}$-dimensional subspaces of $GF(2^n)$. Further we show that the crosscorrelation spectra between two Dillon type bent functions is at most 3-valued and the maximum absolute value in the spectra (except the zero point) is $\leq 2^{\frac{n}{2}+1}$. Then we introduce the concept of generalized autocorrelation (autocorrelation spectra at different decimations) and show that it is meaningful for Dillon type bent functions. Unlike all zero values in the autocorrelation spectra of a bent function at nonzero points, we show that the generalized autocorrelation spectra of Dillon type bent functions contain nonzero values. Further our results have consequences to character sum problems for additive characters. We extend our study for odd number of variables and use the inherent symmetry of Patterson-Wiedemann functions to get the crosscorrelation results. Our analysis provides theoretical justification to the fact that the autocorrelation spectra of Patterson-Wiedemann type functions are few valued and the maximum absolute value at the nonzero points of the spectra is very low.

1.1 Preliminaries

Now we introduce some basic definitions and notations. Let $\mathcal{F}_n$ be the set of all Boolean functions on n variables, that is mappings from $GF(2^n)$ to $GF(2)$. For any subfield $GF(2^t)$ of $GF(2^n)$ define the trace map $Tr_t^n : GF(2^n) \longrightarrow GF(2^t)$ by $Tr_t^n(x) = x + x^{2^t} + x^{2^{2t}} + \ldots + x^{2^{(\frac{n}{t}-1)t}}$. It is known that $GF(2^t)$ is a subfield of $GF(2^n)$ if and only if $t|n$. In particular when $t = 1$ we obtain the map Tr_1^n from $GF(2^n)$ to $GF(2)$ defined by $Tr_t^n(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{(n-1)}}$. Any linear function in $\mathcal{F}_n$ can be written as $Tr_1^n(\lambda x)$ for some $\lambda \in GF(2^n)$ and consequently any affine function can be written as $Tr_1^n(\lambda x) + \epsilon$ where $\epsilon \in GF(2)$.

The nonlinearity of a function $f \in \mathcal{F}_n$, denoted by $nl(f)$ is the distance of this function from the set of all affine functions. The Walsh Hadamard transform of f at $\lambda \in GF(2^n)$ is defined by $W_f(\lambda) = \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(\lambda x)+f(x)}$. By using the definition of Walsh Hadamard transform we get the following expression of nonlinearity of f, $nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in GF(2^n)} |w_f(\lambda)|$. When $n = 2r$, for some positive integer r, that is n is an even positive integer [15], the maximum possible nonlinearity of functions in $\mathcal{F}_n$ is $2^{n-1} - 2^{\frac{n}{2}-1}$. A function in $\mathcal{F}_n$ is called bent if and only if it's nonlinearity is $2^{n-1} - 2^{\frac{n}{2}-1}$, equivalently if and only if $W_f(\lambda) = \pm 2^{\frac{n}{2}}$.

Define additive crosscorrelation between $f, g \in \mathcal{F}_n$ at α by

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

In case $f = g$ then the additive crosscorrelation $C_{f,f}(\alpha)$ is called the autocorrelation of f at α and denoted by $\Delta_f(\alpha)$. An alternate characterization [15] of bent functions states that a function $f \in \mathcal{F}_n$ is bent if and only if $\Delta_f(\alpha) = 0$ for all nonzero $\alpha \in GF(2^n)$. It is well known (see for reference [17]) that for $\omega \in \{0,1\}^n$,

$$C_{f,g}(\omega) = 2^{-n} \sum_{x \in \{0,1\}^n} W_f(x) W_g(x) (-1)^{<\omega,x>},$$

where $< \omega, x >$ denotes the inner product. Note that we will also use the result that for $\omega \in GF(2^n)$, $C_{f,g}(\omega) = 2^{-n} \sum_{x \in GF(2^n)} W_f(x) W_g(x) (-1)^{Tr_1^n(\omega x)}$. It is clear that evaluation in the second case is different from the first case when evaluation is done at a single point. However, when we consider the complete crosscorrelation spectra, then the multiset of values will be the same. Thus we use both the relations as and when required.

We will be using the concept of interleaved sequence [7, 22] extensively in this document. 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. 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.

Definition 1 *Suppose m is a composite number such that $m = d \cdot k$ 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*

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

For detailed discussion on interleaved sequence we refer to [7]. Let $2^n - 1 = d \cdot k$, $\mathbf{a}_{d,k}$ 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 (d,k)-interleaved sequence corresponding to f with respect to ζ and denoted by $S_{(d,k)}(f(x), \zeta)$. 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.

2 Crosscorrelation Results

In this section we first start with some technical results on crosscorrelation of bent functions. The following result heavily depends on the duality property of bent functions. For more details of a bent function and its dual, see [15, 2].

Theorem 1 *Let f and g be n-variable bent functions and $\hat{f}, \hat{g}$ be their dual functions respectively. Then $C_{f,g}(\omega) = W_{\hat{f}(x)+\hat{g}(x)}(\omega)$, for $\omega \in \{0,1\}^n$. Further if $\hat{f}(x) + \hat{g}(x)$ is bent then $C_{f,g}(\omega) = \pm 2^{\frac{n}{2}}$, for all $\omega \in \{0,1\}^n$.*

Proof : From [17], we have the result $C_{f,g}(\omega) = 2^{-n} \sum_{x \in \{0,1\}^n} W_f(x) W_g(x) (-1)^{<\omega, x>}$. If both the functions f, g are bent then $W_f(x), W_g(x)$ can only take the values $\pm 2^{\frac{n}{2}}$ for all x. Hence,

$$C_{f,g}(\omega) = \sum_{x \in \{0,1\}^n} sgn(W_f(x) W_g(x)) (-1)^{<\omega, x>}.$$

From duality results of bent functions, $sgn(W_f(x) W_g(x)) = (-1)^{\hat{f}(x)+\hat{g}(x)}$. This gives,

$$C_{f,g}(\omega) = \sum_{x \in \{0,1\}^n} (-1)^{(\hat{f}(x)+\hat{g}(x))+<\omega, x>} = W_{\hat{f}(x)+\hat{g}(x)}(\omega).$$

If $\hat{f}(x) + \hat{g}(x)$ is bent then $W_{\hat{f}(x)+\hat{g}(x)}(\omega)$ is $\pm 2^{\frac{n}{2}}$ for all $\omega \in \{0,1\}^n$. Thus, $C_{f,g}(\omega) = \pm 2^{\frac{n}{2}}$, for all $\omega \in \{0,1\}^n$. ■

Corollary 1 *For n-variable bent functions f and g, $\sum_{\omega \in \{0,1\}^n} C^2_{f,g}(\omega) = 2^{2n}$.*

Proof : From Parseval's relation [3], for any n-variable Boolean function Φ,

$$\sum_{\omega \in \{0,1\}^n} W^2_{\Phi}(\omega) = 2^{2n}.$$

Thus the result follows from Theorem 1. ■

It is interesting to analyse the value of $\max_{\omega \in \{0,1\}^n, \omega \neq 0} |C_{f,g}(\omega)|$ and the following result shows that improper choice of two bent functions may provide this value as high as 2^n. For the proof we use the Maiorana-McFarland class of bent functions [4] which we briefly describe now. Consider n-variable Boolean functions on $x = (z, y)$, where $z, y \in \{0,1\}^{\frac{n}{2}}$ of the form $\psi(z, y) = z \cdot \pi(y) + g(y)$ where π is a permutation on $\{0,1\}^{\frac{n}{2}}$ and g is any Boolean function on $\frac{n}{2}$ variables.

