Journal of Algebraic Combinatorics 1 (1992), 171–195

Strongly Regular Semi-Cayley Graphs

MARIALUISA J. de RESMINI
Dipartimento di Matematica, Università di Roma "La Sapienza," 2 Piazzale Aldo Moro, I-00185 Roma, Italy

DIETER JUNGNICKEL*
Mathematisches Institut, Justus-Liebig-Universität Giessen, Arndtstr.2, D-6300 Giessen, Germany

Received September 23, 1991; Revised April 7, 1992

Abstract. We consider strongly regular graphs $\Gamma = (V, E)$ on an even number, say $2n$, of vertices which admit an automorphism group G of order n which has two orbits on V. Such graphs will be called strongly regular *semi-Cayley graphs*. For instance, the Petersen graph, the Hoffman–Singleton graph, and the triangular graphs $T(q)$ with $q \equiv 5 \bmod 8$ provide examples which cannot be obtained as Cayley graphs. We give a representation of strongly regular semi-Cayley graphs in terms of suitable triples of elements in the group ring $\mathbf{Z}G$. By applying characters of G, this approach allows us to obtain interesting nonexistence results if G is Abelian, in particular, if G is cyclic. For instance, if G is cyclic and n is odd, then all examples must have parameters of the form $2n = 4s^2 + 4s + 2$, $k = 2s^2 + s$, $\lambda = s^2 - 1$, and $\mu = s^2$; examples are known only for $s = 1$, 2, and 4 (together with a noncyclic example for $s = 3$). We also apply our results to obtain new conditions for the existence of strongly regular Cayley graphs on an even number of vertices when the underlying group H has an Abelian normal subgroup of index 2. In particular, we show the nonexistence of nontrivial strongly regular Cayley graphs over dihedral and generalized quaternion groups, as well as over two series of non-Abelian 2-groups. Up to now these have been the only general nonexistence results for strongly regular Cayley graphs over non-Abelian groups; only the first of these cases was previously known.

Keywords: strongly regular graph, Cayley graph, partial difference set, difference set

1. Introduction

Recall that a *Cayley graph* may be defined as a graph $\Gamma = (V, E)$ which admits an automorphism group H acting regularly on the vertex set V (see [23] for background on Cayley graphs). The present paper addresses the case for which the cardinality of V is even, say $2n$, and where Γ admits an automorphism group G of order n which has two orbits (of size n) on V. For obvious reasons we shall call such a graph Γ a *semi-Cayley graph*. Moreover, we will always assume that Γ is *strongly regular* with parameters k, λ, and μ (i.e., Γ has regularity k and, given any two vertices u and v, there are exactly λ, respectively μ, vertices adjacent to both u and v, depending only on whether u and v are adjacent); see

*During the time of this research, Dieter Jungnickel was a visiting professor at the Università di Roma "La Sapienza." He would like to thank this institution for its hospitality and Consiglio Nazionale Delle Ricerche (Italy) for financial support.

[6] for background material on strongly regular graphs. Both Cayley graphs and strongly regular graphs have been in the center of interest for a long time, and the intersection of both classes of graphs has also found considerable attention; see, e.g., [4], [5], [9], [16]–[18], [21].

We recall that strongly regular Cayley graphs can be described in group theoretic terms as follows. The vertices of such a graph Γ can be identified with the elements of the regular automorphism group H, and adjacency can be defined in terms of a suitable subset S of H as follows:

$$u \sim v \Leftrightarrow uv^{-1} \in S, \tag{1.1}$$

where S is actually a *partial difference set*, i.e, the list of differences cd^{-1} (with $c, d \in S$, $c \neq d$) contains each element $h \neq e$ of H either λ or μ times, depending on whether or not h belongs to S. We now identify S with the formal sum $\Sigma_{s \in S} s$ of its elements in the group ring $\mathbf{Z}H$ (which is a convenient abuse of language) and write $S^{(-1)}$ for the sum $\Sigma_{s \in S} s^{-1}$. In this notation the condition for a partial difference set can be written as follows:

$$S^2 = \lambda S + \mu(H - S - e) + ke = \mu H + \beta S + \gamma e, \tag{1.2}$$

where e denotes the unit element of H and where we write $\beta = \lambda - \mu$ and $\gamma = k - \mu$. (Note that $S = S^{(-1)}$, since Γ is not directed, and that $e \notin S$, since Γ has no loops.)

In Section 2 we generalize an approach of Marusic [19] (who considered only cyclic groups) and give a similar group theoretic description of strongly regular semi-Cayley graphs. In this case one needs three subsets C, D, and D' (called a *partial difference triple*) of the corresponding automorphism group G to describe Γ. We also determine the size of the subsets in the partial difference triple in terms of the parameters of Γ and give a few examples for strongly regular semi-Cayley graphs (including an infinite family consisting of examples which cannot be obtained as Cayley graphs).

From Section 3 on, we assume that G is Abelian. We can then apply ordinary characters to the equations involving the partial difference triple to obtain some necessary conditions on the existence of semi-Cayley graphs with an Abelian group. As we shall see, the group ring element $D + D'$ in $\mathbf{Z}G$ can then only take three distinct values (which are in arithmetic progression) under every nonprincipal character. We somewhat strengthen a result of Ma [17] that characterizes the elements of $\mathbf{Z}G$ with this property in the case in which G is cyclic.

Applying these results, in Section 4 we consider the case where G is cyclic. We show that we cannot have $D = D'$ then (unless Γ is trivial), which will be fundamental for the subsequent results. Assuming that n is odd, we show that all cyclic examples must belong to the series of strongly regular graphs with parameters

$$2n = 4s^2 + 4s + 2,\ k = 2s^2 + s,\ \lambda = s^2 - 1,\ \mu = s^2. \tag{1.3}$$

We thus considerably strengthen the work of Marusic [19], who obtained the result in question in the special case in which n is a prime. The only known examples for this situation arise for $s = 1, 2$, and 4. Additionally, there is a noncyclic example with $s = 3$. We discuss semi-Cayley graphs with parameters (1.3) in Section 6.

In Section 5 we assume that Γ is actually a Cayley graph with regular automorphism group H and that G is a subgroup (of index 2) of H. This somewhat simplifies the description of Γ by a partial difference triple, since it forces D and D' to be related by an inner automorphism of H. Applying the results of the preceding sections, we obtain proofs for the nonexistence of nontrivial strongly regular Cayley graphs over dihedral and generalized quaternion groups, as well as over two other series of non-Abelian 2-groups. These have been up to now, the only known general nonexistence results for strongly regular Cayley graphs over non-Abelian groups; only the first of these cases was previously obtained (by Ma [17] with a different proof).

2. Semi-Cayley graphs and partial difference triples

Standard arguments give the following characterization of semi-Cayley graphs:

LEMMA 2.1. *Let G be a group or order n, and let C, D, and D' be three subsets of G satisfying $e \notin D$, D', as well as $D = D^{(-1)}$ and $D' = D'^{(-1)}$. Define a graph $\Gamma = (V, E) = \Gamma(C, D, D'; G)$ as follows:*

$$V = G \cup G', \tag{2.1}$$

where $G' = \{g' : g \in G\}$ is a copy of G;

$$E = E_1 \cup E_2 \cup E_3, \tag{2.2}$$

where $E_1 = \{\{g, dg\} : d \in D, g \in G\}$, $E_2 = \{\{g', (dg)'\} : d \in D', g \in G\}$, and $E_3 = \{\{g', cg\} : c \in C, g \in G\}$. Then Γ is a semi-Cayley graph with respect to G (which acts on Γ by right translation). Moreover, every semi-Cayley graph can be obtained in this way.

