Journal of Algebraic Combinatorics 2 (1993), 397–409

Partial Difference Triples

KA HIN LEUNG AND SIU LUN MA
Department of Mathematics, National University of Singapore, 10 Kent Ridge Crescent, Singapore, 0511, Republic of Singapore

Received June 22, 1992; Revised April 21, 1993

Abstract. It is known that a strongly regular semi-Cayley graph (with respect to a group G) corresponds to a triple of subsets (C, D, D') of G. Such a triple (C, D, D') is called a partial difference triple. First, we study the case when $D \cup D'$ is contained in a proper normal subgroup of G. We basically determine all possible partial difference triples in this case. In fact, when $|G| \neq 8$ nor 25, all partial difference triples come from a certain family of partial difference triples. Second, we investigate partial difference triples over cyclic group. We find a few nontrivial examples of strongly regular semi-Cayley graphs when $|G|$ is even. This gives a negative answer to a problem raised by de Resmini and Jungnickel. Furthermore, we determine all possible parameters when G is cyclic. Last, as an application of the theory of partial difference triples, we prove some results concerned with strongly regular Cayley graphs.

Keywords: strongly regular graph, semi-Cayley graph, partial difference triple, difference set

1. Introduction

A graph $\Gamma = (V, E)$ with $|V| = v$ is called a (v, k, λ, μ)-*strongly regular graph* if (i) Γ is regular with degree k; and (ii) given any two vertices $u, v \in V$, $uv \in E$ (resp. $uv \notin E$) implies that there are exactly λ (resp. μ) vertices adjacent to both u and v. For basic results concerning strongly regular graphs, see [4]. A strongly regular graph $\Gamma = (V, E)$ is called a *strongly regular Cayley graph* if it admits an automorphism group acting regularly on the vertex set V. The notion has been studied by a number of authors, for reference, please see [3, 5, 9, 10]. A (ν, k, λ, μ)-strongly regular Cayley graph $\Gamma = (V, E)$ can also be described in group theoretic terms. Indeed, the vertex V is identified with the elements of the regular automorphism group H and the edge set E is equal to $\{(g, dg) | d \in S, g \in H\}$ where S is a subset of H satisfying $e \notin S$, $S^{(-1)} = \overline{S}$ and $\overline{S}^2 = \mu\overline{H} + \beta\overline{S} + \gamma e$ where $\beta = \lambda - \mu$ and $\gamma = k - \mu$. Here we use the notation that for any subset U of G, we denote $\sum_{g \in U} g$ in $\mathbb{Z}[G]$ by $\overline{U}$. If t is any integer and $y = \sum_{g \in G} a_g g \in \mathbb{Z}[G]$, we define $y^{(t)} = \sum_{g \in G} a_g g^t$.

Recently, Marušič [11] and de Resmini and Jungnickel [12] started investigating a new kind of strongly regular graphs, namely, *strongly regular semi-Cayley graphs.* A strongly regular graph $\Gamma = (V, E)$ on $2n$ vertices is called a strongly regular semi-Cayley graph if it admits an automorphism group G of order n which has

two orbits on V.

As proved in [12, Lemma 2.1 and Theorem 2.2], any $(2n, k, \lambda, \mu)$-strongly regular semi-Cayley graph $\Gamma = (V, E)$ with respect to a group G can be obtained by using three subsets C, D, D' in G such that they satisfy the following conditions:

$$e \notin D,\ e \notin D', \quad \overline{D}^{(-1)} = \overline{D},\ \overline{D'}^{(-1)} = \overline{D'}; \tag{1}$$

$$\overline{D}^2 + \overline{C}\,\overline{C}^{(-1)} = \mu\overline{G} + \beta\overline{D} + \gamma e; \tag{2}$$

$$\overline{D'}^2 + \overline{C}^{(-1)}\overline{C} = \mu\overline{G} + \beta\overline{D'} + \gamma e; \tag{3}$$

$$\overline{D}\,\overline{C} + \overline{C}\,\overline{D'} = \mu\overline{G} + \beta\overline{C} \tag{4}$$

where e is the identity of G, $\beta = \lambda - \mu$, and $\gamma = k - \mu$. In fact, as described in [12, Lemma 2.1], the vertex set V is identified with two copies of G, say $V = G \cup G'$ where G' is another copy of G. The edge set E is equal to $E_1 \cup E_2 \cup E_3$ with $E_1 = \{(g, dg) | d \in D, g \in G\}$, $E_2 = \{(g', (dg)') | d \in D', g \in G\}$, and $E_3 = \{(g', cg) | c \in C, g \in G\}$.

PROPOSITION 1.1. *Suppose C, D, D' are subsets of a group G satisfying the conditions (1)–(4). Then*

(i) $|D| = |D'|$;
(ii) $(2|D| - \beta)|C| = \mu n$;
(iii) $\Delta = \sqrt{\beta^2 + 4\gamma}$ *is a positive integer and has the same parity as* β;
(iv) $k = |C| + |D| = (4\mu + \Delta^2 - \beta^2)/4$;
(v) $|C| - |D| = (\beta \pm \Delta)/2$.

Proof. (ii) follows the equation (4) and the rest follow by [12, Proposition 2.3]. □

Suppose C, D, D' be subsets of G that satisfy the conditions (1)–(4). Following [12], we call the triple (C, D, D') an $(n; c, d; \lambda, \mu)$- *partial difference triple*. Here $c = |C|$ and $d = |D|$. For convenience, we set $\beta = \lambda - \mu$, $\gamma = c + d - \mu$ and $\Delta = \sqrt{\beta^2 + 4\gamma}$. Note that the triple $(G\backslash C, (G\backslash\{e\})\backslash D, (G\backslash\{e\})\backslash D')$ is an $(n; n - c, n - d - 1; 2(n - c - d) + \mu - 2, 2(n - c - d) + \lambda)$-*partial difference triple* and the associated graph is the complement of the graph associated with the triple (C, D, D'). From now on, we shall say $(G\backslash C, (G\backslash\{e\})\backslash D, (G\backslash\{e\})\backslash D')$ is the complement of (C, D, D').