Proposition 1 *It is possible to construct two n-variable bent functions f, g such that $C_{f,g}(\omega) = 2^n$ for some nonzero ω.*

Proof : Consider two Maiorana-McFarland type bent functions ψ_1, ψ_2 as follows. For both the functions $\pi(y) = y$. For the function ψ_1, $g(y)$ is zero for all y. For the function ψ_2, $g(y)$ is zero when $y_{\frac{n}{2}} = 0$, and $g(y) = 1$ when $y_{\frac{n}{2}} = 1$. Let f, g be bent functions such that $\hat{f} = \psi_1$ and $\hat{g} = \psi_2$. Then $\hat{f} + \hat{g} = 0$ when $x_n = 0$ and $\hat{f} + \hat{g} = 1$ when $x_n = 1$. In fact, $\hat{f} + \hat{g}$ is the linear function x_n. Note that $W_{\hat{f}+\hat{g}}(\omega) = 2^n$, when $\omega = (0, \ldots, 0, 1)$, which gives, $C_{f,g}(\omega) = 2^n$ for some nonzero ω. ■

Natural question in this context is, whether there is any class of bent functions such that the crosscorrelation spectra between any two of them is much better than that presented in Proposition 1. In this direction, we show that if we choose any two Dillon type bent functions then at each point except 0 the maximum absolute value of the additive crosscorrelation is $\leq 2^{\frac{n}{2}+1}$. In fact our analysis demonstrates all the possible values of the additive crosscorrelation spectra between any two Dillon type functions (may not be bent) in Theorem 2 (Subsection 2.1). Results concerning Dillon type bent functions are presented in Corollary 3 (Subsection 2.1).

2.1 Results for Dillon type functions

In this section we concentrate on the crosscorrelation spectra for Dillon type functions. We always consider the functions with $f(0) = 0$. Let us first define the Dillon type functions for even n.

Definition 2 *Suppose n is an even positive integer, i.e., $n = 2r$ for some positive integer r. A function $f \in \mathcal{F}_n$ is called Dillon type function if its $(2^r + 1, 2^r - 1)$-interleaved sequence with respect to a (basically this is true for 'any' primitive element ζ that will be clearer with Proposition 2 and Corollary 2 below) primitive element ζ, consists of all zero and all one columns only and $f(0) = 0$.*

We shall refer to the interleaved sequence $S_{(2^r+1,2^r-1)}(f(x),\zeta)$ by $S(f(x))$ for brevity in this section if not mentioned otherwise. For any two nonnegative integers a and q by $a\%q \in \{0,1,\ldots,q-1\}$ denote the remainder of a when divided by q.

Proposition 2 *A function $f \in \mathcal{F}_n$, where $n = 2r$, is Dillon type with respect to a primitive element ζ if and only if $f(x^c)$ is also Dillon type with respect to the same primitive element for any c coprime to $2^n - 1$.*

Proof : Assume that $f(0) = 0$. Now,

$$\sum_{x\in GF(2^n)} (-1)^{f(x)} = 1 + \sum_{i=0}^{2^n-2} (-1)^{f(\zeta^i)} = 1 + \sum_{i=0}^{2^n-2} (-1)^{f(\zeta^{ci})} = \sum_{x\in GF(2^n)} (-1)^{f(x^c)},$$

where c is coprime to $2^n - 1$ that is the $gcd(c, 2^n - 1) = 1$. Thus the weights of $f(x)$ and $f(x^c)$ are same.

Suppose $f(x)$ is a Dillon type function and therefore $S(f(x))$ consists of only all zero and all one columns. If possible let the i-th column of $S(f(x^c))$ is neither all zero nor all one, i.e., $\sum_{\lambda=0}^{2^r-2}(-1)^{f(\zeta^{ci+c\lambda(2^r+1)})} \neq \pm(2^r-1)$. Since $gcd(c, 2^n - 1) = 1$ implies $gcd(c, 2^r - 1) = 1$ the mapping $\lambda \mapsto (c\lambda)\%(2^r - 1)$ is a permutation on the set $\{0, 1, \ldots, 2^r - 2\}$. Thus we can rewrite the above sum as $\sum_{\lambda=0}^{2^r-2}(-1)^{f(\zeta^{ci+\lambda(2^r+1)})} \neq \pm(2^r-1)$. That is in the interleaved sequence $S(f(x))$, the $(ci)\%(2^r + 1)$-th column is neither all zero nor all one. This is a contradiction. The other direction is similar. Hence the proof. ∎

Corollary 2 *If $f(x)$ is Dillon type with respect to a primitive element then it is also Dillon type with respect to any other primitive element.*

Proof : Suppose ζ and ζ_1 are two distinct primitive elements of $GF(2^n)$. Then there exists a positive integer coprime to $2^n - 1$ such that $\zeta_1 = \zeta^c$. Thus, $S_{(2^r+1,2^r-1)}(f(x), \zeta^c) = S_{(2^r+1,2^r-1)}(f(x^c), \zeta)$, and the proof follows from Proposition 2. ∎

Next we define Dillon type bent functions [4, 5].

Definition 3 *Suppose n is an even positive integer, i.e., $n = 2r$ for some positive integer r. A Dillon type function $f \in \mathcal{F}_n$ is called a Dillon type bent function if $S(f(x))$ contains 2^{r-1} all one columns.*

Suppose ζ is a primitive element of $GF(2^n)$ and $t|n$. Denote $\frac{2^n-1}{2^t-1}$ by d. Define

$$V_i(\zeta, t) = \{0, \zeta^i, \zeta^{i+d}, \ldots, \zeta^{i+(2^t-2)d}\}$$

where $i = 0, 1, \ldots, d - 1$. In the context of Dillon type functions we shall always assume $n = 2r$ and denote $V_i(\zeta, r)$ by V_i (assuming that a primitive element ζ is already fixed). For each i, $V_i(\zeta, t)$ is a t-dimensional subspace of $GF(2^n)$. Moreover for $i = 0$ and for any primitive element ζ of $GF(2^n)$, $V_0(\zeta, t)$ is the subfield $GF(2^t)$ of $GF(2^n)$. For any two Boolean functions $f, g \in \mathcal{F}_n$, for any $\alpha \in GF(2^n)$ and any subset $V \subseteq GF(2^n)$ we denote the sum $\sum_{x\in V}(-1)^{f(x+\alpha)+g(x)}$ by $[C_{f,g}(\alpha)]_V$.

Suppose $f, g \in \mathcal{F}_n$ are two Dillon type functions. We observe that for any $\alpha \in V_i$ the sequence

$$\{f(\alpha+0), f(\alpha+\zeta^i), f(\alpha+\zeta^{i+(2^r+1)}), \ldots, f(\alpha+\zeta^{i+(2^r-2)(2^r+1)})\}$$

is a permutation of the sequence

$$\{f(0), f(\zeta^i), f(\zeta^{i+(2^r+1)}), \ldots, f(\zeta^{i+(2^r-2)(2^r+1)})\}.$$

Since $f(x)$ and $g(x)$ being Dillon type functions are either all zero or all one over $V_i \setminus \{0\}$, the weight of the function $f(x+\alpha)+g(x)$ when restricted to V_i can be computed easily, in the case $\alpha \in V_i$. The case $\alpha \notin V_i$ is described in the following lemma.

Lemma 1 *If $f \in \mathcal{F}_n$ is a Dillon type function, $i \neq j$, then for any $\alpha \notin V_i$ we have $|(\alpha+V_i) \cap V_j| = 1$.*

Proof : Suppose $\alpha \notin V_i$ for some $i \in \{0, 1, \ldots, 2^r\}$. If $x+\alpha \in V_i$ for some $x \in V_i$ then since V_i is a subspace of $GF(2^n)$ the element $\alpha \in V_i$ which is a contradiction. Suppose for two distinct elements $x_1, x_2 \in V_i$ the elements $x_1+\alpha, x_2+\alpha \in V_j$ for some $j \neq i$. Since V_j is a subspace of $GF(2^n)$, $x_1+\alpha+x_2+\alpha = x_1+x_2 \in V_j$, further $x_1+x_2 \in V_i$. Therefore $x_1+x_2 = 0$ since $V_i \cap V_j = \{0\}$. This implies $x_1 = x_2$, since the fields under consideration are of characteristic 2, which contradicts the assumption that $x_1 \neq x_2$.

