Noname manuscript No.
(will be inserted by the editor)

Strongly Regular Graphs Constructed from p-ary Bent Functions

Yeow Meng Chee · Yin Tan · Xian De Zhang

Received: date / Accepted: date

Abstract In this paper, we generalize the construction of strongly regular graphs in [Y. Tan et al., Strongly regular graphs associated with ternary bent functions, J. Combin. Theory Ser. A (2010), 117, 668-682] from ternary bent functions to p-ary bent functions, where p is an odd prime. We obtain strongly regular graphs with three types of parameters. Using certain non-quadratic p-ary bent functions, our constructions can give rise to new strongly regular graphs for small parameters.

Keywords strongly regular graphs · partial difference sets · p-ary bent functions · (weakly) regular bent functions

1 Introduction

Boolean bent functions were first introduced by Rothaus in 1976 in [16]. They have been extensively studied for their important applications in cryptography. Such functions have the maximum Hamming distance to the set of all affine functions. In [11], the authors generalized the notion of a bent function to be defined over a finite field of arbitrary characteristic. Precisely, let f be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. The *Walsh transform* of f is the complex valued function $\mathcal{W}_f : \mathbb{F}_{p^n} \to \mathbb{C}$ defined by

$$\mathcal{W}_f(b) := \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{f(x)+\mathrm{Tr}(bx)}, \quad b \in \mathbb{F}_{p^n},$$

where ζ_p is a primitive p-th root of unity and $\mathrm{Tr}(x)$ is the absolute trace function, i.e. $\mathrm{Tr}(x) := \sum_{i=0}^{n-1} x^{p^i}$. The function f is called *p-ary bent* if every Walsh coefficient $\mathcal{W}_f(b)$ has magnitude $p^{n/2}$, i.e. $|\mathcal{W}_f(b)| = p^{n/2}$ for all $b \in \mathbb{F}_{p^n}$. Moreover, f is called *regular* if there exists some function $f^* : \mathbb{F}_{p^n} \to \mathbb{F}_p$ such that $\mathcal{W}_f(b) = p^{n/2}\zeta_p^{f^*(b)}$, and f is called *weakly regular* if $\mathcal{W}_f(b) = \mu p^{n/2}\zeta_p^{f^*(b)}$ for some constant $\mu \in \mathbb{C}$ with $|\mu| = 1$. Obviously, regularity implies weak regularity.

It is shown in [10,8] that quadratic bent functions and most monomial p-ary bent functions are weakly regular, except one sporadic non-weakly regular example. Recently, a new family of non-quadratic weakly regular p-ary bent functions has been constructed in [9]

Y. M. Chee · Y. Tan · X. Zhang
Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link Singapore 637371, E-mail: itanyinmath@gmail.com
Y. M. Chee, E-mail: ymchee@ntu.edu.sg
X. Zhang, E-mail: xiandezhang@ntu.edu.sg
Y. Tan is currently with Temasek Laboratories, National University of Singapore, 5A Engineering Drive 1, ♯09-02, Singapore 117411.

and a new sporadic non-weakly regular bent function was given. However, there are still few non-quadratic bent functions known over the field $\mathbb{F}_{p^n}$ when $p \geq 5$.

There are many motivations to find more weakly regular bent functions, especially non-quadratic ones. Recently, it is shown in [15], [17] that, under some conditions, weakly regular bent functions can be used to construct certain combinatorial objects, such as strongly regular graphs and association schemes. Precisely, let $f : \mathbb{F}_{3^{2k}} \to \mathbb{F}_3$ be a weakly regular bent function. Define

$$D_i := \{x : x \in \mathbb{F}_{3^{2k}} | f(x) = i\}, \quad 0 \leq i \leq 2.$$

It is shown in [17] that D_0, D_1, D_2 are all regular partial difference sets. The Cayley graphs generated by D_0, D_1, D_2 in the additive group of $\mathbb{F}_{3^{2k}}$ are strongly regular graphs. Some non-quadratic bent functions seem to give rise to new families of strongly regular graphs up to isomorphism (see [17, Tables 2,3]).

In this paper, we generalize the work in [17] by using p-ary bent functions to construct strongly regular graphs. We show that if $f : \mathbb{F}_{p^{2k}} \to \mathbb{F}_p$ satisfying Condition A (defined in Section 3), then the subsets

$$\begin{aligned} D &= \{x \in \mathbb{F}_{p^{2k}}^* | f(x) = 0\}, \\ D_{\mathcal{S}} &= \{x \in \mathbb{F}_{p^{2k}}^* | f(x) \text{ are non-zero squares}\}, \\ D'_{\mathcal{S}} &= \{x \in \mathbb{F}_{p^{2k}}^* | f(x) \text{ are squares}\} \text{ and} \\ D_{\mathcal{N}} &= \{x \in \mathbb{F}_{p^{2k}}^* | f(x) \text{ are non-squares}\} \end{aligned} \tag{1}$$

are regular partial difference sets. Using this construction, it seems that the p-ary bent functions in [9] may give rise to new negative Latin square type strongly regular graphs. For small parameters, we have verified that the graphs are new.

The paper is organized as follows. In Section 2, we give necessary definitions and results. The constructions of strongly regular graphs will be given in Section 3. In Section 4, we discuss the newness of the graphs obtained.

2 Preliminaries

Group rings and character theory are useful tools to study difference sets. We refer to [14] for basic facts of group rings and [12] for character theory on finite fields.

Let G be a multiplicative group of order v. A k-subset D of G is a (v,k,λ,μ) *partial difference set* (PDS) if each non-identity element in D can be represented as gh^{-1} $(g,h \in D, g \neq h)$ in exactly λ ways, and each non-identity element in $G \backslash D$ can be represented as gh^{-1} $(g,h \in D, g \neq h)$ in exactly μ ways. We shall always assume that the identity element 1_G of G is not contained in D. Using the group ring language, a k-subset D of G with $1_G \notin D$ is a (v,k,λ,μ)-PDS if and only if the following equation holds:

$$DD^{(-1)} = (k-\mu)1_G + (\lambda-\mu)D + \mu G. \tag{2}$$

Combinatorial objects associated with partial difference sets are strongly regular graphs. A graph Γ with v vertices is called a (v,k,λ,μ) *strongly regular graph* (SRG) if each vertex is adjacent to exactly k other vertices, any two adjacent vertices have exactly λ common neighbours, and any two non-adjacent vertices have exactly μ common neighbours.