A (v, k, λ, μ)-strongly regular graph Γ is called *trivial* if Γ or the complement of Γ is a union of complete graphs. In case $\mu = 0$ (and hence $\gamma = k$), Γ is a union of complete graphs. Whereas in the other extreme when $\mu = k$ (and hence $\gamma = 0$), Γ is the complement of a union of complete graphs. Therefore, we say an $(n; c, d; \lambda, \mu)$-partial difference triple *trivial* if $\mu = 0$ or $c + d$. Otherwise, we say it is *nontrivial*.

Let us now sum up the objectives of this paper. In Section 2, we determine all partial difference triples (C, D, D') in a group G when $\langle D \cup D' \rangle$ is contained in

a proper normal subgroup of G. (Clearly, in case G is abelian, the requirement of normality can be removed.) In Section 3, we go back to the case when G is cyclic. We construct a few more examples of partial difference triples. Two of them involve a cyclic group of order 8. This answers negatively a problem raised by de Resmini and Jungnickel [12]. We also determine all possible parameters for partial difference triples with respect to a cyclic group. In the last section, we apply the results developed in Section 3 to study strongly regular Cayley graphs with respect to 2-groups which have a cyclic subgroup of index 2.

2. $\langle D \cup D' \rangle$ is contained in a proper normal subgroup of G

We first fix some notation throughout this section. Let (C, D, D') be a nontrivial $(n; c, d; \lambda, \mu)$-partial difference triple in a group G. Throughout this section, we shall assume $D \cup D'$ is *contained in a proper normal subgroup* H in G.

THEOREM 2.1. *Suppose (C, D, D') is nontrivial. Then one of the following statements is true:*

(a) $(n; c, d; \lambda, \mu) = (8; 4, 1; 0, 2)$ *and* $|H| = 2$ or 4;
(b) $(n; c, d; \lambda, \mu) = (25; 5, 2; 0, 1)$ *and* $|H| = 5$;
(c) $(n; c, d; \lambda, \mu) = (2m^2; 2m, 2m-2; 2m-2, 2)$ *and* $|H| = m^2$ *with* $m \geq 2$.

Proof. Let $\rho : \mathbb{Z}[G] \to \mathbb{Z}[G/H]$ be the ring homomorphism extending the natural surjection from G to G/H. Applying ρ to equations (2) and (4), we get

$$d^2 e + \rho(\overline{C})\rho(\overline{C}^{(-1)}) = \mu|H|\overline{G/H} + (\beta d + \gamma)e; \tag{5}$$

$$(2d - \beta)\rho(\overline{C}) = \mu|H|\overline{G/H}. \tag{6}$$

By equation (6), we see that $2d - \beta > 0$ and $\rho(C) = a\overline{G/H}$. It follows that $\rho(\overline{C})\rho(\overline{C}^{(-1)}) = \mu|H|\overline{G/H}$. Therefore $d^2 = \beta d + \gamma$, which implies $d = (\beta + \Delta)/2$ where $\Delta = \sqrt{\beta^2 + 4\gamma}$. Note that $\beta - \Delta$ is discarded as it is negative. Thus, by Proposition 1.1 (v), $c = d + (\beta \pm \Delta)/2 = 0$ or Δ. The case $c = 0$ can be discarded as (C, D, D') is then trivial. Using Proposition 1.1 again, we conclude

$$c = \Delta, d = (\Delta + \beta)/2, n = \Delta^2/\mu,$$
$$\gamma = (\Delta^2 - \beta^2)/4, \mu = (\beta^2 + 2\beta - \Delta^2 + 6\Delta)/4.$$

Note that $0 \leq \lambda = \mu + \beta = (\Delta + \beta)(\beta + 6 - \Delta)/4$. So we must have $0 < \Delta - \beta \leq 6$. As $\Delta - \beta$ is even, we conclude $\Delta - \beta = 2$, 4 or 6. We first discard the case when $\Delta - \beta = 2$. Using the formula we derived earlier, we see that $\mu = \Delta$. Hence $n = d + 1$ which implies $G = D \cup \{e\}$. This contradicts $H \neq G$.

Let us now deal with the case when $\Delta - \beta = 6$. Using the inequality $c + d > \gamma > 0$, we get $3 < \Delta < 6$. Thus $\Delta = 4$ or 5. If $\Delta = 5$, $(n; c, d; \lambda, \mu) = (25; 5, 2; 0, 1)$.

Clearly, $|H| = 5$. If $\Delta = 4$, $(n; c, d; \lambda, u) = (8; 4, 1; 0, 2)$. As $H \neq G$, $|H| = 2$ or 4.