THEOREM 2.2. *Let G be a group of order n, and consider the semi-Cayley graph $\Gamma = (V, E) = \Gamma(C, D, D'; G)$. Denote the regularity of Γ by k. Then Γ is strongly regular with parameters $2n$, k, λ, and μ if and only if the three subsets C, D, and D' of G satisfy the following three equations in the group ring $\mathbb{Z}G$:*

$$D^2 + CC^{(-1)} = \lambda D + \mu(G - D - e) + ke = \mu G + \beta D + \gamma e, \tag{2.3}$$

$$D'^2 + CC^{(-1)} = \lambda D' + \mu(G - D' - e) + ke = \mu G + \beta D' + \gamma e, \tag{2.4}$$

$$DC + CD' = \lambda C + \mu(G - C) = \mu G + \beta C. \tag{2.5}$$

Proof. Again, the proof is quite standard. For the convenience of the reader, we will include part of it. One shows that the three equations stated above directly reflect the defining property of a strongly regular graph for the three possible distributions of two arbitrarily given points u and v over the two "halves" G and G' of Γ. Assume first that $u, v \in G$. By the transitivity of G on itself, we may assume without loss of generality that $u = e$. Consider a third vertex $w \in G$, respectively $w' \in G'$, which is joined to both u and v. We first deal with the case $w \in G$. Here Lemma 2.1 shows that w must belong to D (since it is joined to e) and is of the form $w = dv$ for some $d \in D$ (since it is joined to v). The number of such vertices is the number of solutions of the equation $v = d^{-1}w$ with $d, w \in D = D^{(-1)}$ and hence equals the coefficient of v in the group ring element D^2. Now consider the case $w' \in G'$. We obtain the conditions $e = bw$ and $v = cw$ for some $b, c \in C$ (since w' is joined to both e and v). The number of such vertices is the number of solutions of the equation $v = cb^{-1}$ with $b, c \in C$, i.e., the coefficient of v in $CC^{(-1)}$. It is now clear that Equation (2.3) is satisfied if and only if the number of vertices which are adjacent to both u and v equals λ whenever $v \in D$ (i.e., whenever u and v are adjacent) and μ otherwise. (Note that the coefficient of e agrees on both sides of (2.3) since Γ is regular of degree k.) In the same way, the case $u', v' \in G'$ yields Equation (2.4). Finally, similar arguments for the case $u \in G$ and $v' \in G'$ give Equation (2.5). □

Thus the strongly regular semi-Cayley graphs (with respect to a group G) correspond to the triples of subsets of G satisfying Equations (2.3) through (2.5). We will call any such triple a *partial difference triple*. We give examples for these concepts at the end of this section, but first we determine the sizes of the three subsets of G occurring in a partial difference triple.

PROPOSITION 2.3. *Let G be a group of order n, and let (C, D, D') be a partial difference triple over G associated with a strongly regular semi-Cayley graph with parameters $2n$, k, λ, and μ. Then one has*

$$|C| = \frac{2k - \beta \pm \Delta}{4} \quad \text{and} \quad |D| = |D'| = k - |C|, \tag{2.6}$$

where we write

$$\Delta = \left(\beta^2 + 4\gamma\right)^{1/2} \tag{2.7}$$

and, as usual, $\beta = \lambda - \mu$ and $\gamma = k - \mu$. Moreover, Δ is an integer. (Note that Δ is the square root occurring in the well-known rationality condition for strongly regular graphs.)

Proof. Since Γ is regular with degree k, we clearly have $|C| + |D| = |C| + |D'| = k$.

Thus Equation (2.5) implies

$$2|C|(k - |C|) = \beta|C| + n\mu,$$

which gives

$$|C| = \frac{2k - \beta \pm (4k^2 + \beta^2 - 4k\beta - 8n\mu)^{1/2}}{4};$$

using the standard equation relating the parameters of a strongly regular graph, i.e.,

$$k(k - 1 - \beta) = \mu(2n - 1), \tag{2.8}$$

yields the desired formula for C. Since the number of vertices of Γ is even, Γ cannot be a "type I" strongly regular graph, which shows that Δ must be an integer (see [6]). □

We now give some examples for strongly regular semi-Cayley graphs. Of course, strongly regular Cayley graphs on an even number of vertices will occur here.

Example 2.4. Let Γ be a strongly regular Cayley graph with respect to H on an even number, say $2n$, of vertices. If H contains a (normal) subgroup G of index 2, then Γ is also a semi-Cayley graph with respect to G (since G clearly has two orbits of size n on the set of vertices). Thus any strongly regular Cayley graph on an even number of vertices with an Abelian group also is a semi-Cayley graph. In particular, every difference set S with multiplier -1 which does not contain e satisfies Equation (1.2) with $\beta = 0$ and thus can be considered as a partial difference set. If S contains e, one may omit e from S to obtain a partial difference set with $\beta = -2$. Hence any Abelian difference set with multiplier -1 gives rise to a strongly regular semi-Cayley graph (with $\beta = 0$ or $\beta = -2$) since the order of G has to be even in this case. (We refer the reader to [2] for basic results and to a recent survey [14] for the present state of knowledge on difference sets, in particular, those with multiplier -1.)

The following example gives a family of strongly regular semi-Cayley graphs which cannot be considered as Cayley graphs.

Example 2.5. Let Γ be the triangular graph $T(q)$, a strongly regular graph on $q(q-1)/2$ vertices with $k = 2q - 4$, $\lambda = q - 2$, and $\mu = 4$ (see [6]). We now assume that $q \equiv 5 \bmod 8$ is a prime power and use as vertices of Γ the 2-subsets of the finite field $GF(q)$. It is then clear that the affine group $AGL(1, q)$ is an automorphism group of Γ; let G be the subgroup of index 4 of this group, i.e.,

$$G = \{x \to ax + b : a, b \in GF(q), a \text{ a 4th power}\}. \tag{2.9}$$

Since we have $q - 1 \equiv 4 \bmod 8$, G contains no involutions and hence acts semiregularly on the vertices of Γ (i.e., the only automorphism in G fixing some

vertex is the identity). Thus G has two orbits of size $n = q(q-1)/4$, each on the set of vertices of Γ, which shows that Γ is indeed a strongly regular semi-Cayley graph. We now show that Γ cannot be a Cayley graph. Note that any regular automorphism group H of Γ would actually be a (sharply) 2-homogeneous but not 2-transitive permutation group on the q elements of GF(q). To see this, it suffices to observe that the element x of GF(q) can be identified with the clique C_x of Γ of size $q-1$ formed by the vertices $\{x, y\}$. Since the q cliques C_x are the only cliques of size $q-1$ of Γ, any automorphism of Γ must indeed be induced by a permutation of GF(q). Now a result of Kantor [15] shows that the only sharply 2-homogeneous but not 2-transitive groups are the groups ASL(1, q) with $q \equiv 3 \bmod 4$. Hence the triangular graph T(q) is a Cayley graph if and only if $q \equiv 3 \bmod 4$ is a prime power.