Given a group G of order v and a k-subset D of G with $1_G \notin D$ and $D^{(-1)} = D$, the graph $\Gamma = (V,E)$ defined as follows is called the *Cayley graph* generated by D in G:

(1) The vertex set V is G;
(2) Two vertices g,h are joined by an edge if and only if $gh^{-1} \in D$.

The following result points out the relationship between SRGs and PDSs.

Result 1 ([13]) *Let Γ be the Cayley graph generated by a k-subset D of a multiplicative group G with order v. Then Γ is a (v,k,λ,μ) strongly regular graph if and only if D is a (v,k,λ,μ)-PDS with $1_G \notin D$ and $D^{(-1)} = D$.*

Strongly regular graphs (or partial difference sets) with parameters $(n^2, r(n+\varepsilon), -\varepsilon n + r^2 + 3\varepsilon r, r^2 + \varepsilon r)$ are called of *Latin Square type* if $\varepsilon = -1$, and of *negative Latin Square type* if $\varepsilon = 1$. There are many constructions of SRGs of Latin square type (any collection of $r-1$ mutually orthogonal Latin squares gives rise to such a graph, see [13], for instance), but only a few constructions of negative Latin square type are known. We will show that certain weakly regular p-ary bent functions can be used to construct SRGs of Latin square and of negative Latin square type.

Next we introduce the concept of association schemes. Let V be a finite set of vertices, and let $\{R_0, R_1, \ldots, R_d\}$ be binary relations on V with $R_0 := \{(x,x) : x \in V\}$. The configuration $(V; R_0, R_1, \ldots, R_d)$ is called an *association scheme* of class d on V if the following holds:

(1) $V \times V = R_0 \cup R_1 \cup \cdots \cup R_d$ and $R_i \cap R_j = \emptyset$ for $i \neq j$,
(2) ${}^tR_i = R_{i'}$ for some $i' \in \{0,1,\ldots,d\}$, where ${}^tR_i := \{(x,y) | (y,x) \in R_i\}$. If $i' = i$, we call R_i is *symmetric*,
(3) For $i,j,k \in \{0,1,\ldots,d\}$ and for any pair $(x,y) \in R_k$, the number $|\{z \in V \mid (x,z) \in R_i, (z,y) \in R_j|$ is a constant, which is denoted by p_{ij}^k.

An association scheme is said to be *symmetric* if every R_i is symmetric.

Given an association scheme $(V; \{R_l\}_{0 \le l \le d})$, we can take the union of classes to form graphs with larger sets (this is called *fusion*), but it is not necessarily guaranteed that the fused collection of graphs will form an association scheme on V. If an association scheme has the property that any of its fusions is also an association scheme, then we call the association scheme *amorphic*. Van Dam [7] proved the following result.

Result 2 *Let V be a set of size v, and let $\{G_1, G_2, \ldots, G_d\}$ be an edge-decomposition of the complete graph on V, where each G_i is a strongly regular graph on V. If $G_i, 1 \le i \le d$, are all of Latin square type or all of negative Latin square type, then the decomposition is a d-class amorphic association scheme on V.*

We conclude this section by recording the bent function in [9] as below.

Result 3 *Let $n = 4k$. Then the p-ary function $f(x)$ mapping $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ given by*

$$f(x) = \mathrm{Tr}_n(x^2 + x^{p^{3k}+p^{2k}-p^k+1})$$

is a weakly regular bent function. Moreover, for $b \in \mathbb{F}_{p^n}$ the corresponding Walsh coefficient of $f(x)$ is equal to

$$\mathcal{W}_f(b) = -p^{2k}\zeta_p^{\mathrm{Tr}_k(x_0)/4},$$

where x_0 is a unique solution in $\mathbb{F}_{p^k}$ of the equation

$$b^{p^{2k}+1} + (b^2+x)^{(p^{2k}+1)/2} + b^{p^k(p^{2k}+1)} + (b^2+x)^{p^k(p^{2k}+1)/2} = 0.$$

3 The construction

In this section, we construct SRGs using p-ary bent functions. First we introduce some notations used throughout this section. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a weakly regular p-ary bent function satisfying $f(-x) = f(x)$. Without loss of generality, we may assume $f(0) = 0$. If not, we can replace $f(x)$ with $f(x) - f(0)$. For each $b \in \mathbb{F}_{p^n}$, assume that $\mathcal{W}_f(b) = \mu(\sqrt{p^*})^n \zeta_p^{f^*(b)}$, where $\mu = \pm 1$ and $p^* = (-1)^{\frac{p-1}{2}} p$. Suppose that there exists an integer l with $(l-1, p-1) = 1$ such that for each $\alpha \in \mathbb{F}_p$ and $x \in \mathbb{F}_{p^n}$, $f(\alpha x) = \alpha^l f(x)$ holds. Let

$$D_i := \{x \in \mathbb{F}_{p^n} \mid f(x) = i\}, \quad 0 \le i \le p-1.$$

Denote by G and H the additive groups of $\mathbb{F}_{p^n}$ and $\mathbb{F}_p$ respectively. Clearly we have $\sum_{i=0}^{p-1} D_i = G$. Moreover, $D_i^{(-1)} = D_i$ for each $0 \le i \le p-1$ since $f(-x) = f(x)$. Define the group ring elements in $\mathbb{Z}[\zeta_p](G)$:

$$L_t := \sum_{i=0}^{p-1} D_i \zeta_p^{it},\ 0 \le t \le p-1,$$

in particular $L_0 = \mathbb{F}_{p^n}$. The following result gives some properties of the L_t's (see [15]).

Result 4 (1) *If $s,t,s+t \neq 0$, then $L_tL_s = \mu(\frac{tsv}{p})^n(\sqrt{p^*})^n L_v$ with $s^{1-l}+t^{1-l} = v^{1-l}$;*
(2) *$L_tL_{-t} = p^n$ for $t \in \{1,\ldots,p-1\}$;*
(3) $\sum_{t=1}^{p-1} L_tL_0\zeta_p^{-at} = (p|D_a| - p^n)\mathbb{F}_{p^n}$.