Finally, we consider the case when $\Delta - \beta = 4$. Let $m = \Delta/2$. It is easy to check that $(n; c, d; \lambda, \mu) = (2m^2; 2m, 2m-2; 4m-2, 2)$. Obviously, for any $h \in G$, the coefficient of h in $\overline{D}\,\overline{C} + \overline{C}\,\overline{D'}$ equals $|D^{(-1)}h \cap C| + |hD'^{(-1)} \cap C| = |Dh \cap C| + |hD' \cap C|$. Therefore by equation (4),

$$|Dh \cap C| + |hD' \cap C| = \begin{cases} \mu = 2 & \text{if } h \notin C \\ \mu + \beta = 2m - 2 & \text{if } h \in C \end{cases} \tag{7}$$

Let $g \in C$. Observe that $Dg \subset Hg\backslash\{g\}$, $gD' \subset gH\backslash\{g\}$. On the other hand, $|Hg \cap C| = |gH \cap C| = \mu|H|/(2d - \beta) = 2|H|/\Delta = |H|/m$. It follows that

$$2m = |Dg \cap C| + |gD' \cap C| + 2 \leq |Hg \cap C| + |gH \cap C| = 2|H|/m. \tag{8}$$

Simplifying, we obtain $|H| \geq m^2$. As $H \neq G$, it forces $|H| = m^2$. □

In case $(n; c, d; \lambda, \mu) = (2m^2; 2m, 2m-2; 2m-2, 2)$, we can in fact say more about C.

LEMMA 2.1. *If $(n; c, d; \lambda, \mu) = (2m^2; 2m, 2m-2; 2m-2, 2)$, and $m > 2$, then for any $g \in C$, $A := H \cap Cg^{-1}$ is a subgroup of order m.*

Proof. Since $|H| = m^2$, (8) becomes an equality. As D, D' do not contain e, it follows that

$$Dg \cap C = gD' \cap C = (Hg \cap C)\backslash\{g\}. \tag{9}$$

After multiplying both sides by g^{-1}, we get

$$D \cap Cg^{-1} = gD'g^{-1} \cap Cg^{-1} = A\backslash\{e\}.$$

Observe that for any $a \in A$, $ag \in C \cap Hg$ and $H \cap Cg^{-1}a^{-1} = (H \cap Cg^{-1})a^{-1}$. After replacing g by ag in equation (9) and multiplying both sides by g^{-1}, we get

$$Da \cap Cg^{-1} = agD'g^{-1} \cap Cg^{-1} = A\backslash\{a\}.$$

Thus $A\backslash\{a\}$ is a subset of Da. Consequently, $D \supset Aa^{-1}\backslash\{e\}$. Similarly, we also have $gD'g^{-1} \supset a^{-1}A\backslash\{e\}$.

Let $N := \{a \in G | Aa = A\}$. Clearly, N is a subgroup is A as $e \in A$. It suffices to show $A = N$. Otherwise, we pick any $x \in A\backslash N$. There exists $y \in A$ such that $yx \notin A$. In particular, $yxg \notin C$. By equation (7), we have $|Dyx \cap Cg^{-1}| + |yxgD'g^{-1} \cap Cg^{-1}| = 2$. In particular $|Dyx \cap A| + |yxgD'g^{-1} \cap A| \leq 2$. Recall that $x \in gD'g^{-1}$, so $x^{-1} \in gD'^{(-1)}g^{-1} = gD'g^{-1}$. Hence $y \in yxgD'g^{-1} \cap A$. So, $|Dyx \cap A| \leq 1$. As we have shown above that $D \supset Ay^{-1}\backslash\{e\}$, we conclude $\{x\} \subset Ax \cap A \subset Dyx \cap A$. So, $Ax \cap A = \{x\}$ as $|Dyx \cap A| \leq 1$. Consequently, $A \cap Ax^{-1} = \{e\}$. So $D \supset (A \cup Ax^{-1})\backslash\{e\}$. In fact $D \cup \{e\} = A \cup Ax^{-1}$ as

$|A \cup Ax^{-1}\backslash\{e\}| = |A| - 1 + |Ax^{-1}| - 1 = |D|$. By the same argument, $D \cup \{e\} = A \cup Az^{-1}$ and $A \cap Az^{-1} = \{e\}$ for any $z \in A\backslash N$. Therefore $Ax^{-1} = Az^{-1}$. Hence $z \in xN$. So we conclude $A = N \cup xN$. By the definition of N and the assumption $yx \notin A$, we have $yN \subset A$ and $yxN \cap A = \emptyset$. This gives us $yA \cap A \supset yN$.

Observe we have in fact proved in the above argument that $yxgD'g^{-1} \cap A = \{y\}$. On the other hand, we have $x^{-1}A\backslash\{e\} \subset gD'g^{-1}$ and hence $yA\backslash\{yx\} \subset yxgD'g^{-1}$. Since $yx \notin A$, we have $yA \cap A \subset yxgD'g^{-1} \cap A = \{y\}$. This is possible only when $N = \{e\}$. In other words, $1 = |N| = m/2$. So $m = 2$ which we agree to rule out. This finishes proving A is a subgroup. □

THEOREM 2.2. *(C, D, D') is a $(2m^2; 2m, 2m - 2; 2m - 2, 2)$ partial difference triple in a group G with $D \cup D'$ being contained in a proper normal subgroup H in G iff $C = Kg \cup Lg'$, $D = (K \cup L)\backslash\{e\}$ and $D' = (g^{-1}Kg \cup g'^{-1}Lg')\backslash\{e\}$ where $g \in H$; $g' \in G\backslash H$ and K, L are subgroups of order m such that $K \cap L = \{e\}$ and $g^{-1}Kg \cap g'^{-1}Lg' = \{e\}$.*

Proof. Sufficiency can be checked by routine calculation. We now show the necessity. By equation (8), there exist elements $g \in H \cap C$ and $g' \in (G\backslash H) \cap C$. By Lemma 2.1, $K := H \cap Cg^{-1}$ and $L := H \cap Cg'^{-1}$ are groups of order m in H. Moreover, $(K \cup L)\backslash\{e\} \subset D$. On the other hand, it is obvious that $Kg \cap Lg' = \emptyset$. Since $|C| = 2m$, we must have $C = Kg \cup Lg'$. By equation (2), we obtain

$$\overline{D}^2 + m\overline{K} + m\overline{L} = 2\overline{H} + (2m - 4)\overline{D} + (4m - 4)e. \tag{10}$$