Thus the coset $\alpha+V_i$ intersects each V_j if $j \neq i$ in atmost one point and has no intersection with V_i. The total number of V_j's when $i \neq j$ is 2^r. There are 2^r number of distinct points in $\alpha+V_i$. This proves that $|(\alpha+V_i) \cap V_j| = 1$. ∎

For any Dillon type function $f \in \mathcal{F}_n$ define,

$$H_0^f = \{V_i | f(x) = 0 \text{ for all } x \in V_i\}$$

and

$$H_1^f = \{V_i | f(x) = 1 \text{ for all } x \in V_i \setminus \{0\}\}.$$

Given any two Dillon type functions $f, g \in \mathcal{F}_n$ the value of the sum $[C_{f,g}(\alpha)]_{V_i}$ depends on whether α is in V_i or not and the values of $\mu, \nu \in \{0,1\}$ for which $V_i \in H_\mu^f \cap H_\nu^g$. In the following two lemmas we explore all the possibilities.

Lemma 2 *If $\alpha \in V_i \in H_\mu^f \cap H_\nu^g$, where $\mu, \nu \in \{0,1\}$ then $[C_{f,g}(\alpha)]_{V_i} = (-1)^{\mu+\nu}2^r + 2(\mu+\nu) - 8\mu\nu$.*

Proof : Since $\alpha \in V_i$ we have $x+\alpha \in V_i$ for all $x \in V_i$.

If $V_i \in H_0^f$ then $f(x+\alpha) = 0$ for all $x \in V_i$. Note that $H_0^f = (H_0^f \cap H_0^g) \cup (H_0^f \cap H_1^g)$. If $V_i \in (H_0^f \cap H_0^g)$ then $[C_{f,g}(\alpha)]_{V_i} = 2^r$ and if $V_i \in (H_0^f \cap H_1^g)$ then $[C_{f,g}(\alpha)]_{V_i} = -2^r + 2$.

If $V_i \in H_1^f$ then $f(x+\alpha) = 1$ for all $x \in V_i$ except at $x = \alpha$. At $x = \alpha$, the value of the function is $f(\alpha+\alpha) = f(0) = 0$. In this case $[C_{f,g}(\alpha)]_{V_i} = -2^r + 2$ or $2^r - 4$ according as $V_i \in H_1^f \cap H_0^g$ or $V_i \in H_1^f \cap H_1^g$ respectively.

The above result can be expressed using a single formula:

$$[C_{f,g}(\alpha)]_{V_i} = (-1)^{\mu+\nu}2^r + 2(\mu+\nu) - 8\mu\nu,$$

where $V_i \in H_\mu^f \cap H_\nu^g$ and $\mu, \nu \in \{0,1\}$. ■

In order to write the expression for $C_{f,g}(\alpha)$ in a compact way we introduce the symbol $\epsilon_{\mu,\nu}^\alpha$ for any $\mu, \nu \in \{0,1\}$ and $\alpha \in GF(2^n)^*$. Any $\alpha \in GF(2^n)^*$ belongs to V_k for some $k \in \{0, 1, \ldots, 2^r\}$. The set V_k must be contained in exactly one of the disjoint sets $H_0^f \cap H_0^g$, $H_0^f \cap H_1^g$, $H_1^f \cap H_0^g$ and $H_1^f \cap H_1^g$. Suppose $V_k \in H_\mu^f \cap H_\nu^g$ where $\mu, \nu \in \{0,1\}$. Then the value of $\epsilon_{\mu,\nu}^\alpha = 1$ and the values of $\epsilon_{a,b}^\alpha = 0$ if $a \neq \mu$ or $b \neq \nu$.

Lemma 3 *If $\alpha \notin V_i \in H_a^f \cap H_b^g$ and $f, g \in \mathcal{F}_n$ be two Dillon type functions such that $S(f(x))$ has l all one columns then*

$$[C_{f,g}(\alpha)]_{V_i} = ((-1)^b(2^r - 2l) + 2(a+b-2ab))(\epsilon_{0,0}^\alpha + \epsilon_{0,1}^\alpha) + (-1)^b(2^r - 2l + 2(a+b))(\epsilon_{1,0}^\alpha + \epsilon_{1,1}^\alpha).$$

Proof : $\alpha \notin V_i$. Suppose $\alpha \in V_k$ for some fixed $k \neq i$. By lemma 1, the coset $\alpha + V_i$ intersects each V_j if $j \neq i$ at exactly one point and has no intersection with V_i.

If $V_k \in H_0^f$ then if $V_i \in H_0^f$, the function $f(x+\alpha) = 0$ at $x = 0$ and $|\{x \in V_i | f(x+\alpha) = 1, x \neq 0\}| = l$, $|\{x \in V_i | f(x+\alpha) = 0, x \neq 0\}| = 2^r - l - 1$. If $V_i \in H_0^f \cap H_0^g$ then $[C_{f,g}(\alpha)]_{V_i} = 2^r - 2l$. If $V_i \in H_0^f \cap H_1^g$ then $[C_{f,g}(\alpha)]_{V_i} = -2^r + 2l + 2$.

If $V_i \in H_1^f$, the function $f(x+\alpha) = 0$ at $x = 0$ and $|\{x \in V_i | f(x+\alpha) = 1, x \neq 0\}| = l-1$, $|\{x \in V_i | f(x+\alpha) = 0, x \neq 0\}| = 2^r - l$. If $V_i \in H_1^f \cap H_0^g$ then $[C_{f,g}(\alpha)]_{V_i} = 2^r - 2l + 2$. If $V_i \in H_1^f \cap H_1^g$ then $[C_{f,g}(\alpha)]_{V_i} = -2^r + 2l$.

Combining we write that if $\alpha \in V_k \in H_0^f$ then $[C_{f,g}(\alpha)]_{V_i} = (-1)^b(2^r - 2l) + 2(a+b-2ab)$ where $V_i \in H_a^f \cap H_b^g$.

If $V_k \in H_1^f$ then if $V_i \in H_0^f$, the function $f(x+\alpha) = 1$ at $x = 0$ and $|\{x \in V_i | f(x+\alpha) = 1, x \neq 0\}| = l - 1$, $|\{x \in V_i | f(x+\alpha) = 0, x \neq 0\}| = 2^r - l$. If $V_i \in H_0^f \cap H_0^g$ then $[C_{f,g}(\alpha)]_{V_i} = 2^r - 2l$. If $V_i \in H_0^f \cap H_1^g$ then $[C_{f,g}(\alpha)]_{V_i} = -2^r + 2l - 2$.

If $V_i \in H_1^f$, the function $f(x+\alpha) = 1$ at $x = 0$ and $|\{x \in V_i | f(x+\alpha) = 1, x \neq 0\}| = l-2$, $|\{x \in V_i | f(x+\alpha) = 0, x \neq 0\}| = 2^r - l + 1$. If $V_i \in H_1^f \cap H_0^g$ then $[C_{f,g}(\alpha)]_{V_i} = 2^r - 2l + 2$. If $V_i \in H_1^f \cap H_1^g$ then $[C_{f,g}(\alpha)]_{V_i} = -2^r + 2l - 4$.

Combining we write that if $\alpha \in V_k \in H_0^f$ then $[C_{f,g}(\alpha)]_{V_i} = (-1)^b(2^r - 2l + 2(a+b))$ where $V_i \in H_a^f \cap H_b^g$.