It is clear that we may compute D_i's from L_t's, namely $D_i = \frac{1}{p}\sum_{t=0}^{p-1} L_t\zeta_p^{-it}$. By Result 4, we have

$$\begin{aligned}
p^2 D_aD_b &= \sum_{s,t=0}^{p-1} L_tL_s\zeta_p^{-at-bs} \\
&= L_0^2 + \sum_{\substack{s,t\neq 0\\ s+t\neq 0}} L_tL_s\zeta_p^{-at-bs} + \sum_{s=1}^{p-1} L_sL_{-s}\zeta_p^{s(a-b)} + \sum_{s=1}^{p-1} L_sL_0\zeta_p^{-bs} + \sum_{t=1}^{p-1} L_tL_0\zeta_p^{-at} \\
&= p^n\mathbb{F}_{p^n} + \sum_{\substack{s,t,s+t\neq 0\\ s^{1-l}+t^{1-l}=v^{1-l}}} \mu(\tfrac{tsv}{p})^n(\sqrt{p^*})^n\zeta_p^{-at-bs}L_v + \sum_{s=1}^{p-1} p^n\zeta_p^{s(a-b)} + (p|D_b| - p^n)\mathbb{F}_{p^n} \\
&\quad + (p(|D_a| - p^n)\mathbb{F}_{p^n} \\
&= \sum_{s=1}^{p-1} p^n\zeta_p^{s(a-b)} + (p(|D_a| + |D_b|) - p^n)\mathbb{F}_{p^n} + \sum_{\substack{s,t,s+t\neq 0\\ s^{1-l}+t^{1-l}=v^{1-l}}} \mu(\tfrac{tsv}{p})^n(\sqrt{p^*})^n\zeta_p^{-at-bs}L_v.
\end{aligned} \tag{3}$$

In the following we only work on the field $\mathbb{F}_{p^n}$ with $n = 2k$. Note that in this case the Walsh coefficient of f can be written as the form $\mathcal{W}_f(b) = (-1)^{\frac{(p-1)k}{2}}\mu p^k\zeta_p^{f^*(b)}$. For each $b \in \mathbb{F}_{p^{2k}}$, let χ_b be the additive character of G defined by $\chi_b(x) = \zeta_p^{\mathrm{Tr}(bx)}$, and η be the additive character of H defined by $\eta(x) = \zeta_p^x$. Now for each $b \in \mathbb{F}_{p^n}$,

$$\mathcal{W}_f(b) = \sum_{x\in\mathbb{F}_{p^{2k}}} \zeta_p^{f(x)+\mathrm{Tr}(bx)} = \sum_{i=0}^{p-1}(\sum_{x\in D_i}\zeta_p^{\mathrm{Tr}(bx)})\zeta_p^i = \sum_{i=0}^{p-1}\chi_b(D_i)\zeta_p^i = \chi_b\eta(R),$$

where $R = \{(x, f(x)) : x \in \mathbb{F}_{p^{2k}}\}$. Since f is a bent function, we know that $|\chi_b\eta(R)| = |\mathcal{W}_f(b)| = p^k$.

First we determine the cardinalities of D_i's.

Lemma 1 *Let $f : \mathbb{F}_{p^{2k}} \to \mathbb{F}_p$ be the bent function as above. Then*
(1) $|D_1| = |D_2| = \cdots = |D_{p-1}|$,
(2) *$|D_0| = p^{2k-1} + \varepsilon(p^k - p^{k-1})$ and $|D_i| = p^{2k-1} - \varepsilon p^{k-1}$ for each $1 \le i \le p-1$, where $\varepsilon = (-1)^{\frac{(p-1)k}{2}}\mu$.*

Proof (1) For any $1 \le a,b \le p-1$, by Result 4 (3) we have

$$(p|D_a| - p^{2k})\mathbb{F}_{p^{2k}} = \sum_{t=1}^{p-1} L_tL_0\zeta_p^{-at} = \sum_{t=1}^{p-1} L_tL_0(\zeta_p^{ab^{-1}})^{-bt} = (p|D_b| - p^{2k})\mathbb{F}_{p^{2k}}.$$

The last equality holds since $\zeta_p^{ab^{-1}}$ is also a primitive p-th root of unity. Thus $|D_a| = |D_b|$.

(2) Let χ_0 be the principal character of $\mathbb{F}_{p^{2k}}$, we have

$$\chi_0\eta(R) = |D_0| + \sum_{i=1}^{p-1} |D_i|\zeta_p^i = |D_0| + |D_1|(\zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1}) = |D_0| - |D_1|.$$

Since $\chi_b\eta(R) = \mathcal{W}_f(b) = (-1)^{\frac{(p-1)k}{2}}\mu p^k \zeta_p^{f^*(b)} = \varepsilon p^k \zeta_p^{f^*(b)}$ and $|D_0| - |D_1|$ is a rational integer, we have

$$|D_0| - |D_1| = \varepsilon p^k. \tag{4}$$

On the other hand,

$$|D_0| + (p-1)|D_1| = p^{2k}. \tag{5}$$

By solving Eqs. (4) and (5), the result follows.

Next, we define Condition A for a function f as follows.

Condition A: Let $f : \mathbb{F}_{p^{2k}} \to \mathbb{F}_p$ be a weakly regular bent function with $f(0) = 0$ and $f(-x) = f(x)$, where p is an odd prime. There exists an integer l with $(l-1, p-1) = 1$ such that $f(\alpha x) = \alpha^l f(x)$ for any $\alpha \in \mathbb{F}_p$ and $x \in \mathbb{F}_{p^{2k}}$. For each $b \in \mathbb{F}_{p^{2k}}$, $\mathcal{W}_f(b) = \varepsilon p^k \zeta_p^{f^*(b)}$, where $\varepsilon = (-1)^{\frac{(p-1)k}{2}}\mu$ with $\mu = \pm 1$.

Two functions $f, g : \mathbb{F}_{p^n} \to \mathbb{F}_p$ are called *affine equivalent* if there exist an affine permutation A_1 of $\mathbb{F}_p$ and an affine permutation A_2 of $\mathbb{F}_{p^n}$ such that $g = A_1 \circ f \circ A_2$. Furthermore, they are called *extended affine equivalent (EA-equivalent)* if $g = A_1 \circ f \circ A_2 + A$, where $A : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is an affine function. A polynomial L of the form $L(x) = \sum_{i=0}^{n} a_i x^{p^i} \in \mathbb{F}_p[x]$ is called a *linearized polynomial*. Note that the affine permutations of $\mathbb{F}_p$ are $cx + d$, where $c \in \mathbb{F}_p^*$ and $d \in \mathbb{F}_p$.