If there exists $x \in (K \cap L)\backslash\{e\}$, then the coefficient of x on the left-hand side is $2m$ while that on the right is $2 + (2m - 4)$. This is impossible. We thus prove $K \cap L = \{e\}$. In particular, we have then $D = (K \cup L)\backslash\{e\}$. By using a similar argument, we see also that $D' = (g^{-1}Kg \cup g'^{-1}Lg')\backslash\{e\}$ and $g^{-1}Kg \cap g'^{-1}Lg' = \{e\}$. □

Remark. In the above theorem, it is clear that $KL = H$ and the converse is true without assuming $m \neq 2$.

Example 1. As a special case of Theorem 2.2, we can now construct a family of partial difference triples. For any two groups K, L of order m, we set G to be the direct product of K, L, and $\mathbb{Z}_2$. For convenience, we assume K, L are subgroups of G. Set (C, D, D') as described above, we then get a nontrivial partial difference triple of required parameters.

To complete the picture, we shall look into the case when $m = 2$. In that case $(n; c, d; \lambda, \mu) = (8; 4, 2; 2, 2)$. If G is cyclic, no nontrivial example can be found as $D = D'$ must be the set of elements of order 4, so by [12, Theorem 4.2], the graph is trivial. On the other hand, if H is elementary abelian, then $Aa^{-1} \cap A$ defined above will just be $Aa \cap A \supset \{e, a\}$. Therefore $|N| \geq 2$. So (C, D, D')

must be as described above. This observation then takes care of cases when G is an elementary abelian 2-group and when G is a dihedral group with H being not cyclic. If G is a dihedral group and H is cyclic, then it can be shown that C is a (4, 2, 4, 2)-relative difference set. By [13, Corollary 4.1.8], no such relative difference set exists. However, there are examples which are not of the form described above. For example, if $G = \mathbb{Z}_2 \times \mathbb{Z}_4$, we can set $C = \{(0, 0), (0, 1), (1, 0), (1, 3)\}$ and $D = D' = \{(0, 1), (0, 3)\}$. If $G = \langle g, h | g^2 = h^2, g^4 = e, hg = gh^3 \rangle$, then $C = \{1, g, gh, h\}$ and $D = D' = \{h, h^3\}$ form a partial difference triple (c.f. [12, Example 4.3]).

So far, we have determined all partial difference triples with given parameters as in Theorem 2.1 (c). Our next objective is to determine if there exist partial difference triples with given parameters as in Theorem 2.1 (a) and (b). We first deal with the case when $|G| = 25$. Obviously, G is abelian. By [12, Theorem 4.4, Remark 4.5], G is elementary abelian and a (25; 5, 2; 0, 1)-partial difference triple exists.

Now assume $|G| = 8$. So $D = \{g\}$ and $D' = \{g'\}$. By condition (1), the order of g and g' must be 2. Since $\beta \neq 0$, after subtracting equation (3) from equation (2), we see that $g = g'$. Therefore $\langle D \cup D' \rangle = \{g, e\}$ is of order 2. If G is cyclic, then by [12, Theorem 4.2] (C, D, D') is trivial. However, a nontrivial example does exist if G is not cyclic.

Example 2. Let G be an abelian group of order 8. Suppose G is not cyclic and g is an element of order 2. Let K be a subgroup of order 4 and $g \notin K$. Define $C = \{e\} \cup Kg \backslash \{g\}$, and $D = D' = \{g\}$. It is easy to check that (C, D, D') is an (8; 4, 1; 0, 2)-partial difference triple. Observe that in this case, we may replace C by hC for any $h \in G$ (see [12, Example 4.3]).

If G is nonabelian group of order 8, then it must be isomorphic to a dihedral group or quaternion group.

Example 3. Let G be a dihedral group of order 8. We write $G = \langle g, h | g^4 = h^2 = e, gh = hg^3 \rangle$. Let $C = \{e, gh, g^2h, g^3h\}$ and $D = D' = \{h\}$. We leave it to the reader to check that (C, D, D') is also a partial difference triple. Note that $H = \langle h, g^2 \rangle$ in this case.

Example 4. Let G be a quaternion group of order 8. We write $G = \langle g, h | g^2 = h^2, g^4 = e, hg = gh^3 \rangle$. Then $C = \{e, g, gh, h\}$ and $D = D' = \{h^2\}$ form a partial difference triple.

To end this section, we would like to point out that it is possible to determine all nontrivial triples with $D \cup D'$ contained a proper normal subgroup. In case $|G| \neq 8, 25$, we have already determined all. By routine calculation, it is not hard to find them all. However, since it does not involve any new idea, we shall not proceed into that direction.

3. Cyclic partial difference triples

In this section, we shall assume (C, D, D') is a nontrivial $(n; c, d; \lambda, \mu)$-partial difference triple in cyclic group G. Our main objective is to find all possible values for $(n; c, d; \lambda, \mu)$. We shall show that apart from the parameters $(2m^2 + 2m + 1; m^2, m^2 + m; m^2 - 1, m^2)$ given in [12], there are some other nontrivial partial difference triples with different parameters. This gives a negative answer to a problem raised by de Resmini and Jungnickel [12].

