Designs, Codes and Cryptography (2020) 88:453–470
https://doi.org/10.1007/s10623-019-00692-z

Ramanujan graphs and expander families constructed from *p*-ary bent functions

Jong Yoon Hyun[1] · **Jungyun Lee**[2] · **Yoonjin Lee**[3]

Received: 14 July 2019 / Revised: 18 October 2019 / Accepted: 22 October 2019 /
Published online: 7 November 2019

Abstract

We present a method for constructing an infinite family of non-bipartite Ramanujan graphs. We mainly employ p-ary bent functions of $(p-1)$-form for this construction, where p is a prime number. Our result leads to construction of infinite families of expander graphs; this is due to the fact that Ramanujan graphs play as base expanders for constructing further expanders. For our construction we directly compute the eigenvalues of the Ramanujan graphs arsing from p-ary bent functions. Furthermore, we establish a criterion on the regularity of p-ary bent functions in m variables of $(p-1)$-form when m is even. Finally, using weakly regular p-ary bent functions of ℓ-form, we find (amorphic) association schemes in a constructive way; this resolves the open case that $\ell = p-1$ for $p > 2$ for finding (amorphic) association schemes.

Keywords Ramanujan graph · p-ary bent function · Expanders · (amorphic)association scheme

Mathematics Subject Classification Primary 05E30; Secondary 11T71 · 94C10

Communicated by G. Kyureghyan.

✉ Yoonjin Lee
yoonjinl@ewha.ac.kr

Jong Yoon Hyun
hyun33@kku.ac.kr

Jungyun Lee
lee9311@kangwon.ac.kr

[1] Konkuk University, Glocal Campus, 268 Chungwon-daero, Chungju-si,
Chungcheongbuk-do 27478, South Korea

[2] Department of Mathematics Education, Kangwon National University, Chuncheon-si,
Gangwon-do 24341, South Korea

[3] Department of Mathematics, Ewha Womans University, 52 Ewhayeodae-gil, Seodaemun-gu,
Seoul 03760, South Korea

1 Introduction

Expanders (or expander graphs) have a great deal of applications in various areas such as computer science, network design, coding theory, cryptography, and even in pure mathematics (for instance, refer to [8,10,11,13,16,24,27]). Briefly speaking, an expander is a highly connected sparse graph; this means that every subset of their vertices has a large set of neighbors. It is well known that *Ramanujan graphs* are "good" expanders achieving the spectral bound. In fact, a connected k-regular graph is called *Ramanujan* if it satisfies $|\theta| \leq 2\sqrt{k-1}$ for every eigenvalue $\theta \neq \pm k$ of its adjacency matrix; this definition is motivated by the result that $\liminf_{n \to \infty} \lambda_2(G_{n,k}) \geq 2\sqrt{k-1}$, where $\lambda_2(G_{n,k})$ denotes the second largest eigenvalues of the $G_{n,k}$ being a k-regular graph with n vertices. Furthermore, the spectral gap $k - \lambda_2(G_{n,k})$ should be as large as possible for having expanders of good quality; however, the spectral gap cannot be too large asymptotically as proved by Alon-Boppana [1]. This means that a Ramanujan graph is a connected regular graph whose second largest eigenvalue in absolute value is *asymptotically* the smallest possible. In general, computation of the eigenvalues of graphs is a hard task. In spectral graph theory, there are some invariants related to eigenvalues of regular graphs such as the cheeger constant, the size of the largest independent sets, the chromatic number and the diameter of regular graphs [31].

For construction of expanders, a graph product, called the *zig-zag graph product*, is introduced in [26]. The zig-zag product yields simple explicit constructions of constant-degree expanders of arbitrary size, starting from one constant size expander. Therefore, the role of base expanders is very crucial to construction of expanders. We point out that Ramanujan graphs can play as base expanders. We are therefore highly motivated to work on constructing Ramanujan graphs.

Recently, there has been a great deal of developments on construction of Ramanujan graphs. First of all, constructions of Ramanujan graphs with a fixed degree $p+1$ (that is, $(p+1)$-regular Ramanujan graphs) were independently given in [17,21], where p is an "odd" prime number, and the (p^m+1)-regular Ramanujan graphs were studied in [23], where m is a positive integer. Furthermore, the cubic version (that is, $p = 2$) of Ramanujan graphs was later studied in [6]. We note that these graphs have a fixed degree and increasing number of vertices.

Furthermore, in [3,22], they showed that the Cayley graphs associated with some quasi-perfect Lee codes are Ramanujan graphs of degree $p^m + 1$ with p^{2m} vertices. All of these constructions used a Weil-Deligne bound on estimation of associated character sums instead of directly computing eigenvalues of the graphs. On the other hand, in [2] they found constructions of *bipartite* Ramanujan graphs of degree p (respectively, $p^m - 1$) with $2p^2$ vertices (respectively, $2p^m d$ vertices, d being a positive integer) by direct computation of eigenvalues of their graphs.

We present a method for constructing an infinite family of *non-bipartite* Ramanujan graphs of degrees $p^{m-1} \pm \varepsilon(p,m)$ with p^m vertices, where $\varepsilon(p,m)$ is an explicit formula involved with p and m, p is a prime number, and m is a positive integer (Theorems 4.1 and 4.4). We mainly employ p-ary bent functions of $(p-1)$-form for this construction. Our result leads to construction of infinite families of expander graphs with a fixed degree and increasing number of vertices; this is due to the fact that Ramanujan graphs play as base expanders for construction of further expanders. For our construction we directly compute the eigenvalues of the Ramanujan graphs arising from p-ary bent functions. Furthermore, we establish a criterion on the regularity of p-ary bent functions in m variables of l-form when m is even and $l = p-1$; the case that m is even and $l \neq p-1$ for $p > 3$ is treated in [12]. We also derive an algebraic formula for the diameter of a Cayley graph. Finally, using weakly regular p-ary bent functions of $(p-1)$-form, we find (amorphic) association schemes in a constructive way; this resolves the open case that $\ell = p-1$ for $p > 3$ for finding (amorphic) association schemes.

2 Preliminaries

In this section we introduce the basic definitions and notations regarding p-ary bent functions, strongly regular graphs, Ramanujan graphs, expander graphs and (amorphic) association schemes.

Throughout this paper, m is a positive integer and p is an odd prime number.

2.1 Bent functions

Let $\mathbb{F}_{p^m}$ be the finite field of order p^m. For a subset S of $\mathbb{F}_{p^m}$, we denote by S^* the set of nonzero elements of S.

A *p-ary function* f in m variables is just a function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. We say that a p-ary function f is *even* if $f(-x) = f(x)$ for any $x \in \mathbb{F}_{p^m}$. We define $D_{f,i}$ to be the set

$$D_{f,i} = \{\beta \in \mathbb{F}_{p^m}^* : f(\beta) = i\}.$$

For some $l \in \mathbb{F}_p^*$, we say that a p-ary function f in m variables is an *l-form* if $f(ax) = a^l f(x)$ for any $a \in \mathbb{F}_p^*$ and $x \in \mathbb{F}_{p^m}$.

The *Walsh–Hadamard transform* W_f of a p-ary function f in m variables is a complex-valued function of $\mathbb{F}_{p^m}$ defined by

$$W_f(\beta) = \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{f(x) - \mathrm{Tr}(\beta x)},$$

where $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ is a primitive pth root of unity, and Tr_1^k is the trace function from $\mathbb{F}_{p^k}$ to $\mathbb{F}_p$ defined by $\sum_{j=0}^{k-1} x^{p^j}$. Throughout this paper, let Tr denote Tr_1^m.