We have the following result.

Proposition 1 *Let $L_1, L_2 \in \mathbb{F}_p[x]$ be linearized polynomials, where L_1 is a permutation of $\mathbb{F}_p$ and L_2 is a permutation of $\mathbb{F}_{p^{2k}}$. If $L_1(1) \neq 0$ and f satisfies Condition A, then the function $g = L_1 \circ f \circ L_2$ satisfies Condition A.*

Proof That $g(0) = 0, g(-x) = g(x)$ and $g(\alpha x) = \alpha^l g(x)$ for $\alpha \in \mathbb{F}_p$ are easy to be verified. We only need to prove that for each $b \in \mathbb{F}_{p^{2k}}$, $\mathcal{W}_g(b) = \varepsilon p^k \zeta_p^{g^*(b)}$, where $\varepsilon = (-1)^{\frac{(p-1)k}{2}}\mu$ with $\mu = \pm 1$. First assume that $L_1(x) = cx$. Note that $L_1(1) \neq 0$ implies that $c \neq 0$ and ζ_p^c is also a primitive p-th root of unity. Now

$$\begin{aligned}
\mathcal{W}_g(b) &= \sum_{x \in \mathbb{F}_{p^{2k}}} \zeta_p^{L_1(f(L_2(x)) + \mathrm{Tr}(bx))} = \sum_{x \in \mathbb{F}_{p^{2k}}} (\zeta_p^c)^{f(L_2(x)) + \mathrm{Tr}(c^{-1}bx)} \\
&= \sum_{y \in \mathbb{F}_{p^{2k}}} (\zeta_p^c)^{f(y) + \mathrm{Tr}(c^{-1}bL_2^{-1}(y)} = \sum_{y \in \mathbb{F}_{p^{2k}}} (\zeta_p^c)^{f(y) + \mathrm{Tr}((L_2^{-1})^\star(c^{-1}b)y)} \\
&= \mathcal{W}_f((L_2^{-1})^\star(c^{-1}b)) = \varepsilon p^k \zeta_p^{f^*((L_2^{-1})^\star(c^{-1}b))},
\end{aligned}$$

where $(L_2^{-1})^\star$ is the adjoint operator of L_2^{-1}. We finish the proof.

Remark 1 Clearly the function g in the above Proposition is affine equivalent to f. However, for a function g which is EA-equivalent but not affine equivalent to f, it may be seen that g does not satisfy Condition A. Indeed, assume that $g = A_1 \circ f \circ A_2 + A$, then $g(\alpha x) \neq \alpha^{l-1} g(x)$ for $\alpha \in \mathbb{F}_p$ when $l > 2$.

Now assume that a function $f : \mathbb{F}_{p^{2k}} \to \mathbb{F}_p$ satisfies Condition A, then clearly the functions $L_1 \circ f \circ L_2$ all satisfy Condition A, where $L_1, L_2 \in \mathbb{F}_p[x]$ are linearized polynomials, and L_1 is a permutation of $\mathbb{F}_p$, L_2 is a permutation of $\mathbb{F}_{p^{2k}}$. We see that the functions of the form $L_1 \circ f \circ L_2$ are affine equivalent to f. However, for a function g which is EA-equivalent but not affine equivalent to f, it may be seen that g does not satisfy Condition A.

Now we will prove the first result in this section.

Theorem 1 *Let f be a function satisfying condition A. Let*

$$D := \{x : x \in \mathbb{F}^*_{p^{2k}} | f(x) = 0\}.$$

Then D is a $(v,d,\lambda_1,\lambda_2)$-PDS, where

$$\begin{array}{ll} v &= p^{2k}, \\ d &= (p^k-\varepsilon)(p^{k-1}+\varepsilon), \\ \lambda_1 &= (p^{k-1}+\varepsilon)^2 - 3\varepsilon(p^{k-1}+\varepsilon) + \varepsilon p^k, \\ \lambda_2 &= (p^{k-1}+\varepsilon)p^{k-1}. \end{array} \tag{6}$$

Proof Recall that $L_t = \sum_{i=0}^{p-1} D_i \zeta_p^{it}$. By Eq. (3), we have:

$$p^2 D_0 D_0 = (p-1)p^{2k} + (2p|D_0| - p^{2k})\mathbb{F}_{p^{2k}} + \varepsilon \sum_{\substack{s,t,s+t\neq 0 \\ s^{1-l}+t^{1-l}=v^{1-l}}} p^k L_v, \tag{7}$$

Now we compute the last term of Eq. (7).

$$\begin{aligned} \sum_{\substack{s,t,s+t\neq 0 \\ s^{1-l}+t^{1-l}=v^{1-l}}} p^k L_v &= p^k \sum_{i=1}^{p-1} (p-2)L_i \\ &= (p-2)p^k \sum_{i=1}^{p-1} (D_0 + \sum_{j=1}^{p-1} D_j \zeta_p^{ji}) \\ &= (p-2)p^k ((p-1)D_0 + \sum_{j=1}^{p-1} D_j (\sum_{i=1}^{p-1} \zeta_p^{ji})) \\ &= (p-2)p^k ((p-1)D_0 - \sum_{j=1}^{p-1} D_j) \\ &= (p-2)p^k ((p-1)D_0 - (\mathbb{F}_{p^{2k}} - D_0)) \\ &= (p-2)p^k (pD_0 - \mathbb{F}_{p^{2k}}). \end{aligned} \tag{8}$$

Substituting Eq. (8) in Eq. (7), we have

$$\begin{aligned} p^2 D_0 D_0 &= (p-1)p^{2k} + (2p|D_0| - p^{2k})\mathbb{F}_{p^{2k}} + \varepsilon(p-2)p^k(pD_0 - \mathbb{F}_{p^{2k}}) \\ &= (p-1)p^{2k} + \varepsilon p^{k+1}(p-2)D_0 + (2p|D_0| - p^{2k} - \varepsilon(p-2)p^k)\mathbb{F}_{p^{2k}}. \end{aligned} \tag{9}$$

Note that $D + 0 = D_0$ and $|D_0| = p^{2k-1} + \varepsilon(p^k - p^{k-1})$ (Lemma 1), by Eq. (9) we have

$$p^2(D+0)^2 = (p-1)p^{2k} + \varepsilon p^{k+1}(p-2)(D+0) + (2p|D_0| - p^{2k} - \varepsilon(p-2)p^k)\mathbb{F}_{p^{2k}}.$$

After simplifying, we get the equation

$$D^2 = (p^{2k-1} - p^{2k-2} + \varepsilon p^k - 2\varepsilon p^{k-1} - 1) + (\varepsilon p^k - 2\varepsilon p^{k-1} - 2)D + (\varepsilon p^{k-1} + p^{2k-2})\mathbb{F}_{p^{2k}}.$$

By Eq. (2), the proof is done.

