Des. Codes Cryptogr. (2007) 44:49–62
DOI 10.1007/s10623-007-9057-6

Pseudo-Paley graphs and skew Hadamard difference sets from presemifields

Guobiao Weng · Weisheng Qiu · Zeying Wang · Qing Xiang

Received: 2 October 2006 / Revised: 22 February 2007 / Accepted: 1 March 2007 /
Published online: 30 March 2007

Abstract Let $(K, +, *)$ be an odd order presemifield with commutative multiplication. We show that the set of nonzero squares of $(K, *)$ is a skew Hadamard difference set or a Paley type partial difference set in $(K, +)$ according as q is congruent to 3 modulo 4 or q is congruent to 1 modulo 4. Applying this result to the Coulter–Matthews presemifield and the Ding–Yuan variation of it, we recover a recent construction of skew Hadamard difference sets by Ding and Yuan [7]. On the other hand, applying this result to the known presemifields with commutative multiplication and having order q congruent to 1 modulo 4, we construct several families of pseudo-Paley graphs. We compute the p-ranks of these pseudo-Paley graphs when $q = 3^4, 3^6, 3^8, 3^{10}, 5^4$, and 7^4. The p-rank results indicate that these graphs seem to be new. Along the way, we also disprove a conjecture of René Peeters [17, p. 47] which says that the Paley graphs

Dedicated to Dan Hughes on the occasion of his 80th birthday.

G. Weng (✉) · W. Qiu
LMAM, School of Mathematical Sciences,
Peking University,
Beijing 100871, People's Republic of China
e-mail: fireblbl@math.pku.edu.cn

Z. Wang · Q. Xiang
Department of Mathematical Sciences,
University of Delaware,
Newark, DE 19716, USA

W. Qiu
e-mail: qiuws@math.pku.edu.cn

Z. Wang
e-mail: wangz@math.udel.edu

Q. Xiang
e-mail: xiang@math.udel.edu

of nonprime order are uniquely determined by their parameters and the minimality of their relevant p-ranks.

Keywords Difference set · Paley graph · Planar function · p-rank · Presemifield · Semifield · Skew Hadamard difference set · Strongly regular graph

AMS Classifications 05B10 · 05B25 · 17A35

1 Introduction

Let G be a finite (multiplicative) group of order v. A k-element subset D of G is called a (v, k, λ) *difference set* if the list of "differences" xy^{-1}, $x, y \in D$, $x \neq y$, represents each nonidentity element in G exactly λ times. As an example of difference sets, we mention the classical Paley difference set (in the additive group of $\mathbf{F}_q$) consisting of the nonzero squares of $\mathbf{F}_q$, where $q \equiv 3 \pmod 4$. Difference sets are the same objects as regular (i.e., sharply transitive) symmetric designs. They are the subject of much study in the past 50 years. For a recent survey, see [19].

Again let G be a finite (multiplicative) group of order v. A k-element subset D of G is called a (v, k, λ, μ) *partial difference set* (PDS, in short) provided that the list of "differences" xy^{-1}, $x, y \in D$, $x \neq y$, contains each nonidentity element of D exactly λ times and each nonidentity element of $G \backslash D$ exactly μ times. The set of nonzero squares in $\mathbf{F}_q$, $q \equiv 1 \pmod 4$, is a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$ PDS in the additive group of $\mathbf{F}_q$. Given a (v, k, λ, μ) partial difference set D in G with $1 \notin D$ and $D^{(-1)} = D$, where $D^{(-1)} = \{d^{-1} \mid d \in D\}$, one can construct a strongly regular Cayley graph $\mathrm{Cay}(G, D)$ whose vertex set is G, and two vertices x, y are adjacent if and only if $xy^{-1} \in D$. Such a strongly regular graph $\mathrm{Cay}(G, D)$ has G as a regular automorphism group. On the other hand, if a strongly regular graph has a regular automorphism group G, one can obtain a partial difference set in G. Therefore, partial difference sets are equivalent to strongly regular graphs with a regular automorphism group. For a survey on partial difference sets, we refer to [14].

A difference set D in a finite group G is called *skew Hadamard* if G is the disjoint union of D, $D^{(-1)}$, and $\{1\}$. A classical example of skew Hadamard difference sets is the Paley difference set just mentioned above. Let D be a (v, k, λ) skew Hadamard difference set in an abelian group G. Then we have

$$1 \notin D, \quad k = \frac{v-1}{2} \quad \text{and } \lambda = \frac{v-3}{4}.$$

That is, D will have the so-called Hadamard parameters; justifying the name skew Hadamard difference set.

As a counterpart of skew Hadamard difference sets, we mention Paley type PDS. Let G be a group of order v, $v \equiv 1 \pmod 4$. A subset D of G, $1 \notin D$, is called a *Paley type PDS* if D is a $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$ PDS. Again the set of nonzero squares in $\mathbf{F}_q$, $q \equiv 1 \pmod 4$, is an example of Paley type PDS, which is usually called *the Paley PDS* in $\mathbf{F}_q$. The strongly regular Cayley graph constructed from the Paley PDS is called the *Paley graph*. A strongly regular graph with parameters $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$, where q is a prime power congruent to 1 modulo 4, is called a *Pseudo-Paley graph*.

Let G be an abelian group of order p^{2s+1}, where p is a prime, s is a non-negative integer. It was conjectured that if G contains either a skew Hadamard difference set or a Paley type PDS, then G has to be elementary abelian. This conjecture is still open in general. See [3,20] for some results on this conjecture. It was further conjectured some time ago that the Paley difference sets are the only examples of skew Hadamard difference sets in abelian groups. This latter conjecture is now disproved by Ding and Yuan [7], who constructed new skew Hadamard difference sets in $\mathbf{F}_{3^m}$ by using certain planar functions. Recently more new skew Hadamard difference sets were constructed in [8] by using certain permutation polynomials of $\mathbf{F}_{3^m}$ associated to the Ree-Tits slice spread in $\mathrm{PG}(3, 3^m)$. However, both constructions in [7,8] seemed to be mysterious, and we did not have a satisfactory explanation for them.