We conclude the present section with a few examples. For instance, the Petersen graph is clearly a semi-Cayley graph. (Note that the triangular graph T(5) is the complement of the Petersen graph, so this fits in with Example 2.5.) In Section 4 we shall see that the Hoffman–Singleton graph is also a semi-Cayley graph. We finally give an example with parameters (1.3) for $s = 2$, which is due to Adel'son-Vel'skii, Veisfeiler, Leman, and Faradzev [1]; it is one of the first examples of a distance-regular graph which is not actually distance transitive and is actually the unique semi-Cayley graph with parameters (1.3) and $s = 2$. (This example was rediscovered by Marusic [19].)

Example 2.6. The following three sets form a partial difference triple for the parameters $n = 13$, $k = 10$, $\lambda = 3$, and $\mu = 4$ over $G = \mathbf{Z}_{13}$ (with additive notation):

$$D = \{1, 3, 4, 9, 10, 12\},\ D' = G - D - e = \{2, 5, 6, 7, 8, 11\},\ C = \{0, 1, 3, 9\},$$

as can be easily checked directly. (Alternatively, one may also use multiplicative notation and derive Equations (2.3) through (2.5) by observing that D is a partial difference set for the Paley graph on 13 vertices and that C is a difference set for the projective plane of order 3 and by using the equations satisfied by these two objects; see Proposition 6.4 below.)

3. The Abelian case

From now on we shall assume that G is Abelian, so that we may apply (ordinary complex) characters to our group G, extended by linearity to the group ring $\mathbf{Z}G$. Theorem 2.2 implies the following basic result:

PROPOSITION 3.1. *Let (C, D, D') be a partial difference triple over G for a strongly regular semi-Cayley graph with parameters $2n$, k, λ, and μ, where G is Abelian, and*

let χ be a nonprincipal character of G. Then either

$$\chi(C) = 0 \quad \text{and} \quad \chi(D) = \chi(D') = \frac{1}{2}(\beta \pm \Delta) \tag{3.1}$$

or

$$\chi(D) + \chi(D') = \beta. \tag{3.2}$$

In particular,

$$\chi(D + D') \in \{\beta - \Delta, \beta, \beta + \Delta\} \quad \textit{for every nonprincipal character } \chi. \tag{3.3}$$

Proof. By applying χ to Equations (2.3), (2.4), and (2.5), we obtain the following identities:

$$\chi(D^2) + |\chi(C)|^2 = \beta\chi(D) + \gamma, \tag{3.4}$$

$$\chi(D'^2) + |\chi(C)|^2 = \beta\chi(D') + \gamma, \tag{3.5}$$

$$\chi(C)(\chi(D) + \chi(D')) = \beta\chi(C). \tag{3.6}$$

Clearly (3.6) implies the validity of (3.2) if one has $\chi(C) \neq 0$. Thus we may assume $\chi(C) = 0$. Subtracting (3.5) from (3.4) gives the equation

$$(\chi(D) + \chi(D'))(\chi(D) - \chi(D')) = \beta(\chi(D) - \chi(D')).$$

If one has $\chi(D) \neq \chi(D')$, one again obtains the validity of (3.2). Hence we may now assume $\chi(C) = 0$ and $\chi(D) = \chi(D')$. On substituting these values in (3.4) or (3.5), we obtain the equation

$$\chi(D^2) - \beta\chi(D) - \gamma = 0,$$

which implies (3.1). Now the validity of (3.3) is an immediate consequence. □

We next show that there always must be characters χ with $\chi(C) \neq 0$ (so that (3.2) will hold) unless Γ is trivial.

PROPOSITION 3.2. *Let (C, D, D') be a partial difference triple over G for a strongly regular semi-Cayley graph Γ, and assume $\chi(C) = 0$ for every nonprincipal character χ of G. Then Γ is trivial (i.e., either Γ or its complement is a disjoint union of complete graphs).*

Proof. Recall the well-known inversion formula for group ring elements (which is an immediate consequence of the orthogonality relations for characters): One can recover the coefficients of $A = \sum_{g \in G} a_g g \in \mathbf{Z}G$ by means of the formula

$$a_g = \frac{1}{|G|} \sum_{\chi \in g^*} \chi(A)\chi(g^{-1}),$$

where G^* denotes the character group of G. In particular, if $A, B \in \mathbf{Z}G$ satisfy $\chi(A) = \chi(B)$ for all nonprincipal characters χ of G, then B must be a rational multiple of A. Hence the assumption that $\chi(C) = 0$ for every nonprincipal character χ of G implies that C is a multiple of G and hence $C = G$, since C is a subset of G. But then the complementary graph of Γ is a disconnected strongly regular graph (it contains no edges between the two halves G and G') and is therefore the disjoint union of complete graphs. Hence Γ is trivial. □

We state a simple consequence of the preceding results which will be used later.

COROLLARY 3.3. *Let (C, D, D') be a partial difference triple over G for a strongly regular semi-Cayley graph with parameters $2n$, k, λ, and μ, where G is Abelian, and assume $D = D'$. Then all of β, λ, μ, and Δ are even.*

Proof. Because of Proposition 3.2, we may select a nonprincipal character χ of G satisfying $\chi(C) \neq 0$. Thus Proposition 3.1 shows that χ satisfies Equation (3.2), which (together with $D = D'$) immediately implies that β is even. Hence Equation (2.5) can be written as $2C(D - \beta/2) = \mu G$. Then it is straightforward that μ and hence also λ are even. Finally, (2.7) shows that Δ is likewise even. □

By Propositions 3.1 and 2.3, application of any nonprincipal character χ to the element $D + D'$ of $\mathbf{Z}G$ will yield one of the three integral values $\beta - \Delta$, β, and $\beta + \Delta$, which are in arithmetic progression. Clearly this will severely restrict the possibilities for $D + D'$. In particular, this element will have to be invariant under all *numerical automorphisms* of $\mathbf{Z}G$, i.e, under all automorphisms of the form

$$A = \sum_{g \in G} a_g g \to A^{(t)} = \sum_{g \in G} a_g g^t, \tag{3.7}$$

where t is an integer coprime with the order of G. This assertion already follows from the rationality of the character values.

LEMMA 3.4. *Let $A = \sum_{g \in G} a_g g \in \mathbf{Z}G$, and assume that $\chi(A)$ is rational for every character χ of G. Then A is fixed under every numerical automorphism of $\mathbf{Z}G$.*

Proof. We use a standard argument and consider the cyclotomic field $K = \mathbf{Q}(\zeta)$, where ζ is a primitive nth root of unity (with n the exponent of G). Let σ denote the automorphism of K which maps ζ to ζ^t, to let χ be any character of G. Then we have

$$\begin{aligned} \chi\left(A^{(t)}\right) &= \chi\left(\sum a_g g^t\right) = \sum a_g \chi\left(g^t\right) = \sum a_g (\chi(g))^t \\ &= \sum a_g (\chi(g))^\sigma = \left(\sum a_g \chi(g)\right)^\sigma = \chi(A)^\sigma = \chi(A), \end{aligned}$$

since $\chi(A)$ is rational. Thus the inversion formula implies the assertion. □

If G is actually cyclic, one cay say much more.

