BENT AND VECTORIAL BENT FUNCTIONS, PARTIAL DIFFERENCE SETS, AND STRONGLY REGULAR GRAPHS

AYÇA ÇEŞMELİOĞLU
Altınbaş University, School of Engineering and Natural Sciences
Bağcılar, 34217 Istanbul, Turkey

WILFRIED MEIDL
Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria

(Communicated by Eimear Byrne)

ABSTRACT. Bent and vectorial bent functions have applications in cryptography and coding and are closely related to objects in combinatorics and finite geometry, like difference sets, relative difference sets, designs and divisible designs. Bent functions with certain additional properties yield partial difference sets of which the Cayley graphs are always strongly regular. In this article we continue research on connections between bent functions and partial difference sets respectively strongly regular graphs. For the first time we investigate relations between vectorial bent functions and partial difference sets. Remarkably, properties of the set of the duals of the components play here an important role. Seeing conventional bent functions as 1-dimensional vectorial bent functions, some earlier results on strongly regular graphs from bent functions follow from our more general results. Finally we describe a recursive construction of infinitely many partial difference sets with a secondary construction of \( p \)-ary bent functions.

1. INTRODUCTION

Let \( p \) be a prime, \( n \) be a positive integer and let \( V_n \) be an \( n \)-dimensional vector space over \( \mathbb{F}_p \). For a function \( f \) from \( V_n \) to \( \mathbb{F}_p \), the Walsh transform of \( f \) is defined to be the complex valued function \( \mathcal{W}_f \) on \( V_n \)

\[
\mathcal{W}_f(u) = \sum_{x \in V_n} \epsilon_p^{f(x) - u \cdot x},
\]

where \( \epsilon_p = e^{2\pi i/p} \) and \( u \cdot x \) denotes a (nondegenerate) inner product of \( V_n \). If \( V_n = \mathbb{F}_p^n \), then we may choose the conventional dot product for \( u \cdot x \), the standard inner product when \( V_n = \mathbb{F}_p^n \) is \( u \cdot x = \text{Tr}_n(ux) \), where \( \text{Tr}_n(z) \) denotes the absolute trace of \( z \in \mathbb{F}_p^n \).

The function \( f : V_n \to \mathbb{F}_p \) is called bent if the absolute value of its Walsh transform \( \mathcal{W}_f(u) \) is \( p^{n/2} \) for all \( u \in V_n \).

If \( p = 2 \), then \( \epsilon_p = -1 \) and \( \mathcal{W}_f(u) \) is an integer. Hence a Boolean bent function \( f \) can only exist when \( n \) is even, and then \( \mathcal{W}_f(u) = 2^{n/2}(-1)^{f^*(u)} \) for some Boolean function \( f^* \), called the dual of \( f \). As is well known, \( f^* \) is bent as well. (Strictly speaking, \( f^* \) is the dual of \( f \) with respect to the considered inner product since

2010 Mathematics Subject Classification: 06E30, 05B10, 11T06, 94C10.

Key words and phrases: Bent function, vectorial Boolean function, partial difference set, strongly regular graph, dual bent function, Walsh transform.
differently to the Walsh spectrum, the Walsh coefficient $W_f(u)$ at $u \in V_n$ is not independent from the inner product in (1).

If $p$ is odd, then the Walsh coefficient $W_f(u)$ at $u \in V_n$ of a bent function $f$ always satisfies (cf. [12, 13])

$$W_f(u) = \begin{cases} \pm f^*(u) p^{n/2} & : p^n \equiv 1 \mod 4; \\ \pm \epsilon_f p^{n/2} & : p^n \equiv 3 \mod 4,
\end{cases}$$

where $f^*$ is a function from $V_n$ to $F_p$, again called the dual of $f$. A bent function (which when $p$ is odd, we call a $p$-ary bent function) is said to be weakly regular if $W_f(u) = \zeta f^*(u) p^{n/2}$, where $\zeta \in \{\pm 1, \pm i\}$ does not depend on $u$. If $\zeta = 1$, we call $f$ regular. A Boolean bent function is hence always regular. A bent function for which $\zeta$ changes with $u$ is called non-weakly regular. Weakly regular bent functions $f$ always appear in pairs since the dual function $f^*$ in (2) is also a (weakly regular) bent function, [12]. This is in general not true for non-weakly regular bent functions, see [5, 6].

Motivated by connections to cryptography and coding, bent functions, and generalizations, have been investigated in many aspects, see for instance [16]. One approach which provides to the understanding of bent functions is to relate them to combinatorial objects, first of all they can be identified with relative difference sets in the elementary abelian group. In this paper we are interested in partial difference sets and strongly regular graphs obtained from bent functions.

Let $G$ be a group of order $v$. A subset $D$ of $G$ with $k$ elements is called a $(v, k, \lambda, \mu)$ partial difference set (PDS) of $G$, if every nonzero element of $D$ can be represented as $d_1 - d_2$, $d_1, d_2 \in D$, in exactly $\lambda$ ways, and every nonzero element of $G \setminus D$ can be represented as $d_1 - d_2$, $d_1, d_2 \in D$, in exactly $\mu$ ways. Combinatorial objects related with partial difference sets are strongly regular graphs. A $k$-regular graph with $v$ vertices is called a $(v, k, \lambda, \mu)$ strongly regular graph, if every two adjacent vertices have exactly $\lambda$ common neighbours, and every two non-adjacent vertices have exactly $\mu$ common neighbours.

For a group $G$ and a subset $D$ of $G$ such that $-D = -D$ and $0 \notin D$, we can define a graph, called Cayley graph generated by $D$, as follows: The vertices of the graph are the elements of $G$, and two vertices $g, h$ are adjacent if $g - h \in D$. Let now $G$ be a group of order $v$ and $D$ be a subset of $G$ for which $-D = -D$ and $0 \notin D$. The Cayley graph generated by $D$ is a $(v, k, \lambda, \mu)$ strongly regular graph if and only if $D$ is a $(v, k, \lambda, \mu)$ partial difference set of $G$, see [15].

Connections between bent functions and strongly regular graphs were already observed in [1, 2], where it is shown that the Cayley graph of $D_f^0 = \{x : f(x) = 0\}$ for a Boolean bent function $f$ is strongly regular. Indeed, Boolean bent functions have been precisely characterized by this property. (In [1, 2], 0 is included in the PDS). In the significant paper [19], constructions of strongly regular graphs from certain classes of ternary bent functions are proposed, and families of strongly regular graphs are obtained, some of which were previously unknown. In [8, 11] the construction is generalized for $p$-ary bent functions.

In this article we for the first time investigate connections between vectorial bent functions and partial difference sets respectively strongly regular graphs. Notably, a property of the duals of vectorial bent functions which was investigated only recently in [7] plays here a crucial role. In this light, some results on connections between strongly regular graphs and conventional bent functions can be seen as a special case of our results on vectorial bent functions. Finally, in the last section we
employ a secondary construction of bent functions to recursively generate infinite sequences of strongly regular graphs.

2. Preliminaries

In this section we recall vectorial bent functions and discuss some properties of their duals, which recently have been investigated in [7]. As it turns out, it exactly depends on these properties, whether a vectorial bent function induces partial difference sets.

A function $F(x) = (f_1(x), f_2(x), \ldots, f_m(x))$ from $V_n$ to $\mathbb{F}_p^n$ is called a vectorial bent function if every nontrivial linear combination $c_1f_1 + c_2f_2 + \cdots + c_mf_m$ is bent, or equivalently, for every nonzero $c \in \mathbb{F}_p^n$, the $p$-ary function $f_c(x) = c \cdot F(x)$ is bent. We call $f_c$ a component function of $F$. In the framework of finite fields, a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_p^m$ for a divisor $m$ of $n$, is a vectorial bent function, if for all nonzero $\alpha \in \mathbb{F}_{p^m}$, the component function $f_\alpha : \mathbb{F}_{p^n} \to \mathbb{F}_p$ defined as $f_\alpha(x) = \text{Tr}_m(\alpha F(x))$ is bent.