In this paper, we show that the Ding–Yuan construction is a special case of a much more general construction. It turns out that just as in the field case, for any presemifield $(K, +, *)$ with commutative multiplication, where $|K| = q$ is odd, the set of nonzero squares of $(K, *)$ is either a skew Hadamard difference set or a Paley type PDS in $(K, +)$ according as $q \equiv 3 \pmod 4$ or $q \equiv 1 \pmod 4$. We remark that this result is actually proved in the more general context of planar functions. Specializing to the Coulter–Matthews presemifield and the Ding–Yuan variation of it, we obtain the Ding–Yuan skew Hadamard difference sets. On the other hand, applying our construction to other known odd order presemifields with commutative multiplication, we obtain three families and one sporadic example of Paley type PDS. From these PDS, we get pseudo-Paley graphs. We compute the p-ranks of these pseudo-Paley graphs when the orders of the graphs are $3^4, 3^6, 3^8, 3^{10}, 5^4$ or 7^4. The p-rank results indicate that these graphs seem to be new. We also give a formula for the p-ranks of the $\mathcal{P}^*$-graphs (see the definition of the $\mathcal{P}^*$-graphs in Sect. 2). By comparing the p-ranks of the Paley graphs and the the $\mathcal{P}^*$-graphs, we disprove a conjecture of René Peeters [17, p. 47] which says that the Paley graphs of nonprime order are uniquely determined by their parameters and the minimality of their relevant p-ranks.

2 Skew Hadamard difference sets and Paley type PDS from planar functions and presemifields

Let G and H be groups of the same order v. A map $f: G \to H$ is called a *planar function* of degree v if for every nonidentity element $a \in G$, both $\Delta_{f,a}: x \mapsto f(ax)f(x)^{-1}$ and $\nabla_{f,a}: x \mapsto f(x)^{-1}f(xa)$ are bijective. Planar functions were introduced in 1968 by Dembowski and Ostrom [5], in which they used such functions to construct affine planes with certain collineation group. We refer the reader to [6, p. 227] for an introduction to planar functions.

Let G and H be two finite groups, and $f: G \to H$ be a map. For $y \in H$, let $f^{-1}(y) = \{x \in G \mid f(x) = y\}$ and $w(y) = |f^{-1}(y)|$. Also we use 1_H to denote the identity element of H.

Lemma 2.1 *Let G and H be two groups of the same order v. Let $f: G \to H$ be a planar function. For any $y \in H$, we have*

$$\sum_{u \in H} w(yu)w(u) = \begin{cases} v - 1, & \text{if } y \neq 1_H, \\ 2v - 1, & \text{if } y = 1_H. \end{cases} \tag{1}$$

Proof We consider two cases.

Case 1 $y \neq 1_H$.

$$\sum_{u\in H} w(yu)w(u) = \sum_{u\in H} |\{(z_1, z_2) \in G \times G \,|\, f(z_1) = yu, f(z_2) = u\}|$$
$$= |\{(z_1, z_2) \in G \times G \,|\, f(z_1)f(z_2)^{-1} = y\}|.$$

Let $S_y = \{(z_1, z_2) \in G \times G \,|\, f(z_1)f(z_2)^{-1} = y\}$. Define the map ϕ as follows:

$$\begin{aligned} \phi &: S_y \to G \setminus \{1\}, \\ (z_1, z_2) &\mapsto z_1 z_2^{-1}. \end{aligned} \tag{2}$$

We claim that ϕ is a bijection between S_y and $G \setminus \{1\}$.

(1) $\phi(z_1, z_2) \neq 1$ (so that the map ϕ is well defined). If $\phi(z_1, z_2) = 1$, then $z_1 = z_2$, which implies that $y = 1_H$, a contradiction.
(2) ϕ is one to one.
If $(z_1, z_2) \in S_y$ and $(z_3, z_4) \in S_y$ satisfy $\phi(z_1, z_2) = \phi(z_3, z_4)$, then

$$z_1 z_2^{-1} = z_3 z_4^{-1} := a \in G \setminus \{1\}. \tag{3}$$

It follows that $z_1 = az_2, z_3 = az_4$, and $f(az_2)f(z_2)^{-1} = f(az_4)f(z_4)^{-1} = y$. Hence $z_2 = z_4$ by the assumption that f is planar. As a result, we also have $z_1 = z_3$.
(3) ϕ is onto.

For any $a \in G \setminus \{1\}$, since f is planar, we can find a unique $z \in G$ such that $f(az)f(z)^{-1} = y$. Hence $(az, z) \in S_y$ and $\phi(az, z) = a \in G \setminus \{1\}$.

Summing up, we have

$$\sum_{u\in H} w(yu)w(u) = |S_y| = |\phi(S_y)| = |G \setminus \{1\}| = v - 1. \tag{4}$$

Case 2 $y = 1_H$.

$$\sum_{u\in H} w(u)^2 = |\{(z_1, z_2) \in G \times G | f(z_1)f(z_2)^{-1} = 1\}$$
$$= |\{(z_1, z_2) \in G \times G | z_1 \neq z_2, f(z_1)f(z_2)^{-1} = 1\}| + |\{(z_1, z_1) \in G \times G\}|$$
$$= (v - 1) + v = 2v - 1.$$

The proof is complete. □

Let G and H be two groups of the same odd order v. A map $f: G \to H$ is said to be *2-to-1* if for every nonidentity $y \in H$, $|f^{-1}(y)| = 0$ or 2, and $f^{-1}(1_H) = \{1_G\}$, where 1_G and 1_H are the identities of G and H, respectively.