The inverse Walsh–Hadamard transform of a p-ary function f is given by

$$\zeta_p^{f(\beta)} = p^{-m} \sum_{x \in \mathbb{F}_{p^m}} W_f(x) \zeta_p^{\mathrm{Tr}(\beta x)}.$$

The *Fourier transform* $\hat{f}$ of a p-ary function f in m variables is a complex-valued function of $\mathbb{F}_{p^m}$ defined by

$$\hat{f}(\beta) = \sum_{x \in \mathbb{F}_{p^m}} f(x) \zeta_p^{\mathrm{Tr}(\beta x)}.$$

We say that a p-ary function f in m variables is *bent* if $|W_f(\beta)|^2 = p^m$ for any $\beta \in \mathbb{F}_{p^m}$. In this case, it is known [15] that

$$W_f(\beta) = \begin{cases} \pm p^{\frac{m}{2}} \zeta_p^{g(\beta)} & \text{if } m \text{ even, or } m \text{ odd and } p \equiv 1 \pmod 4, \\ \pm\sqrt{-1}\, p^{\frac{m}{2}} \zeta_p^{g(\beta)} & \text{if } m \text{ odd and } p \equiv 3 \pmod 4 \end{cases}$$

for some p-ary function g in m variables. We denote by 1_S the *characteristic function* of a subset S of $\mathbb{F}_{p^m}$. Then the Walsh–Hadamard transform of a p-ary bent function f can be written as

$$W_f(\beta) = (-1)^{1_S(\beta)}(p^*)^{\frac{m}{2}}\zeta_p^{g(\beta)},$$

where S is a subset of $\mathbb{F}_{p^m}$, $p^* = (-1)^{(p-1)/2}p$, and g is a p-ary function in m variables. A p-ary bent function f is *weakly regular* if there is a complex α with unit magnitude such that $W_f(\beta) = \alpha p^{\frac{m}{2}}\zeta_p^{\tilde{f}(\beta)}$ for some p-ary function $\tilde{f}$ in m variables. That is, if S is the ambient space or an empty set, then f is weakly regular bent. In this case, we call $\tilde{f}$ the *dual of* f. In particular, when $\alpha = 1$ (or $S = \emptyset$), we say that f is *regular* p-ary bent. When f is weakly regular bent, we have

$$W_{\tilde{f}}(\beta) = \left(\frac{-1}{p}\right)^m (-1)^{1_S(\beta)}(p^*)^{\frac{m}{2}}\zeta_p^{f(-\beta)}, \tag{1}$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol. This shows that the dual $\tilde{f}$ of a weakly regular p-ary bent function f is also weakly regular p-ary bent and $\tilde{\tilde{f}}(x) = f(-x)$ for all $x \in \mathbb{F}_{p^m}$.

Let $\mathcal{B}_l(m, p)$ (respectively, $\mathcal{B}_l^w(m, p)$) be the set of p-ary bent functions (respectively, weakly regular p-ary bent functions) in m variables of l-form, where $(l-1, p-1) = 1$ and $f(0) = 0$. In this paper, we mainly deal with $\mathcal{B}_{p-1}(m, p)$; for the case that $l \neq p-1$, $\mathcal{B}_l(m, p)$ were studied by the authors in [12].

We introduce a family of p-ary bent functions in m variables of $(p-1)$-form, which can be found in [29] as follows.

Firstly, we consider the case that $m = 2k$ and p is an odd prime number. A p-ary function f from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ defined by

$$f(x) = \sum_{i=1}^{p^k-1} \mathrm{Tr}_1^m(c_i x^{i(p^k-1)}) + \mathrm{Tr}_1^l\left(\alpha x^{\frac{p^m-1}{e}}\right),$$

is known to be regular bent of $(p-1)$-form, called *Dillon-type bent*, where $e \mid (p^k+1)$, $c_i \in \mathbb{F}_{p^m}$ for $0 \le i \le p^k - 1$, α in $\mathbb{F}_{p^l}$ and l is the smallest positive integer such that $l \mid m$ and $e \mid (p^l - 1)$. On the other hand, there is a sporadic example of a ternary bent function which is not weakly regular bent, that is, $f(x) = \mathrm{Tr}(\zeta_3^7 x^{98})$ in $\mathbb{F}_{3^6}$.

Secondly, we consider the case that m is odd and p is an odd prime number. Regarding an example of a p-ary monomial bent function of $(p-1)$ form, to the best of our knowledge, a ternary monomial bent function of 2 form is the only example which is known so far. Weakly regular bent functions of Coulter-Matthews class are $f(x) = \mathrm{Tr}(cx^{\frac{3^i+1}{2}})$, where $c \in \mathbb{F}_3^*$, i is odd and $(i, m) = 1$.

The *character sum* $\chi_\beta(S)$ of S with respect to $\beta \in \mathbb{F}_{p^m}$ for a subset of $\mathbb{F}_{p^m}$ is defined by

$$\chi_\beta(S) = \sum_{x \in S} \zeta_p^{\mathrm{Tr}(\beta x)}.$$

2.2 Strongly regular Cayley graphs, Ramanujan graphs and expander graphs

We can refer to [9,14] for this subsection. Let G be a *simple undirected graph*, that is, an undirected graph without loops and parallel edges. The *degree* of a vertex is the number of edges adjacent to its vertex. A graph G is called k*-regular* if every vertex has degree k. The *distance* $d_G(x, y)$ between two vertices x and y in G is the number of edges in the shortest path from x to y. The *diameter* of a graph is the maximum among distances between every pair of vertices of G.

The *adjacency matrix* A of a graph with rows and columns indexed by its vertices is defined by

$$A_{xy} = \begin{cases} 1 & \text{if } x \text{ is adjacent to } y, \\ 0 & \text{otherwise.} \end{cases}$$

Any eigenvalue θ of A is real because A is symmetric, and $|\theta| \leq k$ whenever a graph is k-regular. A connected k-regular graph is called *Ramanujan* if it satisfies

$$|\theta| \leq 2\sqrt{k-1}$$

for every eigenvalue $\theta \neq \pm k$ of its adjacency matrix. A k-regular graph is bipartite if and only if $-k$ is also an eigenvalue of its adjacency matrix. In [20], it is shown that for every $k \geq 3$, there is a bipartite k-regular Ramanujan graph using a nonconstructive method.

A k-regular graph G with v vertices is said to be *strongly regular* (SRG) with parameters (v, k, λ, μ) if there are integers λ and μ such that any two adjacent vertices have λ common neighbors, and any two non-adjacent vertices have μ common neighbors. The complete graph and disjoint unions of complete graphs are the only SRG's with two eigenvalues. Otherwise, the adjacency matrix of a SRG has precisely two distinct restricted eigenvalues (eigenvectors perpendicular to the all-ones vector), say, θ_1 and θ_2. There are relations between them as follows; $\mu - k = \theta_1\theta_2$ and $\lambda - \mu = \theta_1 + \theta_2$. A connected regular graph with only two or three eigenvalues is strongly regular. We say that a SRG with parameters $(n^2, r(n+\delta), -\delta n + r^2 + 3\delta r, r^2 + \delta r)$ is of *Latin square type* if $\delta = -1$ and of *negative Latin square type* if $\delta = 1$.

Let S be a subset of $\mathbb{F}_{p^m}$ such that $0 \notin S$ and $S = -S$. The *Cayley graph* $G = \mathrm{Cay}(\mathbb{F}_{p^m}, S)$ has a vertex set $\mathbb{F}_{p^m}$, and two vertices α and β in $\mathbb{F}_{p^m}$ are joined by an edge if and only if $\alpha - \beta \in S$. Then the Cayley graph G is a simple undirected graph, $|S|$-regular and vertex-transitive. Moreover, G is connected if and only if S generates $\mathbb{F}_{p^m}$.

Result 1 [9] Let S be a subset of $\mathbb{F}_{p^m}$ such that $S = -S$ and $0 \notin S$. Then the set $\{\chi_\beta(S) : \beta \in \mathbb{F}_{p^m}\}$ is precisely the set of eigenvalues of the adjacency matrix of $\mathrm{Cay}(\mathbb{F}_{p^m}, S)$.

In order to construct Ramanujan graphs from the Cayley graph $\mathrm{Cay}(\mathbb{F}_{p^m}, S)$, we require an inequality that

$$|\chi_\beta(S)| \leq 2\sqrt{|S| - 1}$$

for all $\beta \in \mathbb{F}^*_{p^m}$.

Finally, we introduce the expander families of k-regular graphs. The *isoperimetric constant* $h(G)$ of a graph G with a vertex set V is defined by

$$h(G) = \min\{|\partial F|/|F| : F \subset V \text{ and } |F| \leq |V|/2\},$$

where ∂F, called the *boundary* of F, is the set of edges connecting F to $V \setminus F$.

Let k be a positive integer. Let (G_n) be a sequence of k-regular graphs with $|G_n| \to \infty$ as $n \to \infty$. We say that (G_n) is an *expander family* if the sequence $(h(G_n))$ is bounded away from zero, that is, there is a real number $\varepsilon > 0$ such that $h(G_n) \geq \varepsilon$ for all n.

Let (G_n) be a sequence of k-regular graphs with $|G_n| \to \infty$ as $n \to \infty$. Then (G_n) is an expander family if and only if the sequence

$$(k - (\text{the second largest eigenvalue of } G_n)/k$$

is bounded away from zero.

We say that G is a (v, k, ε)-expander if it is a k-regular expander graph with v vertices such that there is a constant $\varepsilon > 0$ provided that

$$\text{(the second largest eigenvalue of } G)/k \leq \varepsilon.$$

Reingold et al. in [26] proved the following result which allows us to construct the families of expander graphs with constant degree.

Result 2 Let G be a $(v_1, k_1, \varepsilon_1)$-expander and H be a $(k_1, k_2, \varepsilon_2)$-expander. Then the zig-zag product $G \circ_Z H$ is a $(v_1 k_1, k_2^2, \varepsilon_1 + \varepsilon_2 + \varepsilon_2^2)$-expander, where for the definition of zig-zag product, see [26].