LEMMA 3.5. *Let $A = \sum_{g \in G} a_g g \in \mathbf{Z}G$, where G is a cyclic group of order n. Assume $\chi(A) \in \{x - y, x, x + y\}$ for every nonprincipal character χ of G, where x and y are integers. Then one has*

$$A = \sum_{m|n} c_m U_m \quad \text{for some integers } c_m, \tag{3.8}$$

where U_m denotes the unique subgroup of order m of G. If $m \neq 1, n$, then c_m has the form

$$c_m = \frac{y w_m}{m}, \tag{3.9}$$

where $w_m \in \mathbf{Z}$ and $w_m \neq 0$ only if m divides $2y$. Moreover, if the coefficients of A can take only the values 0, 1, and 2, one has

$$c_m = 0 \quad \text{unless } m \in M := \{1, n, 2y, y, y/2\} \cap \{k : k|n\}; \tag{3.10}$$

finally, if the coefficients of A can take only the values 0 and 1, one even has

$$c_m = 0 \quad \text{unless } m \in M' := \{1, n, 2y, y\} \cap \{k : k|n\}. \tag{3.11}$$

Proof. By Lemma 3.4, A is fixed under every numerical automorphism of $\mathbf{Z}G$. This implies that the coefficients in A of any two elements of G which have the same order must agree. A simple induction argument now shows that A is indeed an integral linear combination of the subgroups of G. The validity of (3.9) will also be proved by induction. Thus assume that $m \neq 1, n$ is a divisor of n, and (3.9) holds for all divisors $d \neq 1, m$ of m. Note first that

$$A^{(m)} = \sum_{d|n} c_d U_d^{(m)} = \sum_{d|m} c_d d + \sum_{d|n,\, d \nmid m} c_d U_d^{(m)}, \tag{3.12}$$

where the terms in the last sum correspond to nontrivial subgroups of G (and where we have extended the notation introduced in (3.7) to arbitrary integers). We now apply a character χ of order n to Equations (3.8) and (3.12) to obtain

$$\chi(A) = c_1 \quad \text{and} \quad \chi^m(A) = \chi(A^{(m)}) = \sum_{d|m} c_d d,$$

since χ annihilates nontrivial subgroups. These two equations give

$$\sum_{d|m,\, d \neq 1} c_d d = \chi^m(A) - \chi(A) \in \pm\{0, y, 2y\}$$

by our hypothesis on the values nontrivial characters can take when applied to A. Hence we have

$$c_m m = \varepsilon y - \sum_{d|m,\, d\neq 1,\, m} c_d d \quad (\text{with } \varepsilon \in \pm\{0, 1, 2\})$$

and, by induction,

$$c_m m = y\left(\varepsilon - \sum_{d|m,\, d\neq 1,\, m} w_d\right) =: y w_m \tag{3.13}$$

for suitable integers w_d. It immediately follows that c_m also has the form asserted in (3.9). It still remains to show that $c_m = 0$ if m does not divide $2y$. In this case we write $\delta = \gcd(m, 2y)$; now an argument similar to the previous one gives

$$\chi\left(A^{(m)}\right) - \chi\left(A^{(\delta)}\right) = \sum_{d|m,\, d\nmid\delta} c_d d = c_m m \in \{0, y, 2y\},$$

since the only value of d for which c_d is possibly not 0 is $d = m$ (for all other values of d, the induction hypothesis gives $c_d = 0$). Using the assumption that m does not divide $2y$, we obtain the desired conclusion $c_m = 0$. This finishes the proof of (3.9).

We now assume that A has only coefficients 0, 1, and 2. If $g \in G$ has order m, we see from (3.8) that

$$a_g = s_m := \sum_{m|d|n} c_d \in \{0, 1, 2\}. \tag{3.14}$$

It remains to show that $c_m = 0$ if m divides $2y$ and n but does not belong to M. By induction, we may assume that this assertion holds for all proper multiples of m dividing n. Denote by q the smallest element of M which is a multiple of m. We then obtain from (3.9) and (3.14)

$$\frac{y w_m}{m} = c_m = s_m - \sum_{m|d|n,\, d\neq m} c_d = s_m - s_q \in \pm\{0, 1, 2\}.$$

In particular, we see that

$$y\,|w_m| \leq 2m. \tag{3.15}$$

But since w_m is an integer, we have $|w_m| \geq 1$ for $w_m \neq 0$; in view of (3.15), this can hold only if we have $m \geq y/2$. By assumption, m divides $2y$ but does not belong to M. Hence the only possible value for m would be $2y/3$. But in this case $w_m \neq 0$ implies that w_m is even (since c_m is an integer) and (3.15) yields the contradiction $m \geq y$. Thus we indeed obtain the validity of (3.10). A similar argument rules out the possibility that $m = y/2$ and thus shows the validity of (3.11) if we assume that A has coefficients 0 and 1 only. □

Except for the case of coefficients 0, 1, and 2, Lemma 3.5 is essentially due to Ma [17]: It is a translation of his Lemma 3.2 from the language of roots of unity and polynomials over **Z** into that of group rings and characters.

4. The Cyclic Case

In this section we shall assume that Γ is a strongly regular semi-Cayley graph with respect to a cyclic group G. Here the parameters (1.3) will play a prominent role. We begin with a relatively simple example of a situation leading to these parameters.

THEOREM 4.1. *Let Γ be a strongly regular semi-Cayley graph with respect to a cyclic group G with parameters $2n$, k, λ, and μ, and assume that Δ does not divide $2n$ (where Δ is defined as in (2.7)). If Γ is nontrivial, then it has—up to complementation—parameters of the form*

$$2n = 4s^2 + 4s + 2, \quad k = 2s^2 + s, \quad \lambda = s^2 - 1, \quad \mu = s^2. \tag{4.1}$$

Proof. Let (C, D, D') be the partial difference triple associated with Γ. Because of Proposition 3.2, we may select a nonprincipal character Ψ of G satisfying $\Psi(C) \neq 0$. By Proposition 3.1, this implies $\Psi(D) + \Psi(D') = \beta$. Because of (3.3) and Proposition 2.3, we may apply Lemma 3.5 to $D + D'$. Since $D + D'$ has coefficients 0, 1, and 2 only and since Δ does not divide $2n$ by hypothesis, we obtain

$$D + D' = aG + be \tag{4.2}$$

for suitable integers a and b. Applying Ψ to this equation shows that $b = \beta$. Since neither D nor D' involves e, we also obtain $a = -\beta$. Thus (4.2) becomes

$$D + D' - \beta e = -\beta G. \tag{4.3}$$

But $D + D'$ has to involve at least one group element with coefficient 1 (because Γ is nontrivial); thus (4.3) implies $\beta = -1$ i.e.,

$$D + D' + e = G. \tag{4.4}$$

Clearly this implies $|D| = (n - 1)/2$. We can now use Proposition 2.3 to show that Γ has the desired parameters. Define s by $\Delta^2 = 1 + 4(k - \mu) = (2s + 1)^2$, i.e.,

$$\mu = k - s^2 - s. \tag{4.5}$$

If we use this, (2.6) gives

$$k = |C| + |D| = \frac{2k + 1 \pm (2s + 1)}{4} + \frac{n - 1}{2}. \tag{4.6}$$

If we choose the minus sign in (4.6), we obtain

$$n = k + s + 1. \tag{4.7}$$

Substituting these values for μ and n (and $\beta = -1$) in the standard equation (2.8) gives

$$k^2 = (k - s^2 - s)(2k + 2s + 1),$$

which gives the solution $k = 2s^2 + s$ leading to the parameters (4.1). If one instead chooses the plus sign in (4.6), one obtains

$$n = k - s, \tag{4.7'}$$

which will lead to the complementary parameters of (4.1). □

The next result requires more work. Although it looks quite special, it will have interesting consequences.