We first recall some results concerning the character values of C, D and D'. Recall that any character χ of an abelian group G can be extended to a homomorphism from $\mathbb{Z}[G]$ to $\mathbb{C}$. We shall also denote the extension by χ. As proved in [12, Proposition 3.1], we have the following.

PROPOSITION 3.1. *Let (C, D, D') be an $(n; c, d; \lambda, \mu)$-partial difference triple in an abelian group G. Let χ be a nontrivial character of G. Then either*

(i) $\chi\overline{C} = 0$ *and* $\chi\overline{D} = \chi\overline{D'} = (\beta \pm \Delta)/2$ *or*

(ii) $\chi\overline{D} + \chi\overline{D'} = \beta$.

In any case, $\chi\overline{D} + \chi\overline{D'} \in \{\beta - \Delta, \beta, \beta + \Delta\}$.

We now go back to the case when G is cyclic. Let (C, D, D') be an $(n; c, d; \lambda, \mu)$-partial difference triple in G. For any positive integer w, we define H_w to be the unique subgroup of order w if w is a divisor of n. Otherwise, we define $H_w = \emptyset$. By [12, Lemma 3.5], there exist $x_0, \ldots, x_4 \in \mathbb{Z}$ such that

$$\overline{D} + \overline{D'} = x_0\overline{G} + x_1\overline{H}_{2\Delta} + x_2\overline{H}_{\Delta} + x_3\overline{H}_{\Delta/2} + x_4 e. \tag{11}$$

In equation (11), the readers are reminded that if a set is empty, the corresponding coefficient will be taken as 0. When $H_{2\Delta} = G$, we shall always set $x_1 = 0$. Thus $x_1 \neq 0$ would mean that $H_{2\Delta}$ is a proper subgroup of G. Note that the subgroups concerned form a chain. Thus by considering the number of elements which lie in a certain subgroup, we conclude $0 \leq \sum_{i=0}^{s} x_i \leq 2$ for $s = 0, 1, 2, 3$. Since $D \cup D'$ does not contain e, $\sum_{i=0}^{4} x_i = 0$. Therefore $-2 \leq x_4 = -\sum_{i=0}^{3} x_i \leq 0$.

LEMMA 3.1. $\beta = x_4 = -2, -1, 0$ *and* x_3 *is even.*

Proof. Let (C', E, E') be the complement of (C, D, D'). It is easy to see that β' for (C', E, E') is $-2 - \beta$. If we write

$$\overline{E} + \overline{E'} = x_0'\overline{G} + x_1'\overline{H}_{2\Delta} + x_2'\overline{H}_{\Delta} + x_3'\overline{H}_{\Delta/2} + x_4' e,$$

then $x_4' = -2 - x_4$. Therefore $\beta = x_4$ iff $\beta' = x_4'$. Thus, we can assume $\beta < 0$. Let H be the smallest nonempty subset in $\{G, H_{2\Delta}, H_{\Delta}, H_{\Delta/2}\}$. Let χ be a nonprincipal character on H. Applying χ to equation (11), we get $\chi(\overline{D} + \overline{D'}) = x_4$. By Proposition 3.1, $x_4 = \beta$ or $\beta \pm \Delta$. Since $\Delta + |\beta| > 0$, $x_4 \neq \beta + \Delta$. On the other

hand, $\Delta \geq \sqrt{4\gamma} \geq 2$ as (C, D, D') is nontrivial. As $\beta < 0$, $\beta - \Delta < -2 \leq x_4$. We thus prove $x_4 = \beta$.

Next, we may assume $x_3 \neq 0$. Let χ' be a character which is principal on $H_{\Delta/2}$ but not on H_Δ. Then $\chi'(D + D') = (x_3/2)\Delta + \beta$. By Proposition 3.1, x_3 must be even. □

In Section 2, we have already proved that there is no nontrivial partial difference triple in any cyclic group when $D \cup D'$ is contained in a proper subgroup H. By considering the complement, we may assume $G\backslash(D \cup D')$ cannot be contained in a proper subgroup also. We may thus assume $x_0 = 1$.

LEMMA 3.2. *If n is even and (C, D, D') is nontrivial, then up to complementation, $\overline{D} + \overline{D'}$ is one of the following:*

(a) $\overline{G} - \overline{H}_\Delta$
(b) $\overline{G} + \overline{H}_{2\Delta} - 2\overline{H}_{\Delta/2}$.
(c) $\overline{G} + \overline{H}_\Delta - 2\overline{H}_{\Delta/2}$.
(d) $\overline{G} - \overline{H}_{2\Delta} + 2\overline{H}_\Delta - 2\overline{H}_{\Delta/2}$.

In particular, we may assume $\beta = 0$.

Proof. Since n is even and (C, D, D') is nontrivial, [12, Theorem 4.4] implies n is divisible by Δ. Up to complementation, we may assume $\beta = 0$ or -1. As we have discussed earlier, x_0 must be 1. By (11) and Lemma 3.1, we have

$$\overline{D} + \overline{D'} = \overline{G} + x_1\overline{H}_{2\Delta} + x_2\overline{H}_\Delta + x_3\overline{H}_{\Delta/2} + \beta e. \tag{12}$$

First, we assume $x_1 \neq 0$. Recall that $H_{2\Delta}$ is now a proper subgroup of G. Let χ and χ' be characters of G such that χ is principal on H_Δ but not on $H_{2\Delta}$, and χ' is principal on $H_{2\Delta}$ but not on G. Applying χ and χ' on (12), we get

$$\chi(\overline{D} + \overline{D'}) = [x_2 + (x_3/2)]\Delta + \beta \text{ and} \tag{13}$$
$$\chi'(\overline{D} + \overline{D'}) = [2x_1 + x_2 + (x_3/2)]\Delta + \beta. \tag{14}$$