Using this result, they provided a simple combinatorial construction of constant-degree expander graphs. See Theorem 1.4 of [26].

2.3 Association schemes

Let X be a finite set. A *symmetric d-class association scheme* $(X, \{R_l\})_{l=0}^d$ is a partition of $X \times X$ into binary relations (or classes) $R_0, R_1, \ldots, R_d$ with the properties that

- $R_0 = \{(x, x) : x \in X\}$;
- R_l is symmetric for $l = 1, 2, \ldots, d$, that is, $(x, y) \in R_l$ if and only if $(y, x) \in R_l$;
- for all i, j, k in {0,1,...,d} there is an integer c_{ij}^k such that for all $(u, v) \in R_k$,

$$c_{ij}^k = |\{w \in X : (u, w) \in R_i \text{ and } (w, v) \in R_j\}|.$$

Zinoviev and Ericson in [32] proved the following result.

Result 3 Let $P = P_0|P_1|\ldots|P_d$ be a partition of $\mathbb{F}_{p^m}$, where $P_0 = \{0\}$, and let R_i be a partition of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ defined by

$$(\alpha, \beta) \in R_i \Leftrightarrow \alpha - \beta \in P_i, i = 0, 1, \ldots, d.$$

Then $(\mathbb{F}_{p^m}, \{R_l\})_{l=0}^d$ is a symmetric association scheme on $\mathbb{F}_{p^m}$ if and only if there is another partition $Q = Q_0|Q_1|\ldots,|Q_d$ such that for any $i, j \in \{0, 1, \ldots, p-1\}$, the sum $\chi_\alpha(P_i)$ does not depend on the choice of $\alpha \in Q_j$, and the sum $\chi_\beta(Q_i)$ does not depend on the choice of $\beta \in P_j$.

Each symmetric relation R_l $(1 \leq l \leq d)$ corresponds to an undirected Cayley graph $G_l = \text{Cay}(X, R_l)$ [9] with a vertex set X and an edge set R_l, where R_l is defined by the following: uv is an edge of G_l if and only if $(u, v) \in R_l$. We thus regard an association scheme $(X, \{R_l\})_{l=0}^d$ as an edge-decomposition of the complete graph on X into graphs G_l such that for all i, j, k in $\{1, 2, \ldots, d\}$ and for all $uv \in E(G_k)$,

$$|\{w \in X : uw \in E(G_i) \text{ and } wv \in E(G_j)\}| = c_{ij}^k,$$

where $E(G_l)$ denotes the edge set of G_l. The Cayley graphs G_l will be called the *graphs of the association scheme* $(X, \{R_l\})_{l=1}^d$. Each Cayley graph G_l of the association scheme $(X, \{R_l\})_{l=0}^d$ is regular with valency (or degree) c_{ll}^0; that is, each vertex of G_l is adjacent to exactly c_{ll}^0 edges.

An association scheme is *amorphic* if any of the union of its classes is also an association scheme. van Dam proved the following result in [30]:

Result 4 [30] Let X be a finite set and $\{G_1, G_2, \ldots, G_d\}$ be an edge-decomposition of the complete graph on X, where each G_l is a strongly regular graph on X. If the G_l are all of Latin square type or all of negative Latin square type, then the decomposition is a d-class amorphic association scheme on X.

3 Auxiliary results

In this section, we introduce basic results on the p-ary bent functions of $(p-1)$-form which will be used in the next sections. In particular, we provide a characterization of p-ary bent functions of $(p-1)$-form in terms of strongly regular graphs. We also develop an algebraic formula of a Cayley graph by computing its diameter.

Lemma 3.1 *Let S_1 and S_2 be nonempty subsets of $\mathbb{F}_{p^m}$. Then the following statements hold.*

(i) *If $\chi_\beta(S_1) = \chi_\beta(S_2)$ for all $\beta \in \mathbb{F}_{p^m}$, then $S_1 = S_2$.*
(ii) *$\chi_\beta(S_1)^{\sigma_a} = \chi_\beta(aS_1) = \chi_{a\beta}(S_1)$ for all $a \in \mathbb{F}_p^*$, where σ_a is a Galois automorphism defined by $\sigma_a(\zeta_p) = \zeta_p^a$.*

Proof (i) The result follows from [12, Lemma IV.2].
(ii) It follows that for $a \in \mathbb{F}_p^*$,

$$\chi_\beta(S_1)^{\sigma_a} = \sum_{x \in S_1} \zeta_p^{\mathrm{Tr}(\beta a x)} = \sum_{x \in aS_1} \zeta_p^{\mathrm{Tr}(\beta x)} = \chi_\beta(aS_1).$$

□

Lemma 3.2 *Let $f \in \mathcal{B}_l(m, p)$. We write $W_f(\beta)$ as $W_f(\beta) = (-1)^{1_{s(\beta)}}(p^*)^{\frac{m}{2}}\zeta_p^{g(\beta)}$ for all $\beta \in \mathbb{F}_{p^m}$. Then $g(0) = 0$.*

Proof The result follows from the same argument of the proof in [29, Proposition 4]. □

In the following proposition, we provide a characterization for p-ary bent functions of $(p-1)$-form. It will be exploited in Lemmas 3.4 and 3.7.

Proposition 3.3 *Let $f \in \mathcal{B}_l(m, p)$. Then the following statements are equivalent.*

(i) *Every eigenvalue of* $\mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,i})$ $(0 \le i \le p-1)$ *is a rational integer, where f is even.*
(ii) *$aD_{f,i} = D_{f,i}$ for all $a \in \mathbb{F}_p^*$ and $i = 0, 1, \ldots, p-1$.*
(iii) *f is $(p-1)$-form, i.e., $f(ax) = f(x)$ for all $(a, x) \in \mathbb{F}_p^* \times \mathbb{F}_{p^m}$.*

Proof $(i) \Rightarrow (ii)$; by the assumption and Result 1, the sum $\chi_\beta(D_{f,i})$ is a rational integer for all $\beta \in \mathbb{F}_{p^m}$ and $i = 1, 2, \ldots, p-1$. By Lemma 3.1-(ii), we have that

$$\chi_\beta(D_{f,i}) = \chi_\beta(D_{f,i})^{\sigma_a} = \chi_\beta(aD_{f,i})$$

for all $a \in \mathbb{F}_p^*$. The result follows from Lemma 3.1-(i).

$(ii) \Rightarrow (iii)$; let $W_f(\beta) = (-1)^{1_{s(\beta)}}(p^*)^{\frac{m}{2}}\zeta_p^{g(\beta)}$. Then by the assumption and Lemma 3.1-(ii), we have that for $a \in \mathbb{F}_p^*$,

$$(-1)^{1_{s(a\beta)}}(p^*)^{\frac{m}{2}}\zeta_p^{g(a\beta)} = W_f(a\beta) = \sum_{i=0}^{p-1} \chi_{a\beta}(D_{f,i})\zeta_p^i = \sum_{i=0}^{p-1} \chi_\beta(aD_{f,i})\zeta_p^i$$

$$= \sum_{i=0}^{p-1} \chi_\beta(D_{f,i})\zeta_p^i = (-1)^{1_S(\beta)}(p^*)^{\frac{m}{2}}\zeta_p^{g(\beta)},$$

so that $g(a\beta) = g(\beta)$ and $1_S(a\beta) = 1_S(\beta)$ for all $(a, \beta) \in \mathbb{F}_p^* \times \mathbb{F}_{p^m}$. This implies that $W_f(a\beta) = W_f(\beta)$ for all $(a, \beta) \in \mathbb{F}_p^* \times \mathbb{F}_{p^m}$. It then follows from the inversion formula of $W_f(\beta)$ that for $(a, \beta) \in \mathbb{F}_p^* \times \mathbb{F}_{p^m}$,

$$\begin{aligned}\zeta_p^{f(a\beta)} &= p^{-m} \sum_{x\in\mathbb{F}_{p^m}} W_f(x)\zeta_p^{\mathrm{Tr}(a\beta x)} = p^{-m} \sum_{x\in\mathbb{F}_{p^m}} W_f(a^{-1}x)\zeta_p^{\mathrm{Tr}(\beta x)}\\ &= p^{-m} \sum_{x\in\mathbb{F}_{p^m}} W_f(x)\zeta_p^{\mathrm{Tr}(\beta x)} = \zeta_p^{f(\beta)}.\end{aligned}$$

The result follows.

$(iii) \Rightarrow (ii)$; let $x \in aD_{f,i}$ for $a \in \mathbb{F}_p^*$. Then $x = ay$ for some $y \in D_{f,i}$, and so by the assumption, $f(x) = f(ay) = f(y) = i$. Thus $x \in D_{f,i}$. Conversely, let $x \in D_{f,i}$. By the assumption, for $a \in \mathbb{F}_p^*$, we have $f(a^{-1}x) = f(x) = i$, and so $a^{-1}x \in D_{f,i}$. Thus $x \in aD_{f,i}$.