THEOREM 4.2. *Let G be a cyclic group of order n, and let (C, D, D') be a partial difference triple over G associated with a strongly regular semi-Cayley graph Γ with parameters $2n$, k, λ, and μ. If $D = D'$, then Γ is trivial.*

Proof. Assume that Γ is nontrivial. By Proposition 3.1, we have

$$\chi(D) \in \{(\beta - \Delta)/2, \beta/2, (\beta + \Delta)/2\} \tag{4.8}$$

for every nonprincipal character χ. By Corollary 3.3, both β and Δ are even, so that the assumptions of Lemma 3.5 are satisfied for $A = D$ with $x = \beta/2$ and $y = \Delta/2$. Since D has coefficients 0 and 1 only, it is a linear combination of the subgroups $G = U_n$, U_Δ, $U_{\Delta/2}$, and $U_1 = \{e\}$ satisfying the restriction given in (3.11). Without loss of generality we assume $|D| < n/2$ (if necessary, we replace Γ by its complement and thus D by $G - D - e$). Then the linear combination for D cannot involve G. By taking into account that e does not belong to D, we obtain only the following three possibilities for D:

Case 1. $D = U_\Delta - e$;
Case 2. $D = U_{\Delta/2} - e$;
Case 3. $D = U_\Delta - U_{\Delta/2}$.

Since Γ is nontrivial, we may select a nonprincipal character χ of G satisfying $\chi(C) \neq 0$ and hence

$$\chi(D) = \beta/2 \tag{4.9}$$

by Propositions 3.1 and 3.2. We also note

$$\Delta \geq |\beta| + 1, \tag{4.10}$$

which is immediate by (2.7). We now consider the Cases 1 and 2 first and claim that χ is actually nontrivial on U_Δ and $U_{\Delta/2}$, respectively. Assume otherwise. Then applying χ to D gives

$$\Delta - 1 = \chi(D) = \beta/2 \tag{4.11}$$

in Case 1 and

$$\Delta/2 - 1 = \chi(D) = \beta/2 \tag{4.11'}$$

in Case 2. We note that (4.10) obviously contradicts (4.11), proving our auxiliary assertion for Case 1. In Case 2 we would obtain

$$\Delta = \beta + 2, \tag{4.12}$$

which implies $\gamma = \beta + 1$ by (2.7). Substituting $\beta = \lambda - \mu$ and $\gamma = k - \mu$, we obtain $\lambda = k - 1$. It is easily seen that this forces Γ to be a disjoint union of copies of K_{k+1}, a contradiction. Hence χ is indeed nontrivial on the subgroup involved in D, and we now obtain (because of (4.9)) $-1 = \chi(D) = \beta/2$, i.e.,

$$\beta = -2 \tag{4.13}$$

for Cases 1 and 2. Substituting the value for D and (4.13) in (2.5) yields

$$2CH = \mu G \quad \text{(with } H = U_\Delta \text{ and } H = U_{\Delta/2}, \text{ respectively).} \tag{4.14}$$

We now obtain from Equations (2.3) and (4.14)

$$\mu G|C| = 2CC^{(-1)}H = \left[2\mu G - 4(H - e) + 2\gamma e - 2(H - e)^2\right] H,$$

i.e., an identity of the form

$$(\mu|C| - 2\mu|H|)G = HX, \tag{4.15}$$

where X is a linear combination of H and e. Clearly this implies that both sides of (4.15) are equal to 0. Using $\mu \neq 0$ and $|C| = k - |D| = k - |H| + 1$, we obtain the condition

$$0 = |C| - 2|H| = k + 1 - 3|H|. \tag{4.16}$$

By applying Proposition 2.3, we have

$$4k - 4|H| + 4 = 4|C| = 2k + 2 \pm \Delta;$$

hence from (4.16)

$$6|H| = 4|H| \pm \Delta.$$

This implies $H = U_{\Delta/2}$, ruling out Case 1. Thus $k = 3\Delta/2 - 1$ by (4.16), and therefore

$$\Delta^2 = \beta^2 + 4\gamma = 4 + 4(k - \mu) = 6\Delta - 4\mu \leq 6\Delta - 8.$$

Using (2.8) also, we get either the parameters

$$\Delta = 2,\ \lambda = 0,\ \mu = 2,\ k = 2,\ n = 2$$

(and thus $\Gamma = K_{2,2}$ is trivial, a contradiction) or

$$\Delta = 4,\ \lambda = 0,\ \mu = 2,\ k = 5,\ n = 8. \tag{4.17}$$

We now substitute these values into Equation (2.3) and obtain

$$(U_2 - e)^2 + CC^{(-1)} = 2G - 2U_2 + 5e,$$

implying

$$CC^{(-1)} = 2(G - U_2) + 4e. \tag{4.18}$$

One can now either check directly that Equation (4.18) has no solution or appeal to the theory of relative difference sets: (4.18) means that C would be a cyclic relative difference set with parameters (2, 4, 4, 2), and it is well known that such a relative difference set does not exist. (We refer the reader to [12] for background on relative difference sets; we use the notation of this paper. The result quoted is due to Elliott and Butson [7].) This contradiction rules out Case 2, and we are left with Case 3. As in Cases 1 and 2, one first shows that χ is actually nontrivial on both U_Δ and $U_{\Delta/2}$; this is easily seen by using (4.9) and (4.10). Applying χ to D now gives, by using (4.9) and (2.7),

$$\beta = 0 \text{ and } \Delta^2 = 4\gamma \quad \text{in Case 3.} \tag{4.19}$$

On the other hand, from (2.6) we obtain $2\Delta = 4|D| = 4k - (2k \pm \Delta)$, i.e.,

$$2\Delta = 2k \pm \Delta \tag{4.20}$$

We first show that we cannot have the plus sign in (4.20), i.e., $k = \Delta/2$. Otherwise, (4.19) would yield

$$\Delta^2 = 2\Delta - 4\mu \leq 2\Delta - 4$$

(since $\lambda = \mu \neq 0$), a contradiction. Thus we must have the minus sign in (4.20), i.e., $k = 3\Delta/2$. Now (4.19) implies

$$\Delta^2 = 6\Delta - 4\mu \leq 6\Delta - 4$$

Using (2.8) also, we get either the parameters

$$\Delta = 2,\ \lambda = \mu = 2,\ k = 3,\ n = 2$$

(and thus $\Gamma = K_4$ is trivial, a contradiction) or

$$\Delta = 4,\ \lambda = \mu = 2,\ k = 6,\ n = 8. \tag{4.21}$$

We now substitute these values into Equation (2.3) and obtain

$$(U_4 - U_2)^2 + CC^{(-1)} = 2G + 4e.$$

Again this reduces to Equation (4.18), which we have already seen is impossible. This final contradiction finishes the proof. □

One of the referees pointed out that Theorem 4.2 is somewhat related to the work of Bridges and Mena [4]. As an immediate consequence of 4.2, one obtains the nonexistence of a nontrivial strongly regular circulant graph of even order, which gives a special case of the results in [4]. In the opposite direction, if one also assumes that C is symmetric (i.e., $C = C^{(-1)}$) and n is odd in Theorem 4.2, then Γ is actually a circulant graph (since it then admits an involution commuting with the underlying cyclic automorphism); so this special case follows from [4].