Remark 2 When $\varepsilon = -1$ in Theorem 1, we get negative Latin square type SRGs. When $p = 3$, some new SRGs arise using non-quadratic ternary bent functions; see [17, Tables 2,3]. Unfortunately, when $p \geq 5$, for the known bent functions, we don't get new graphs.

To give another construction of SRGs using p-ary bent functions, we show two lemmas first.

Lemma 2 *Let S and T be the sets of non-zero squares and non-squares in $\mathbb{F}_p$ respectively, where p is an odd prime. Then we have*

(1) *when $p \equiv 1 \pmod 4$,*

$$\begin{aligned} S^2 &= \tfrac{p-1}{2} + \tfrac{p-5}{4}S + \tfrac{p-1}{4}T, \\ T^2 &= \tfrac{p-1}{2} + \tfrac{p-1}{4}S + \tfrac{p-5}{4}T, \\ ST &= TS = \tfrac{p-1}{4}(S+T); \end{aligned}$$

(2) *when $p \equiv 3 \pmod 4$,*

$$\begin{aligned} S^2 &= \tfrac{p-3}{4}S + \tfrac{p+1}{4}T, \\ T^2 &= \tfrac{p+1}{4}S + \tfrac{p-3}{4}T, \\ ST &= TS = \tfrac{p+1}{4} + \tfrac{p-3}{4}\mathbb{F}_p. \end{aligned}$$

Proof (1) Note that -1 is a square when $p \equiv 1 \pmod 4$ and $S^{(-1)} = S, T^{(-1)} = T$ in this case. By [1, Theorem 2], S is a $(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{2})$ almost difference set in $\mathbb{F}_p$, which implies that

$$SS^{(-1)} = S^2 = \frac{p-1}{2} + \frac{p-5}{4}S + \frac{p-1}{4}T.$$

It is easy to see that $T = \mathbb{F}_p - 0 - S$, and hence $TT^{(-1)} = T^2 = (\mathbb{F}_p - 0 - S)^2$. Now the results can be followed by direct computation.

(2) When $p \equiv 3 \pmod 4$, -1 is a non-square, and $S^{(-1)} = T, T^{(-1)} = S$. It is well known that the subset S is a $(p, \frac{p-1}{2}, \frac{p-3}{4})$ difference set in $\mathbb{F}_p$. Hence

$$SS^{(-1)} = ST = \frac{p+1}{4} + \frac{p-3}{4}\mathbb{F}_p.$$

The computations are similar to those in (1).

Lemma 3 *Let ζ_p be a primitive p-th root of unity, S and T be the sets of non-zero squares and non-squares of $\mathbb{F}_p$ respectively. Define $m = \sum_{i\in S}\zeta_p^{-i}$, then*

(1) when $p \equiv 1 \pmod 4$, $-m(1+m) = -\frac{p-1}{4}$;

(2) when $p \equiv 3 \pmod 4$, $-m(1+m) = \frac{p+1}{4}$.

Proof We only prove the case $p \equiv 1 \pmod 4$, the proof of (2) is similar. Note that $-(1+m) = \sum_{i\in T}\zeta_p^{-i}$, hence $-m(1+m) = \sum_{i\in S, j\in T}\zeta_p^{-(i+j)}$. By Lemma 2 (1), we know that $\sum_{i\in S, j\in T}\zeta_p^{-(i+j)} = \frac{p-1}{4}\sum_{i\in\mathbb{F}_p^*}\zeta_p^{-i} = -\frac{p-1}{4}$.

Now we prove the following result.

Theorem 2 *Let f be a function satisfying Condition A. Let*

$$D_S := \{x : x \in \mathbb{F}_{p^{2k}}^* | f(x) \text{ are non-zero squares}\},$$

then D_S is a $(v, d, \lambda_1, \lambda_2)$-PDS, where

$$\begin{aligned} v &= p^{2k}, \\ d &= \tfrac{1}{2}(p^k - p^{k-1})(p^k - \varepsilon), \\ \lambda_1 &= \tfrac{1}{4}(p^k - p^{k-1})^2 - \tfrac{3\varepsilon}{2}(p^k - p^{k-1}) + p^k\varepsilon, \\ \lambda_2 &= \tfrac{1}{2}(p^k - p^{k-1})(\tfrac{1}{2}(p^k - p^{k-1}) - \varepsilon). \end{aligned} \tag{10}$$

Proof We only prove the case $p \equiv 1 \pmod 4$, the proof of the case $p \equiv 3 \pmod 4$ is similar. Let S and T be the sets of non-zero squares and non-squares of $\mathbb{F}_p$ respectively. Now by Eq. (3), we have

$$\begin{aligned} p^2 D_S^2 &= p^2 \sum_{a,b\in S} D_a D_b \\ &= \sum_{a,b\in S} (\sum_{s=1}^{p-1} p^{2k} \zeta_p^{s(a-b)} + (2p|D_1| - p^{2k})\mathbb{F}_{p^{2k}} + \varepsilon p^k \sum_{\substack{s,t,s+t\neq 0 \\ s^{1-l}+t^{1-l}=v^{1-l}}} \zeta_p^{-at-bs} L_v). \end{aligned} \tag{11}$$

Now

$$\begin{aligned} &\sum_{a,b\in S} (\sum_{s=1}^{p-1} p^{2k} \zeta_p^{s(a-b)}) = \tfrac{p^{2k}(p-1)(p+1)}{4}, \\ &\sum_{a,b\in S} (2p|D_1| - p^{2k})\mathbb{F}_{p^{2k}} = (\tfrac{p(p-1)^2}{2}|D_1| - \tfrac{p^{2k}(p-1)^2}{4})\mathbb{F}_{p^{2k}}. \end{aligned} \tag{12}$$