$(ii) \Rightarrow (i)$; it follows from Lemma 3.1-(ii) and the assumption that $\chi_\beta(D_{f,i})^{\sigma_a} = \chi_\beta(aD_{f,i}) = \chi_\beta(D_{f,i})$ for all $(a, \beta) \in \mathbb{F}_p^* \times \mathbb{F}_{p^m}$, where σ_a is a Galois automorphism. Thus $\chi_\beta(D_{f,i})$ is a rational integer. □

Lemma 3.4 *Let m be a positive even integer. Let $f \in \mathcal{B}_l(m, p)$ with $l = p-1$ and $W_f(\beta) = (-1)^{1_S(\beta)}p^{\frac{m}{2}}\zeta_p^{g(\beta)}$ for all β in $\mathbb{F}_{p^m}$. Then* Cay$(\mathbb{F}_{p^m}, D_{f,i})$ *has at most five eigenvalues for all $i = 0, 1, \ldots, p-1$ as follows:*

$$\begin{aligned}|D_{f,0}| &= p^{m-1} + (-1)^{1_S(0)}p^{\frac{m}{2}-1}(p-1) - 1,\\ |D_{f,i}| &= p^{m-1} - (-1)^{1_S(0)}p^{\frac{m}{2}-1}\ (1 \le i \le p-1),\\ \chi_\beta(D_{f,i}) &= \begin{cases}(-1)^{1_S(\beta)}p^{\frac{m}{2}-1}(p-1) & \text{if } i = g(\beta), \beta \neq 0,\\ -(-1)^{1_S(\beta)}p^{\frac{m}{2}-1} & \text{if } i \neq g(\beta), \beta \neq 0.\end{cases}\end{aligned}$$

Proof We use the set $\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\}$, which is linearly independent over $\mathbb{Q}$. Let us put $D_i = D_{f,i}$ for a simplicity of notation.

Since m is even, we can write $W_f(\beta)$ as $W_f(\beta) = (-1)^{1_S(\beta)}p^{\frac{m}{2}}\zeta_p^{g(\beta)}$, where S is a subset of $\mathbb{F}_{p^m}$ and g is a p-ary function in m variables. Applying the equation $\sum_{i=0}^{p-1}\zeta_p^i = 0$, we have that

$$(-1)^{1_S(\beta)}p^{\frac{m}{2}}\zeta_p^{g(\beta)} = W_f(\beta) = \sum_{i=0}^{p-1}\chi_\beta(D_i)\zeta_p^i = \sum_{i=0}^{p-2}(\chi_\beta(D_i) - \chi_\beta(D_{p-1}))\zeta_p^i. \quad (2)$$

It then follows from Lemma 3.2 that for $\beta = 0$,

$$(-1)^{1_S(0)}p^{\frac{m}{2}} = \sum_{i=0}^{p-2}(|D_i| - |D_{p-1}|)\zeta_p^i,$$

which implies that

$$\begin{aligned}|D_i| - |D_{p-1}| &= 0,\quad 1 \le i \le p-2,\\ |D_0| - |D_{p-1}| &= (-1)^{1_S(0)}p^{\frac{m}{2}}.\end{aligned}$$

Solving these equations together with $\sum_{i=0}^{m} |D_i| = p^m - 1$, we have the first two parts. To demonstrate the last part, we consider the following two cases with $\beta \in \mathbb{F}_{p^m}^*$. Firstly, assume that $g(\beta) \neq p - 1$. It follows from (2) and Proposition 3.3 that

$$\chi_\beta(D_i) - \chi_\beta(D_{p-1}) = 0,\ i \neq g(\beta),$$
$$\chi_\beta(D_i) - \chi_\beta(D_{p-1}) = (-1)^{1s(\beta)} p^{\frac{m}{2}} \zeta_p^{g(\beta)},\ i = g(\beta).$$

Solving these equations together with $\sum_{i=0}^{p-1} \chi_\beta(D_i) = 1$, we get the last part. Secondly, assume that $g(\beta) = p - 1$. It follows from (2) that

$$-(-1)^{1s(\beta)} p^{\frac{m}{2}} \sum_{i=0}^{p-2} \zeta_p^i = \sum_{i=0}^{p-2} (\chi_\beta(D_i) - \chi_\beta(D_{p-1}))\zeta_p^i,$$

which implies by Proposition 3.3 that

$$\chi_\beta(D_i) - \chi_\beta(D_{p-1}) = -(-1)^{1s(\beta)} p^{\frac{m}{2}},\ 0 \leq i \leq p - 2.$$

Solving these equations together with $\sum_{i=0}^{p-1} \chi_\beta(D_i) = 1$, we also have the last part. These complete the lemma. □

Corollary 3.5 *Let m be a positive even integer and $f \in \mathcal{B}_l^w(m, p)$ with $l = p - 1$. Then the following statements are true.*

(i) *If $p > 3$, then f must be regular bent.*

(ii) $\mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,0})$ *is a strongly regular graph with parameters*

$$(p^m, p^{m-1} + (p-1)p^{\frac{m}{2}-1} - 1, p^{m-2} + (p-1)p^{\frac{m}{2}-1} - 2, p^{m-2} + p^{\frac{m}{2}-1}) \tag{3}$$

and $\mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,i})$ *is a strongly regular graph with parameters*

$$(p^m, p^{m-1} - p^{\frac{m}{2}-1}, p^{m-2} + p^{\frac{m}{2}-1}(p-3), p^{m-2} - p^{\frac{m}{2}-1}) \tag{4}$$

for all $i = 1, \ldots, p - 1$.

Proof (i) Assume that f is weakly p-ary regular bent, which is not regular bent. It follows from Lemma 3.4 with $S = \mathbb{F}_{p^m}$ and Preliminaries 2.2 that we can compute the parameters of $\mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,i})$ for $i = 1, \ldots, p - 1$ as follows:

$$(p^m, p^{m-1} + p^{\frac{m}{2}-1}, p^{m-2} - p^{\frac{m}{2}-1}(p-3), p^{m-2} + p^{\frac{m}{2}-1}).$$

Notice that $\Delta = \sqrt{(\lambda - \mu)^2 + 4(k - \mu)} = p^m$, which is a square. Applying Ma's result [18, Theorem 6.8] under condition that Δ is a square, their degrees are divided by $p - 1$. This implies that $p = 3$, a contradiction. This proves (i).

(ii) By using Proposition 3.4 with $S = \emptyset$ and Preliminaries 2.2, the result follows. □

Remark 3.6 A SRG with parameters (2) which is known in [5] is of Latin square type. A SRG with parameters (3) which do not occur in [29] is also of Latin square type. When $p = 3$, the parameters (2) and (3) coincide with those of the result in [28]. However, for the case that $p \neq 3$, it is hard to check if SRG's with parameters (3) is new since there are too many SRG's of Latin square type [4] constructed from the block graphs [7] of orthogonal arrays.

Lemma 3.7 *Let m be a positive odd integer. Let $f \in \mathcal{B}_l(m, p)$ with $l = p-1$ and $W_f(\beta) = (-1)^{1s(\beta)}(p^*)^{\frac{m}{2}}\zeta_p^{g(\beta)}$ for all β in $\mathbb{F}_{p^m}$. Then $\mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,i})$ has at most four eigenvalues for all $i = 0, 1, \ldots, p-1$ as follows:*

$$|D_{f,i}| = \begin{cases} p^{m-1} - 1 & \text{if } i = 0, \\ p^{m-1} + (-1)^{1s(0)} p^{\frac{m-1}{2}} & \text{if } i \neq 0 \text{ and } \left(\frac{i}{p}\right) = 1, \\ p^{m-1} - (-1)^{1s(0)} p^{\frac{m-1}{2}} & \text{if } i \neq 0 \text{ and } \left(\frac{i}{p}\right) = -1, \end{cases}$$

$$\chi_\beta(D_{f,i}) = \begin{cases} 0 & \text{if } i = g(\beta), \beta \neq 0, \\ (-1)^{1s(\beta)} p^{\frac{m-1}{2}} & \text{if } i \neq g(\beta), \beta \neq 0, \text{ and } \left(\frac{i-g(\beta)}{p}\right) = 1, \\ -(-1)^{1s(\beta)} p^{\frac{m-1}{2}} & \text{if } i \neq g(\beta), \beta \neq 0, \text{ and } \left(\frac{i-g(\beta)}{p}\right) = -1, \end{cases}$$

where $\left(\frac{i}{p}\right)$ stands for the Legendre symbol.

Proof We use the set $\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\}$, which is linearly independent over $\mathbb{Q}$. Let us put $D_i = D_{f,i}$ for a simplicity of notation.