For a vectorial bent function we always must have $m \leq n$. If all component functions are regular, then $m \leq n/2$, see [17]. In particular when $p = 2$, then $m \leq n/2$.

Let $f_1$ and $f_2$ be (weakly regular) bent functions, let $f_1^*$ and $f_2^*$ be their duals and suppose that $f_1 + f_2$ is also bent. In [7] it is pointed out that then $f_1^* + f_2^*$ is in general not a bent function. In general, the collection of the duals of the component functions of a vectorial bent function, does not even form a vector space. Accordingly, in [7] the following definition was given.

**Definition 1.** For two vector spaces $V_n$, $V_m$ over $\mathbb{F}_p$ of dimension $n$ and $m$, let $F : V_n \to V_m$ be a vectorial bent function. We say that $F$ is a vectorial dual-bent function if the set of the dual functions of the component functions of $F$ (together with the zero function) forms a vector space of bent functions of the same dimension $m$. The dual functions of the component functions of $F$ are then the component functions of some vectorial bent function $F^*$ from $V_n$ to $V_m$, called a vectorial dual of $F$.

For Boolean bent functions, the concept of a vectorial dual is a generalization of a Boolean bent function and its dual seen as a 1-dimensional vector space over $\mathbb{F}_2$. This is different for a $p$-ary (weakly regular) bent function $f$, which seen as a 1-dimensional vector space over $\mathbb{F}_p$ consists of all constant multiples of $f$. The set of the duals is in general not closed under addition. Hence, seen as a 1-dimensional vector space, a (weakly regular) $p$-ary bent function does in general not have a vectorial dual.

Though several classical constructions of vectorial bent functions are vectorial dual-bent, this property seems to be quite rare. Some examples are given in the following. For more details we refer to [7].

1. $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $p$ odd, $F(x) = x^2$. Then $f_\alpha(x) = \text{Tr}_n(\alpha x^2)$, $\alpha \in \mathbb{F}_{p^n}$, $f_\alpha^*(x) = \text{Tr}_n(-x^2/(4\alpha))$, and $F^*(x) = F(x)$, see [7, Example 1].

2. $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}, F(x, y) = axy^k$, $a \in \mathbb{F}_{p^m}$, $\gcd(k, p^m - 1) = 1$. Then $F^*(x, y) = -y(x/a)^{k'}$, $kr \equiv 1 \mod (p^m - 1)$, see [7, Theorem 3(ii)].

3. $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p'}, F(x, y) = G(x/y)$ for a divisor $s$ of $m$ and a balanced function $G : \mathbb{F}_{p^m} \to \mathbb{F}_{p'}$ (and the convention that $1/0 = 0$). Then for $\alpha \in \mathbb{F}_{p'}$, $f_\alpha(x, y) = \text{Tr}_s(\alpha G(x/y))$, $f_\alpha^*(x, y) = \text{Tr}_s(\alpha G(-y/x))$, and $F^*(x, y) = G(-y/x)$, see [7, Theorem 5].
3. Strongly regular graphs from vectorial bent functions

In this section we investigate for the first time partial difference sets respectively strongly regular graphs obtained from vectorial bent functions $F(x) = (f_1(x), f_2(x), \ldots, f_m(x))$ from $V_n$ to $\mathbb{F}_p^m$ for some odd prime $p$. Vectorial bent functions which we consider here, will always have the following properties: $n$ is even, and all component functions $f_e$ of $F$ are regular or all are weakly regular with $\epsilon = -1$. Equivalently, for all component functions we have $W_{f_i}(u) = \epsilon p^{n/2} f_p^{(u)}$ where $\epsilon = 1$ or $\epsilon = -1$ is independent from $c$. Furthermore, we always suppose that $F(0) = 0 = (0, \ldots, 0)$, and we suppose that $F$ satisfies the condition that $F(x) = F(-x)$. The last condition seems quite restrictive, but every vectorial dual-bent function we know so far does satisfy this condition.

The main tool is the following characterization of partial difference sets via characters, see [15, 19].

**Lemma 1.** Let $G$ be an abelian group of order $\nu$. Suppose that $D$ is a $k$-subset of $G$ which satisfies $-D = D$ and $0 \notin D$. Then $D$ is a $(\nu, k, \lambda, \mu)$ partial difference set if and only if for each non-principal character $\chi$,

$$\chi(D) = \frac{\beta \pm \sqrt{\Delta}}{2}$$

where $\beta = \lambda - \mu, \gamma = k - \mu$ and $\Delta = \beta^2 + 4\gamma$.

We will further use the following relation between the parameters of a partial difference set, see for instance [15, Proposition 1.4(b)]:

$$k = \frac{(\nu + \beta) \pm \sqrt{(\nu + \beta)^2 - (\Delta - \beta^2)(\nu - 1)}}{2}.$$  

Let $F(x) = (f_1(x), f_2(x), \ldots, f_m(x))$ be a vectorial bent function from $V_n$ to $\mathbb{F}_p^m$ (such that all component functions are regular or all are weakly regular with $\epsilon = -1$), for each $i = 1, 2, \ldots, m$, let $D_0^i$ be the set $D_0^i = \{ x \in V_n : f_i(x) = 0 \}$, and let $D_0^c = \{ x \in V_n : F(x) = 0 \}$.

We consider the set

$$D = D_0^c \setminus \{0\} = \bigcap_{i=1}^m D_0^i \setminus \{0\},$$

and show that under some condition, $D$ is a partial difference set, hence gives rise to a strongly regular graph. Most notably the property of $F$ being vectorial dual-bent will play a central role. We start with a lemma, which relates $\chi(D)$ with the Walsh transforms of the component functions of $F$. For $u \in V_n$, we denote by $\chi_u : V_n \rightarrow \mathbb{C}$ the character $\chi_u(x) = \epsilon_p^{u \cdot x}$.

**Lemma 2.** Let $f_1(x), f_2(x), \ldots, f_m(x)$ be functions from $V_n$ to $\mathbb{F}_p$ and let $D_0 = \{ x \in V_n : f_1(x) = f_2(x) = \cdots = f_m(x) = 0 \}$. Then

$$|D_0| = p^{n-m} + p^{-m} \sum_{(c_1, c_2, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0\}} W_{c_1 f_1 + c_2 f_2 + \cdots + c_m f_m}(0),$$

and for $u \neq 0$,

$$p^m \chi_u(D_0) = \sum_{(c_1, c_2, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0\}} W_{c_1 f_1 + c_2 f_2 + \cdots + c_m f_m}(u).$$
Proof. Denote by \( D_{j_1, \ldots, j_m} \) the set
\[
D_{j_1, \ldots, j_m} = \{ x \in \mathbb{V}_n : f_1(x) = j_1, \ldots, f_m(x) = j_m \}.
\]
Then we have
\[
\tag{5} \sum_{x \in D_0} \epsilon_{u-x}^u + \sum_{x \in D_{0, \ldots, 0, 1}} \epsilon_{u-x}^u + \cdots + \sum_{x \in D_{p-1, \ldots, p-1, p-1}} \epsilon_{u-x}^u = \begin{cases} 0 & : u \neq 0, \\ p^n & : u = 0. \end{cases}
\]
For \( c = (c_1, c_2, \ldots, c_m) \neq 0 \in \mathbb{F}_p^m \), let
\[
f_c = c_1 f_1 + c_2 f_2 + \cdots + c_m f_m.
\]
Then
\[
W_{f_c}(u) = \sum_{x \in D_0} \epsilon_{p-x}^u + \sum_{x \in D_{0, \ldots, 0, 1}} \epsilon_{c_1}^u \epsilon_{p-x}^u + \cdots + \sum_{x \in D_{p-1, \ldots, p-1, p-1}} \epsilon_{c_1 \cdots c_m}^u \epsilon_{p-x}^u.
\]
Summing (5) with all \( p^m - 1 \) equations for \( W_{f_c}(u) \), for \( u \neq 0 \) we get
\[
\sum_{(c_1, c_2, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0\}} W_{c_1 f_1 + c_2 f_2 + \cdots + c_m f_m}(u) = p^m \sum_{x \in D_0} \epsilon_{u-x}^u + \sum_{j \in \mathbb{F}_p^m} \sum_{c \in \mathbb{F}_p^m} \epsilon_{c}^j \sum_{x \in D_j} \epsilon_{u-x}^u.
\]
Observing that \( \sum_{c \in \mathbb{F}_p^m} \epsilon_{c}^j = 0, \ j \neq 0 \), we get the assertion. For \( u = 0 \) this summation yields
\[
p^n + \sum_{(c_1, c_2, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0\}} W_{c_1 f_1 + c_2 f_2 + \cdots + c_m f_m}(0) = p^m |D_0|,
\]
and the result on the cardinality of \( D_0 \) follows. \( \square \)

From Lemma 2, for the cardinality of \( D_0^F \) for a vectorial bent function, we obtain the following corollary.