Subtracting equation (14) from (13), we see that $\chi(\overline{D} + \overline{D'}) - \chi'(\overline{D} + \overline{D'}) = 2x_1\Delta$. Since $x_1 \neq 0$, it follows from Proposition 3.1 that $x_1 = -[x_2 + (x_3/2)] = \pm 1$. Thus for any nontrivial character ϕ principal on H_Δ, we have $\phi(\overline{D} + \overline{D'}) \neq \beta$ and therefore $\phi(\overline{D} - \overline{D'}) = 0$. As before, we let $\rho : \mathbb{Z}[G] \to \mathbb{Z}[G/H_\Delta]$ be the ring homomorphism extending the natural projection from G to G/H_Δ. It follows that $\psi(\rho(\overline{D}) - \rho(\overline{D'})) = 0$ for any nontrivial character ψ on G/H_Δ. Hence we obtain $\rho(\overline{D}) = \rho(\overline{D'})$. In particular, we have $|D \cap gH_\Delta| = |D' \cap gH_\Delta|$ for any $g \notin H_\Delta$. Recall that $G \neq H_{2\Delta}$, so there exists $g \in G\backslash H_{2\Delta}$. But by equation (12), we see that gH_Δ is a disjoint union of $D \cap gH_\Delta$ and $D' \cap gH_\Delta$. It follows that $\Delta = 2|D \cap gH_\Delta|$ which is even. In particular, $\beta \neq -1$. Thus, we may assume $\beta = x_4 = 0$. Recall that $1 + x_1 + x_2 + x_3 + x_4 = 0$ and $0 \leq 1 + x_1 + x_2 \leq 2$. So, we have $1 + x_1 + x_2 + x_3 = 0$ and $-2 \leq x_3 \leq 0$. But by the last lemma,

x_3 is also even. So, $x_3 = 0$ or -2. If $x_3 = 0$, $x_1 = -x_2 = \pm 1$. In any case, $1 + x_1 + x_2 + x_3 \neq 0$ which is impossible. So, we must have $x_3 = -2$. Then we have either $x_2 = 2$, $x_1 = -1$ or $x_2 = 0$, $x_1 = 1$. The former case gives us (d) and the latter case gives us (b).

Next, we assume $x_1 = 0$. Suppose $\beta = -1$. Then $x_4 = -1$ and Δ is odd. In particular, $x_3 = 0$. Since $\sum_{i=0}^{4} x_i = 0$, we conclude $x_2 = 0$. Thus, $n = |G| = 2|D| + 1$ is odd. This is a contradiction. Finally, we assume $\beta = 0$. Using $1 + x_2 + x_3 = 0$, we see that either $x_3 = 0$, $x_2 = -1$ or $x_3 = -2$, $x_2 = 1$. So $\overline{D} + \overline{D'} = \overline{G} - \overline{H}_\Delta$ or $\overline{G} - \overline{H}_\Delta - 2\overline{H}_{\Delta/2}$. □

THEOREM 3.1. *Up to complementation, the parameters for any nontrivial partial difference triples in cyclic groups are the following:*

(a) $(n; c, d; \lambda, \mu) = (2m^2 + 2m + 1; m^2, m^2 + m; m^2 - 1, m^2)$*where* $m \geq 1$.
(b) $(n; c, d; \lambda, \mu) = (2m^2; m^2, m^2 - m; m^2 - m, m^2 - m)$*where* $m \geq 2$.
(c) $(n; c, d; \lambda, \mu) = (2m^2; m^2, m^2 + m; m^2 + m, m^2 + m)$*where* $m \geq 3$.
(d) $(n; c, d; \lambda, \mu) = (2m^2; m^2 \pm m, m^2; m^2 \pm m, m^2 \pm m)$*where* $m \geq 2$.

Proof. As proved in [12, Theorem 4.4], (a) holds whenever n is odd or n is not divisible by Δ. We may therefore assume n is even and n is divisible by Δ. Let (C, D, D') be a nontrivial partial difference triple. As before, we may assume $x_0 = 1$. By Lemma 3.2, we may also assume $\beta = 0$ and $|D| = n/2$ or $(n \pm \Delta)/2$.

Suppose $|D| = n/2$. Then by Proposition 1.1 (ii), $\mu = |C|$. Therefore $\Delta^2 = 4\gamma = 4(|C| + |D| - \mu) = 2n$. Hence, we obtain $n = \Delta^2/2$. Putting $\Delta = 2m$, we thus get $(n; c, d; \lambda, \mu)$ as in (d). Note that in this case $(G\backslash C, D, D')$ is also a partial difference triple.

Next, if $|D| = (n \pm \Delta)/2$, then $|C| = n/2$ or $(n \pm 2\Delta)/2$. If $|C| = n/2$, then $\mu = |D|$. So, by a similar argument, we obtain $(n; c, d; \lambda, \mu)$ as in (b) or (c). Note that in (c), $m \geq 3$. Otherwise, say $m = 2$ and (C', E, E') is the complement of (C, D, D'), then $|E| = |E'| = 1$. That means $E = E' = \{g\}$ where g is the unique element of order 2 in G. By [12, Theorem 4.2], (C', E, E') is trivial. Hence (C, D, D') must also be trivial.