Combining all these expressions together and noting that when $V_k \in H_0^f$ then $\epsilon_{0,0}^\alpha + \epsilon_{0,1}^\alpha = 1$, $\epsilon_{1,0}^\alpha + \epsilon_{1,1}^\alpha = 0$ and when $V_k \in H_1^f$ then $\epsilon_{0,0}^\alpha + \epsilon_{0,1}^\alpha = 0$, $\epsilon_{1,0}^\alpha + \epsilon_{1,1}^\alpha = 1$ we derive the expression for $[C_{f,g}(\alpha)]_{V_i}$ when $\alpha \notin V_i$. ■

Finally we are in a position to prove the main theorem of this section.

Theorem 2 *Consider two Dillon type functions $f, g \in \mathcal{F}_n$, where $n = 2r$. Then the additive crosscorrelation spectra between f and g can be at most 5-valued. In particular at any nonzero point $\alpha \in GF(2^n)$, $C_{f,g}(\alpha)$ takes one of the following values:*

$$2l + 2s - 4w + (2^r - 2s)(2^r - 2l), \quad -2^{r+1} + 2l + 2s - 4w + (2^r - 2l)(2^r - 2s + 2),$$
$$-4w - 2s + 2l + (2^r - 2s)(2^r - 2l), \quad 2^{r+1} + 2l - 4w - 2s + (2^r - 2l)(2^r + 2 - 2s).$$

Here l, s are the number of all one columns in $S(f(x))$ and $S(g(x))$ respectively and w is the number of all one columns of $S(f(x))$ that gets added to all one columns of $S(g(x))$ in $S(f(x)) + S(g(x))$ (the addition is element wise mod 2). Further $C_{f,g}(0) = 2^n - 2(l + s - 2w)(2^{\frac{n}{2}} - 1)$.

Proof : For the Dillon type functions $f, g \in \mathcal{F}_n$, comparing the interleaved sequences $S(f(x))$ and $S(g(x))$ we obtain: $|H_0^f \cap H_0^g| = 2^r + w + 1 - s - l = w_{0,0}$, $|H_0^f \cap H_1^g| = s - w = w_{0,1}$, $|H_1^f \cap H_0^g| = l - w = w_{1,0}$, $|H_1^f \cap H_1^g| = w = w_{1,1}$. Let $\alpha \in V_k$ and $V_k \in H_\mu \cap H_\nu$. By lemmas 2, 3.

1. If $V_k \in H_\mu^f \cap H_\nu^g$ then $[C_{f,g}(\alpha)]_{V_k} = (-1)^{\mu+\nu} 2^r + 2(\mu + \nu) - 8\mu\nu$.
2. If $V_i \in H_a^f \cap H_b^g$ then

$$\begin{aligned}[C_{f,g}(\alpha)]_{V_i} &= ((-1)^b(2^r - 2l) + 2(a + b - 2ab))(\epsilon_{0,0}^\alpha + \epsilon_{0,1}^\alpha) \\ &\quad +(-1)^b(2^r - 2l + 2(a + b))(\epsilon_{1,0}^\alpha + \epsilon_{1,1}^\alpha).\end{aligned}$$

The crosscorrelation of f, g at α is given by

$$\begin{aligned}C_{f,g}(\alpha) &= \sum_{x \in GF(2^n)} (-1)^{f(x+\alpha)+g(x)} = (-2^r)(-1)^{f(\alpha)+g(0)} + \sum_{i=0}^{2^r} [C_{f,g}(\alpha)]_{V_i} \\ &= (-2^r)(-1)^{f(\alpha)+g(0)} + [C_{f,g}(\alpha)]_{V_k} + \sum_{a=0}^{1}\sum_{b=0}^{1} \sum_{V_i \in H_a^f \cap H_b^g, i \neq k} [C_{f,g}(\alpha)]_{V_i} \\ &= (-2^r)(-1)^{f(\alpha)+g(0)} + ((-1)^{\mu+\nu} 2^r + 2(\mu + \nu) - 8\mu\nu) \\ &\quad + \sum_{a=0}^{1}\sum_{b=0}^{1} (w_{a,b} - \epsilon_{a,b}^\alpha)(((-1)^b(2^r - 2l) + 2(a + b - 2ab))(\epsilon_{0,0}^\alpha + \epsilon_{0,1}^\alpha) \\ &\quad +(-1)^b(2^r - 2l + 2(a + b))(\epsilon_{1,0}^\alpha + \epsilon_{1,1}^\alpha)).\end{aligned}$$

Since the set V_k is contained in one of the disjoint sets $H_0^f \cap H_0^g$, $H_0^f \cap H_1^g$, $H_1^f \cap H_0^g$, $H_1^f \cap H_1^g$, all the possible values of (μ, ν) are $(0,0)$, $(0,1)$, $(1,0)$ and $(1,1)$.

By putting all possible values of (μ, ν) that is $(0,0)$, $(0,1)$, $(1,0)$ and $(1,1)$ we obtain the four crosscorrelation values given above. Details of the calculation is given below.

Case 1. If $\mu = 0$, $\nu = 0$ then $\epsilon_{00}^\alpha = 1$, $\epsilon_{01}^\alpha = 0$, $\epsilon_{10}^\alpha = 0$, $\epsilon_{11}^\alpha = 0$. Therefore crosscorrelation value is:

$$-2^r + 2^r + w(-2^r + 2l) + (l - w)(2^r - 2l + 2) + (s - w)(-2^r + 2l + 2) + (2^r + w - s - l)(2^r - 2l)$$

$$= 2l + 2s - 4w + (2^r - 2s)(2^r - 2l).$$

In the particular case $l = s = 2^{r-1}$ the crosscorrelation value is $2^{r+1} - 4w$.

Case 2. If $\mu = 0$, $\nu = 1$ then $\epsilon_{00}^\alpha = 0$, $\epsilon_{01}^\alpha = 1$, $\epsilon_{10}^\alpha = 0$, $\epsilon_{11}^\alpha = 0$. Therefore the crosscorrelation value is:

$$-2^r - 2^r + 2 + w(-2^r + 2l) + (l - w)(2^r - 2l + 2) + (s - w - 1)(-2^r + 2l + 2)$$

$$+(2^r+1+w-s-l)(2^r-2l) = -2^{r+1}+2l+2s-4w+(2^r-2l)(2^r-2s+2).$$

In the particular case $l = s = 2^{r-1}$ the crosscorrelation value is $-4w$.

Case 3. If $\mu = 1$, $\nu = 0$ then then $\epsilon_{00}^{\alpha} = 0$, $\epsilon_{01}^{\alpha} = 0$, $\epsilon_{10}^{\alpha} = 1$, $\epsilon_{11}^{\alpha} = 0$. Therefore the crosscorrelation values are:

$$(2^r)+(-2^r+2)+(w)(-2^r+2l-4)+(l-w-1)(2^r-2l+2)+(s-w)(-2^r+2l-2)$$

$$+(2^r+1+w-s-l)(2^r-2l) = -4w-2s+2l+(2^r-2s)(2^r-2l)$$

In the particular case $l = s = 2^{r-1}$ the crosscorrelation value is $-4w$.

Case 4. If $\mu = 1$, $\nu = 1$ then $\epsilon_{00}^{\alpha} = 0$, $\epsilon_{01}^{\alpha} = 0$, $\epsilon_{10}^{\alpha} = 0$, $\epsilon_{11}^{\alpha} = 1$. Therefore the crosscorrelation value is:

$$(2^r)+(2^r-4)+(w-1)(-2^r+2l-4)+(l-w)(2^r-2l+2)+(s-w)(-2^r+2l-2)$$

$$+(2^r+1+w-s-l)(2^r-2l) = 2^{r+1}+2l-4w-2s+(2^r-2l)(2^r+2-2s).$$

In the particular case $l = s = 2^{r-1}$ the crosscorrelation value is $2^{r+1}-4w$.