Corollary 1. Let \( n \) be even and \( F(x) = (f_1(x), f_2(x), \ldots, f_m(x)) \) be a vectorial bent function from \( \mathbb{V}_n \) to \( \mathbb{F}_p^m \). Then the cardinality of \( D_0^F \) is \( \{ x \in \mathbb{V}_n : f_1(x) = f_2(x) = \cdots = f_m(x) = 0 \} \) satisfies
\[
p^n - m - (p^{n/2} - p^{n/2-m}) \leq |D_0^F| \leq p^{n-m} + p^{n/2} - (p^{n/2-m}).
\]
Equality on the left side holds if and only if all component functions \( f_c \) are weakly regular but not regular, and satisfy \( f_c^*(0) = 0 \). We have equality on the right side if and only if all component functions \( f_c \) are regular, and satisfy \( f_c^*(0) = 0 \).

Proof. By our assumption, \( W_{c_1 f_1 + c_2 f_2 + \cdots + c_m f_m}(0) = \epsilon(c) p^{n/2} c_p^F(0) \) for all nonzero \( c = (c_1, c_2, \ldots, c_m) \in \mathbb{F}_p^m \), where \( \epsilon(c) \) is \( \{ \pm 1 \} \). With Lemma 2, the cardinality of the set \( D_0^F \) is then
\[
|D_0^F| = p^n - m + p^{n/2-m} \sum_{(c_1, c_2, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0\}} \epsilon(c) c_p^F(0).
\]
As obvious, the smallest respectively the largest possible value for \( |D_0^F| \) is obtained exactly if \( f_c^*(0) = 0 \) (i.e. \( c_p^F(0) = 1 \)), and \( \epsilon(c) = -1 \) respectively \( \epsilon(c) = 1 \) for all \( c \in \mathbb{F}_p^m \setminus \{0\} \). The latter condition equivalently means that \( f_c \) is weakly regular but not regular respectively regular for all \( c \in \mathbb{F}_p^m \setminus \{0\} \). \( \square \)

With Lemma 2 we also obtain the following proposition for a special class of vectorial bent functions, namely for vectorial dual-bent functions. We remark that then the condition \( f_c^*(0) = 0 \) for all \( c \in \mathbb{F}_p^m \setminus \{0\} \) simply means that \( F^*(0) = 0 \).
**Proposition 1.** Let $F(x) = (f_1(x), f_2(x), \ldots, f_m(x))$ be a vectorial dual-bent function, and let $\{g_1^*, g_2^*, \ldots, g_m^*\}$ be a basis for the space of the dual $F^*$ of $F$. For each non-principal character $\chi_u$ of $V_n$, 
\[ \chi_u(D_0^m) = \chi_u(\bigcap_{j=1}^m D_0^{f_j}) = \begin{cases} p^{n/2-m}(p^m - 1)\epsilon, & g_m^*(u) = \cdots = g_1^*(u) = 0 \\ -p^{n/2-2m}\epsilon, & otherwise. \end{cases} \]

**Proof.** By our assumption, for every $(c_1, c_2, \ldots, c_m) \neq 0 \in \mathbb{F}_p^m$ we have $\mathcal{W}_{c_1 f_1 + c_2 f_2 + \cdots + c_m f_m}(u) = c_1^{x_0 f_1} c_2^{x_1 f_2} \cdots c_m^{x_m f_m} \epsilon^u$, where $\epsilon = \pm 1$ is independent from $(c_1, c_2, \ldots, c_m)$. By Lemma 2 we have 
\[ p^m \chi_u(D_0^m) = p^{n/2} \epsilon^{c_1 g_1^*(u) + c_2 g_2^*(u) + \cdots + c_m g_m^*(u)}. \]

Since $\{g_1^*, g_2^*, \ldots, g_m^*\}$ is a basis for the vectorial dual $F^*$ of $F$, the above sum can be written as 
\[ \chi_u(D_0^m) = p^{n/2-m}\epsilon \sum_{(c_1, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0\}} \epsilon^{c_1 g_1^*(u) + c_2 g_2^*(u) + \cdots + c_m g_m^*(u)}. \]

As the (nonzero) $u \in \mathbb{F}_p^n$ is fixed by the non-principal character $\chi_u$, also $g_1^*(u), g_2^*(u), \ldots, g_m^*(u)$ are fixed. We write the above sum as 
\[ \sum_{(c_1, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0\}} \epsilon^{c_1 g_1^*(u) + c_2 g_2^*(u) + \cdots + c_m g_m^*(u)} = \sum_{(c_1, \ldots, c_m-1) \in \mathbb{F}_p^{m-1} \setminus \{0\}} \epsilon^{c_1 g_1^*(u) + c_2 g_2^*(u) + \cdots + c_{m-1} g_{m-1}^*(u)} \sum_{c_m \in \mathbb{F}_p} \epsilon^{c_m g_m^*(u)}. \]

If $(c_1, \ldots, c_{m-1}) = 0$, then 
\[ \sum_{c_m \in \mathbb{F}_p} \epsilon^{c_m g_m^*(u)} = \begin{cases} p-1, & g_m^*(u) = 0 \\ -1, & g_m^*(u) \neq 0. \end{cases} \]

Hence 
\[ \sum_{(c_1, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0\}} \epsilon^{c_1 g_1^*(u) + c_2 g_2^*(u) + \cdots + c_m g_m^*(u)} = \sum_{(c_1, \ldots, c_{m-1}) \in \mathbb{F}_p^{m-1} \setminus \{0\}} \epsilon^{c_1 g_1^*(u) + c_2 g_2^*(u) + \cdots + c_{m-1} g_{m-1}^*(u)} \sum_{c_m \in \mathbb{F}_p} \epsilon^{c_m g_m^*(u)} + \sum_{c_m \in \mathbb{F}_p \setminus \{0\}} \epsilon^{c_m g_m^*(u)} = \begin{cases} p-1 + p \sum_{(c_1, \ldots, c_{m-1}) \in \mathbb{F}_p^{m-1} \setminus \{0\}} \epsilon^{c_1 g_1^*(u) + \cdots + c_{m-1} g_{m-1}^*(u)}, & g_m^*(u) = 0 \\ -1, & g_m^*(u) \neq 0 \end{cases} \]

Applying the same procedure to the sum 
\[ \sum_{(c_1, \ldots, c_{m-1}) \in \mathbb{F}_p^{m-1} \setminus \{0\}} \epsilon^{c_1 g_1^*(u) + c_2 g_2^*(u) + \cdots + c_{m-1} g_{m-1}^*(u)}, \]

**Advances in Mathematics of Communications** Volume 12, No. 4 (2018), 691–705

Avşa Çeşmelioğlu and Wilfried Meidl
distinguishing the cases \( g_{m-1}^*(u) = 0 \) and \( g_{m-1}^*(u) \neq 0 \), we obtain

\[
\sum_{(c_1, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0\}} \epsilon_p^{c_1 g_1^*(u) + c_2 g_2^*(u) + \cdots + c_m g_m^*(u)} = \\
\begin{cases}
p - 1 + p(p - 1) + p^2 \sum_{(c_1, \ldots, c_{m-2}) \in \mathbb{F}_p^{m-1} \setminus \{0\}} \epsilon_p^{c_1 g_1^*(u) + \cdots + c_{m-2} g_{m-2}^*(u)}, \\
g_{m-1}^*(u) = g_m^*(u) = 0 - 1, g_{m-1}^*(u) \neq 0 \text{ or } g_m^*(u) \neq 0
\end{cases}
\]