Theorem 2.2 *Let G and H be two finite groups of the same order v. Let $f: G \to H$ be a 2-to-1 planar function and $D = f(G) \setminus \{1_H\}$.*

(1) *If $v \equiv 3 \pmod 4$, then D is a skew Hadamard difference set in H.*
(2) *If $v \equiv 1 \pmod 4$, then D is a $(v, (v-1)/2, (v-5)/4, (v-1)/4)$ partial difference set in H.*

Proof Since f is planar, by Lemma 2.1, we have for $y \in H$,

$$\sum_{u \in H} w(yu)w(u) = \begin{cases} v-1, & \text{if } y \neq 1_H, \\ 2v-1, & \text{if } y = 1_H. \end{cases} \tag{5}$$

By the assumption that f is 2-to-1, we have for $u \in H$,

$$w(u) = \begin{cases} 1, & \text{if } u = 1_H, \\ 2, & \text{if } u \in D, \\ 0, & \text{if } u \notin f(G). \end{cases} \tag{6}$$

For any $y \in H$, $y \neq 1_H$, it follows from (5) and (6) that

$$v - 1 = 4|\{u \mid yu, u \in D\}| + 2|\{u \mid u \in D, u = y, y^{-1}\}|. \tag{7}$$

(1) If $v \equiv 3 \pmod 4$, then $v - 1 \equiv 2 \pmod 4$. Note that

$$0 \leq |\{u \mid u \in D, u = y, y^{-1}\}| \leq 2.$$

We see from (7) that

$$|\{u \mid u \in D, u = y, y^{-1}\}| = 1$$

and

$$|\{u \mid yu, u \in D\}| = (v-3)/4.$$

Hence D is a skew Hadamard difference set in H.

(2) If $v \equiv 1 \pmod 4$, then $v - 1 \equiv 0 \pmod 4$. Again note that

$$0 \leq |\{u \mid u \in D, u = y, y^{-1}\}| \leq 2.$$

We see from (7) that

$$|\{u \mid u \in D, u = y, y^{-1}\}| = 0 \text{ or } 2$$

and

$$|\{u \mid yu, u \in D\}| = \begin{cases} (v-5)/4, & \text{if } y \in D, \\ (v-1)/4, & \text{if } y \notin D. \end{cases}$$

Thus, D is a Paley type PDS in H. □

Our next observation is that under a reasonable assumption on the size of the image of a planar function $f: G \to H$, one can actually show that the planar function f must be 2-to-1. We state the observation as a lemma.

Lemma 2.3 *Let G and H be two finite groups of the same odd order v. Let $f: G \to H$ be a planar function, and $D = f(G) \setminus \{1_H\}$. If $|D| \leq \frac{v-1}{2}$ and $f^{-1}(1_H) = \{1_G\}$, then f is 2-to-1 from G to H. In particular, if $f(x^{-1}) = f(x)$ for every $x \in G$ and $f^{-1}(1_H) = \{1_G\}$, then f is 2-to-1.*

Proof Since f is a planar function from G to H, by Lemma 2.1, we have

$$\sum_{u \in D} w(u)^2 + w(1_H)^2 = 2v - 1 \tag{8}$$

and

$$\sum_{u\in D} w(u) + w(1_H) = v. \tag{9}$$

Combining (8) and (9), we have

$$\sum_{u\in D} (w(u)-2)^2 + (w(1_H)-2)^2 = 4|D| - 2v + 3. \tag{10}$$

Since the left hand side of (10) is non-negative, it follows that $4|D| - 2v + 3 \geq 0$. That is,

$$|D| \geq \frac{2v-3}{4}.$$

Now since v is odd, it follows that

$$|D| \geq \frac{v-1}{2}. \tag{11}$$

If we assume that $|D| \leq \frac{v-1}{2}$, then by (11) we must have $|D| = \frac{v-1}{2}$. Now (10) becomes

$$\sum_{u\in D} (w(u)-2)^2 + (w(1_H)-2)^2 = \frac{4(v-1)}{2} - 2v + 3 = 1.$$

It follows that there exists a unique $u_0 \in f(G)$ satisfying $w(u_0) = 1$ or $w(u_0) = 3$ while $w(u) = 2$ for any other $u \in f(G)$. Furthermore, we see from (9) that $w(u_0)$ cannot be 3.

If we furthermore assume that $f^{-1}(1_H) = \{1_G\}$, then the above u_0 must be 1_H. And for any $u \in f(G)$, $u \neq 1_H$, there are precisely two preimages of u. That is, f is a 2-to-1 function from G to H.

In particular, if $f(x^{-1}) = f(x)$ for every $x \in G$ and $f^{-1}(1_H) = \{1_G\}$, then $|D| \leq \frac{v-1}{2}$. By the above arguments, we see that f is a 2-to-1 function. The proof is complete. □

Let G and H be two finite groups. For convenience, a map $f: G \to H$ is called *even* if $f(x^{-1}) = f(x)$ for every $x \in G$ and $f^{-1}(1_H) = \{1_G\}$.

Corollary 2.4 *Let G and H be two groups of the same odd order v, let $f: G \to H$ be a planar function, and $D = f(G) \setminus \{1_H\}$. If f is even, then D is a skew Hadamard difference set in H or a Paley type PDS in H according as $v \equiv 3 \pmod 4$ or $v \equiv 1 \pmod 4$.*

The proof of the corollary is immediate from Lemma 2.3 and Theorem 2.2.

Next, we will examine the known planar functions to see which ones are even. It turns out that the planar functions coming from odd order presemifields with commutative multiplication are always even. We first give the definition of presemifields and semifields.

Definition 2.5 Let $(K, +, *)$ be a set equipped with two binary operations $+$ and $*$. We call $(K, +, *)$ a presemifield if the two operations satisfy the following conditions:

(1) K is an abelian group with respect to $+$;
(2) $x * (y + z) = x * y + x * z$, $(x + y) * z = x * z + y * z$ for all $x, y, z \in K$;
(3) if $x * y = 0$, then $x = 0$ or $y = 0$.

If furthermore there exists $1 \in K$ such that $1 * x = x * 1 = x$ for all $x \in K$, then we call $(K, +, *)$ a semifield.

The following theorem is well known. For example, see [11,9].

Theorem 2.6 *Let $(K, +, *)$ be a finite presemifield with commutative multiplication and $|K| = q$ odd. Define $f: K \to K$ by $f(x) = x * x$. Then f is a planar function from $(K, +)$ to itself.*

For the convenience of the reader, we give a quick proof of Theorem 2.6 here.