To compute the third term in Eq. (11), for $s,t \in \mathbb{F}_p^*$, we define $\delta(s,t)$ as follows

$$\delta(s,t) = \begin{cases} m^2 & \text{if } s,t \text{ both are squares} \\ (1+m)^2 & \text{if } s,t \text{ both are nonsquares} \\ -m(1+m) & \text{others,} \end{cases}$$

where $m = \sum_{i\in S} \zeta_p^{-i}$. For convenience, denote the set $\{(s,t) : s,t \in \mathbb{F}_p | s \neq 0, t \neq 0, s+t \neq 0\}$ by Ω. For $s,t,s+t \neq 0$, define the function $\sigma(s,t) = v$, where $s^{1-l} + t^{1-l} = v^{1-l}$. Since $(l-1, p-1) = 1$, σ is well defined. Now we compute the third term of Eq. (11):

$$\begin{aligned} &\sum_{a,b\in S} \sum_{(s,t)\in\Omega} \zeta_p^{-at-bs} L_{\sigma(s,t)} \\ = &\sum_{(s,t)\in\Omega} (\sum_{a\in S} (\zeta_p^{-t})^a)(\sum_{b\in S} (\zeta_p^{-s})^b) L_{\sigma(s,t)} = \sum_{(s,t)\in\Omega} \delta(s,t) L_{\sigma(s,t)} \\ = &\sum_{(s,t)\in\Omega\cap(S\times S)} m^2 L_{\sigma(s,t)} + \sum_{(s,t)\in\Omega\cap(T\times T)} (1+m)^2 L_{\sigma(s,t)} - \sum_{\substack{(s,t)\in \\ \Omega\setminus((S\times S)\cup(T\times T))}} m(1+m) L_{\sigma(s,t)}. \end{aligned} \tag{13}$$

By Lemma 2(1), we know that the multiset $\{* \ \sigma(s,t) : (s,t) \in \Omega \cap (S\times S) \ *\} = \frac{p-5}{4} S + \frac{p-1}{4} T$, then

$$\sum_{(s,t)\in\Omega\cap(S\times S)} m^2 L_{\sigma(s,t)} = m^2 (\frac{p-5}{4} \sum_{v\in S} L_v + \frac{p-1}{4} \sum_{v\in T} L_v).$$

Using similar argument, we can compute the last two terms of Eq. (13). Then we have

$$\begin{aligned} &\textstyle\sum_{a,b\in S} \sum_{(s,t)\in\Omega} \zeta_p^{-at-bs} L_{\sigma(s,t)} \\ = \ & m^2 (\tfrac{p-5}{4} \textstyle\sum_{v\in S} L_v + \tfrac{p-1}{4} \sum_{v\in T} L_v) + (1+m)^2 (\tfrac{p-1}{4} \sum_{v\in S} L_v + \tfrac{p-5}{4} \sum_{v\in T} L_v) \\ & -2m(1+m)(\tfrac{p-1}{4} \textstyle\sum_{v\in\mathbb{F}_p^*} L_v), \\ = \ & A \textstyle\sum_{v\in S} L_v + B \sum_{v\in T} L_v, \end{aligned} \tag{14}$$

where $A = \frac{p-5}{4} m^2 + \frac{p-1}{4}(1+m)^2 - \frac{p-1}{2} m(1+m)$ and $B = \frac{p-1}{4} m^2 + \frac{p-5}{4}(1+m)^2 - \frac{p-1}{2} m(1+m)$. Now we see that

$$\begin{aligned} \sum_{a,b\in S} \sum_{(s,t)\in\Omega} \zeta_p^{-at-bs} L_{\sigma(s,t)} &= A \textstyle\sum_{v\in S} L_v + B \sum_{v\in T} L_v \\ &= A \textstyle\sum_{v\in S} (\sum_{i=0}^{p-1} D_i \zeta_p^{vi}) + B \sum_{v\in T} (\sum_{i=0}^{p-1} D_i \zeta_p^{vi}) \\ &= \textstyle\sum_{i=0}^{p-1} (A \sum_{v\in S} \zeta_p^{vi} + B \sum_{v\in T} \zeta_p^{vi}) D_i. \end{aligned} \tag{15}$$

Denote $a_i = A\sum_{v\in S}\zeta_p^{vi} + B\sum_{v\in T}\zeta_p^{vi}$ for $0 \le i \le p-1$. Clearly,

$$\begin{aligned} a_0 &= \tfrac{p-1}{2}(A+B) \\ &= \tfrac{p-1}{2}(-2m^2-2m+\tfrac{p-3}{2}) \\ &= -(p-1)m(1+m)+\tfrac{(p-1)(p-3)}{4} \\ &= -\tfrac{(p-1)^2}{4}+\tfrac{(p-1)(p-3)}{4} \\ &= -\tfrac{p-1}{2}. \end{aligned}$$

Similarly, we get the following:

$$a_i = \begin{cases} -(p-1)/2 & i \in \{0\}\cup T, \\ (p+1)/2 & i \in S. \end{cases}$$

Now

$$\sum_{a,b\in S}\sum_{(s,t)\in\Omega}\zeta_p^{-at-bs}L_{\sigma(s,t)} = -\tfrac{p-1}{2}(\mathbb{F}_{p^{2k}}-D_S)+\tfrac{p+1}{2}D_S\,. \tag{16}$$

By Eqs. (11), (12) and (16), we know that

$$\begin{aligned} & p^2D_SD_S^{(-1)} = p^2D_S^2 \\ = \;& \tfrac{p^{2k}(p-1)(p+1)}{4}+(\tfrac{p(p-1)^2}{2}|D_1|-\tfrac{p^{2k}(p-1)^2}{4})\mathbb{F}_{p^{2k}}+\varepsilon p^k(-\tfrac{p-1}{2}(\mathbb{F}_{p^{2k}}-D_S)+\tfrac{p+1}{2}D_S) \\ = \;& C_1+C_2D_S+C_3\mathbb{F}_{p^{2k}}, \end{aligned}$$

where $C_1 = \frac{1}{4}p^{2k}(p-1)(p+1), C_2 = p^{k+1}\varepsilon$ and $C_3 = \frac{1}{4}p^{2k}(p-1)^2 - \frac{1}{2}p^{k+1}(p-1)\varepsilon$. The proof follows by Eq. (2).