Continuing this procedure, after \( m \) steps we get

\[
\sum_{(c_1, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0\}} \epsilon_p^{c_1 g_1^*(u) + c_2 g_2^*(u) + \cdots + c_m g_m^*(u)} = \\
\begin{cases}
p - 1(1 + p + \cdots + p^{m-1}) = p^m - 1, & g_m^*(u) = \cdots = g_1^*(u) = 0 \\
-1, & \text{otherwise}
\end{cases}
\]

As a consequence,

\[
\chi_u(D_0^F) = p^{n/2-m} \epsilon \sum_{(c_1, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0\}} \epsilon_p^{(c_1 f_1 + c_2 f_2 + \cdots + c_m f_m)^*(u)} = \\
\begin{cases}
p^{n/2-m}(p^m - 1) \epsilon, & g_m^*(u) = \cdots = g_1^*(u) = 0 \\
-p^{n/2-m} \epsilon, & \text{otherwise}
\end{cases}
\]

From Proposition 1, for \( D = D_0^F \setminus \{0\} = \bigcap_{i=1}^m D_0^{f_i} \setminus \{0\} \), we obtain

\[
\chi_u(D) = \chi_u(D_0^F) - 1 = \\
\begin{cases}
p^{n/2-m}(p^m - 1) \epsilon - 1, & g_m^*(u) = \cdots = g_1^*(u) = 0 \\
-p^{n/2-m} \epsilon - 1, & \text{otherwise}
\end{cases}
\]

Since \( \chi_u(D), u \neq 0 \), takes on two different values, the set \( D \) is a partial difference set in \( V_n \).

**Theorem 1.** For an even integer \( n \), let \( F : V_n \to \mathbb{F}_p^m \) with \( F(x) = (f_1(x), f_2(x), \ldots, f_m(x)) \) be a vectorial dual-bent function with \( F(x) = F(-x) \) for which all component functions are regular (\( \epsilon = 1 \)) or weakly regular with \( \epsilon = -1 \). The set

\[
D = \{ x \in V_n \setminus \{0\} : F(x) = 0 \in \mathbb{F}_p^m \}
\]

is a \((v, k, \lambda, \mu)\) partial difference set in \( V_n \) with

\[
\begin{align*}
k &= p^{n-m} + \epsilon(p^{n/2} - p^{n/2-m}) - 1, \\
\mu &= p^{n/2-m} + \epsilon p^{n/2-m}, \\
\lambda &= p^{n/2-m} + \epsilon(p^{n/2} - p^{n/2-m}) - 2.
\end{align*}
\]

**Proof.** With Proposition 1, \( \chi_u(D), u \neq 0 \), takes on only two values. It remains to show the parameters of the partial difference set. By definition we have \( v = p^n \), and by Lemma 1,

\[
\chi_u(D) = \frac{\beta \pm \sqrt{\Delta}}{2} = \\
\begin{cases}
p^{n/2-m}(p^m - 1) \epsilon - 1 \\
-p^{n/2-m} \epsilon - 1
\end{cases}
\]

from which we immediately get \( \sqrt{\Delta} = p^{n/2} \), and \( \beta = \epsilon(p^{n/2} - 2p^{n/2-m}) - 2 \). With the help of Equation (4) we can then determine \( k \) as \( k = |D| = p^{n-m} + \)
\( \epsilon(p^{n/2} - p^{n/2-m}) - 1 \). Since we require \( \Delta = \beta^2 + 4\gamma = p^n \), we follow that \( \gamma = p^{n-m} - p^{n-2m} + \epsilon p^{n/2} - 2\epsilon p^{n/2-m} - 1 \). Finally, with \( \mu = k - \gamma \) and \( \lambda = \beta + \mu \) we obtain \( \mu = p^{n-2m} + \epsilon p^{n/2-m} \) and \( \lambda = p^{n-2m} + (p^{n/2} - p^{n/2-m}) - 2 \). \( \square \)

Note that \( |D_0^F| \) is maximal respectively minimal by the bound in Corollary 1.

**Remark 1.** A strongly regular graph with parameters \((n^2, r(n - \epsilon), cn + r^2 - 3\epsilon r, r^2 - \epsilon r)\) is called Latin Square or Negative Latin Square type when \( \epsilon = 1 \) or \( \epsilon = -1 \), respectively. Comparing with the parameters of the partial difference sets in Theorem 1, we observe that the Cayley graph of \( D_0^F \) in Theorem 1 is of Latin Square type if \( \epsilon = 1 \), hence all components \( f_\epsilon \) are regular, and of Negative Latin Square type if \( \epsilon = -1 \), i.e. all components \( f_\epsilon \) are weakly regular but not regular.

There are many constructions of graphs of Latin Square type, however new graphs of Negative Latin Square type obtained from bent functions, which are not equivalent to earlier known graphs with the same parameters, have been presented e.g. in [19], see also our discussion in the next section and [19] for details.

Since vectorial dual-bent functions always appear in pairs, assuming that \( F \) and \( F^* \) both satisfy our conditions, also partial difference sets as obtained in Theorem 1 come in pairs. Recall that all vectorial dual-bent functions we know so far satisfy \( F(x) = F(-x) \).

**Corollary 2.** Let \( F : V_n \to \mathbb{F}_p^n \) be a vectorial dual-bent function with the vectorial dual \( F^* \). Then both, \( D_0^F \setminus \{0\} \) and \( D_0^{F^*} \setminus \{0\} \) are partial difference sets with the same parameters given as in Theorem 1.

Recall from [8, 11, 19] that (weakly) regular bent functions \( f : V_n \to \mathbb{F}_p \), \( n \) even, for which \( f(\alpha x) = \alpha^f f(x) \) for all \( \alpha \in V_n \) and some fixed positive integer \( \ell \) with \( \gcd(\ell - 1, p - 1) = 1 \), give rise to strongly regular graphs. The next proposition connects our results on vectorial bent functions and strongly regular graphs with results in [8, 11, 19].

**Proposition 2.** Let \( f : V_n \to \mathbb{F}_p \) be a weakly regular bent function for which there exists an integer \( \ell \) with \( \gcd(\ell - 1, p - 1) = 1 \) such that \( f(\alpha x) = \alpha^f f(x) \) for all \( \alpha \in \mathbb{F}_p^\ast \). Then \( f \) (seen as a 1-dimensional vector space of bent functions) is a vectorial dual-bent function.

**Proof.** We will use that (see [4, Theorem 1] and its proof)

\[
(\alpha f)^* (\alpha u) = \alpha f^* (u), \quad \text{for all } \alpha \in \mathbb{F}_p^\ast .
\]

Further observe that for \( c \in \mathbb{F}_p^\ast \)

\[
\mathcal{W}_{f(\alpha x)}(u) = \sum_{x \in V_n} \epsilon_p f(\alpha x - u) = \sum_{x \in V_n} \epsilon_p f(x - u) \cdot c^{-1} x
\]

\[
= \sum_{x \in V_n} \epsilon_p f(x - c^{-1} u) \cdot x = \mathcal{W}_f(c^{-1} u).
\]

Hence \( (f(\alpha x))^* (u) = f^* (c^{-1} u) \). As a consequence, with \( z = u/\alpha \),

\[
(\alpha^{-f} f(x))^* (u) = (\alpha f(x/\alpha))^* (\alpha z) = \alpha (f(x/\alpha))^* (z) = \alpha f^* (\alpha z) = \alpha f^* (u).
\]

Since \( \gcd(\ell - 1, p - 1) = 1 \), the mapping \( \alpha \to \alpha^{-f} \) is a permutation of \( \mathbb{F}_p^\ast \). Therefore \( \{(\alpha f(x))^* : \alpha \in \mathbb{F}_p^\ast \} = \{\alpha f^* (x) : \alpha \in \mathbb{F}_p^\ast \} \), i.e. \( f \) is vectorial dual-bent. \( \square \)

By Proposition 2 and Theorem 1 we can see the result of [8, 11, 19] as summarized below, as special case of the general result for vectorial dual-bent functions. Bent
functions $f$ with the above described properties in fact induce strongly regular graphs as these properties guarantee that $f$ (seen as 1-dimensional vectorial bent function) is vectorial dual-bent.