Note that

$$\sum_{i=0}^{p-1} \zeta_p^{i^2} = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ \sqrt{-p} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

We then have that

$$(-1)^{1s(\beta)} \left(\sum_{i=0}^{p-1} \zeta_p^{i^2} \right) p^{\frac{m-1}{2}} \zeta_p^{g(\beta)} = W_f(\beta) = \sum_{i=0}^{p-1} \chi_\beta(D_i)\zeta_p^i. \tag{5}$$

Set $T := \{i \in \mathbb{Z}_p : i \equiv a^2 \pmod p),\ a \in \mathbb{Z}_p^*\}$. Then the left hand side of (4) is written as follows:

$$(-1)^{1s(\beta)} p^{\frac{m-1}{2}} \left(\zeta_p^{g(\beta)} + 2\sum_{i\in T} \zeta_p^{i+g(\beta)} \right) = (-1)^{1s(\beta)} p^{\frac{m-1}{2}} \times \left(-\sum_{i=0, i\neq g(\beta)}^{p-1} \zeta_p^i + 2\sum_{i\in T} \zeta_p^{i+g(\beta)} \right) \tag{6}$$

because $-\sum_{i=0,i\neq g(\beta)}^{p-1} \zeta_p^i = \zeta_p^{g(\beta)}$. On the other hand, the right hand side of (4) is equal to

$$\sum_{i=0, i\neq g(\beta)}^{p-1} \Big(\chi_\beta(D_i) - \chi_\beta(D_{g(\beta)}) \Big) \zeta_p^i. \tag{7}$$

We now use the linearly independence of $\{1, \zeta_p, \ldots, \zeta^{g(\beta)-1}, \zeta^{g(\beta)+1}, \ldots, \zeta_p^{p-1}\}$ over $\mathbb{Q}$. By comparing (5) with (6) and using Proposition 3.3, we get the following:

$$\chi_\beta(D_i) - \chi_\beta(D_{g(\beta)}) = (-1)^{1s(\beta)} p^{\frac{m-1}{2}} \text{ if } \left(\frac{i - g(\beta)}{p} \right) = 1 \text{ and } i \neq g(\beta), \tag{8}$$

$$\chi_\beta(D_i) - \chi_\beta(D_{g(\beta)}) = -(-1)^{1s(\beta)} p^{\frac{m-1}{2}} \text{ if } \left(\frac{i - g(\beta)}{p} \right) = -1 \text{ and } i \neq g(\beta). \tag{9}$$

From (7) and (8), we have that

$$\sum_{i=0,i\neq g(\beta)}^{p-1}(\chi_\beta(D_i)-\chi_\beta(D_{g(\beta)}))=0. \tag{10}$$

The second part of this lemma follows from solving Eqs. (7–9) together with $\sum_{i=0}^{p-1}\chi_\beta(D_i)=1$ for $\beta\in\mathbb{F}_p^*$.

Now, we consider the case that $\beta=0$. By Lemma 3.2 we have that $g(0)=0$. It follows from (7) and (8) that

$$|D_i|-|D_0|=(-1)^{1_S(0)}p^{\frac{m-1}{2}} \text{ if } \left(\frac{i}{p}\right)=1, \tag{11}$$

$$|D_i|-|D_0|=-(-1)^{1_S(0)}p^{\frac{m-1}{2}} \text{ if } \left(\frac{i}{p}\right)=-1. \tag{12}$$

The first part of this lemma follows from solving Eqs. (10) and (11) together with $\sum_{i=0}^{p-1}|D_i|=p^m-1$. □

To derive an algebraic formula for the diameter of a Cayley graph, we require the following lemma.

Lemma 3.8 *Let γ be contained in $\mathbb{F}_{p^m}$ and let S be a nonempty subset of $\mathbb{F}_{p^m}$. Then the number of t-tuples $(\alpha_1,\alpha_2,\ldots,\alpha_t)\in S^t$ such that $\alpha_1+\alpha_2+\cdots+\alpha_t=\gamma$ is equal to*

$$\sum_{\beta\in\mathbb{F}_{p^m}}\chi_\beta(-S)^t\zeta_p^{Tr(\beta\gamma)}.$$

Proof We compute the following sum:

$$\sum_{\alpha_1\ldots,\alpha_t\in\mathbb{F}_{p^m}}1_S(\alpha_1)\ldots1_S(\alpha_t)1_{\{\gamma\}}(\alpha_1+\cdots+\alpha_t).$$

Then this sum becomes

$$\begin{aligned}&\frac{1}{p^m}\sum_{\alpha_1\ldots,\alpha_t\in\mathbb{F}_{p^m}}1_S(\alpha_1)\ldots1_S(\alpha_t)\sum_{\delta\in\mathbb{F}_{p^m}}\hat{1}_{\{\gamma\}}(\delta)\zeta_p^{-\mathrm{Tr}((\alpha_1+\alpha_2+\cdots+\alpha_t)\delta)}\\&=\frac{1}{p^m}\sum_{\delta\in\mathbb{F}_{p^m}}\hat{1}_{\{\gamma\}}(\delta)\prod_{i=1}^{t}\sum_{\alpha_i\in\mathbb{F}_{p^m}}1_S(\alpha_i)\zeta_p^{-\mathrm{Tr}(\alpha_i\delta)}\\&=\frac{1}{p^m}\sum_{\delta\in\mathbb{F}_{p^m}}\zeta_p^{\mathrm{Tr}(\delta\gamma)}\chi_\delta(-S)^t.\end{aligned}$$

The result thus follows. □

Proposition 3.9 *Let S be a nonempty subset of $\mathbb{F}_{p^m}$ with $S=-S$ and $0\notin S$. Then the diameter of $G=\mathrm{Cay}(\mathbb{F}_{p^m},S)$ is the smallest integer $t>1$ such that*

$$\sum_{\beta\in\mathbb{F}_{p^m}}\chi_\beta(S)^t\zeta_p^{Tr(\beta\gamma)}$$

does not vanish for all $\gamma\in\mathbb{F}_{p^m}$.

Proof Notice that the diameter of G is the smallest integer $t>1$ such that $\mathbb{F}_{p^m}=S+S+\cdots+S$ (t times), where $S+S=\{\alpha+\beta:\alpha,\beta\in S\}$, and the result follows from Lemma 3.8. □

4 Ramanujan graphs

Let $f \in \mathcal{B}_l(m, p)$ with $l = p - 1$. Recall from Lemmas 3.4 and 3.7 that each Cayley graph generated by $D_{f,i}$ for $i = 0, 1, \ldots, p-1$ has at most four eigenvalues when m is odd, or five eigenvalues when m is even. In this section, using these lemmas, the regularity of f is characterized in terms of strongly regular graphs as in [12,28], and (strongly regular) Ramanujan graphs are also derived. It allows us to construct the families of expander graphs using the zig-zag construction introduced in [26]. We divide this section into two subsections depending on m being even or odd.

4.1 Even dimensional cases

Theorem 4.1 *Let m be a positive even integer. Let $f \in \mathcal{B}_l(m, p)$ with $l = p - 1$ and $W_f(\beta) = (-1)^{1_S(\beta)} p^{\frac{m}{2}} \zeta_p^{g(\beta)}$ for all β in $\mathbb{F}_{p^m}$. Then*

(i) $\mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,0})$ *is a Ramanujan graph if and only if* $0 \in S$ *and* $p = 3, 5$ $(m \geq 4)$, *or* $0 \notin S$ *and* $p = 3$ $(m \geq 4)$, $p = 5$ $(m \geq 2)$, *where its degree is given in Lemma* 3.4. *Further, if* $f \in \mathcal{B}_l^w(m, p)$ *and either of the above cases holds, then it has diameter* 2.

(ii) $\mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,i})$ *is a Ramanujan graph of diameter* 2 *for all* $i = 1, 2, \ldots, p-1$ *if and only if* $0 \in S$ *and* $p = 3, 5$ $(m \geq 2)$, *or* $0 \notin S$ *and* $p = 3$ $(m \geq 2)$, $p = 5$ $(m \geq 4)$, *where their degrees are given in Lemma* 3.7.

Proof To check if it is a Ramanujan graph, we need to find p and m satisfying that $\Omega_\beta(D_{f,i}) := 4(|D_{f,i}| - 1) - \chi_\beta(D_{f,i})^2 \geq 0$ for any $\beta \in \mathbb{F}_{p^m}^*$.