Remark 3 (1) Using similar proof, we may also prove that the set

$$D_{\mathcal{N}} := \{x : x \in \mathbb{F}_{p^{2k}}^* | f(x) \text{ are non-squares}\}$$

is a PDS with the same paramters as in Theorem 2.

(2) In [17], it is shown that for weakly regular ternary bent function $f : \mathbb{F}_{3^{2k}} \to \mathbb{F}_3$, the set $D_i := \{x \in \mathbb{F}_{3^{2k}}^* | f(x) = i\}$ is a partial difference set for each $0 \le i \le 2$. We may see that Theorem 2 is the generalization of the result in [17].

With a small modification, we may get the following result.

Theorem 3 *Let f be a function satisfying Condition A. Let*

$$D_S' := \{x : x \in \mathbb{F}_{p^{2k}}^* | f(x) \textit{ are squares}\},$$

then D_S' is a $(v,d,\lambda_1,\lambda_2)$-PDS, where

$$\begin{aligned} & v = p^{2k}, \\ & d = \tfrac{1}{2}(p^k+p^{k-1}+2\varepsilon)(p^k-\varepsilon), \\ & \lambda_1 = \tfrac{1}{4}(p^k+p^{k-1}+2\varepsilon)^2 - \tfrac{3\varepsilon}{2}(p^k+p^{k-1}+2\varepsilon)+p^k\varepsilon, \\ & \lambda_2 = \tfrac{1}{4}(p^k+p^{k-1})(p^k+p^{k-1}+2\varepsilon). \end{aligned} \tag{17}$$

Proof Clearly $D_S' = D+D_S$, where $D = \{x : x \in \mathbb{F}_{p^{2k}}^* | f(x) = 0\}$. Then $D_S'(D_S')^{(-1)} = (D_S+D)(D_S+D)$. The result follows from Theorems 1, 2 and similar group ring computations as those in Theorem 2.

Remark 4 By using MAGMA, we know that Theorems 1, 2, 3 are not true for non-weakly regular bent function $f(x) = \mathrm{Tr}(\xi^7 x^{98})$ over $\mathbb{F}_{3^6}$, where ξ is a primitive element of $\mathbb{F}_{3^6}$. This implies that the weakly regular condition is necessary.

We conclude this section by a result on association schemes. Combining Result 2 and Theorems 1,2,3, we have the following result.

Theorem 4 *Let f be a function satisfying Condition A. Define the following sets:*

$$\begin{aligned} D &= \{x : x \in \mathbb{F}_{p^{2k}}^* | f(x) = 0\}, \\ D_{\mathcal{S}} &= \{x : x \in \mathbb{F}_{p^{2k}}^* | f(x) \text{ are non-zero squares}\}, \\ D_{\mathcal{N}} &= \{x : x \in \mathbb{F}_{p^{2k}}^* | f(x) \text{ are non-squares}\}. \end{aligned}$$

Then $\{\mathbb{F}_{p^{2k}}; \{0\}, D, D_{\mathcal{S}}, D_{\mathcal{N}}\}$ is an amorphic association scheme of class 3.

4 Newness

In this section, we discuss the known constructions of the SRGs with parameters (10) and (17). Since there are many constructions of the Latin square type SRGs, we only discuss the newness of the negative Latin square type SRGs with the above parameters, namely, $\varepsilon = -1$ in parameters (10) and (17).

One may check the known constructions of the SRGs with the parameters (10), (17) via the online database [2]. It is well known that projective two-weight codes can be used to construct SRGs ([3]), one can check the known constructions of two-weight codes via the online database [4]. Next we give the following constructions of SRGs with parameters (10) and (17).

Result 5 *[3] Let $k = 2m$ and Q be a non-degnerate quadratic form on $\mathbb{F}_q$ with q odd. Let*

$$M = \{v \in \mathbb{F}_q^k \setminus \{0\} | \mathrm{Tr}(Q(v)) \text{ are non-zero squares}\},$$

and

$$M' = \{v \in \mathbb{F}_q^k \setminus \{0\} | \mathrm{Tr}(Q(v)) \text{ are squares}\}.$$

Then:

(1) *the Cayley graph generated by M in $(\mathbb{F}_q^k, +)$ is a $(p^{2k}, \frac{1}{2}(p^k - p^{k-1})(p^k - \varepsilon), \frac{1}{4}(p^k - p^{k-1})^2 - \frac{3\varepsilon}{2}(p^k - p^{k-1}) + p^k\varepsilon, \frac{1}{2}(p^k - p^{k-1})(\frac{1}{2}(p^k - p^{k-1}) - \varepsilon))$ strongly regular graph, where $\varepsilon = \pm 1$ and depends on Q.*

(2) *the Cayley graph generated by M' in $(\mathbb{F}_q^k, +)$ is a $(p^{2k}, \frac{1}{2}(p^k + p^{k-1} + 2\varepsilon)(p^k - \varepsilon), \frac{1}{4}(p^k + p^{k-1} + 2\varepsilon)^2 - \frac{3\varepsilon}{2}(p^k + p^{k-1} + 2\varepsilon) + p^k\varepsilon, \frac{1}{4}(p^k + p^{k-1})(p^k + p^{k-1} + 2\varepsilon))$ strongly regular graph, where $\varepsilon = \pm 1$ and depends on Q.*

The SRGs constructed by Result 5 (1) are called *FE1*, and the SRGs from Result 5 (2) are called *RT2* in [3]. They both are also called *affine polar graphs* in [6, P. 852]. To the best of our knowledge, affine polar graphs are the only known infinitive construction of the SRGs with parameters (10) and (17) when $p \geq 5$.

For small parameters, now we discuss the known constructions of the SRGs with parameters (10) and (17).

When $p = 3$, by Theorem 2 and the bent function in Result 3, in field $\mathbb{F}_{3^8}$, we get an SRG with parameter $(6561, 2214, 729, 756)$. Computed by MAGMA, the order of its automorphism group and the 3-rank of the adjacent matrix of the SRG are $(2^4 \cdot 3^8, 566)$. By comparing to [17, Table 4], we know that this graph is new.

When $p = 5$, in the field $\mathbb{F}_{5^4}$, the known constructions of the SRGs with parameters $(625, 260, 105, 110), (625, 364, 213, 210)$ are affine polar graphs, or from Theorems 2,3, or from the projective two weight codes in Chen ([5]). It is verified that Chen's SRGs are isomorphic to affine polar graphs and the SRGs from the bent function in Result 3 are new.