**Corollary 3.** [8, 11, 19] Let $p$ be an odd prime, $n$ be an even integer, and let $f : V_n \to \mathbb{F}_p$ be a (weakly) regular bent function, hence $W_f(u) = \epsilon p^n/2 \ell^m(u)$ for all $u \in V_n$, and fixed $\epsilon = \pm 1$. Suppose that for some positive integer $\ell$ with $\gcd(\ell - 1, p - 1) = 1$ we have $f(\alpha x) = \alpha^\ell f(x)$ for any $\alpha \in \mathbb{F}_p$ (which also implies $f(0) = 0$ and $f(-x) = f(x)$). Then the set $D_0^F \setminus \{0\}$ is a $(\nu, k, \lambda, \mu)$-PDS with

\[
\nu = p^n, \quad k = (p^{\frac{n}{2}} - \epsilon)(p^{\frac{n}{2}} - 1 + \epsilon),
\]

\[
\lambda = (p^{\frac{n}{2}} - 1 + \epsilon)^2 - 3\epsilon(p^{\frac{n}{2}} - 1 + \epsilon) + \epsilon(p^{\frac{n}{2}} - 1 + \epsilon)p^{\frac{n}{2}} - 1.
\]

**Remark 2.** By Corollary 2, also $f^*$ is vectorial dual-bent. Moreover, as shown in Lemma 4 in [18] we have $f^*(\alpha x) = \alpha^\ell f^*(x)$ for all $\alpha \in \mathbb{F}_p$, where $\ell - 1$ is the inverse of $\ell - 1$ modulo $(p - 1)$. This also follows from Equation (6). Furthermore we see that $f^*(0) = 0$.

We finish this section pointing to some interesting properties of partial difference sets obtained from vectorial bent functions.

Supposing that at least some of the subspaces of a vectorial-bent function $F$ (satisfying our conditions) are also vectorial-dual-bent, then Theorem 1 reveals several partial difference sets on the same group. For instance, if $F(x) = (f_1(x), \ldots, f_m(x))$ is a vectorial dual-bent function for which the component functions $f_j$, $1 \leq j \leq m$, are also (1-dimensional) vectorial dual-bent functions, then all sets $D_0^F \setminus \{0\}$ and $D_0^{f_j} \setminus \{0\}$, $1 \leq j \leq m$, are partial difference sets where the first is the intersection of all the latter ones. The Cayley graphs $G_F$, $G_{f_j}$, $1 \leq j \leq m$, of all sets $D_0^F \setminus \{0\}$ and $D_0^{f_j} \setminus \{0\}$, $1 \leq j \leq m$, are strongly regular. Two vertices are adjacent in $G_F$ if and only if they are adjacent in all strongly regular graphs $G_{f_j}$, $1 \leq j \leq m$. When $m = 2$ for example, $D_0^F \setminus \{0\} = D_0^{f_1} \setminus \{0\} \cap D_0^{f_2} \setminus \{0\}$, the strongly regular graph $G_F$ one obtains by taking the edges which are in both strongly regular graphs, $G_{f_1}$ and $G_{f_2}$.

A similar observation we will now deduce about the union of two related partial difference sets: If $F = \langle f_1, f_2, \ldots, f_m \rangle$ is an $m$-dimensional vectorial-bent function (with $F(x) = F(-x)$ and satisfying our regularity condition), and $F_1 = \langle f_1, f_2, \ldots, f_k \rangle$, $k < m$, is a $k$-dimensional subspace of $F$, and both, $F$ and $F_1$ are vectorial-dual-bent, then $D_0^F \setminus \{0\}$ is a partial difference set containing the partial difference set $D_0^{F_1} \setminus \{0\}$ as a subset. We have moreover the following result on the complement of $D_0^F$ as a subset of $D_0^{F_1}$.

**Corollary 4.** Let $F = \langle f_1, f_2, \ldots, f_m \rangle$ be a vectorial dual-bent function from $V_n$ to $\mathbb{F}_p^m$ such that all component functions are regular (weakly regular with $\epsilon = -1$), and suppose that the $k$-dimensional subspace $F_1 = \langle f_1, f_2, \ldots, f_k \rangle$ is also vectorial dual-bent (from $V_n$ to $\mathbb{F}_p^k$). Then the set $\overline{D} = D_0^{F_1} \setminus D_0^F$ is a $(p^n, k, \lambda, \mu)$ partial difference set with

\[
k = (p^{m-k} - 1)p^{n-m} - \epsilon(p^{m-k} - 1)p^{n/2-m},
\]

\[
\lambda = (p^{m-k} - 1)^2p^{n-2m} + \epsilon(p^{n/2} - 3(p^{m-k} - 1)p^{n/2-m}),
\]

\[
\mu = (p^{m-k} - 1)^2p^{n-2m} - \epsilon(p^{m-k} - 1)p^{n/2-m}.
\]
Proof. With Corollary 1, we obtain the cardinality of $\bar{D}$ as

$$|\bar{D}| = |D_0^\prime| - |D_0^F| = p^{n-k} + \epsilon(p^{n/2} - p^{(n/2)-k} - p^{n-m} - \epsilon(p^{n/2} - p^{n/2-m})$$

$$= (p^{m-k} - 1)p^{n-m} - \epsilon(p^{m-k} - 1)p^{n/2-m}.$$  

By our assumption that both, $F$ and $F_1$ are vectorial dual-bent, we can write $F^*$ as $F^* = \langle g_1^*, \ldots, g_k^*, g_{k+1}^*, \ldots, g_m^* \rangle$, for component functions $g_i$ of $F$, $1 \leq i \leq m$, such that $F_1^* = \langle g_1^*, \ldots, g_k^* \rangle$. Then by Proposition 1, for $\chi_u(\bar{D}) = \chi_u(D_0^F) - \chi_u(D_0^F)$, $u \neq 0$, we have

$$\chi_u(\bar{D}) = \begin{cases} p^{n/2-k}(p^k - 1)\epsilon - p^{n/2-m}(p^n - 1)\epsilon, & \text{if } g_i^*(u) = 0, 1 \leq i \leq m, \\ p^{n/2-k}(p^k - 1)\epsilon + p^{n/2-m}\epsilon, & \text{if } (g_1^*(u), \ldots, g_k^*(u)) = 0, \\ -p^{n/2-k}\epsilon + p^{n/2-m}\epsilon, & \text{if } (g_{k+1}^*(u), \ldots, g_m^*(u)) \neq 0, \\ -p^{n/2-k}\epsilon, & \text{otherwise.} \end{cases}$$

Therefore $\chi_u(\bar{D})$ takes on the two different values

$$\chi_u(\bar{D}) = \begin{cases} (p^{n/2} - (p^{m-k} - 1)p^{n/2-m})\epsilon, & \text{if } (g_1^*(u), \ldots, g_k^*(u)) = 0, \\ - (p^{m-k} - 1)p^{n/2-m}\epsilon, & \text{if } (g_{k+1}^*(u), \ldots, g_m^*(u)) \neq 0, \\ \text{otherwise.} \end{cases}$$