Example 4.3. The assumption of Theorem 4.2 that G is cyclic is necessary. To give an explicit example, it is possible to construct strongly regular semi-Cayley graphs with parameters (4.17) and (4.21), respectively, in the additively written group $G = \mathbf{Z}_4 \oplus \mathbf{Z}_2$: Suitable partial difference triples are given by $C = \{(0, 0), (1, 0), (0, 1), (3, 1)\}$, together with $D = D' = \{(2, 0)\}$ and $D = D' = \{(1, 0), (3, 0)\}$, respectively. More generally, it is well known that the elementary Abelian group of order 2^{2d+2} contains difference sets with parameters $v = 2^{2d+2}$, $k = 2^{2d+1} \pm 2^d$, and $\lambda = 2^{2d} \pm 2^d$, which have -1 as a multiplier (see [2] or [14]). These difference sets lead to strongly regular Cayley graphs and thus also to semi-Cayley graphs with $D = D'$ (see Example 2.4 and Lemma 5.1 below).

We can now improve Theorem 4.1 as follows:

THEOREM 4.4. *Let G be a cyclic group of order n, and let (C, D, D') be a partial difference triple over G associated with a nontrivial strongly regular semi-Cayley graph Γ with parameters $2n$, k, λ, and μ. If n is odd or not divisible by Δ, then Γ has—up to complementation—parameters of the form (4.1).*

Proof. We may assume without loss of generality

$$|D| = |D'| < n/2. \tag{4.22}$$

Because of Theorem 4.2 we must have

$$D \neq D'. \tag{4.23}$$

As in the proof of Theorem 4.1, we can use Lemma 3.5 to write $D + D'$ as a linear combination of subgroups of G. By our hypothesis on n, this linear combination does not involve the subgroup $U_{2\Delta}$. Moreover, the subgroup $U_{\Delta/2}$

can occur only if Δ is even and if some element of G has coefficient 2 in $D + D'$. In this case neither U_Δ nor G can occur (by the hypothesis on n and by (4.22), respectively). This leaves only the possibility $D = D' = U_{\Delta/2} - e$, contradicting (4.23). Hence $U_{\Delta/2}$ cannot occur, and $D + D'$ is a linear combination of G, U_Δ, and e. Taking into account (4.22), (4.23), and $e \notin D, D'$, we are left with the following three possibilities:

Case 1. $D + D' = G - e$;
Case 2. $D + D' = G - U_\Delta$;
Case 3. $D + D' = U_\Delta - e$.

In Case 1 we obtain the assertion as in the second part of the proof of Theorem 4.1. Thus we have to consider only Cases 2 and 3; here n must be divisible by Δ, and thus n is odd by hypothesis. Since Γ is nontrivial, we may select a nonprincipal character χ of G satisfying $\chi(C) \neq 0$, and hence

$$\chi(D + D') = \beta \tag{4.24}$$

by Propositions 3.1 and 3.2. As before, we also have the validity of (4.10). Using (4.10) and (4.24), one immediately obtains that χ must be nonprincipal on U_Δ in Case 2. We claim that this assertion also holds in Case 3. Otherwise, we would obtain $\Delta = \beta + 1$, and then (2.7) would yield the contradiction $2\beta + 1 = 4\gamma$. Hence χ is indeed nonprincipal on U_Δ. In Case 2, (4.24) and (2.7) now imply $\beta = 0$ and $\Delta^2 = 4\gamma$, hence Δ is an even divisor of n, a contradiction. Thus we are left with Case 3. Here we obtain

$$\beta = -1 \quad \text{and} \quad \Delta^2 = 4\gamma + 1. \tag{4.25}$$

By Proposition 2.3, we also have

$$2(\Delta - 1) = 4|D| = 4k - (2k + 1 \pm \Delta),$$

and therefore either

$$2k = \Delta - 1 \tag{4.26}$$

or

$$2k = 3\Delta - 1. \tag{4.27}$$

If (4.26) would hold, we would obtain $4\mu = 1 + 4k - \Delta^2 = 2\Delta - 1 - \Delta^2$ by (4.25). But this is impossible because $\lambda \geq 0$, and hence $\mu \geq 1$. Thus we must have (4.27), and therefore

$$4\mu = 6\Delta - 1 - \Delta^2. \tag{4.28}$$

Since Δ is odd and $\mu \geq 1$, (4.28) and (2.8) give

$$\Delta = 1,\ \lambda = 0,\ \mu = 1,\ k = 1,\ n = 1 \text{ (so that } \Gamma \text{ would be trivial)}$$

or

$$\Delta = 3,\ \lambda = 1,\ \mu = 2,\ k = 4,\ 2n - 1 = 8 \text{ (a contradiction)}$$

or

$$\Delta = 5,\ \lambda = 0,\ \mu = 1,\ k = 7,\ n = 25,\ |D| = 2,\ |C| = 5. \tag{4.29}$$

In this final case we have to use the equations in Theorem 2.2 for a more detailed analysis. Equations (2.3) and (2.5) now yield

$$D^2 + CC^{(-1)} = G - D + 6e \tag{4.30}$$

and

$$CU_5 = G. \tag{4.31}$$

Note that (4.31) forces C to be the sum of a system of coset representatives of $U = U_5$ in G. Hence $CC^{(-1)}$ cannot contain any element of U except for e. On the other hand, D^2 contains only elements of U. Because of these two facts, Equation (4.30) is equivalent to the following condition:

$$CC^{(-1)} = G - U + 5e \text{ and } D^2 + D = U + e. \tag{4.32}$$

But this means that C would be a cyclic relative difference set with parameters (5, 5, 5, 1), and once more it is well known that such a relative difference set does not exist (by a result of [7]). This finishes the proof. □

Example 4.5. There exists a unique strongly regular graph with parameters (4.29), the Hoffman–Singleton graph (see [6] and [9]). Now let G be the elementary Abelian group of order 25, and let U be a subgroup of order 5 generated by an element $u \neq e$. Then G contains a relative difference set C with parameters (5, 5, 5, 1) with respect to U. Thus C and $D = \{u, u^4\}$ satisfy condition (4.32), and therefore (C, D, D') with $D' = U - D - e$ is a partial difference triple for the parameters (4.29) over G. The resulting strongly regular graph Γ must be the Hoffman–Singleton graph, which thus is a semi-Cayley graph. It follows from Proposition 5.2 below that Γ cannot be a Cayley graph.

Theorem 4.4. considerably strengthens a result of Marusic [19], who obtained the special case where $n = p$ is an odd prime (stating the parameters in terms of p, not as in (4.1)). We note that strongly regular graphs with parameters (4.1) are known to exist whenever $2s + 1$ is a prime power; see, e.g., [6, p. 40]. We shall discuss the existence question for strongly regular semi-Cayley graphs with parameters (4.1) in Section 6. An interesting open problem is the following:

Problem 4.6. Does Theorem 4.4. remain valid if the assumption that n is odd or not a multiple of Δ is dropped?

With the present method of attack, one would have to analyze too many further cases which, moreover, become increasingly involved.