Proof For any $a \in K$, define the map $\Delta_{f,a}: K \to K$ by setting $\Delta_{f,a}(x) = f(x+a) - f(x)$ for all $x \in K$. Straightforward computations show that $\Delta_{f,a}(x) = 2a * x + a * a$ for all $x \in K$. If $a \neq 0$ and $\Delta_{f,a}(x) = \Delta_{f,a}(y)$, for some $x, y \in K$, then $2a * x = 2a * y$. It follows that $x = y$. Hence $\Delta_{f,a}$ is a bijection from K to itself for all $a \neq 0$. Therefore, f is planar. The proof is complete. □

Corollary 2.7 *Let $(K, +, *)$ be an odd order presemifield with commutative multiplication. Then $\{x * x \mid x \in K, x \neq 0\}$, i.e., the set of nonzero squares of K, is a skew Hadamard difference set in $(K, +)$ or a Paley type PDS in $(K, +)$ according as $q \equiv 3 \pmod 4$ or $q \equiv 1 \pmod 4$.*

Proof Define $f: K \to K$ by $f(x) = x * x$. The conclusion of the corollary will follow from Corollary 2.4 if we can show that f is an even planar function from K to itself.

(1) By Theorem 2.6, we know that f is a planar function.
(2) The only preimage of 0 is 0. (If $f(x) = x * x = 0$, then $x = 0$.)
(3) For any $x \in K$, $f(-x) = (-x) * (-x) = x * x = f(x)$.

Hence we have shown that f is indeed an even planar function from K to itself. The proof of the corollary is complete. □

Now we examine the list of all known presemifields with commutative multiplication in the recent survey [12] by Kantor. Certain special Albert twisted fields can have commutative multiplication. But these presemifields give rise to difference sets equivalent to the Paley difference sets. Other than the Albert twisted semifields, only the Coulter–Matthews presemifield [4] and the Ding–Yuan variation of it [7] have orders congruent to 3 modulo 4. Applying Corollary 2.7 to these two presemifields, we recover the Ding–Yuan construction of skew Hadamard difference sets in [7]. Therefore, we now have a satisfactory explanation for the Ding–Yuan construction. (We remark that the construction in [8] still looks mysterious since it does not seem to follow from Corollary 2.7.) The rest of the known odd-order presemifields all have orders congruent to 1 modulo 4. By Corollary 2.7, they produce Paley type PDS in elementary abelian p-groups, which are listed below.

Example 2.8 (*Dickson semifields*) Assume that q is an odd prime power. Let j be a nonsquare in $K = \mathbf{F}_q$, and let $1 \neq \sigma \in Aut(K)$. The Dickson semifield $(K^2, +, *)$ is defined by

$$(a, b) * (c, d) = (ac + jb^\sigma d^\sigma, ad + bc).$$

By Corollary 2.7, the subset

$$D(q, \sigma) = \{(x^2 + jy^{2\sigma}, 2xy) \mid (x, y) \in K^2,\ (x, y) \neq (0, 0)\} \tag{12}$$

is a Paley type PDS in $(K^2, +)$, where $|K^2| = q^2 \equiv 1 \pmod 4$.

Example 2.9 (*Ganley semifields*) Let $K = \mathbf{F}_q$, $q = 3^r$, with $r \geq 3$ odd. The Ganley semifield $(K^2, +, *)$ is defined by

$$(a, b) * (c, d) = (ac - b^9 d - bd^9, ad + bc + b^3 d^3).$$

By Corollary 2.7, the subset

$$G(q) = \{(x^2 + y^{10}, 2xy + y^6) \mid (x, y) \in K^2,\ (x, y) \neq (0, 0)\} \tag{13}$$

is a Paley type PDS in $(K^2, +)$, where $|K^2| = 3^{2r} \equiv 1 \pmod 4$.

Example 2.10 (*Cohen–Ganley semifields*) Let $q \geq 9$ be a power of 3 and let $j \in K = \mathbf{F}_q$ be a nonsquare. The Cohen–Ganley semifield $(K^2, +, *)$ is defined by

$$(a, b) * (c, d) = (ac + jbd + j^3 (bd)^9, ad + bc + j(bd)^3).$$

By Corollary 2.7, the subset

$$CG(q) = \{(x^2 + jy^2 + j^3 y^{18}, 2xy + jy^6) \mid (x, y) \in K^2,\ (x, y) \neq (0, 0)\} \tag{14}$$

is a Paley type PDS in $(K^2, +)$, where $|K^2| = q^2 \equiv 1 \pmod 4$ is an even power of 3.

Example 2.11 (*Penttila–Williams semifield*) Let $K = \mathbf{F}_{3^5}$. The Penttila–Williams semifield is defined by

$$(a, b) * (c, d) = (ac + (bd)^9, ad + bc + (bd)^{27}).$$

By Corollary 2.7, the subset

$$PW = \{(x^2 + y^{18}, 2xy + y^{54}) \mid (x, y) \in K^2,\ (x, y) \neq (0, 0)\} \tag{15}$$

is a Paley type PDS in $(K^2, +)$.

There exists a construction of Paley type PDS by using partial congruence partitions (PCP, in short). Following [14], we describe the construction as follows.

Construction 2.12 (*PCP construction*) *Let G be the additive group of a 2-dimensional vector space V over $\mathbf{F}_q$. Let $H_1, H_2, \ldots, H_r$, where $r \leq q + 1$, be r hyperplanes of V. Then $D = (H_1 \cup H_2 \cup \cdots \cup H_r) \setminus \{0\}$ is a $(q^2, r(q-1), q + r^2 - 3r, r^2 - r)$-PDS in G. Choosing $r = (q + 1)/2$, one obtains a Paley type PDS in G.*

Besides the Paley type PDS produced by the above construction, two infinite families of Paley type PDS in elementary abelian p-groups were previously known. The corresponding Cayley graphs are the Paley graphs and the $\mathcal{P}^*$-graphs (see [18]). We give the definitions of these graphs below. (We mention that in the process of determining all PDS in groups of order p^2, Heinze [10] also constructed some Paley type PDS whose corresponding Cayley graphs are not isomorphic to the Paley graphs.)