Note that $C_{f,g}(0) = \sum_{x\in GF(2^n)}(-1)^{f(x)+g(x)}$, which is $2^n - 2wt(f(x)+g(x)))$ and the further calculation is routine. ■

Corollary 3 *If $f, g \in \mathcal{F}_n$ and both are Dillon type bent then the crosscorrelation spectra between f, g can be at most 3-valued. In particular, $C_{f,g}(\alpha)$ at any nonzero $\alpha \in GF(2^n)$ can have only two values $2^{\frac{n}{2}+1}-4w$ or $-4w$, where w has the usual meaning as in Theorem 2 and the maximum absolute value is $\leq 2^{\frac{n}{2}+1}$. Further $C_{f,g}(0) = 2^n - 2(2^{\frac{n}{2}}-2w)(2^{\frac{n}{2}}-1)$.*

Proof : We recall that any function $f \in \mathcal{F}_n$ is a Dillon type bent if its $(2^r+1, 2^r-1)$-interleaved sequence consists of only all zero columns and all one columns and the number of all one columns is 2^{r-1}. Thus, $l = s = 2^{r-1}$. Putting these values in $2l+2s-4w+(2^r-2s)(2^r-2l)$, $-2^{r+1}+2l+2s-4w+(2^r-2l)(2^r-2s+2)$, $-4w-2s+2l+(2^r-2s)(2^r-2l)$, $2^{r+1}+2l-4w-2s+(2^r-2l)(2^r+2-2s)$ as mentioned in Theorem 2, we get only two distinct values, namely, $2^{r+1}-4w$ or $-4w$. Now, $0 \leq w \leq min\{l, s\}$, i.e., $0 \leq w \leq 2^{r-1}$. Hence, the maximum absolute value of the crosscorrelation spectra at nonzero point is at most $2^{\frac{n}{2}+1}$. The value of $C_{f,g}(0)$ also follows from Theorem 2. ■

If f, g are Dillon type bent functions, then direct sum of f, g is also Dillon type if and only if $w = 2^{r-2}$. By Corollary 3 the possible crosscorrelation values of f and g at any α is $\pm 2^r = \pm 2^{\frac{n}{2}}$. This result agrees with the result of Theorem 1 which is a more general result for bent functions.

2.2 Generalized Autocorrelation

In [22], Youssef and Gong introduced generalized nonlinearity of Boolean functions and studied the Dillon type functions under this framework. Instead of the set of all affine functions, they considered the set $\{Tr_1^n(\lambda x^c)+\epsilon | \lambda \in GF(2^n), \epsilon \in GF(2), c$ is coprime to $2^n-1\}$

and defined the generalized nonlinearity of a function $f \in \mathcal{F}_n$ as the distance of the function from the above set. The functions of the form $Tr_1^n(\lambda x^c)$ where $\lambda \in GF(2^n)$ and c is coprime to $2^n - 1$ are called bijective monomials. Clearly the linear functions are also bijective monomials. They also extended Walsh Hadamard transform as, $W_f(\lambda, c) = \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(\lambda x^c) + f(x)}$, where c is coprime to $2^n - 1$. The generalized nonlinearity of $f \in \mathcal{F}_n$ was defined as $nlg(f) = 2^{n-1} - \frac{1}{2} max_{\lambda \in GF(2^n), gcd(c, 2^n-1)=1} |w_f(\lambda, c)|$. The bent functions whose generalized nonlinearity equals the nonlinearity are called hyper-bent functions. The class of hyper-bent functions are more restricted than the class of bent functions. The subclass of hyper-bent functions described in [22] are the Dillon type bent functions as pointed out by Carlet [22].

We define *generalized autocorrelation* the analogue of autocorrelation in this set up and show that unlike autocorrelation for bent functions, for hyper-bent functions generalized autocorrelation need not be always zero. Suppose $U(2^n - 1)$ is the set of all positive integers coprime to $2^n - 1$.

Definition 4 *The generalized autocorrelation of a function $f \in \mathcal{F}_n$ at $\alpha \in GF(2^n)$ and $c \in U(2^n - 1)$ is defined as $\Delta_f(\alpha, c) = \sum_{x \in GF(2^n)} (-1)^{f(x) + f(x^c + \alpha)}$.*

It is desirable that the generalized autocorrelation of a function is low for all values of α and c, that is, $\max_{\alpha \in GF(2^n), c \in U(2^n-1)} |\Delta_f(\alpha, c)|$ is low (except the cases $\alpha = 0$ when $f(x), f(x^c)$ are identical).

Let $f(x)$ be a Dillon type bent function (same as hyperbent function constructed by Youssef and Gong [22]). For any $c \in U(2^n - 1)$, $f(x^c)$ is also a Dillon type bent function.

Proposition 3 *Let $f(x)$ be a Dillon type function on $n = 2r$ variables. If $c \equiv c_1 \bmod 2^r + 1$ for $c, c_1 \in U(2^n - 1)$ then $f(x^c) = f(x^{c_1})$.*

Proof : If $f(x)$ is a Dillon type function then $f(x)$ can be written as $g(x^{2^r - 1})$. Suppose $c, c_1 \in U(2^n - 1)$ are such that $c \equiv c_1 \bmod 2^r + 1$, that is $c = c_1 + q(2^r + 1)$ for some integer q. Then $f(x^c) = f(x^{c_1 + q(2^r+1)}) = g(x^{c_1(2^r-1)}) = f(x^{c_1})$. ∎

Definition 5 *Let $n = 2r$. For $c, c_1 \in U(2^n - 1)$, c is related to c_1 if and only if $c \equiv c_1 \bmod 2^r + 1$. This partitions the set $U(2^n - 1)$ in distinct equivalence classes. By $L(2^n - 1)$, we denote the set of smallest elements from each equivalence class.*

Note that the autocorrelation property of any bent function is known [15], i.e., $\Delta_f(\alpha, c = 1) = 0$ for all nonzero $\alpha \in GF(2^n)$. Thus we will be interested in the generalized spectra even when $c \neq 1$. Based on this discussion and Proposition 3, it is enough to discuss the generalized autocorrelation of a Dillon type bent function $f \in \mathcal{F}_n$ at $\alpha \in GF(2^n)$ and $c \in L(2^n - 1) \setminus \{1\}$. Now we have the following result related to generalized autocorrelation spectra of Dillon type bent functions, i.e., Youssef and Gong type hyper-bent functions.

Lemma 4 *Let $f(x) \in \mathcal{F}_n$ be a Dillon type bent function. Then for $c \in L(2^n - 1) \setminus \{1\}$,*

$$\begin{aligned} \Delta_f(\alpha, c) &= 2^{\frac{n}{2}+1} - 4w_c \text{ or } -4w_c, \text{ for nonzero } \alpha \in GF(2^n), \\ &= 2^n - 2(2^{\frac{n}{2}} - 2w_c)(2^{\frac{n}{2}} - 1) \text{ for } \alpha = 0, \end{aligned}$$

where w_c is the number of all one columns of $S(f(x))$ that gets added to all one columns of $S(f(x^c))$ in $S(f(x)) + S(f(x^c))$ as in Theorem 2. Further $\Delta_f(\alpha, c) \leq 2^{\frac{n}{2}+1}$ for nonzero α. In addition, if $f(x) + f(x^c)$ is bent, then $\Delta_f(\alpha, c) = \pm 2^{\frac{n}{2}}$.