When $p = 7$, in the field $\mathbb{F}_{7^4}$, the known constructions of the SRGs with parameters $(2401, 1050, 455, 462), (2401, 1350, 761, 756)$ are the same as the case $p = 5$. Using

MAGMA, it is verified that Chen's SRGs ([5]) are also isomorphic to affine polar graphs and the SRGs from the bent function in Result 3 are new.

In the following two tables, we give some computational results of the SRGs from different constructions. In the first column, we list the parameters of the SRGs. The group $Aut(\mathcal{G})$ is the full automorphism group of the SRG $\mathcal{G}$, and M denotes an adjacency matrix of $\mathcal{G}$, to be considered in $\mathbb{F}_p$. The abbreviation *n.L.* means the SRG is of negative Latin square type. The symbol $\heartsuit$ means the SRG is constructed by the bent function in Result 3.

Table 1 SRGs with parameters (10)

(v,k,λ,μ)	Type	Rank of M	$\lvert Aut(\mathcal{G})\rvert$	note
$(625,260,105,110)$	n.L.	86	$2^6\cdot 3\cdot 5^6\cdot 13$	affine polar
$(625,260,105,110)\heartsuit$	n.L.	104	$2^4\cdot 5^4$	new
$(2401,1050,455,462)$	n.L.	237	$2^6\cdot 3^2\cdot 5^2\cdot 7^6$	affine polar
$(2401,1050,455,462)\heartsuit$	n.L.	335	$2^3\cdot 3\cdot 7^4$	new

Table 2 SRGs with parameters (17)

(v,k,λ,μ)	Type	Rank of M	$\lvert Aut(\mathcal{G})\rvert$	note
$(625,364,213,210)$	n.L.	625	$2^6\cdot 3\cdot 5^6\cdot 13$	affine polar
$(625,364,213,210)\heartsuit$	n.L.	625	$2^4\cdot 5^4$	new
$(2401,1350,761,756)$	n.L.	2401	$2^6\cdot 3^2\cdot 5^2\cdot 7^6$	affine polar
$(2401,1350,761,756)\heartsuit$	n.L.	2401	$2^3\cdot 3\cdot 7^4$	new

Remark 5 From Tables 1 and 2, we conjecture that the bent functions in Result 3 can give a family of SRGs of negative Latin square type which are not isomorphic to the affine polar graphs. It is difficult to prove it in general cases.

We may see that the automorphism groups of the Cayley graphs generated by the PDSs in (1) have the subgroup of order p^{2k} coming from translations $\tau_c : x \mapsto x+c$ for any $c \in \mathbb{F}_{p^{2k}}$ and the subgroup of order $2k$ coming from the Galois automorphism of $\mathbb{F}_{p^{2k}}$. This means that $2kp^{2k}$ divides the order of the automorphism groups of the Cayley graphs of (1). For the bent functions given by Result (3), we conjecture that $|Aut(\mathcal{G}(X))|$ is not divisible by p^{2k+1}, where $X = D_S$ or D'_S. This is a possible method to prove that they are new.

Acknowledgements Research supported by the National Research Foundation of Singapore under Research Grant NRF-CRP2-2007-03 and by the Nanyang Technological University under Research Grant M58110040. The authors would like to thank Professor Alexander Pott for helpful discussions. They are also indebted to one of the anonymous referees to point out the result in Proposition 1 and the two subgroups of the automorphism groups of the SRGs in this paper.

References

1. Arasu, K., Ding, C., Helleseth, T., Kumer, P. and Martinsen, H., Almost difference sets and their sequences with optimal autocorrelation, IEEE Trans. Inform. Theory 47, 2934–2943, (2001).
2. Brouwer, A., Web database of strongly regular graphs, http://www.win.tue.nl/~aeb/graphs/srg/srgtab.html (online).
3. Calderbank, R. and Kantor, W., The geometry of two-weight codes, Bull. London Math. Soc. 18 (2), 97–122, (1986).
4. Chen, E., Web database of two-weight codes, http://moodle.tec.hkr.se/~chen/research/2-weight-codes/search.php (online).
5. Chen, E., Construction of two-weight codes, internal reports, (2008).
6. Colbourn, C. and Dinitz, J., Handbook of Combinatorial Designs, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, second edition, (2007).
7. Edwin, R., van D., Strongly regular decompositions of the complete graph, J. Algebraic Combin. 17 (2), 181–201, (2003).
8. Helleseth, T., Hollmann, H., Kholosha, A., Wang, Z. and Xiang, Q., Proofs of two conjectures on ternary weakly regular bent functions, IEEE Trans. Inform. Theory 55 (5), 5272–5283, (2009).

9. Helleseth, T. and Kholosha, A., New binomial bent functions over the finite fields of odd characteristic, IEEE Trans. Inform. Theory 56 (9), 4646–4652, (2010).
10. Helleseth, T. and Kholosha, A., Monomial and quadratic bent functions over the finite fields of odd characteristic, IEEE Trans. Inform. Theory 52 (5), 2018–2032, (2006).
11. Kumar, P., Scholtz, R. and Welch, L., Generalized bent functions and their properties, J. Combin. Theory Ser. A 40 (1), 90–107, (1985).
12. Lidl, R. and Niederreiter, H., Finite Fields, Encyclopedia of Mathematics and its Applications 20, second edition, Cambridge University Press, (1997).
13. Ma, S., A survey of partial differential sets, Des. Codes Cryptogr. 4 (3), 221–261, (1994).
14. Passman, D., The Algebraic Structure of Group Rings, Robert E. Krieger Publishing Co. Inc., Melbourne, FL, Reprint of the 1977 original, (1985).
15. Pott, A., Tan, Y., Feng, T. and Ling, S., Association schemes arising from bent functions, Preproceedings of The International Workshop on Coding and Cryptography, Bergen, 48–61, (2009).
16. Rothaus, O., On “bent” functions, J. Combin. Theory Ser. A 20 (3), 300-305, (1976).
17. Tan, Y., Pott, A. and Feng, T., Strongly regular graphs associated with ternary bent functions, J. Combin. Theory Ser. A 117 (6), 668–682, (2010).
18. Tan, Y., Yang, J. and Zhang, X., A recursive approach to construct p-ary bent functions which are not weakly regular, to appear in Proceedings of IEEE International Conference on Information Theory and Information Security, Beijing, (2010).