Definition 2.13 (*Paley graphs*) Let q be a prime power congruent to 1 modulo 4. Then the set S of nonzero squares of $\mathbf{F}_q$ is a $(q, \frac{1}{2}(q-1), \frac{1}{4}(q-5), \frac{1}{4}(q-1))$ PDS in $(\mathbf{F}_q, +)$. We mention that if q is a square, then S can also be obtained by using the above PCP construction. The Paley graph $P(q)$ is obtained from the Paley PDS by the standard Cayley graph construction. Namely $P(q)$ has the elements of $\mathbf{F}_q$ as vertices; two vertices are adjacent if and only if their difference is in S.

Definition 2.14 ($\mathcal{P}^*$*-graphs*) Let $q = p^{2s}$, where p is a prime congruent to 3 modulo 4. Let g be a primitive element of $\mathbf{F}_q$, and let $C_0 = \{g^{4k} \mid k = 0, 1, \ldots, \frac{q-5}{4}\}$, $C_1 = gC_0$. Then the set $S' = C_0 \cup C_1$ is a Paley type PDS in $(\mathbf{F}_q, +)$. The $\mathcal{P}^*$-graph $P^*(q)$ is obtained from S' by the standard Cayley graph construction.

A graph is said to be *self-complementary* if it is isomorphic to its complement. A graph is said to be *vertex (resp. edge) transitive* if the automorphism group of the graph acts transitively on the vertex (resp. edge) set. A graph which is both vertex transitive and edge transitive is called a *symmetric* graph. Both the Paley graphs and $\mathcal{P}^*$-graphs are self-complementary symmetric graphs (see [18]). Peisert [18] classified all self-complementary and symmetric graphs.

Theorem 2.15 (Peisert [18]) *With one exception, every self-complementary, symmetric graph is ismorphic to either a Paley graph or a* $\mathcal{P}^*$*-graph.*

3 Inequivalence issues

Now we have to consider the question whether the PDS constructed from presemifields are new or not. We first give the precise definitions of equivalence of PDS.

Definition 3.1 Let $D_1, D_2 \subset G$ be two partial difference sets in a group G. The partial difference sets D_1, D_2 are said to be CI-equivalent if there exists an automorphism $\phi \in Aut(G)$ such that $\phi(D_1) = D_2$.

Definition 3.2 Let $D_1, D_2 \subset G$ be two partial difference sets in a group G. The partial difference sets D_1, D_2 are said to be srg-equivalent if the corresponding Cayley graphs are isomorphic, i.e., $\mathrm{Cay}(G, D_1) \cong \mathrm{Cay}(G, D_2)$.

It is clear that CI-equivalence implies srg-equivalence. The converse is not true: there are examples [10] of PDS which are srg-equivalent but not CI-equivalent.

Since the partial congruence partition construction produces a large number of Paley type PDS, it seems quite difficult to decide whether the PDS constructed from presemifields (presemifield PDS, in short) are inequivalent to the PDS from the PCP construction. We will only address the problem whether the presemifield PDS are inequivalent to S and S' defined in Definitions 2.13 and 2.14.

If we can show that the SRG obtained from the presemifield PDS (presemifield SRG, in short) are not isomorphic to the Paley graph or the $\mathcal{P}^*$-graph, then not only we prove that the PDS are inequivalent to S and S', but also the presemifield SRG are not isomorphic to the Paley graph or the $\mathcal{P}^*$-graph. For this purpose, we introduce p-ranks of strongly regular graphs.

Let Γ be a strongly regular graph with parameters (v, k, λ, μ), and let A be its adjacency matrix. Then A has three eigenvalues k, r, and s, with multiplicities $1, f$ and g, respectively, where

$$f + g = v - 1, \quad k + fr + gs = 0.$$

If $f = g$ (i.e., the so-called "half case"), then v must be congruent to 1 modulo 4,

$$(v, k, \lambda, \mu) = \left(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4}\right)$$

and Γ has eigenvalues $(-1 \pm \sqrt{v})/2$. Otherwise the eigenvalues r and s are integers.

Let p be a prime and c be an integer. Then it was shown in [2] that the p-rank of $A + cI$ is completely determined by the parameters of Γ except possibly for the p-ranks

$$\mathrm{rk}_p(2A + I), \quad \text{with } p|v \text{ in the half case, and} \tag{16}$$

$$\mathrm{rk}_p(A - sI), \quad \text{with } p|(r - s) \text{ in all other cases.} \tag{17}$$

So only for these p-ranks, the structure of Γ can play a role. Hence these p-ranks can be used to distinguish between nonisomorphic SRG with the same parameters. We will only be concerned with p-ranks in (16) since the presemifield SRG all fall into the half case.

The p-ranks of the Paley graphs were computed in [2]. We state the result below.

Theorem 3.3 ([2]) *Let $q = p^t$ be a prime power congruent to 1 modulo 4, and let A be the adjacency matrix of the Paley graph $P(q)$. Then*

$$\mathrm{rk}_p(2A + I) = \left(\frac{p+1}{2}\right)^t.$$

Next we compute the p-ranks of the $\mathcal{P}^*$-graphs.

Theorem 3.4 *Let p be a prime congruent to 3 modulo 4, $t = 2s$ be a positive integer, and $q = p^t$. Let A be the adjacency matrix of the $\mathcal{P}^*$-graph $P^*(q)$. Then*

$$\mathrm{rk}_p(2A + I) = 2\left(\frac{p+1}{4}\right)^s \left(\left(\frac{3(p+1)}{4}\right)^s - \left(\frac{p+1}{4}\right)^s\right).$$

The technique is based on the following lemma, which was used in [2] for the Paley graphs.

Lemma 3.5 ([2]) *Let $p(x,y) = \sum_{i=0}^{d-1} \sum_{j=0}^{e-1} c_{ij} x^i y^j$ be a polynomial with coefficients in a field $\mathbf{F}$. Let $M, N \subseteq \mathbf{F}$, with $m := |M| \geq d$ and $n := |N| \geq e$. Consider the $m \times n$ matrix $B = (p(a,b))_{a \in M, b \in N}$ and the $d \times e$ matrix $C = (c_{ij})$. Then $\mathrm{rk}_{\mathbf{F}}(B) = \mathrm{rk}_{\mathbf{F}}(C)$.*

We are now ready to give the proof of Theorem 3.4.