(i) It follows from Lemma 3.4 that

$$\begin{aligned} 0 \leq \min_{\beta \in \mathbb{F}_{p^m}^*} \Omega_\beta(D_{f,0}) &= 4(p^{m-1} + (-1)^{1_S(0)} p^{\frac{m}{2}-1}(p-1) - 2) - p^{m-2}(p-1)^2 \\ &= p^{m-2}(-p^2 + 6p - 1) + 4(-1)^{1_S(0)} p^{\frac{m}{2}-1}(p-1) - 8. \end{aligned}$$

(ii) It follows from Lemma 3.4 that for $i = 1, 2, \ldots, p-1$,

$$\begin{aligned} 0 \leq \min_{\beta \in \mathbb{F}_{p^m}^*} \Omega_\beta(D_{f,0}) &= 4(p^{m-1} - (-1)^{1_S(0)} p^{\frac{m}{2}-1} - 1) - p^{m-2}(p-1)^2 \\ &= p^{m-2}(-p^2 + 6p - 1) - 4(-1)^{1_S(0)} p^{\frac{m}{2}-1} - 4. \end{aligned}$$

Let us now determine the diameter of $\mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,i})$ for $i = 0, 1, \ldots, p-1$. It follows from Lemma 3.4 that

$$\begin{aligned} E_i(\gamma) &:= \sum_{\beta \in \mathbb{F}_{p^m}} \chi_\beta(D_{f,i})^2 \zeta_p^{\mathrm{Tr}(\beta\gamma)} \\ &= |D_{f,i}|^2 + \sum_{\beta \in \mathbb{F}_{p^m} \setminus \{0\}} \chi_\beta(D_{f,i})^2 \zeta_p^{\mathrm{Tr}(\beta\gamma)} \\ &= |D_{f,i}|^2 + \sum_{\substack{\beta \in \mathbb{F}_{p^m} \setminus \{0\} \\ g(\beta) = i}} p^{m-2}(p-1)\zeta_p^{\mathrm{Tr}(\beta\gamma)} + \sum_{\substack{\beta \in \mathbb{F}_{p^m} \setminus \{0\} \\ g(\beta) \neq i}} p^{m-2} \zeta_p^{\mathrm{Tr}(\beta\gamma)}. \end{aligned} \tag{13}$$

Since $\sum_{\beta \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}(\beta\gamma)} = 0$ for $\gamma \neq 0$, $E_i(\gamma)$ is equal to

$$\begin{aligned} &|D_{f,i}|^2 - p^{m-2} + \sum_{\substack{\beta \in \mathbb{F}_{p^m} \setminus \{0\} \\ g(\beta)=i}} p^{m-2}(p-1)\zeta_p^{\mathrm{Tr}(\beta\gamma)} - \sum_{\substack{\beta \in \mathbb{F}_{p^m} \setminus \{0\} \\ g(\beta)=i}} p^{m-2}\zeta_p^{\mathrm{Tr}(\beta\gamma)} \\ &\quad = |D_{f,i}|^2 - p^{m-2} + p^{m-2}(p-2)(\chi_\gamma(D_{g,i}) + \delta_{g,i}), \end{aligned} \tag{14}$$

where $\delta_{g,i} = \begin{cases} 1 & \text{if } 0 \in D_{g,i}, \\ 0 & \text{if } 0 \notin D_{g,i}. \end{cases}$

From the fact that g is also a weakly regular bent function and $f(-\beta) = f(\beta)$ for any $\beta \in \mathbb{F}_p$, using (1), we have that

$$W_g(\beta) = (-1)^{1_S(\beta)} \sqrt{p}^m \zeta_p^{f(\beta)}. \tag{15}$$

In the case that $\gamma \neq 0$ and $f(\gamma) \neq 0$, $E_i(\gamma)$ is equal to

$$\begin{aligned} &|D_{f,i}|^2 - p^{m-2} + p^{m-2}(p-2)(\chi_\gamma(D_{g,i}) + \delta_{g,i}) \\ &\quad = \begin{cases} (p^{m-1} - (-1)^{1_S(0)} p^{\frac{m}{2}-1})^2 - p^{m-2} + p^{m-2}(p-2)((-1)^{1_S(\gamma)} p^{\frac{m}{2}-1}(p-1) + \delta_{g,i}) \\ \text{if } i \neq 0 \text{ and } i = f(\gamma), \\ (p^{m-1} - (-1)^{1_S(0)} p^{\frac{m}{2}-1})^2 - p^{m-2} + p^{m-2}(p-2)(-(-1)^{1_S(\gamma)} p^{\frac{m}{2}-1}(p-1) + \delta_{g,i}) \\ \text{if } i \neq 0 \text{ and } i \neq f(\gamma), \\ (p^{m-1} - (-1)^{1_S(0)} p^{\frac{m}{2}-1}(p-1) - 1)^2 - p^{m-2} + p^{m-2}(p-2)(-(-1)^{1_S(\gamma)} p^{\frac{m}{2}-1}(p-1) + \delta_{g,i}) \\ \text{if } i = 0 \text{ and } i \neq f(\gamma). \end{cases} \end{aligned} \tag{16}$$

In the case that $\gamma \neq 0$ and $f(\gamma) = 0$, $E_i(\gamma)$ is equal to

$$\begin{aligned} &|D_{f,i}|^2 - p^{m-2} + p^{m-2}(p-2)(\chi_\gamma(D_{g,i}) + \delta_{g,i}) \\ &\quad = \begin{cases} (p^{m-1} - (-1)^{1_S(0)} p^{\frac{m}{2}-1}(p-1) - 1)^2 - p^{m-2} + p^{m-2}(p-2)((-1)^{1_S(\gamma)} p^{\frac{m}{2}-1}(p-1) + \delta_{g,i}) \\ \text{if } i = 0, \\ (p^{m-1} + (-1)^{1_S(0)} p^{\frac{m}{2}-1})^2 - p^{m-2} + p^{m-2}(p-2)(-(-1)^{1_S(\gamma)} p^{\frac{m}{2}-1}(p-1) + \delta_{g,i}) \\ \text{if } i \neq 0. \end{cases} \end{aligned} \tag{17}$$

We note that

$$\begin{aligned} E_i(0) &= |D_{f,i}|^2 + \sum_{\substack{\beta \in \mathbb{F}_{p^m} \setminus \{0\} \\ g(\beta)=i}} p^{m-2}(p-1) + \sum_{\substack{\beta \in \mathbb{F}_{p^m} \setminus \{0\} \\ g(\beta)\neq i}} p^{m-2} \\ &= |D_{f,i}|^2 + p^{m-2}(p-1)(|D_{g,i}| - \delta_{g,i}) + p^{m-2}(p^m - |D_{g,i}| - \delta_{g,i} + 1). \end{aligned} \tag{18}$$

It follows from Lemma 3.7 that

$$\begin{aligned} E_i(0) &= |D_{f,i}|^2 + p^{2m-2} + p^{m-2} + p^{m-2}(p-2)|D_{g,i}| - p^{m-1}\delta_{g,i} \\ &= \begin{cases} (p^{m-1} + (-1)^{1_S(0)} p^{\frac{m}{2}-1}(p-1) - 1)^2 + p^{2m-2} + p^{m-2} & \\ +p^{m-2}(p-2)(p^{m-1} + (-1)^{1_S(0)} p^{\frac{m}{2}-1}(p-1) - 1) - p^{m-1}\delta_{g,i} & \text{if } i = 0, \\ (p^{m-1} + (-1)^{1_S(0)} p^{\frac{m}{2}-1})^2 + p^{2m-2} + p^{m-2} & \\ +p^{m-2}(p-2)(p^{m-1} + (-1)^{1_S(0)} p^{\frac{m}{2}-1}) - p^{m-1}\delta_{g,i} & \text{if } i \neq 0. \end{cases} \end{aligned} \tag{19}$$

We can see from (16)–(19) that $E_i(\gamma) \neq 0$ for any $\gamma \in \mathbb{F}_{p^m}$. This completes the proof by using Proposition 3.9. □

As pointed out in preliminaries, a family of weakly regular p-ary bent functions of $(p-1)$-form exists. This leads to the following corollary, which is a direct consequence of Corollary 3.5 and Theorem 4.1. It can be obtained from the result of [28] as well when $p = 3$.

Corollary 4.2 *Let m be a positive even integer, and let $f \in \mathcal{B}_l^w(m, p)$ with $l = p - 1$. If $p \in \{3, 5\}$, then $\mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,i})$ is a strongly regular Ramanujan graph for all $i = 0, 1, 2, \ldots, p-1$ and $m \geq 4$.*

In [28], a characterization for weakly regularity of a ternary bent function was given, and it was generalized [12] to a p-ary bent function f of l-form except when f is not of $(p-1)$-form.

We now study the regularity of a p-ary bent function of $(p-1)$-form in the following theorem.

Theorem 4.3 *Let m be a positive even integer, and let $f \in \mathcal{B}_l(m, p)$ with $l = p - 1$. Then the following statements are equivalent.*

(i) *f is regular bent.*
(ii) *$\mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,i})$ is a strongly regular graph for some $i = 0, 1, \ldots, p-1$.*

Further, if (ii) holds, then $\mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,i})$ is a strongly regular graph for all $i = 0, 1, \ldots, p-1$.