Proof : From Proposition 2 it follows that $f(x)$ is Dillon type bent if and only if $f(x^c)$ is Dillon type bent. Then the result follows from Corollary 3. The last result follows from the last result of Theorem 1. That we need to vary c only in $L(2^n - 1) \setminus \{1\}$ follows from Proposition 3. ■

It is now important to see whether there is any Dillon type bent function so that either (i) $f(x)+f(x^c)$ is bent or (ii) $f(x) = f(x^c)$ for all $c \in L(2^n-1)\setminus\{1\}$. The reason is, in case such a function $f(x)$ exists, $|\Delta_f(\alpha, c)|$ can take values $0, \pm 2^{\frac{n}{2}}$ (except the cases $\alpha = 0$ when $f(x), f(x^c)$ are identical). This is clearly the best possible generalized autocorrelation spectra for a Dillon type (hyper) bent function. We experimentally checked that such Dillon type bent functions are available for $n = 4, 6$, but not available for $n = 8$. It is open whether such functions are available for even $n \geq 10$, though given the combinatorial restriction on these functions, it is unlikely that such functions exist.

2.3 Character Sums

In this section we show that the crosscorrelation results on Dillon type bent functions have important consequences in improving the upper bound on the absolute values of Weil sums [21, 19, 12] for a particular class of polynomials. Additive character of $GF(p^n)$ is a homomorphism from $GF(p^n)$ into the set of all complex numbers with absolute value 1. The additive character $\chi_1(x) = e^{\frac{2\pi i Tr(x)}{p}}$ is called the canonical additive character, where $Tr(x) = x + x^p + x^{p^2} + \ldots + x^{p^{n-1}}$. It is well known that [10] for any additive character χ of $GF(p^n)$ there exists some fixed $a \in GF(p^n)$ such that $\chi(x) = \chi_1(ax)$ for all $x \in GF(p^n)$. In case $p = 2$ the canonical additive character takes the form $\chi_1(x) = (-1)^{Tr(x)}$. If χ is a *nontrivial* additive character of the field $GF(p^n)$ and $g(x) \in GF(p^n)[x]$ of degree $deg(g(x))$. It is well known [21, 19] that $\left|\sum_{x \in GF(p^n)} \chi(g(x))\right| \leq (deg(g(x)) - 1)p^{\frac{n}{2}}$, where $gcd(deg(g(x)), p) = 1$. We shall refer to the sum $\sum_{x \in GF(p^n)} \chi(g(x))$ as the *Weil sum* for $g(x)$ and the above upper bound as the *Weil bound*. Mullen and Shparlinski [12] have mentioned the problem of evaluating the upper bounds of the absolute value of the Weil sum for special fields and polynomials. Several such bounds are described in [18, 20]. We here characterize a class of polynomials for which the Weil bound is improved.

Lemma 5 *Let n be an even positive integer. There exists nonzero $\lambda \in GF(2^{\frac{n}{2}})$ such that*

$$\left| \sum_{x \in GF(2^n)} \chi_1(\lambda(\gamma^i (x)^{2^{\frac{n}{2}}-1} + \gamma^j (x+\delta)^{2^{\frac{n}{2}}-1})) \right| \leq 2^{\frac{n}{2}+1},$$

for nonzero $\delta \in GF(2^n)$.

Proof : For even $n = 2r$, let γ be a generator of the cyclic group of order $2^r + 1$. Lachaud and Wolfmann [9] have proved that there exists $\lambda \in GF(2^r)$ such that $f_j(x) = Tr(\lambda \gamma^j x^{2^r-1})$

is bent (basically Dillon type) for all $0 \leq j \leq 2^r$ (see also [1]). From Corollary 3, if $i \neq j$ then $\left|\sum_{x \in GF(2^n)} (-1)^{f_i(x)+f_j(x+\delta)}\right| = \left|\sum_{x \in GF(2^n)} (-1)^{Tr(\lambda \gamma^i x^{2^r-1})+Tr(\lambda \gamma^j (x+\delta)^{2^r-1})}\right| \leq 2^{r+1}$. ■

The result in Lemma 5 improves the Weil bound for this class of polynomial. Note that

$$deg(\lambda(\gamma^i x^{2^{\frac{n}{2}}-1} + \gamma^j (x+\delta)^{2^{\frac{n}{2}}-1})) = 2^{\frac{n}{2}} - 1$$

for $i \neq j$. So Weil bound gives,

$$|\sum_{x \in GF(2^n)} \chi_1(\lambda(\gamma^i x^{2^{\frac{n}{2}}-1} + \gamma^j (x+\delta)^{2^{\frac{n}{2}}-1}))| \leq (2^{\frac{n}{2}} - 2)2^{\frac{n}{2}} = 2^n - 2^{\frac{n}{2}+1},$$

for nonzero $\delta \in GF(2^n)$. Our result is much more improved for canonical additive character and for this special class of polynomials.

Let us denote the first row of $S(Tr(\alpha x^{2^{\frac{n}{2}}-1}))$ by R_α and the number of 1's in R_α as $wt(R_\alpha)$. It follows from [9, Theorem 6.6] that $2^{\frac{n}{2}-1} - \min_{\alpha \in GF(2^n)^*} wt(R_\alpha) \leq 2^{\frac{n}{4}} + 1$ and $\max_{\alpha \in GF(2^n)^*} wt(R_\alpha) - 2^{\frac{n}{2}-1} \leq 2^{\frac{n}{4}} + 1$. However, it seems that the bound is much better in practice as is shown by the following experimental result for even n, $4 \leq n \leq 24$.

n	4	6	8	10	12	14	16	18	20	22	24
$\min_{\alpha \in GF(2^n)^*} wt(R_\alpha)$	2	2	6	12	26	54	114	234	482	980	1986
$2^{\frac{n}{2}-1}$	2	4	8	16	32	64	128	256	512	1024	2048
$\max_{\alpha \in GF(2^n)^*} wt(R_\alpha)$	4	6	12	22	40	74	144	278	544	1068	2112

We observe that $2^{\frac{n}{2}-1} - \min_{\alpha \in GF(2^n)^*} wt(R_\alpha)$ and $\max_{\alpha \in GF(2^n)^*} wt(R_\alpha) - 2^{\frac{n}{2}-1}$ are both $\leq n\lfloor \log_2 n \rfloor$ for even n, $4 \leq n \leq 24$, which is much better than $2^{\frac{n}{4}}+1$ that has been proved in [9]. However, we will use the result of [9] to present a more general statement than Lemma 5, though the bound is little bit weaker.

Theorem 3 *Let n be an even positive integer. For any $\alpha, \beta, \delta \in GF(2^n)^*$,*

$$\left|\sum_{x \in GF(2^n)} \chi_1(\alpha(x)^{2^{\frac{n}{2}}-1} + \beta(x+\delta)^{2^{\frac{n}{2}}-1})\right| \leq 8 \cdot 2^{\frac{n}{2}} + 20 \cdot 2^{\frac{n}{4}} + 16.$$

Proof : Consider that for any $\alpha \in GF(2^n)^*$, $|wt(R_\alpha) - 2^{\frac{n}{2}-1}| \leq v$. Now consider two Dillon type functions f, g (may not be bent) on n variables, such that the first row of their interleaved sequences $S(f(x)), S(g(x))$ are R_α, R_β respectively. Following the notation of Theorem 2, it can be checked that maximum absolute value of $C_{f,g}(\delta) \leq 4v^2 + 12v + 2^{r+2}$, for $n = 2r$. It follows from [9, Theorem 6.6] that $v \leq 2^{\frac{n}{4}} + 1$. Hence the result. ■

The result in Theorem 3 improves the Weil bound for this class of polynomial. Note that $deg(\alpha(x)^{2^{\frac{n}{2}}-1} + \beta(x+\delta)^{2^{\frac{n}{2}}-1}) = 2^{\frac{n}{2}} - 1$ for $\alpha \neq \beta$. Thus Weil bound gives the value $2^n - 2^{\frac{n}{2}+1}$ for nonzero $\delta \in GF(2^n)$. Our result is much more improved for canonical additive character and for this extended class of polynomials than in Lemma 5.