5. Applications to strongly regular Cayley graphs

We now apply the results of the preceding sections to obtain some interesting restrictions on strongly regular Cayley graphs with an even number of vertices. To this purpose, we first note the following simple but fundamental result.

LEMMA 5.1. *Let Γ be a strongly regular Cayley graph with parameters $2n$, k, λ, and μ with respect to a group H which contains a normal subgroup G of index 2 (so that Γ is also a semi-Cayley graph with respect to G), and let h be an element of $H\backslash G$. Then Γ may be represented by a partial difference triple (C, D, D') over H satisfying*

$$D' = D^h, \tag{5.1}$$

where $D^h = h^{-1}Dh$ denotes the image of D under conjugation with h.

Proof. Because Γ is a Cayley graph with respect to H, the vertices may be identified with the elements of H, as described in the introduction. Then the two orbits of the subgroup G of H are G and $G' = H\backslash G$. Without loss of generality, we can select the given element h of H as the base point e' of G', i.e., we define the copy G' of G in (2.1) by

$$g' = hg \quad \text{for } g \in G. \tag{5.2}$$

Because Γ is a Cayley graph with respect to H, (5.2) implies

$$u \sim v \Leftrightarrow uh \sim vh \Leftrightarrow h(h^{-1}uh) \sim h(h^{-1}vh) \Leftrightarrow (h^{-1}uh)' \sim (h^{-1}vh)' \tag{5.3}$$

for any two vertices $u, v \in G$. By Lemma 2.1, we have

$$u \sim v \Leftrightarrow uv^{-1} \in D \quad \text{for all } u, v \in G \tag{5.4}$$

and

$$u' \sim v' \Leftrightarrow uv^{-1} \in D' \quad \text{for all } u', v' \in G'. \tag{5.5}$$

Combining (5.3) through (5.5), we see that

$$uv^{-1} \in D \Leftrightarrow (h^{-1}uh)(h^{-1}vh)^{-1} \in D' \Leftrightarrow (uv^{-1})^h \in D', \tag{5.6}$$

implying the validity of (5.1). □

We now use Lemma 5.1 to obtain some nonexistence results for strongly regular Cayley graphs over certain non-Abelian groups. The first of these is particularly simple.

PROPOSITION 5.2. *Let Γ be a nontrivial strongly regular Cayley graph with parameters $2n$, k, λ, and μ with respect to a group H which contains an Abelian normal subgroup G of index 2, and let h be an element of $H\backslash G$. If*

$$D^h = D, \tag{5.7}$$

then all of β, λ, μ, and Δ are even. In particular, this conclusion holds if H is an Abelian or a generalized dihedral group.

Proof. The first assertion is an immediate consequence of Lemma 5.1 and Corollary 3.3. If H is a generalized dihedral group, there is an involution $h \in H\backslash G$ such that h acts on G as inversion. Thus one has $D^h = D^{(-1)} = D$ by Lemma 2.1. In the Abelian case, (5.7) holds for every choice of h. □

THEOREM 5.3. *Let H be either the dihedral group D_m of order $2m$ or the group Q_m of order $4m$ defined by*

$$Q_m = \left\langle x, y \,\middle|\, x^m = y^2,\ y^{-1}xy = x^{-1} \right\rangle; \tag{5.8}$$

see [22, p. 258]. (If m is even, this group is usually called the generalized quaternion group of order $4m$.) Then there is no strongly regular Cayley graph with respect to H.

Proof. Recall that the dihedral group may be defined as follows:

$$D_m = \left\langle x, y \,\middle|\, x^m = y^2 = 1,\ y^{-1}xy = x^{-1} \right\rangle. \tag{5.9}$$

In both cases the element y acts on the cyclic normal subgroup G of index 2 generated by x as inversion. Since we have $D = D^{(-1)}$, we obtain the validity of $D^h = D$ for the partial difference triple (C, D, D') corresponding to the choice $h = y$ in Lemma 5.1. Thus the assertion is an immediate consequence of (5.1) and Theorem 4.2. □

The case of dihedral groups in Theorem 5.3 was already proved by Ma [17] in terms of partial difference sets (without mentioning strongly regular graphs). Up to now, this was the only general nonexistence result for strongly regular graphs with respect to a non-Abelian group. Theorem 5.3 thus rules out a further interesting series of non-Abelian groups and also gives a unified proof for the impossibility of these two families. We shall exclude two further series of groups below.

It is tempting to suggest the following conjecture:

Conjecture 5.4. Every strongly regular Cayley graph with respect to a group G which has a cyclic normal subgroup H of index 2 is trivial.

For every such group, the elements of odd order form a characteristic subgroup N, and G is a semidirect product of N with the Sylow 2-subgroup S of H. The possible Sylow 2-subgroups are as follows (see Hupper [11, Satz I.14.9]):

Result 5.5. Let G be a group of order $2n$ which has a cyclic normal subgroup of order n, where $n = 2^m$, $m \geq 3$. Then G is isomorphic to one of the following

six groups: the cyclic group of order $2n$, the group $\mathbf{Z}_2 \oplus \mathbf{Z}_n$, the dihedral group of order $2n$, the generalized quaternion group of order $2n$, the group defined by

$$SD_m = \left\langle x, y \,\middle|\, x^{2^m} = y^2 = 1, y^{-1}xy = x^{-1+2^{m-1}} \right\rangle \tag{5.10}$$

(the *semidihedral group* of order $2n$), and the group defined by

$$M_m(2) = \left\langle x, y \,\middle|\, x^{2^m} = y^2 = 1, y^{-1}xy = x^{1+2^{m-1}} \right\rangle \tag{5.11}$$

(which does not seem to have a name; our notation is as in Gorenstein [8, p. 193]).

We now obtain some further evidence for Conjecture 5.4 by proving its validity for 2-groups or order $\neq 16, 64$.

THEOREM 5.6. *Let H be a 2-group of order $\neq 16, 64$ with a cyclic subgroup G of index 2. Then there is no nontrivial strongly regular Cayley graph with respect to H.*

Proof. By Result 5.5, there are six cases to be considered. If H is one of the two Abelian groups occurring, then clearly any $h \in H \backslash G$ satisfies $D^h = D$ (where (C, D, D') is an arbitrary partial difference triple over H), and the assertion follows from Lemma 5.1 and Theorem 4.2. (Alternatively, it may be obtained as a special case of the general theory due to Bridges and Mena [4], [5].) The cases for which H is either a dihedral or a generalized quaternion group are covered by Theorem 5.3. Thus it remains to consider the two groups defined in (5.10) and (5.11), respectively. Denote the unique involution in G by z, and note that y operates on G as follows :

$$y^{-1}gy = \begin{cases} g^{\varepsilon} & \text{if } g \in U, \\ g^{\varepsilon}z & \text{if } g \notin U, \end{cases} \tag{5.12}$$

where $U = U_{n/2}$ denotes the unique subgroup of G of index 2 and where $\varepsilon = -1$ in case (5.10) and $\varepsilon = 1$ in case (5.11). Now let Γ be a nontrivial strongly regular Cayley graph with respect to H, and consider the partial difference triple (C, D, D') corresponding to the choice $h = y$ in Lemma 5.1. Because of Lemma 5.1, we have