Again, with (3) we get $\sqrt{\Delta} = p^{n/2}$, $\beta = (p^{n/2} - 2(p^{m-k} - 1)p^{n/2-m})\epsilon$. Then

$$\gamma = \frac{\Delta - \beta^2}{4} = \frac{p^n - (p^n - 4(p^{m-k} - 1)p^{n-m}) - 4(p^{m-k} - 1)^2p^{n-2m}}{4} = p^{n-2m}(p^{m-k} - 1) - (p^{m-k} - 1)^2 = (p^{m-k} - 1)(p^m - p^{m-k} + 1)p^{n-2m},$$

$$\nu = k - \gamma = (p^{m-k} - 1)p^{n-m} - \epsilon(p^{m-k} - 1)p^{n/2-m} - (p^{m-k} - 1)(p^m - p^{m-k} + 1)p^{n-2m} = (p^{m-k} - 1)^2p^{n-2m} - \epsilon(p^{m-k} - 1)p^{n/2-m},$$

and

$$\lambda = \beta + \mu = (p^{n/2} - 2(p^{m-k} - 1)p^{n/2-m})\epsilon + (p^{m-k} - 1)^2p^{n-2m} - \epsilon(p^{m-k} - 1)p^{n/2-m} = (p^{m-k} - 1)^2p^{n-2m} + \epsilon(p^{n/2} - 3(p^{m-k} - 1)p^{n/2-m}).$$

By Corollary 4 the partial difference set $D_0^F \setminus \{0\}$ is the disjoint union of two partial difference sets, $D_0^F \setminus \{0\}$ and $D_0^F \setminus D_0^F$. If $G_F$, $G_{F_1}$ and $\bar{G}_F$ are the strongly regular graphs corresponding to the partial difference sets $D_0^F \setminus \{0\}$, $D_0^F \setminus \{0\}$ and $D_0^F \setminus D_0^F$, then the graph $\bar{G}_F$ is a strongly regular subgraph of $G_F$, and two vertices in the strongly regular graph $\bar{G}_F$ are adjacent if and only if they are adjacent in $G_{F_1}$, but not $G_F$. Equivalently, $G_F$ and $\bar{G}_F$ are two disjoint strongly regular graphs (no common edges), for which the union is again strongly regular. We remark, that for two partial difference sets $D_1, D_2$ with $D_2 \subset D_1$ it does in general not hold that $D_1 \setminus D_2$ is again a partial difference set, but it is also not an unusual property, see e.g. [10].

AVÇA ÇEŞMEİLGİLU AND WILFRIED MEIDL

ADVANCES IN MATHEMATICS OF COMMUNICATIONS Volume 12, No. 4 (2018), 691–705
Remark 3. In Corollary 4 we require that besides from $F$, also the $k$-dimensional subspace $F_1$ is vectorial dual-bent. All our examples of vectorial dual-bent bent functions have this property for any of their subspaces. However, duality of bent functions is a quite complex topic. By now we cannot exclude the existence of a vectorial dual-bent function $F$ with a subspace $F_1$ for which the set of the duals of its components only forms a subset in the vector space of the duals of the components of $F$.

As for also many other objects, examples for vectorial-dual bent functions are obtained with spreads of $V_n$. For these functions all components have algebraic degree $n/2$. The unions of certain numbers of spread elements are then the partial difference sets described in this section. We here described connections between partial difference sets and vectorial bent functions in terms of properties of duals. This may also raise interest in finding more classes of vectorial dual-bent functions. Some examples (also of algebraic degree smaller than $n/2$) are 1-dimensional vectorial dual-bent functions investigated in connection with strongly regular graphs in [8, 19], and functions in the list in the preliminaries. Some of the 1-dimensional examples yield new graphs, see [19] or the construction in the next section. We checked some graphs for the functions in the list in the introduction for some small parameters, all of which are of Latin Square type and solely yield new interpretations of known graphs. To further investigate vectorial dual-bent functions and to test the graphs for (non-quadratic) examples in also higher dimension should be a worthwhile topic.

4. A SECONDARY (RECURSIVE) CONSTRUCTION OF STRONGLY REGULAR GRAPHS

In [8, 11, 19] several $p$-ary bent functions satisfying the properties in Corollary 3, i.e. bent functions which - seen as vectorial bent functions in dimension 1 - are dual-bent, have been considered. By this, even some new strongly regular graphs have been found, [19]. However, in general $p$-ary bent functions do not have these properties. In this section we construct from bent functions that satisfy the conditions in Corollary 3 new such bent functions in a higher dimension. By this we obtain a recursive procedure to generate (infinitely many) bent functions for strongly regular graphs. Finally we analyse the resulting graphs and give some examples.

For the convenience of the reader and for the sake of completeness, we first summarize some facts on $p$-ary bent functions and strongly regular graphs. For a function $f$ from $V_n$ to $\mathbb{F}_p$, let $D_i^f = \{ x \in V_n : f(x) = i \}$, $i = 0, 1, \ldots, p - 1$, and let $S := \{ x \in \mathbb{F}_p^* : x \text{ is a square in } \mathbb{F}_p^* \}$ and $N := \{ x \in \mathbb{F}_p^* : x \text{ is a nonsquare in } \mathbb{F}_p^* \}$. We then define the sets $D_S^f$ and $D_N^f$ as

$$D_S^f = \cup_{i \in S} D_i^f, \quad D_N^f = \cup_{i \in N} D_i^f.$$  

The following summarizes Theorem 1, Theorem 2 and Remark 3(i) in [8].

Let $p$ be an odd prime, $n$ be an even integer, and let $f : V_n \rightarrow \mathbb{F}_p$ be a (weakly) regular bent function, hence $W_f(u) = \epsilon p^{n/2} \ell_p^f(u)$ for all $u \in V_n$, and fixed $\epsilon = \pm 1$. Suppose that for some positive integer $\ell$ with $\gcd(\ell - 1, p - 1) = 1$ we have $f(\alpha x) = \alpha^\ell f(x)$ for any $\alpha \in \mathbb{F}_p$.

(i) The set $D_0^f \setminus \{0\}$ is a $(\nu, k, \lambda, \mu)$-PDS with

$$\nu = p^n, \quad k = (p^{\frac{n}{2}} - \epsilon)(p^{\frac{n}{2}} - 1 + \epsilon),$$  

$$\lambda = \epsilon p^{n/2} \ell_p^f(u)$$  

and

$$\mu = \epsilon (p^{n/2} - \epsilon)(p^{n/2} - 1 + \epsilon).$$
\[ \lambda = (p^{n-1} + \epsilon)^2 - 3\epsilon(p^{n-1} + \epsilon) + \epsilon p^{\frac{n}{2}}, \mu = (p^{n-1} + \epsilon)p^{\frac{n}{2}-1}, \]

see also our Corollary 3.

(ii) The sets \( D_S^f, D_N^f \) form \((\nu, k, \lambda, \mu)\)-PDSs with
\[
\nu = p^n, k = \frac{1}{2}(p^\frac{n}{2} - p^{\frac{n}{2}-1})(p^\frac{n}{2} - \epsilon),
\lambda = \frac{1}{4}(p^\frac{n}{2} - p^{\frac{n}{2}-1})^2 - \frac{3\epsilon}{2}(p^\frac{n}{2} - p^{\frac{n}{2}-1}) + p^\frac{n}{2} \epsilon,
\mu = \frac{1}{2}(p^\frac{n}{2} - p^{\frac{n}{2}-1})(\frac{1}{2}(p^\frac{n}{2} - p^{\frac{n}{2}-1}) - \epsilon).
\]

Recall that a strongly regular graph with parameters \((n^2, r(n - \epsilon), cn + r^2 - 3\epsilon r, r^2 - \epsilon)\) is called Latin Square or Negative Latin Square type when \(\epsilon = 1\) or \(\epsilon = -1\), respectively. The Cayley graphs of \( D_S^f, D_N^f \) and the Cayley graph of \( D_0^f \backslash \{0\} \) (see also Remark 1) are of Latin Square type if \(\epsilon = 1\), hence \(f\) is regular, and of Negative Latin Square type if \(\epsilon = -1\), i.e. \(f\) is weakly regular but not regular.

There are many constructions of strongly regular graphs of Latin Square type, quadratic bent functions yield affine polar graphs, which can also be constructed using projective two-weight codes, see Result 7 in [19] and the discussion thereafter. Hence graphs from weakly regular, but not regular, non-quadratic bent functions seem most interesting. Several examples of partial difference sets respectively strongly regular graphs can be found in [8, 19].