Proof of Theorem 3.4 Let $B = 2A + I - J$, where I is the identity matrix of order q and J is the all-one matrix of order q. We will first determine $\mathrm{rk}_p(B)$.

Let g be a primitive element of $\mathbf{F}_q$, and $\beta = g^{\frac{q-1}{4}}$. Also let $C_0 = \{g^{4i} \mid i = 0, 1, \ldots, \frac{q-5}{4}\}$, $C_1 = gC_0$ and $S' = C_0 \cup C_1$. Define

$$f(x) = \frac{1}{1+\beta}\left(x^{\frac{q-1}{4}} + \beta x^{\frac{3(q-1)}{4}}\right) \in \mathbf{F}_q[x]. \tag{18}$$

Then we have

$$f(x) = \begin{cases} 1, & x \in S', \\ 0, & x = 0, \\ -1, & x \notin S', \quad x \neq 0. \end{cases} \tag{19}$$

The above property of $f(x)$ allows us to represent the entries of B in a compact manner, that is, $B = (f(a-b))_{a\in\mathbf{F}_q, b\in\mathbf{F}_q}$. Let $p(x,y) := f(x-y) = \sum_{i=0}^{q-1}\sum_{j=0}^{q-1} c_{ij}x^i y^j$, where $c_{ij} \in \mathbf{F}_q$, and $C = (c_{ij})_{0\le i\le q-1,\, 0\le j\le q-1}$. By Lemma 3.5, we have $\mathrm{rk}_{\mathbf{F}_q}(B) = \mathrm{rk}_{\mathbf{F}_q}(C)$. Now we want to find explicit expressions for c_{ij}. From (18), we have

$$\begin{aligned} p(x,y) &= \frac{1}{1+\beta}\left((x-y)^{\frac{q-1}{4}} + \beta(x-y)^{\frac{3(q-1)}{4}}\right) \\ &= \frac{1}{1+\beta}\sum_{k=0}^{q-1}\left(\binom{\frac{q-1}{4}}{k}x^{\frac{q-1}{4}-k} + \beta\binom{\frac{3(q-1)}{4}}{k}x^{\frac{3(q-1)}{4}-k}\right)(-y)^k. \end{aligned} \tag{20}$$

Denote by $\langle a_{t-1}a_{t-2}\cdots a_1a_0\rangle_p$ the integer $a_{t-1}p^{t-1}+a_{t-2}p^{t-2}+\cdots+a_1p+a_0$, where $0 \le a_i \le p-1$, for all i. Then $\frac{q-1}{4} = \langle abab\cdots ab\rangle_p$, and $\frac{3(q-1)}{4} = \langle baba\cdots ba\rangle_p$, where $a = \frac{p-3}{4}$, $b = \frac{3p-1}{4}$.

From (20) and the well-known Lucas theorem (for example, see [13]), we have

$$\begin{aligned} (1+\beta)p(x,y) &= \sum_{k=0}^{q-1}\left(\binom{\frac{q-1}{4}}{k}x^{\frac{q-1}{4}-k} + \beta\binom{\frac{3(q-1)}{4}}{k}x^{\frac{3(q-1)}{4}-k}\right)(-y)^k \\ &= \sum_{0\le a_i\le p-1,\forall i} g_{a_{t-1}a_{t-2}\cdots a_0}(x)(-y)^{\langle a_{t-1}a_{t-2}\cdots a_0\rangle_p}, \end{aligned} \tag{21}$$

where

$$\begin{aligned} g_{a_{t-1}a_{t-2}\cdots a_0}(x) = &\binom{a}{a_{t-1}}\binom{b}{a_{t-2}}\cdots\binom{a}{a_1}\binom{b}{a_0}x^{\langle(a-a_{t-1})(b-a_{t-2})\cdots(a-a_1)(b-a_0)\rangle_p} \\ &+\beta\binom{b}{a_{t-1}}\binom{a}{a_{t-2}}\cdots\binom{b}{a_1}\binom{a}{a_0}x^{\langle(b-a_{t-1})(a-a_{t-2})\cdots(b-a_1)(a-a_0)\rangle_p}. \end{aligned}$$

We consider the columns of C, which are labeled by k, $k = \langle a_{t-1}a_{t-2}\cdots a_0\rangle_p$, $0 \le a_i \le p-1$, for all i. There are three cases where a column of C is nonzero.

Case 1 When $0 \le a_i \le a$, $i = 0, 1, \ldots, t-1$, the kth column of C has two nonzero entries, one in row $r_1 = \langle(a-a_{t-1})(b-a_{t-2})\cdots(a-a_1)(b-a_0)\rangle_p$, the other in row $r_2 = \langle(b-a_{t-1})(a-a_{t-2})\cdots(b-a_1)(a-a_0)\rangle_p$, where $0 \le r_1 \le \frac{q-1}{4}$, $\frac{q-1}{2} \le r_2 \le \frac{3(q-1)}{4}$. Denote the $\mathbf{F}_q$-vector space spanned by such column vectors of C by V_1.

Case 2 When $a_{2i_0} > a$ for some i_0, and $a_{t-1} \le a$, $a_{t-2} \le b$, …, $a_1 \le a$, $a_0 \le b$, the kth column of C has exactly one nonzero entry, which is in row $r = \langle(a-a_{t-1})(b-a_{t-2})\cdots(a-a_1)(b-a_0)\rangle_p$, where $0 \le r \le \frac{q-1}{4}$. Denote the $\mathbf{F}_q$-vector space spanned by such column vectors of C by V_2.

Case 3 When $a_{2i_0-1} > a$ for some i_0, and $a_{t-1} \le b$, $a_{t-2} \le a$, …, $a_1 \le b$, $a_0 \le a$, the kth column of C has exactly one nonzero entry, which is in row $r = \langle(b-a_{t-1})(a-a_{t-2})\cdots(b-a_1)(a-a_0)\rangle_p$, where $0 \le r \le \frac{3(q-1)}{4}$. Denote the $\mathbf{F}_q$-vector space spanned by such column vectors of C by V_3.