Suppose $|D| = (n \pm \Delta)/2$ and $|C| = (n \pm 2\Delta)/2$. Then using Proposition 1.1 (ii) and (iv), we see that

$$4n \pm 6\Delta = \Delta^2 + 2(n \pm \Delta)(n \pm 2\Delta)/n.$$

(Note that $\beta = 0$.) Therefore, $n = (\Delta^2 + \Delta\sqrt{\Delta^2 + 32})/4$. It is easily checked that $\Delta^2 + 32$ is a perfect square iff $\Delta = 2$ or 7. As $\beta = 0$, Δ is even, so 7 can be dropped. But when $\Delta = 2$, $n = 4$ and $|D| = 1$. Again, (C, D, D') must be trivial. □

The above theorem only gives us necessary conditions for the parameters. As constructed in [12], there are some nontrivial partial difference triples with parameters given in (a). It is natural to ask if there are nontrivial partial

difference triples with parameters given in (b), (c), or (d). Lemma 3.2 provides a useful clue for the following examples.

Example 5. Let $G = \mathbb{Z}_8$.

(i) Set $C = \{0, 1, 2, 5\}$, $D = \{1, 7\}$ and $D' = \{3, 5\}$. Then (C, D, D') form a $(8; 4, 2; 2, 2)$-partial difference triple.
(ii) Set $C = \{1, 3\}$, $D = \{2, 3, 5, 6\}$ and $D' = \{1, 2, 6, 7\}$. Then (C, D, D') is a $(8; 2, 4; 2, 2)$-partial difference triple and $(G\backslash C, D, D')$ is a $(8; 6, 4; 6, 6)$-partial difference triple.

Remark.

(I) The parameters in (i) and (ii) correspond respectively to (b) and (d) given in Theorem 3.1. However, we have not yet been able to find a nontrivial example with its parameters given in (c).
(II) The semi-Cayley graphs obtained from the partial difference triples in (i) and (ii) are isomorphic and equal to one of the two well-known (16, 6, 2, 2)-strongly regular graphs.

In [12], de Resmini and Jungnickel ask if $(n; c, d; \lambda, \mu)$ is of the form $(2m^2 + 2m + 1; m^2, m^2 + m; m^2 - 1, m^2)$ for all nontrivial partial difference triples. It is clear that examples quoted above say otherwise. Next, we shall improve Theorem 3.1. If $|G| = 2m^2$, as we have pointed out earlier, β can be assumed 0. By defining $x = 2\overline{D} - \overline{G}$ and $y = 2\overline{C} - \overline{G}$, equation (2) becomes

$$xx^{(-1)} + yy^{(-1)} = 4m^2e$$

Observe that all the coefficients in x, y are ± 1. Any x, y satisfying the above equation form a pair of *periodic Golay complementary sequences* of length $2m^2$ (see [1, 6]). Using the nonexistence results of Golay complementary sequences by Arasu and Xiang [1], we obtain the following:

THEOREM 3.2. *Let p be a prime congruent to 3 modulo 4 and $m = p^r u$ where p, u are relatively prime. If $u^2 < p^r$, then there is no nontrivial partial difference triple in any cyclic group of order $2m^2$.*

4. Strongly regular Cayley graphs

In this section, we consider nontrivial strongly regular Cayley graphs with respect to a 2-group H which has a cyclic subgroup of index 2. In [12], it is proved that there is no nontrivial strongly regular Cayley graph with respect to H if $|H| > 64$. Here, we shall apply some results proved in Section 3 and a theorem on difference sets to give another proof of the above result. Moreover, we

shall prove that the above result is also true for $|H| \leq 64$ unless H is as given in Example 6.

Let G be a cyclic subgroup of index 2 in H. As we have discussed in Section 1, a $(2n, k, \lambda, \mu)$-strongly regular Cayley graph with respect to H corresponds to a subset S of H satisfying $e \notin S$, $\overline{S}^{(-1)} = \overline{S}$ and $\overline{S}^2 = \mu\overline{H} + \beta\overline{S} + \gamma e$ where $\beta = \lambda - \mu$ and $\gamma = k - \mu$. Fix an element $h \in H \backslash G$, we can then write $S = D \cup Ch$ where C, D are subsets of G. It is easy to see that

$$e \notin D,\ \overline{D}^{(-1)} = \overline{D},\ h^{(-1)}\overline{C}^{(-1)} = \overline{C}h; \tag{15}$$

$$\overline{D}^2 + \overline{C}\,\overline{C}^{(-1)} = \mu\overline{G} + \beta\overline{D} + \gamma e; \tag{16}$$

$$\overline{D}\,\overline{C} + \overline{C}h\overline{D}h^{-1} = \mu\overline{G} + \beta\overline{C}. \tag{17}$$

Note that (C, D, hDh^{-1}) is in fact a $(n; c, d; \lambda, \mu)$-partial difference triple where $c = |C|$ and $d = |D|$. By Theorem 3.1 (c.f. the proof of [12, Theorem 5.6]), we conclude that up to complementation, $n = 2m^2, c + d = 2m^2 \pm m$ and $\lambda = \mu = m^2 \pm m$ for some $m = 2^{2s} \geq 2$. Hence, we have

$$\overline{S}\,\overline{S}^{(-1)} = (m^2 \pm m)\overline{H} + m^2 e. \tag{18}$$

In the literature, any set S which satisfies the above equation is called a $(2^{2s+2}, 2^{2s+1} \pm 2^s, 2^{2s} \pm 2^s)$-difference set in H. For reference, please see [2] and [8]. Next, we recall a result due to Turyn [14].