Proof $(i) \Rightarrow (ii)$; this follows from Corollary 3.5.

$(ii) \Rightarrow (i)$; let $W_f(\beta) = (-1)^{1_S(\beta)} p^{\frac{m}{2}} \zeta_p^{g(\beta)}$, where S is a subset of $\mathbb{F}_{p^m}$ and g is a p-ary function in m variables. It follows from Lemma 3.4 that $G_{f,i} = \mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,i})$ has at most five eigenvalues for all $i = 0, 1, \ldots, p-1$. However, by our assumption, $G_{f,i}$ has two or three eigenvalues. Consequently, S must be either the empty set or the ambient set, that is, f is weakly regular bent. It follows from Corollary 3.5-(i) that f is regular bent. □

4.2 Odd dimensional cases

Theorem 4.4 *Let m be a positive odd integer. Let $f \in \mathcal{B}_l(m, p)$ and $W_f(\beta) = (-1)^{1_S(\beta)} (p^*)^{\frac{m}{2}} \zeta_p^{g(\beta)}$ for all β in $\mathbb{F}_{p^m}$.*

(i) *$\mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,0})$ is a Ramanujan graph for all $m \geq 3$.*
(ii) *Assume $\left(\frac{i}{p}\right) = 1$ for $i = 1, 2, \ldots, p-1$. Then $\mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,i})$ is a Ramanujan graph if and only if $0 \in S$ and $m \geq 3$, or $0 \notin S$ and $m \geq 1$.*
(iii) *Assume $\left(\frac{i}{p}\right) = -1$ for $i = 1, 2, \ldots, p-1$. Then $\mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,i})$ is a Ramanujan graph if and only if $0 \in S$ and $m \geq 1$, or $0 \notin S$ and $m \geq 3$.*

In particular, if $f \in \mathcal{B}_l^w(m, p)$, then $\mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,i})$ has diameter 2 for $i = 0, 1, \ldots, p-1$ and $m \geq 3$.

Proof In order to check if $\mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,i})$ is a Ramanujan graph, we have to determine p and m satisfying that $\Omega_\beta(D_{f,i}) := 4(|D_{f,i}| - 1) - \chi_\beta(D_{f,i})^2 \geq 0$ for any $\beta \in \mathbb{F}_{p^m}^*$.

(i) It follows from Lemma 3.7 that

$$0 \le \min_{\beta\in\mathbb{F}_{p^m}^*} \Omega_\beta(D_{f,0}) = 3p^{m-1} - 8.$$

$(ii), (iii)$ They follow from Lemma 3.7 that for $i = 1, 2, \ldots, p-1$ and $\left(\frac{i}{p}\right) = 1$,

$$0 \le \min_{\beta\in\mathbb{F}_{p^m}^*} \Omega_\beta(D_{f,i}) = 3p^{m-1} + 4(-1)^{1_S(0)} p^{\frac{m-1}{2}} - 4,$$

and for $\left(\frac{i}{p}\right) = -1$,

$$0 \le \min_{\beta\in\mathbb{F}_{p^m}^*} \Omega_\beta(D_{f,i}) = 3p^{m-1} - 4(-1)^{1_S(0)} p^{\frac{m-1}{2}} - 4.$$

For $\gamma \in \mathbb{F}_{p^m}$ and $i = 0, 1, \ldots, p-1$, we define

$$E_i(\gamma) = \sum_{\beta\in\mathbb{F}_{p^m}} \chi_\beta(D_{f,i})^2 \zeta_p^{\mathrm{Tr}(\beta\gamma)}.$$

To prove that $\mathrm{Cay}(\mathbb{F}_{p^m}, D_{f,i})$ has the diameter 2, we show that $E_i(\gamma) \neq 0$ for any $\gamma \in \mathbb{F}_{p^m}$. We note that

$$\begin{aligned} E_i(\gamma) &= \sum_{\beta\in\mathbb{F}_{p^m}} \chi_\beta(D_{f,i})^2 \zeta_p^{\mathrm{Tr}(\beta\gamma)} = |D_{f,i}|^2 + \sum_{\beta\in\mathbb{F}_{p^m}\setminus\{0\}} \chi_\beta(D_{f,i})^2 \zeta_p^{\mathrm{Tr}(\beta\gamma)} \\ &= |D_{f,i}|^2 + p^{m-1} \sum_{\substack{\beta\in\mathbb{F}_{p^m}\setminus\{0\} \\ g(\beta)\neq i}} \zeta_p^{\mathrm{Tr}(\beta\gamma)}. \end{aligned} \tag{20}$$

We first assume that $\gamma \neq 0$. It follows from $\sum_{\beta\in\mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}(\beta\gamma)} = 0$ that

$$E_i(\gamma) = |D_{f,i}|^2 - \sum_{\substack{\beta\in\mathbb{F}_{p^m} \\ \beta=0 \text{ or } g(\beta)=i}} p^{m-1}\zeta_p^{\mathrm{Tr}(\beta\gamma)} = |D_{f,i}|^2 - p^{m-1}(\chi_\gamma(D_{g,i}) + \delta_{g,i}), \tag{21}$$

where $\delta_{g,i} = \begin{cases} 0 & \text{if } 0 \in D_{g,i}, \\ 1 & \text{if } 0 \notin D_{g,i}. \end{cases}$

From the fact that the dual function g of f is also a weakly regular bent function and $f(-\beta) = f(\beta)$ for any $\beta \in \mathbb{F}_p$, using (1), we have that

$$W_g(\beta) = (-1)^{\frac{p-1}{2} + 1_S(\beta)} \sqrt{p^*}^m \zeta_p^{f(\beta)}. \tag{22}$$

We have two cases to consider. Assume $f(\gamma) \neq 0$. It follows from (22) and Lemma 3.7, we have that

$$\begin{aligned} E_i(\gamma) &= |D_{f,i}|^2 - p^{m-1}(\chi_\gamma(D_{g,i}) + \delta_{g,i}) \\ &= \begin{cases} (p^{m-1} - 1)^2 - p^{m-1}(w_\gamma(i) p^{\frac{m-1}{2}} + \delta_{g,i}) & \text{if } i \neq f(\gamma) \text{ and } i = 0, \\ (p^{m-1} + u_0(i) p^{\frac{m-1}{2}})^2 - p^{m-1}\delta_{g,i} & \text{if } i = f(\gamma) \text{ and } i \neq 0, \\ (p^{m-1} + u_0(i) p^{\frac{m-1}{2}})^2 - p^{m-1}(w_\gamma(i) p^{\frac{m-1}{2}} + \delta_{g,i}) & \text{if } i \neq f(\gamma) \text{ and } i \neq 0, \end{cases} \end{aligned} \tag{23}$$

where $w_\gamma(i) = \begin{cases} (-1)^{\frac{p-1}{2}+1} s(\gamma) (\frac{i-f(\gamma)}{p}) & \text{if } \gamma \neq 0, \\ (-1)^{\frac{p-1}{2}+1} s(0) (\frac{i}{p}) & \text{if } \gamma = 0. \end{cases}$

In the case that $f(\gamma) = 0$, we have

$$\begin{aligned} E_i(\gamma) &= |D_{f,i}|^2 - p^{m-1}(\chi_\gamma(D_{g,i}) + \delta_{g,i}) \\ &= \begin{cases} (p^{m-1}-1)^2 & \text{if } i = 0, \\ (p^{m-1} + u_0(i)p^{\frac{m-1}{2}})^2 - p^{m-1}(w_0(i)p^{\frac{m-1}{2}} + \delta_{g,i} + 1) & \text{if } i \neq 0. \end{cases} \end{aligned} \tag{24}$$

Finally, in the case that $\gamma = 0$, we find from (20) that

$$\begin{aligned} E_i(0) &= |D_{f,i}|^2 + p^{m-1} \sum_{\substack{\beta \in \mathbb{F}_{p^m} \setminus \{0\} \\ g(\beta) \neq i}} 1 \\ &= |D_{f,i}|^2 + p^{m-1}(p^m - |D_{g,i}| - \delta_{g,i} + 1). \end{aligned} \tag{25}$$

It then follows from (22) and Lemma 3.7 that

$$E_i(0) = \begin{cases} (p^{m-1}-1)^2 + p^{m-1}(p^m - p^{m-1} + 2 + \delta_{g,i}) & \text{if } i = 0, \\ (p^{m-1} + u_0(i)p^{\frac{m-1}{2}})^2 + p^{m-1}(p^m - p^{m-1} - w_0(i)p^{\frac{m-1}{2}} + \delta_{g,i} + 1) & \text{if } i \neq 0. \end{cases} \tag{26}$$

We can see from (23) and (26) that $E_i(\gamma) \neq 0$ for any $\gamma \in \mathbb{F}_p^m$ with $m \geq 3$. This completes the proof by using Proposition 3.9. □

5 Association schemes

There are several results [5,12,25,28] on constructing (amorphic) association schemes from $f \in \mathcal{B}_l^w(m, p)$. In [28], they constructed amorphic association schemes from $f \in \mathcal{B}_l^w(m, 3)$. This result was extended [5,12] to the weakly regular p-ary bent functions in $\mathcal{B}_l^w(m, p)$.