So $\mathrm{rk}_p(C) = \dim(V_1+V_2+V_3)$. It is easy to see that $V_1 \cap (V_2+V_3) = \{0\}$. Hence

$$\begin{aligned} \mathrm{rk}_p(C) &= \dim(V_1+V_2+V_3) = \dim(V_1)+\dim(V_2+V_3) \\ &= \dim(V_1)+\dim(V_2)+\dim(V_3)-\dim(V_2\cap V_3) \end{aligned} \tag{22}$$

From the definitions of V_1, V_2, and V_3, we see that

$$\dim(V_1) = (a+1)^t, \text{ and } \dim(V_2) = \dim(V_3) = (a+1)^s(b+1)^s - (a+1)^t.$$

It remains to find $\dim(V_2 \cap V_3)$, which can be obtained by counting the number of row vectors of C having at least two nonzero entries. To this end, we expand $p(x, y)$ in a different way:

$$p(x,y) = \sum_{0 \le b_i \le p-1, \forall i} h_{b_{t-1}b_{t-2}\cdots b_0}(-y)x^{\langle b_{t-1}b_{t-2}\cdots b_0\rangle_{(p)}},$$

where

$$h_{b_{t-1}b_{t-2}\cdots b_0}(-y) = \binom{a}{b_{t-1}}\binom{b}{b_{t-2}}\cdots\binom{a}{b_1}\binom{b}{b_0}(-y)^{\langle (a-b_{t-1})(b-b_{t-2})\cdots(a-b_1)(b-b_0)\rangle_p}$$
$$+\beta\binom{b}{b_{t-1}}\binom{a}{b_{t-2}}\cdots\binom{b}{b_1}\binom{a}{b_0}(-y)^{\langle (b-b_{t-1})(a-b_{t-2})\cdots(b-b_1)(a-b_0)\rangle_p}.$$

Let $\ell = \langle b_{t-1}b_{t-2}\cdots b_0\rangle_p$. From above expansion, it is easy to see that the ℓth row of C has at least two nonzero entries (hence exactly two nonzero entries) if and only if $0 \le b_i \le a$, $i = 0, 1, \ldots, t-1$. There are $(a+1)^t$ such rows of C.

As $0 \le b_i \le a$ implies that $b - b_i \ge b - a > a$, if a row vector of C has at least two nonzero entries, then none of those nonzero entries is in a column vector of V_1. We therefore find that $\dim(V_2 \cap V_3) = (a+1)^t$.

Hence

$$\begin{aligned}\mathrm{rk}_p(C) &= \dim(V_1) + \dim(V_2) + \dim(V_3) - \dim(V_2 \cap V_3)\\ &= (a+1)^t + 2\left((a+1)^s(b+1)^s - (a+1)^t\right) - (a+1)^t\\ &= 2(a+1)^s[(b+1)^s - (a+1)^s]\end{aligned}$$

As $B = 2A + I - J$, where A is the adjacency matrix of the $\mathcal{P}^*$-graph $P^*(q)$, we have $B^2 \equiv -J \pmod p$ and $(2A+I)^2 \equiv -J \pmod p$. From $2A + I = B + J \equiv B - B^2 \equiv B(I - B) \pmod p$, it follows that $\mathrm{rk}_p(2A + I) \le \mathrm{rk}_p(B)$. From $B = 2A + I - J \equiv (2A+I) + (2A+I)^2 \equiv (2A+I)(2A+2I)$, it follows that $\mathrm{rk}_p(B) \le \mathrm{rk}_p(2A+I)$. Hence $\mathrm{rk}_p(2A + I) = \mathrm{rk}_p(B) = \mathrm{rk}_p(C) = 2\left(\frac{p+1}{4}\right)^s\left(\left(\frac{3(p+1)}{4}\right)^s - (\frac{p+1}{4})^s\right)$, as claimed. The proof of the theorem is now complete. □

Proposition 3.6 *Let p be a prime congruent to 3 modulo 4, $t = 2s$ be a positive integer, and $q = p^t$. Let A_1, A_2 be the adjacency matrices of the Paley graph $P(q)$ and the $\mathcal{P}^*$-graph $P^*(q)$, respectively. Then $\mathrm{rk}_p(2A_1 + I) > \mathrm{rk}_p(2A_2 + I)$ except when $t = 2$ or 4.*

Proof By Theorems 3.3 and 3.4, we have

$$\mathrm{rk}_p(2A_1 + I) = \left(\frac{p+1}{2}\right)^t$$

and

$$\mathrm{rk}_p(2A_2 + I) = 2\left(\frac{p+1}{4}\right)^s\left(\left(\frac{3(p+1)}{4}\right)^s - \left(\frac{p+1}{4}\right)^s\right).$$

Table 1 $\mathrm{rk}_p(2A+I)$ of the Paley graph, $\mathcal{P}^*$-graph and presemifield SRGs

Order q	Paley graph	$\mathcal{P}^*$-graph	Dickson SRG	Ganley SRG	CG SRG	PW SRG
3^4	$2^4=16$	16	20	N/A	20	N/A
3^6	$2^6=64$	52	85	88	94	N/A
3^8	$2^8=256$	160	376	N/A	448	N/A
3^{10}	$2^{10}=1,024$	484	1,654	1,534	2,084	2,059
5^4	$3^4=81$	N/A	105	N/A	N/A	N/A
7^4	$4^4=256$	256	336	N/A	N/A	N/A

Let $r=\frac{p+1}{4}$. Then

$$\mathrm{rk}_p(2A_1+I)=(2r)^{2s}=4^s\cdot r^{2s}$$

and

$$\mathrm{rk}_p(2A_2+I)=2r^s\left((3r)^s-r^s\right)=2(3^s-1)r^{2s}.$$

Since $4^s>2(3^s-1)$ for $s>2$, we see that $\mathrm{rk}_p(2A_1+I)>\mathrm{rk}_p(2A_2+I)$ except when $t=2$ or 4. □