LEMMA 4.1. *Let K be a cyclic 2-group and $z = \sum_{g \in K} a_g g \in \mathbb{Z}[K]$ with $0 \leq a_g \leq M$. If there exist integers m and c such that $zz^{(-1)} = c\overline{K} + m^2$, then $M \geq m$.*

THEOREM 4.1. *Let H be a group of order 2^{2s+2}. Suppose H has a normal subgroup U of order 2^r where $r < s$. Then no $(2^{2s+2}, 2^{2s+1} \pm 2^s, 2^{2s} \pm 2^s)$-difference set S exists in H if H/U is a cyclic or a dihedral group. If we further assume $\overline{S}^{(-1)} = \overline{S}$, then the same result is true if H/U is a quaternion group or isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{2^{2s-r+1}}$.*

Proof. Let us write m for 2^s. Suppose such S exists. Let $\rho : \mathbb{Z}[H] \to \mathbb{Z}[H/U]$ be the ring homomorphism induced by the natural epimorphism. Then by equation (18), we have $\rho\overline{S}\rho\overline{S}^{(-1)} = (m^2 \pm m)|U|\overline{H/U} + m^2$. Note that the coefficients in $\rho\overline{S}$ lies between 0 and $|U| < m$. In particular, it follows from Lemma 4.1 that H/U cannot be cyclic.

For other cases, we fix a cyclic subgroup V of index 2 in H/U and an element $a \notin V$. Clearly, we can write $\rho\overline{S} = x + ya$ where $x, y \in \mathbb{Z}[V] \subset \mathbb{Z}[H/U]$.

If H/U is a dihedral group, then it is easy to check that $xx^{(-1)} + yy^{(-1)} = (m^2 \pm m)|U|\overline{V} + m^2$ and $xy = [(m^2 \pm m)|U|/2]\overline{V}$. To get a contradiction, we extend V to a cyclic group K of order $2|V|$. Let $b \in K \backslash V$ and $z = x + y^{(-1)}b$. It is easy to check that $zz^{(-1)} = (m^2 \pm m)|U|\overline{K} + m^2$. Again, this is impossible as by the construction, the coefficients of z are between 0 and $|U|$.

For the other cases, we need the assumption $S^{(-1)} = S$. Observe that in this case, we have $x^{(-1)} = x$ and $a^{-1}y^{(-1)} = ya$. Consequently, we conclude $xx^{(-1)} + yy^{(-1)} = (m^2 \pm m)|U|\overline{V} + m^2$ and $xy = [(m^2 \pm m)|U|/2]\overline{V}$. Using a similar argument as before, our desired results follow. □

By checking all 2-groups with a cyclic subgroup of index 2 (see [7, Satz I.14.9] or [12, Result 5.5]), only the following two groups do not satisfy the condition of Theorem 4.1:

(a) $H = \langle g, h \mid g^8 = h^2 = e, hgh^{-1} = g^3 \rangle$ and
(b) $H = \langle g, h \mid g^8 = h^2 = e, hgh^{-1} = g^5 \rangle$.

In these two cases, nontrivial strongly regular Cayley graphs with respect to H do exist.

Example 6.

(a) For $H = \langle g, h \mid g^8 = h^2 = e, hgh^{-1} = g^3 \rangle$, the subset $S = \{g, g^7, h, gh, g^2h, g^5h\}$ generates a (16, 6, 2, 2)-strongly regular Cayley graph.
(b) For $H = \langle g, h \mid g^8 = h^2 = e, hgh^{-1} = g^5 \rangle$, the subset $S = \{g^2, g^3, g^5, g^6, gh, g^3h\}$ generates a (16, 6, 2, 2)-strongly regular Cayley graph.

Remark. The Cayley graphs obtained in Example 6 are isomorphic.

Summarizing, we obtain the following theorem.

THEOREM 4.2. *There is no nontrivial strongly regular Cayley graph with respect to any 2-group H with a cyclic subgroup of index 2 except when $H = \langle g, h \mid g^8 = h^2 = e, hgh^{-1} = g^3 \rangle$ or $\langle g, h \mid g^8 = h^2 = e, hgh^{-1} = g^5 \rangle$.*

Acknowledgment

The authors would like to thank Prof. D. Jungnickel for reading through the original manuscript and for his helpful comments.

References

1. K.T. Arasu and Q. Xiang, "On the existence of periodic complementary binary sequences," submitted.
2. T. Beth, D. Jungnickel, and H. Lenz, *Design Theory,* Cambridge University Press, Cambridge, 1986.
3. W.G. Bridges and R.A. Mena, "Rational G-matrices with rational eigenvalues," *J. Combin. Theory Series A,* **32** (1982), 264–280.
4. P.J. Cameron and J.H. van Lint, *Graphs, Codes and Designs,* Cambridge University Press, Cambridge, 1980.

5. D. Ghinelli and S. Löwe, "On multipliers of partial addition sets," *Geometriae Dedicata* **40** (1991), 53–58.
6. M.J.E. Golay, "Complementary series," *IRE Trans. on Information Theory* **IT-7** (1961), 82–87.
7. B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.
8. E.S. Lander, *Symmetric Designs: An Algebraic Approach*, Cambridge University Press, Cambridge, 1983.
9. S.L. Ma, "Partial difference sets," *Discrete Math.* **52** (1984), 75–89.
10. S.L. Ma, "On association schemes, Schur rings, strongly regular graphs and partial difference sets," *Ars Combin.* **27** (1989), 211–220.
11. D. Marušič, "Strongly regular bicirculants and tricirculants," *Ars Combin.* **25** C (1988), 11–15.
12. M.J. de Resmini and D. Jungnickel, "Strongly regular semi-Cayley graphs," *J. Algebraic Combin.*, **1** (1992), 171–195.
13. V. Tan, "On divisible difference sets," M. Phil. Thesis, National University of Singapore, 1990.
14. R.J. Turyn, "Character sums and difference sets," *Pacific J. Math.* **15** (1965), 319–346.