Corollary 4 *Let n be an even positive integer. For any $\alpha, \beta, \delta \in GF(2^n)^*$,*

$$|\sum_{x \in GF(2^n)} \chi(\alpha(x)^{2^{\frac{n}{2}}-1} + \beta(x+\delta)^{2^{\frac{n}{2}}-1})| \leq 8 \cdot 2^{\frac{n}{2}} + 20 \cdot 2^{\frac{n}{4}} + 16,$$

for any nontrivial additive character χ of $GF(2^n)$.

Proof : The proof is direct from the fact that Theorem 3 is true for any $\alpha, \beta \in GF(2^n)$ and the relationship between any additive character to the canonical additive character defined on a finite field. ■

Finally we prove the following result.

Corollary 5 *Let n be an even positive integer. Let $p(x) \in GF(2^n)[x]$ be a polynomial of the form $p(x) = \alpha x^{2^{\frac{n}{2}}-1} + x^{2^{\frac{n}{2}}-2} + x^{2^{\frac{n}{2}}-3} + \ldots + x + 1$, where $1 \neq \alpha \in GF(2^n)^*$. Then for any nontrivial additive character χ of $GF(2^n)$ the Weil sum $|\sum_{x \in GF(2^n)} \chi(p(x))| \leq 8 \cdot 2^{\frac{n}{2}} + 20 \cdot 2^{\frac{n}{4}} + 16$.*

Proof : The proof follows from

$$|\sum_{x \in GF(2^n)} \chi(\alpha x^{2^{\frac{n}{2}}-1} + x^{2^{\frac{n}{2}}-2} + x^{2^{\frac{n}{2}}-3} + \ldots + x + 1)| = |\sum_{x \in GF(2^n)} \chi((x+1)^{2^{\frac{n}{2}}-1} + (\alpha+1)x^{2^{\frac{n}{2}}-1})|$$

and Corollary 4. ■

3 Results on Patterson-Wiedemann type functions

Patterson and Wiedemann [13, 14] extended the concept introduced by Dillon when the number of input variables n is odd and succeeded in finding out functions having nonlinearity strictly greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ for odd $n \geq 15$. This result is pioneering as this is the first instance when such a high nonlinearity has been demonstrated and further till date there is no other strategy to get such functions. Later in [11] these functions have been changed heuristically to get highly nonlinear balanced functions. Also it has been noted in [11] that the autocorrelation spectra of Patterson-Wiedemann functions are very nice and some theoretical justification in this direction has been provided recently in [6]. In this section we present crosscorrelation results for Patterson-Wiedemann type functions and provide a more generalized framework than what obtained in [6]. In fact our results provide some justification why the maximum absolute value in the autocorrelation spectra of Patterson-Wiedemann type functions are very low. We also describe this construction using interleaved sequence as was exploited in [6]. Now we formally describe Patterson-Wiedemann construction using interleaved sequence.

Definition 6 *Let n be a positive odd integer such that $n = tq$, where both t and q are primes and $t > q$. Let $\mathcal{K} = GF(2^t)^* \cdot GF(2^q)^*$ be the cyclic group of order $k = (2^t - 1)(2^q - 1)$ in $GF(2^n)$. Let $\langle \phi_2 \rangle$ be the group of Frobenius automorphisms where $\phi_2 : GF(2^n) \longrightarrow GF(2^n)$ is defined by $x \mapsto x^2$. We call a function $f \in \mathcal{F}_n$ Patterson-Wiedemann (PW) type if it is invariant under the action of both $\mathcal{K}$ and $\langle \phi_2 \rangle$.*

Suppose $d = \frac{2^n-1}{2^t-1}$ and $d_1 = \frac{2^n-1}{k}$. The equivalence relation denoted by ρ_{d_1} is defined as follows:

$$i \rho_{d_1} j \Leftrightarrow \text{ there exists a positive integer } s \text{ such that } i \equiv 2^s j \bmod d_1.$$

Now from Definition 6, it is clear that (d_1, k)-interleaved sequence of a PW function consists of only all 0 or all 1 columns. Further the columns in each equivalence class with respect to ρ_{d_1} have the same value.

In order to compute the distance of a function of the above type from a linear function $Tr_1^n(\beta x)$ where $\beta \in GF(2^n)$ the $(d, 2^t-1)$-interleaved sequence of both the functions (the PW one and the linear one) are to be considered.

1. In a $(d, 2^t-1)$-interleaved sequence of $Tr_1^n(\beta x)$ with resepect of any primitive element ζ, the weight of each column is either 2^{t-1} or 0. It is also known that the number of zero columns is $d - 2^{n-t}$.

2. Since $GF(2^t)^* \subseteq \mathcal{K}$, $S_{(d,2^t-1)}(f(x), \zeta)$ consists of all one columns and all zero columns only.

Because of this by using $(d, 2^t-1)$-interleaved sequences one can compute the distances of $f(x)$ and $Tr_1^n(\beta x)$ and the nonlinearity of the function can be computed (see [6] for more details). It has been shown in [6] that $W_f(\zeta^i) = W_f(\zeta^j)$ if $i \rho_{d_1} j$. Thus the maximum number of distinct Walsh transform values of $f(x)$, at nonzero points, is r, where r is the number of equivalence classes when ρ_{d_1} acts on $\{0, \ldots, 2^n-2\}$. In [6], $c_{i,j}$ is defined as the number of all zero columns of the $(d, 2^t-1)$-interleaved sequence of $Tr_1^n(\zeta^i x)$ that are in the j-th $(0 \leq j \leq r-1)$ equivalence class corresponding to ρ_{d_1}.

Theorem 4 *Let f, g be two PW type functions on n-variables and the Walsh transform values of f, g at each point of the j-th equivalence class be $w(f, j), w(g, j)$ respectively. Then $C_{f,g}(\zeta^i) = \frac{1}{2^n}[\sum_{j=0}^{r-1}(2^t c_{i,j} - b_j) w(f, j) w(g, j) + W_f(0) W_g(0)]$, where b_j is the number of elements in the j-th equivalence class of ρ_{d_1} when it is defined on the set $\{0, 1, \ldots, d-1\}$. Further the additive crosscorrelation spectra contains at most r distinct values at nonzero points (at most $r+1$ including the zero point).*

Proof : If ζ is a primitive element of $GF(2^n)$ then all the elements of $GF(2^n)^*$ can be written as powers of ζ. We know that all these elements are partitioned into r equivalence classes by ρ_{d_1}. Walsh transform values at the elements from the same equivalence class are same [6]. From [17], we have the result $C_{f,g}(\zeta^i) = 2^{-n} \sum_{x \in GF(2^n)} W_f(x) W_g(x) (-1)^{Tr(\zeta^i x)}$. Note that both

$$\{W_f(\zeta^0) W_g(\zeta^0), W_f(\zeta^1) W_g(\zeta^1), \ldots, W_f(\zeta^{2^n-2}) W_g(\zeta^{2^n-2})\}$$

and

$$\{(-1)^{Tr(\zeta^i \zeta^0)}, (-1)^{Tr(\zeta^i \zeta^1)}, \ldots, (-1)^{Tr(\zeta^i \zeta^{2^n-2})}\}$$

can be written as $(d, 2^t - 1)$-interleaved sequences. Denote them by $\hat{W}(f(x), g(x))$ and $L(Tr(\zeta^i x))$ respectively.

When a column from the j-th equivalence class $\hat{W}(f(x), g(x))$ is element wise multiplied to an 'all one' column of the $(d, 2^t - 1)$-interleaved sequence of $(-1)^{Tr(\zeta^i x)}$, $L(Tr(\zeta^i x))$, and all the products are added we get $(2^t - 1)w(f, j)w(g, j)$. Since there are $c_{i,j}$ columns of the j-th class that get multiplied to 'all one' columns of $L(Tr(\zeta^i x))$ the total contribution from this source by summing over all the equivalence classes is $\sum_{j=0}^{r-1} c_{i,j}(2^t - 1)w(f, j)w(g, j)$.