Some comments are in order. Let p be a prime congruent to 1 modulo 4. In [16,17], it is shown that

$$\mathrm{rk}_p(2A+I)=\frac{p+1}{2},$$

where A is the adjacency matrix of an arbitrary $\left(p,\frac{p-1}{2},\frac{p-5}{4},\frac{p-1}{4}\right)$ SRG. Therefore, it is not possible to use p-rank to distinguish the Paley graph of **prime** order from other SRG with the same parameters. It was then conjectured in [17, p. 47] that the Paley graphs of nonprime order are characterized among the SRG with the same parameters by the property that their relevant p-ranks are minimal. The idea behind this conjecture is similar to that behind Hamada's conjecture (see [1]), namely, the "nicest" or "most regular" SRG with some given parameters can be characterized by its parameters and the minimality of its p-rank for suitable prime p. Proposition 3.6 shows that the Peeters conjecture is not true. We mention that $\mathrm{Aut}(P^*(q))$ is smaller than $\mathrm{Aut}(P(q))$, when $q>23^2$ (see [18]). So in a sense, the Paley graphs are nicer than the $\mathcal{P}^*$-graphs. However, as shown by Proposition 3.6, the p-ranks of the $\mathcal{P}^*$-graphs are smaller than those of the Paley graphs.

It seems difficult to compute theoretically the p-ranks of the presemifield SRG. The difficulty lies in the fact that we do not have compact representations for the entries of the adjacency matrices of the presemifield SRG. Currently, we have the following computer results on p-ranks of the presemifield SRG (see Table 1 below). Based on these results, we see that the presemifield SRG of orders 3^4, 3^6, 3^8, 3^{10}, 5^4, and 7^4 are not isomorphic to Paley graphs or the $\mathcal{P}^*$-graphs. Furthermore, except when $q=3^4$, the presemifield SRG are pairwise nonisomorphic.

There are of course other ways to show that the presemifield SRG are not isomorphic to Paley graphs or the $\mathcal{P}^*$-graphs. Since the Paley graphs and the $\mathcal{P}^*$-graphs are both self-complementary, we may try to argue that the presemifield SRG are not self-complementary. Using a computer, we can show that the Cohen–Ganley SRG and the

Dickson SRG on 3^4 vertices are isomorphic, and they are self-complementary. So we have found a new example of self-complementary SRG on 81 vertices (cf. [15]). Other presemifield SRG in Table 1 are not self-complementary. We conjecture that the presemifield SRG are not self-complementary if the order is greater than 81. Finally, we mention that since the Paley graphs and the $\mathcal{P}^*$-graphs are both rank-3 graphs, we may try to argue that the presemifield SRG are not rank-3. Using a computer, we have checked that all presemifield SRG in Table 1 are not rank-3. We conjecture that the presemifield SRG are always nonrank-3.

Acknowledgments The work of G. B. Weng and W. S. Qiu is partially supported by NSF of China grant 10331030. The work of Q. Xiang is partially supported by NSF grant DMS 0400411. We thank Robert Coulter and Gary Ebert for helpful discussions. We also thank David Saunders for helping us compute p-ranks of some presemifield strongly regular graphs by using the LINBOX package.

References

1. Assmus EF Jr, Key JD (1992) Designs and their codes. Cambridge Tracts in Mathematics 103, Cambridge U.P., Cambridge
2. Brouwer AE, van Eijl CA (1992) On the p-rank of the adjacency matrices of strongly regular graphs. J Algebraic Combin 1:329–346
3. Chen YQ, Xiang Q, Sehgal SK (1994) An exponent bound on skew Hadamard abelian difference sets. Des Codes Cryptogr 4:313–317
4. Coulter RS, Matthews RW (1997) Planar functions and planes of Lenz-Barlotti class II. Des Codes Cryptogr 10:167–184
5. Dembowski P, Ostrom TG (1968) Planes of order n with collineation groups of order n^2. Math Z 103:239–258
6. Dembowski P (1997) Finite geometries. Reprint of the 1968 original. Classics in mathematics. Springer, Berlin
7. Ding CS, Yuan J (2006) A family of skew Hadamard difference set. J Combin Theory (A) 113:1526–1535
8. Ding CS, Wang ZY, Xiang Q Skew Hadamard difference sets from the Ree-Tits slice symplectic spreads in PG$(3, 3^{2h+1})$. J Combin Theory (A), in press
9. Ghinelli D, Jungnickel D (2006) Some geometric aspects of finite abelian groups. Rend Mat Ser VII 26:29–68
10. Heinze HA (2001) Applications of Schur rings in algebraic combinatorics: graphs, partial difference sets and cyclotomy scheme, Ph.D. thesis, University of Oldenburg, Germany
11. Hughes DR (1956) Partial difference sets. Amer J Math 78:650–674
12. Kantor WM (2006) Finite semifields. In: Finite geometries, groups, and computation (Proc. of Conf. at Pingree Park, CO Sept. 2005), de Gruyter, Berlin, New York, pp 103–114
13. Lucas ME (1878) Sur les congruences des nombres eulériens, et des coefficients différentiels des fonctions trigonométriques, suivant un module premier. Bull Soc Math France 6:49–54
14. Ma SL (1994) A survey of partial difference sets. Des Codes Cryptogr 4:221–261
15. Mathon R (1988) On self-complementary strongly regular graphs. Discrete Math 69:263–281
16. Peeters R (1995) Uniqueness of strongly regular graphs having minimal p-rank. Linear Algebra Appl 226/228:9–31
17. Peeters R (1995) Ranks and structure of graphs. Ph.D. thesis, Tilburg University
18. Peisert W (2001) All self-complementary symmetric graphs. J Algebra 240:209–229
19. Xiang Q (2005) Recent progress in algebraic design theory. Finite Fields Appl 11:622–653
20. Xiang Q (1996) Note on Paley type partial difference sets, Groups, difference sets, and the Monster (Columbus, OH, 1993). Ohio State Univ. Math. Res. Inst. Publ., 4, de Gruyter, Berlin, pp 239–244