In [25], they proved the existence of association schemes from $f \in \mathcal{B}_l^w(m, p)$ by using a *non-constructive* proof method. In those cases, the intersection number of the association scheme is independent of l. In the following Theorem 5.2 we also constructed association schemes from $f \in \mathcal{B}_l^w(m, p)$; we used a constructive proof method.

In [12], we constructed amorphic association schemes from $f \in \mathcal{B}_l^w(m, p)$ whose intersection numbers depend on l, where $l \neq p-1$ and $p > 3$; the case that $l = p-1$ for $p > 2$ was open. In the following Theorem 5.1 we solve this open case that $\ell = p-1$ for $p > 2$.

5.1 Even dimensional cases

Theorem 5.1 *Let m be a positive even integer, and let $f \in \mathcal{B}_l^w(m, p)$ with $l = p-1$. Then the decomposition*

$$\{D_{f,0}, D_{f,1}, \ldots, D_{f,p-1}\}$$

is a p-class amorphic association scheme.

Proof It is straightforward from Result 4 and Remark 3.6. □

5.2 Odd dimensional cases

Theorem 5.2 *Let m be a positive odd integer, and let $f \in \mathcal{B}_l^w(m, p)$ with $l = p - 1$. Let $P = \{0\}|D_{f,0}|D_{f,1}|\dots|D_{f,p-1}$ be a partition of $\mathbb{F}_{p^m}$. Then the set of relations $\{R_{f,-1}, R_{f,0}, \dots, R_{f,p-1}\}$ is a p-class association scheme, where $R_{f,-1} = \{(0,0)\}$ and $R_{f,i}$ is defined by*

$$(\alpha, \beta) \in R_{f,i} \textit{ if and only if } \alpha - \beta \in D_{f,i}.$$

Proof Let f be a weakly regular bent function with its dual $\tilde{f}$. Then by Lemma 3.7 and $\tilde{\tilde{f}}(x) = f(-x) = f(x)$, we see that for any $i, j \in \{0, 1, \dots, p-1\}$, the sum $\chi_\alpha(D_{f,i})$ does not depend on the choice of $\alpha \in D_{\tilde{f},j}$, and the sum $\chi_\beta(D_{\tilde{f},i})$ does not depend on the choice of $\beta \in D_{f,j}$. The proof follows immediately from Result 3. □

The first and second eigenmatrices (for the definition, we refer to [19]) of the schemes in Theorems 5.1 and 5.2 can be computed explicitly by using Lemmas 3.4 and 3.7, respectively.

Acknowledgements J.Y. Hyun was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (NRF-2017R1D1A1B05030707), J. Lee by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (NRF-2017R1A6A3A11030486) and 2019 Research Grant from Kangwon National University, and Y. Lee by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (Grant No. 2019R1A6A1A11051177) and also by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (NRF-2017R1A2B2004574). We express our gratitude to the reviewers for their very helpful comments, which lead to improvement of the exposition of this paper.

References

1. Alon N.: Eigenvalues and expanders. Combinatorica **6**(2), 83–96 (1986).
2. Arias de Reyna J.: Finite fields and Ramanujan graphs. J. Combin. Theory Ser. B **70**(2), 259–264 (1997).
3. Bibak K., Kapron B.M., Srinivasan V.: The Cayley graphs associated with some quasi-perfect Lee codes are Ramanujan graphs. IEEE Trans. Inf. Theory **62**(11), 6355–6358 (2016).
4. Brouwer A.: Web database of strongly regular graphs. https://www.win.tue.nl/~aeb/graphs/srg/srgtab.html.
5. Chee Y.M., Tan Y., Zhang X.D.: Strongly regular graphs constructed from p-ary bent functions. J. Algebr. Combin. **34**(2), 251–266 (2011).
6. Chiu P.: Cubic Ramanujan graphs. Combinatorica **12**, 275–285 (1992).
7. Colbourn C.J., Dinitz J.H.: Handbook of Combinatorial Designs. Discrete Mathematics and Its Applications, 2nd edn. Chapman & Hall/CRC, Boca Raton (2007).
8. Davidoff G., Sarnak P., Valette A.: Elementary Number Theory, Group Theory, and Ramanujan Graphs. Cambridge University Press, Cambridge (2003).
9. Godsil C.D.: Algebraic Combinatorics. Chapman & Hall/CRC, Boca Raton (1993).
10. Goldreich O., Impagliazzo R., Levin L., Venkatesan R., Zuckerman D.: Security preserving amplification of hardness. In: 31st Annual Symposium on Foundations of Computer Science, vol. I (1990), IEEE Computer Society Press, Los Alamitos, CA, pp. 318–326. Proofs of two conjectures on ternary weakly regular bent functions. IEEE Trans. Inf. Theory **55**(11), 5272–5283 (2009).
11. Hoory S., Linial N., Wigderson A.: Expander graphs and their applications. Bull. Am. Math. Soc. **43**(4), 439–561 (2006).
12. Hyun J.Y., Lee Y.: Characterization of p-ary bent functions in terms of strongly regular graphs. IEEE Trans. Inf. Theory **65**(1), 676–684 (2019).
13. Kalton N.J., Roberts J.W.: Uniformly exhaustive submeasures and nearly additive set functions. Trans. Am. Math. Soc. **278**(2), 803–816 (1983).
14. Krebs M., Shaheen A.: Expander families and Cayley Graphs: A Beginner's Guide. Oxford University Press, Oxford (2011).
15. Kumar P.V., Scholtz R.A., Welch L.R.: Generalized bent functions and their properties. J. Combin. Theory Ser. A **40**(1), 90–107 (1985).

16. Lubotzky A.: Expander graphs in pure and applied mathematics. Bull. Am. Math. Soc. **49**(1), 113–162 (2012).
17. Lubotzky A., Phillips R., Sarnak P.: Ramanujan graphs. Combinatorica **8**(3), 261–277 (1988).
18. Ma S.L.: A survey of partial difference sets. Des. Codes Cryptogr. **4**(3), 221–261 (1994).
19. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1998).
20. Marcus A.W., Spielman D.A., Srivastava N.: Interlacing families I: Bipartite Ramanujan graphs of all degrees. Ann. Math. (2) **182**(1), 307–325 (2015).
21. Margulis G.A.: Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators. Probl. Inf. Transm. **24**(1), 39–46 (1988).
22. Mesnager S., Tang C., Qi Y.: 2-correcting Lee codes: (quasi)-perfect spectral conditions and some constructions. IEEE Trans. Inf. Theory **64**(4), part 2, 3031–3041 (2018).
23. Morgenstern M.: Existence and explicit constructions of $q+1$ regular Ramanujan graphs for every prime power q. J. Combin. Theory Ser. B **62**(1), 44–62 (1994).
24. Pippenger N.: Sorting and selecting in rounds. SIAM J. Comput. **16**(6), 1032–1038 (1987).
25. Pott A., Tan Y., Feng T., Ling S.: Association schemes arising from bent functions. Des. Codes Cryptogr. **59**(1–3), 319–331 (2011).
26. Reingold O., Vadhan S., Wigderson A.: Entropy waves, the zig-zag graph product, and new constant-degree expanders. Ann. Math. (2) **155**(1), 157–187 (2002).
27. Sipser M., Spielman D.A.: Expander codes. IEEE Trans. Inf. Theory **42**(6), part 1, 1710–1722 (1996).
28. Tan Y., Pott A., Feng T.: Strongly regular graphs associated with ternary bent functions. J. Combin. Theory Ser. A **117**(6), 668–682 (2010).
29. Tang C., Li N., Qi Y., Zhou Z., Helleseth T.: Linear codes with two or three weights from weakly regular bent functions. IEEE Trans. Inf. Theory **62**(3), 1166–1176 (2016).
30. van Dam E.R.: Strongly regular decompositions of the complete graph. J. Algebr. Combin. **17**(2), 181–201 (2003).
31. Williamson C.: Spectral Graph Theory, Expanders, and Ramanujan Graphs. University of Washington (2014). https://sites.math.washington.edu/~morrow/papers/chris-thesis.pdf.
32. Zinovev V.A., Ericson T.: Fourier-invariant pairs of partitions of finite abelian groups, and association schemes. Probl. Inf. Transm. **45**(3), 221–231 (2009).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.