The following theorem enables a recursive construction of bent functions which induce strongly regular graphs.

**Theorem 2.** Let \( g_0, g_1 : V_n \rightarrow \mathbb{F}_p \) be two (distinct) bent functions for which there exists an integer \( \ell \) with \( \gcd(\ell - 1, p - 1) = 1 \), such that \( g_i(\alpha x) = \alpha^i g_i(x), i = 0, 1, \) for all \( \alpha \in \mathbb{F}_p \). Then the function \( F : V_n \times \mathbb{F}_p^2 \rightarrow \mathbb{F}_p \) given by
\[
F(x, y, z) = (g_1(x) - g_0(x))z^{p-1} + uy\ell^{-1} + g_0(x),
\]
for a non-zero element \( u \in \mathbb{F}_p \), is a bent function satisfying \( F(\alpha x, y, z) = \alpha^\ell F(x, y, z) \) for all \( \alpha \in \mathbb{F}_p \).

**Proof.** For \( a \in V_n \) and \( b, c \in \mathbb{F}_p \) we have
\[
\mathcal{W}_F(a, b, c) = \sum_{x \in V_n} \sum_{y, z \in \mathbb{F}_p} \epsilon_{\mathbb{F}_p}^{F(x, y, z) - ax - by - cz} = \sum_{x \in V_n} \epsilon_{\mathbb{F}_p}^{g_0(x) - ax} \sum_{y, z \in \mathbb{F}_p} \epsilon_{\mathbb{F}_p}^{(g_1(x) - g_0(x))z^{p-1} + uy\ell^{-1} - by - cz}
\]
\[
= \sum_{x \in V_n} \epsilon_{\mathbb{F}_p}^{g_0(x) - ax} \left( \sum_{y \in \mathbb{F}_p} \epsilon_{\mathbb{F}_p}^{-by} + \sum_{z \in \mathbb{F}_p} \epsilon_{\mathbb{F}_p}^{g_1(x) - g_0(x) + uy\ell^{-1} - by - cz} \right)
\]
\[
= \mathcal{W}_{g_0}(a) \sum_{y \in \mathbb{F}_p} \epsilon_{\mathbb{F}_p}^{-by} + \mathcal{W}_{g_1}(a) \sum_{y \in \mathbb{F}_p} \sum_{z \in \mathbb{F}_p} \epsilon_{\mathbb{F}_p}^{uy\ell^{-1}-by-cz}
\]
\[
= \mathcal{W}_{g_0}(a) \sum_{y \in \mathbb{F}_p} \epsilon_{\mathbb{F}_p}^{-by} + \mathcal{W}_{g_1}(a) \sum_{y \in \mathbb{F}_p} \sum_{z \in \mathbb{F}_p} \epsilon_{\mathbb{F}_p}^{uy\ell^{-1} - bz}.
\]
we obtain \( W_g \) construction of a strongly regular graph from the graphs obtained with graphs in dimension \( \rho \).

Observing that 

\[
\sum_{y \in \mathbb{F}_p} e_p^{-by} = \begin{cases} 
0 & \text{if } b \neq 0 \\
1 & \text{if } b = 0
\end{cases} \quad \sum_{y \in \mathbb{F}_p} e_p^{(uz^{\ell-1}-b)y} = \begin{cases} 
0 & \text{if } b \neq uz^{\ell-1} \\
1 & \text{if } b = uz^{\ell-1}
\end{cases}
\]

we obtain \( W_F(a,0,c) = pW_{p_0}(a) \), and for \( b \neq 0 \), \( W_F(a,b,c) = pW_{p_0}(a)e^{-(b/c)a} \), where \( \rho(\ell - 1) \equiv 1 \mod p - 1 \). Note that \( 1 \leq \rho \leq p - 2 \) is uniquely determined, since \( \gcd(\ell - 1, p - 1) = 1 \). Consequently \( F \) is bent. The property \( F(\alpha(x,y,z)) = \alpha^F(x,y,z) \) for all \( \alpha \in \mathbb{F}_p \) follows with the assumption that \( g_i(ax) = \alpha^F g_i(x) \) holds for all \( \alpha \in \mathbb{F}_p \).

**Remark 4.** If \( g_1 - g_0 \) has degree \( d \), then \( F \) has degree \( d + p - 1 \). The obtained function can be used in a further step to generate bent functions for strongly regular graphs in dimension \( n + 4 \).

Before we give some examples, we interpret the construction in Theorem 2 as a construction of a strongly regular graph from the graphs obtained with \( g_0 \) and \( g_1 \).

By definition of the graph obtained from \( F \), the vertices \( (x,y,z), (x_1,y_1,z_1) \), \( x,x_1 \in V_n, y,y_1,z,z_1 \in \mathbb{F}_p \), are adjacent if and only if \( F(x-x_1,y-y_1,z-z_1) \) is a nonzero square (nonsquare, equal zero). With the observation that

\[
F(x-x_1,y-y_1,z-z_1) = \begin{cases} 
g_0(x-x_1) : z_1 = z, \\
g_1(x-x_1) + u(y-y_1)(z-z_1)^{-1} & z_1 \neq z
\end{cases}
\]

we obtain that \( (x,y,z), (x_1,y_1,z_1) \) are adjacent if and only if \( g_0(x-x_1) \) is a nonzero square (nonsquare, equal zero), i.e. \( x \) and \( x_1 \) are adjacent in the strongly regular graph of \( g_0 \). We remark that for every \( (y,z) \in \mathbb{F}_p \times \mathbb{F}_p \) the set of vertices \( \{(x,y,z) | x \in \mathbb{F}_p \} \) forms a subgraph which is a copy of the strongly regular graph of \( g_0 \).

Again with (7), we obtain that \( (x,y,z), (x_1,y_1,z_1) \), \( z_1 \neq z \), are adjacent if and only if \( g_1(x-x_1) + u(y-y_1)(z-z_1)^{-1} \) is a nonzero square (nonsquare, equal zero), or equivalently

\[
y = y + \frac{g_1(x-x_1) - a}{u(z-z_1)^{-1}}
\]

for a nonzero square \( a \in \mathbb{F}_p \) (nonsquare \( a \in \mathbb{F}_p, a = 0 \)).

We finish with some examples for the construction. We will employ the very well understood class of quadratic bent functions. Note that a quadratic bent function \( f \) always satisfies the condition \( f(ax) = \alpha^F f(x) \) with \( \ell = 2 \). Recall that a quadratic bent function is always weakly regular, and a quadratic function from \( \mathbb{F}_p^n \) to \( \mathbb{F}_p \), \( n \) even, \( p \) odd, of the form \( c_1x_1^2 + c_2x_2^2 + \cdots + c_nx_n^2 \), is a weakly regular, but not a regular bent function, if and only if \( n \equiv 2 \mod 4 \) and \( \Delta := \prod_{i=1}^n c_i \) is a nonzero square in \( \mathbb{F}_p \), or \( n \equiv 0 \mod 4 \) and \( \Delta \) is a non-square in \( \mathbb{F}_p \), see [12]. In our examples we will only consider the (more interesting) case of weakly regular but not regular bent functions, hence they give rise to strongly regular graphs of Negative Latin Square type. The articles [8, 19] contain tables of strongly regular graphs with relevant parameters, which are based on the comprehensive lists [3, 9]. Using MAGMA we determine the size of their automorphism group and the \( p \)-rank of their adjacency matrix, to examine equivalence to the graphs listed in [8, 19], respectively to graphs in the comprehensive list in [3].

**Example 1.** \( g_0(x_1,x_2) = x_1^2 + x_2^2, g_1(x_1,x_2) = 2x_1^2 + 2x_2^2 \in \mathbb{F}_3[x_1,x_2], u = 1. \) Then

\[
F(x_1,x_2,x_3,x_4) = 2x_1^2(2x_2^2 + 2x_3^2) + x_3x_4 + x_1^2 + x_2^2.
\]
For $D^F_k \setminus \{0\}$, the graph has parameters $(\nu, k, \lambda, \mu) = (81, 20, 1, 6)$, the automorphism group has cardinality $|\text{Aut}(D^F_6 \setminus \{0\})| = 232320 = 2^6 \cdot 3^6 \cdot 5$, the $p$-rank is $\wp(D^F_6 \setminus \{0\}) = 81$.