Rest of the $b_j - c_{i,j}$ columns of the j-th equivalence class of $\hat{W}(f(x), g(x))$ get multiplied to the 'mixed' columns of $L(Tr(\zeta^i x))$. These columns of $L(Tr(\zeta^i x))$ contain 2^{t-1}, -1's and $2^{t-1} - 1$, 1's. Thus when we take the sum of the products (after element wise multiplication) we obtain $(b_j - c_{i,j})(-w(f, j)w(g, j))$. Summing over all the equivalence classes we get total contribution from this source as, $\sum_{j=0}^{r-1}(b_j - c_{i,j})(-w(f, j)w(g, j))$.

Thus the crosscorrelation $C_{f,g}(\zeta^i)$ of the Patterson-Wiedemann type functions at ζ^i is

$$C_{f,g}(\zeta^i) = \frac{1}{2^n}[\sum_{j=0}^{r-1} c_{i,j}(2^t - 1)w(f, j)w(g, j) + \sum_{j=0}^{r-1}(b_j - c_{i,j})(-w(f, j)w(g, j)) + W_f(0)W_g(0)],$$

that is,

$$C_{f,g}(\zeta^i) = \frac{1}{2^n}[\sum_{j=0}^{r-1}(2^t c_{i,j} - b_j)w(f, j)w(g, j) + W_f(0)W_g(0)].$$

Next we show that the number of distinct crosscorrelation values is r. It is enough to show that if $i\rho_{d_1} l$ then $c_{i,j} = c_{l,j}$. Suppose the column number e in the j-th equivalence class is such that $Tr_1^n(\zeta^i \zeta^{e+\lambda d}) = 0$ for all $\lambda = 0, 1, \ldots, 2^t - 2$; that is in the $(d, 2^t - 1)$-interleaved sequence of $Tr_1^n(\zeta^i x)$ the e th column is 0.

$i\rho_{d_1} l \Rightarrow i = 2^k l + \mu d_1$. From this we obtain

$$\begin{aligned} Tr_1^n(\zeta^{2^k l + \mu d_1} \zeta^{e+\lambda d}) &= Tr_1^n(\zeta^{2^k l} \zeta^{(e+\mu d_1)+\lambda d}) \\ &= Tr_1^n(\zeta^l \zeta^{2^{n-k}(e+\mu d_1)+\lambda 2^{n-k} d}). \end{aligned}$$

Since $\lambda \mapsto (\lambda 2^{n-k})\%(2^t - 1)$ is a permutation on $\{0, 1, \ldots, 2^t - 2\}$, the $2^{n-k}(e + \mu d_1)\%d$-th column of the $(d, 2^{t-1})$-interleaved sequence of $Tr_1^n(\zeta^l x)$ is all zero.It can be directly checked that this column number is in the j th equivalence class.

It is also clear that if $e_1 \equiv e_2 \bmod d$ then $2^{n-k}(e_1 + \mu d_1)\%d = 2^{n-k}(e_2 + \mu d_1)\%d$. Thus $c_{i,j} \geq c_{l,j}$. Similarly it can be shown that $c_{l,j} \geq c_{i,j}$. Hence $c_{l,j} = c_{i,j}$. Thus while computing crosscorrelation it is enough to compute $C_{f,g}(\zeta^i)$ by choosing one i from each equivalence class of ρ_{d_1}. Thus there can be atmost r distinct values of crosscorrelation at nonzero points. At 0, $C_{f,g}(0) = \sum_{x \in GF(2^n)}(-1)^{f(x)+g(x)} = 2^n - 2wt(f(x) + g(x))$. ∎

Patterson-Wiedemann obtained two functions (upto complementation and affine transform) for $n = 15$ which posses nonlinearity 16276. Call these functions f, g. Note that $C_{f,g}(0) = 6728$. Now we calculate the crosscorrelation spectra at the nonzero points. There are $r = 11$ equivalence classes and the values at each of the classes are as follows: 904, 280, 184, 136, 40, 8, -8, -104, -152, -184, -248.

To get the autocorrelation spectra of PW type functions we put $f = g$ and obtain,

$$\Delta_f(\zeta^i) = C_{f,f}(\zeta^i) = \frac{1}{2^n}\left[\sum_{j=0}^{r-1}(2^t c_{i,j} - b_j)w(f,j)^2 + W_f(0)^2\right].$$

It is clear that the spectra is at most r-valued at the nonzero points. This has been proved in [6] independently using a different technique. Here, this is a consequence of a more general crosscorrelation result as described in Theorem 4.

It has been experimentally checked in [11] that the maximum absolute value in the autocorrelation spectra is very low (only 160) for the two highly nonlinear PW type functions and till date there is no clear answer why these should be so low (even the theoretical analysis in [6] does not provide a clear answer). Note that as the nonlinearity of the these functions are very high, the Walsh transform values are low. It is now interesting to study the following expression that appears in Theorem 4:

$$\sum_{j=0}^{r-1}(2^t c_{i,j} - b_j) = 2^t \sum_{j=0}^{r-1} c_{i,j} - \sum_{j=0}^{r-1} b_j = 2^t\left(\frac{2^n-1}{2^t-1} - 2^{n-t}\right) - \frac{2^n-1}{2^t-1} = 2^n - 1 - 2^n = -1.$$

Note that, if we consider the Walsh spectra values are almost constant, this gives the reason why the functions of this type have very low autocorrelation values.

References

[1] A. Canteaut and P. Charpin. Decomposing Bent Functions. *IEEE Transactions on Information Theory*, August, 2003.

[2] C. Carlet. Recent results on binary bent functions. In *International Conference on Combinatorics, Information Theory and Statistics*, 1997.

[3] C. Ding, G. Xiao, and W. Shan. *The Stability Theory of Stream Ciphers.* Number 561 in Lecture Notes in Computer Science. Springer-Verlag, 1991.

[4] J. F. Dillon. Elementary Hadamard Difference sets. PhD Thesis, University of Maryland, 1974.

[5] 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.

[6] S. Gangopadhyay, P. H. Keskar and S. Maitra. Patterson-Wiedemann functions revisited. Web address: http://eprint.iacr.org/, Report no. 2003/176.

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

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

[9] G. Lachaud and J. Wolfmann. The weights of the orthogonal of the extended quadratic binary Goppa codes. *IEEE Transactions on Information Theory*, 36(3):686–692, September 1990.

[10] R. Lidl and H. Niederreiter. Introduction to finite fields and their applications. Cambridge University Press, 1994.

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

[12] G. L. Mullen, I. E. Shparlinski. *Open Problems and Conjectures in finite fields*. LMS Lecture Notes Series, vol. 233, pages 243 - 268, 1996.

[13] 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.

[14] 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.

[15] O. S. Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A*, 20:300–305, 1976.

[16] P. Sarkar and S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. In *Advances in Cryptology - EUROCRYPT 2000*, number 1807 in Lecture Notes in Computer Science, pages 485–506. Springer Verlag, May 2000.

[17] P. Sarkar and S. Maitra. Cross-Correlation Analysis of Cryptographically Useful Boolean Functions and S-boxes. Theory of Computing Systems, 35(1):39–57, 2002.

[18] I. E. Shparlinski. *Computational and algorithmic problems in finite fields*. Kluwer Acad. Publ., Dordrecht, The Netherlands, 1992.

[19] S. A. Stepanov. *Arithmetic of Algebraic Curves*. Plenum, New York 1994.

[20] S. A. Stepanov. *Character sums and coding theory*. LMS Lect. Notes Series 233, pp. 355–378, 1996.

[21] A. Weil. *On some exponential sums*. Proc. Nat. Acad. Sci. U.S.A. 1948, **34** pp. 204 - 207.

[22] 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.