$|\text{Aut}(D^F_8\{x\})| = |\text{Aut}(D^F_8\{x\})| = 116640 = 2^5 \cdot 3^6 \cdot 5$, $\wp(D^F_8) = \wp(D^F_8) = 19$, $(\nu, k, \lambda, \mu) = (81, 30, 9, 12)$.

The examples are of affine polar type, the latter equivalent to an example in [14], see also [19, Section 4.2].

**Example 2.** $p = 3$, $g_0(x_1, x_2, x_3, x_4) = 2x_1^2 + 2x_2^2 + 2x_3^2 + 2x_4^2$, $g_1(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + 2x_3^2 + 2x_4^2$, $u = 1$. Then

$F(x_1, x_2, x_3, x_4) = x_1^2x_2^2 + x_1x_2x_3 + 2x_1x_2x_4 + x_2x_3x_4 + x_2x_3x_4 + x_2x_4x_3 + x_2x_4x_3 + x_2x_4x_3 + x_2x_4x_3$.

$|\text{Aut}(D^F_6 \setminus \{0\})| = 5758272 = 2^7 \cdot 3^{10}$, $\wp(D^F_6 \setminus \{0\}) = 729$, $(\nu, k, \lambda, \mu) = (729, 224, 61, 72)$. $|\text{Aut}(D^F_8)\{x\}| = |\text{Aut}(D^F_8)\{x\}| = 3779136 = 2^6 \cdot 3^{10}$, $\wp(D^F_8) = \wp(D^F_8) = 55$, $(\nu, k, \lambda, \mu) = (729, 252, 81, 90)$.

**Example 3.** $g_0(x_1, x_2) = 2x_1^2 + x_2^2$, $g_1(x_1, x_2) = 3x_1^2 + x_2^2 \in F_5[x_1, x_2]$, $u = 1$. Then

$F(x_1, x_2, x_3, x_4) = x_1^2x_2^4 + x_1x_2x_4 + 2x_1x_2x_4 + x_2x_3x_4 + x_2x_3x_4 + x_2x_4x_3 + x_2x_4x_3 + x_2x_4x_3 + x_2x_4x_3$.

$|\text{Aut}(D^F_6 \setminus \{0\})| = 2^7 \cdot 3^{5} \cdot 13$, $\wp(D^F_6 \setminus \{0\}) = 85$, $(\nu, k, \lambda, \mu) = (625, 104, 3, 20)$.

$|\text{Aut}(D^F_8)\{x\}| = |\text{Aut}(D^F_8)\{x\}| = 3^5 \cdot 5^6$, $\wp(D^F_8) = 94$, $(\nu, k, \lambda, \mu) = (625, 260, 105, 110)$.

Examples 2 and 3 appear to be representations of four graphs in the comprehensive regularly updated list [3]. The next example indicates that our construction potentially yields further graphs.

**Example 4.** $p = 3$, $g_0(x_1, x_2, x_3, x_4, x_5, x_6) = 2x_1^2 + 2x_2^2 + 2x_3^2 + x_2x_4 + x_3x_5 + x_5x_6$, $g_1(x_1, x_2, x_3, x_4, x_5, x_6) = x_1^2 + x_2^2 + 2x_3^2 + 2x_4^2 + x_5 + x_6$, $u = 1$. Then

$F(x_1, x_2, \ldots, x_8) = 2x_1^2(x_1^2 + x_2^2 + 2x_3 + 2x_4^2) + x_7x_8 + 2x_1^2 + 2x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2$.

$|\text{Aut}(D^F_6 \setminus \{0\})| = 2^{26} \cdot 3^{24}$, $\wp(D^F_6 \setminus \{0\}) = 6561$.

$|\text{Aut}(D^F_8)\{x\}| = |\text{Aut}(D^F_8)\{x\}| = 2^{25} \cdot 3^{24}$, $\wp(D^F_8) = \wp(D^F_8) = 104$.

The graphs are not equivalent to a graph in Tables 2-4 given in [19] and graphs in [3].

**Acknowledgment**

The second author is supported by the Austrian Science Fund (FWF) Project no. M 1767-N26.

**References**

[1] A. Bernasconi and B. Codenotti, Spectral analysis of Boolean functions as a graph eigenvalue problem, *IEEE Trans. Comput.*, 58 (1999), 345–351.

[2] A. Bernasconi, B. Codenotti and J. M. VanderKam, A characterization of bent functions in terms of strongly regular graphs, *IEEE Trans. Comput.*, 50 (2001), 984–985.

[3] A. E. Brouwer, Web database of strongly regular graphs, [http://www.win.tue.nl/~aeb/grasgrats HTML](http://www.win.tue.nl/~aeb/grasgrats.html)

[4] A. Çeşmelioğlu and W. Meidl, A Construction of bent functions from plateaued functions, *Des. Codes Cryptogr.*, 66 (2013), 231–242.

[5] A. Çeşmelioğlu, W. Meidl and A. Pott, On the dual of (non)-weakly regular bent functions and self-dual bent functions, *Advances in Mathematics of Communications*, 7 (2013), 425–440.

[6] A. Çeşmelioğlu, W. Meidl and A. Pott, There are infinitely many bent functions for which the dual is not bent, *IEEE Trans. Inform. Theory*, 62 (2016), 5204–5208.

[7] A. Çeşmelioğlu, W. Meidl and A. Pott, Vectorial bent functions and their duals, *Linear Algebra and its Applications*, 548 (2018), 305–320.
[8] Y. M. Chee, Y. Tan and Y. D. Zhang, Strongly regular graphs constructed from $p$-ary bent functions, *J. Algebraic Combin.*, 34 (2011), 251–266.

[9] E. Z. Chen, Web database of two-weight codes, [http://moodle.tec.hkr.se/~chen/research/2-weight-codes/search.php](http://moodle.tec.hkr.se/~chen/research/2-weight-codes/search.php) (online).

[10] E. R. van Dam and M. Muzychuk, Some implications on amorphic association schemes, *J. Combin. Theory Ser. A*, 117 (2010), 111–127.

[11] T. Feng, B. Wen, Q. Xiang and J. Yin, Partial difference sets from quadratic forms and $p$-ary weakly regular bent functions, *Number Theory and Related Areas, Adv. Lect. Math. (ALM)*, Int. Press, Somerville, MA, 27 (2013), 25–40.

[12] T. Helleseth and A. Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic, *IEEE Trans. Inform. Theory*, 52 (2006), 2018–2032.

[13] P. V. Kumar, R. A. Scholtz and L. R. Welch, Generalized bent functions and their properties, *J. Combin. Theory Ser. A*, 40 (1985), 90–107.

[14] J. H. van Lint and A. Schrijver, Constructions of strongly regular graphs, two-weight codes and partial geometries by finite fields, *Combinatorica*, 1 (1981), 63–73.

[15] S. L. Ma, A survey of partial difference sets, *Des., Codes, Cryptogr.*, 4 (1994), 221–261.

[16] S. Mesnager, *Bent Functions. Fundamentals and Results*, Springer, 2016.

[17] K. Nyberg, Perfect nonlinear S-boxes, *Advances in cryptology–EUROCRYPT ’91 (Brighton, 1991)*, 378–386, Lecture Notes in Comput. Sci., 547, Springer, Berlin, 1991.

[18] A. Pott, Y. Tan, T. Feng and S. Ling, Association schemes arising from bent functions, *Des., Codes, Cryptogr.*, 59 (2011), 319–331.

[19] Y. Tan, A. Pott and T. Feng, Strongly regular graphs associated with ternary bent functions, *J. Combin. Theory Ser. A*, 117 (2010), 668–682.

Received for publication May 2017.

*E-mail address*: ayca.cesmelioğlu@altinbas.edu.tr

*E-mail address*: meidlwilfried@gmail.com