$$D' = y^{-1}Dy. \tag{5.13}$$

Thus (5.12) implies $D = D'$ if D is a subset of U; in this case the assertion follows from Theorem 4.2. Hence we may assume now that D is not contained in U, which means that in the representation of $D + D'$ as a linear combination of the subgroups $G = U_n, U_{2\Delta}, U_{\Delta}, U_{\Delta/2}$ and $U_1 = \{e\}$ of G (as in Lemma 3.5) the group G itself has to occur. As usual, without loss of generality we assume

$$|D| < n/2; \tag{5.14}$$

hence G occurs with coefficient 1. In view of (5.12) and (5.13), no element of U can occur in $D + D'$ with coefficient 1. Thus the putative linear combination must involve the subgroup U. In particular, this implies (by Lemma 3.5)

$$\Delta \in \{n, n/2, n/4\}. \tag{5.15}$$

Because of (5.14), we see that U occurs with coefficient -1 in the linear combination. It is now easily seen that $D + D'$ has the following form:

$$D + D' = G - U_{n/2} + A \text{ with } A \in \{0, 2U_{n/4} - 2U_{n/8}, 2U_{n/4} - 2e, 2U_{n/8} - 2e\}. \tag{5.16}$$

We now choose a character χ of G satisfying $\chi(z) = -1$ and obtain from (5.16)

$$\chi(D + D') \in \{0, -2\}. \tag{5.17}$$

By comparing this with condition (3.3), we conclude

$$\beta \in \{0, -2, \pm\Delta, \pm\Delta - 2\}. \tag{5.18}$$

Of these cases, $\Delta = \pm\beta$ cannot occur since this would contradict condition (4.10). If we have $\pm\Delta = \beta + 2$ (i.e., essentially Equation (4.12)), we obtain a contradiction exactly as in the proof of Theorem 4.2. Hence (5.18) leaves only two cases:

Case 1. $\beta = 0$. In this case the partial difference set S in the 2-group H associated with the Cayley graph Γ (as in the introduction) is an ordinary difference set with multiplier -1 (see Example 2.4). It is well known that this forces S to have parameters

$$v' = 2^{2d+2},\ k' = 2^{2d+1} \pm 2^d,\ \lambda' = 2^{2d} \pm 2^d; \tag{5.19}$$

see, e.g., [2] or [14]. Hence the parameters of Γ are

$$n = 2^{2d+1},\ k = 2^{2d+1} \pm 2^d,\ \lambda = \mu = 2^{2d} \pm 2^d,\ \Delta = 2^{d+1}. \tag{5.20}$$

In view of (5.15), this forces $d \leq 2$, i.e., $n = 8, 32$, contradicting the hypothesis $|H| \neq 16, 64$.

Case 2. $\beta = -2$. In this case the partial difference set S in the 2-group H associated with the Cayley graph Γ (as in the introduction) yields the ordinary difference set $T = S \cup \{e\}$ with multiplier -1 (see Example 2.4). Thus T has parameters (5.19), and we now obtain

$$n = 2^{2d+1},\ k = 2^{2d+1} \pm 2^d - 2,\ \mu = 2^{2d} \pm 2^d,\ \lambda = \mu - 2,\ \Delta = 2^{d+1} \tag{5.21}$$

for the parameters of Γ. As in Case 1, this gives the contradiction $d \leq 2$, i.e., $n = 16, 32$. □

We note that Conjecture 5.4 would be an immediate consequence of Lemma 5.1 if Problem 4.6 could be answered in the affirmative. This might be another indication that Problem 4.6 is presumably quite difficult.

6. Strongly regular semi-Cayley graphs with parameters (4.1)

In this final section, we discuss the existence question for strongly regular Cayley graphs with parameters (4.1). In view of the results of Section 4, this is a very natural problem (in particular, in the cyclic case). We begin with a nonexistence result which is an immediate consequence of Proposition 5.2.

PROPOSITION 6.1. *No strongly regular graph with parameters (4.1) can be a Cayley graph with respect to an Abelian or a generalized dihedral group.*

Let us note the following interesting consequence of Theorem 4.4 and Proposition 6.1.

COROLLARY 6.2. *Let Γ be a nontrivial strongly regular Cayley graph with parameters $2n$, k, λ, and μ with respect to a group H of order $2n$ which has a cyclic normal subgroup G of order n. Then n is a multiple of Δ.*

Proof. Assume otherwise. Then Γ must have parameters (4.1) because of Theorem 4.4. Hence n is odd, and thus H is either an Abelian or a dihedral group. But this contradicts Proposition 6.1. □

Proposition 6.1 is also of some interest in the study of conference matrices (and generalized conference matrices [10]) which are invariant under a group. It has been shown in [13] that a conference matrix of order $2\lambda+2$ which is invariant under a group H (of the same order) can exist only if one has $2\lambda+2 = 4s^2+4s+2$ for a suitable integer s; moreover, in this case such a matrix exists if and only if there is a strongly regular Cayley graph with parameters (4.1) with respect to H. By applying a result of Bridges and Mena [5], it was also shown in [13] that such a graph cannot exist if H is Abelian, but the non-Abelian case was left undecided. Now Proposition 6.1 rules out a large family of possible candidates. In fact, we propose the following conjecture.

Conjecture 6.3. There are no strongly regular Cayley graphs with parameters (4.1) and hence no group invariant conference matrices.

However, there do exist at least a few semi-Cayley graphs with parameters (4.1). Obviously, the Petersen graph is a cyclic example for $s = 1$, and the graph of Example 2.6 covers the case $s = 2$. The following generalization of the construction given in Example 2.6 is basically due to Marusic [19].

PROPOSITION 6.4. *Assume that* $q = 2s^2 + 2s + 1$ *is a prime power, and let* D *be the set of nonzero squares in the additive group* G *of* GF(q) *(i.e.,* D *is a partial difference set describing the Paley graph* $P(q)$*; see [6]). Then* D *forms part of a partial difference triple* $(C, D, D' = G - D - e)$ *for a strongly regular semi-Cayley graph with parameters (4.1) if and only if* G *contains a difference set* C *with parameters*

$$(2s^2 + 2s + 1, s^2, s(s-1)/2). \tag{6.1}$$

Proof. Switching to multiplicative notation, we find that D satisfies the following equation in $\mathbf{Z}G$:

$$D^2 = -D + \frac{s(s+1)}{2}G + \frac{s(s+1)}{2}. \tag{6.2}$$

Substituting (6.2) in Equation (2.3) shows that C has to satisfy the following identity:

$$CC^{(-1)} = \frac{s(s-1)}{2}G + \frac{s(s+1)}{2}, \tag{6.3}$$

which is the defining equation for a difference set with parameters (6.1). □

Unfortunately, no such difference set is known for any $s \geq 3$; in fact, none exists in the range $3 \leq s \leq 7$; see the table given in [14]. Of course, this does not yet rule out the existence of strongly regular semi-Cayley graphs with parameters (4.1) for these values of s. First of all, there may be other groups of order $2s^2 + 2s + 1$, and even if one uses the group G of Proposition 6.4, it is not at all clear whether D must be a Paley partial difference set for every partial difference triple (C, D, D') over G. In fact, we will now give a construction which will provide examples for $s = 3$ and $s = 4$; this is essentially due to one of the referees, who pointed out the example for $s = 3$ to us. For the required background from design theory (i.e., Steiner systems and difference families), the reader may consult [2]; line graphs of Steiner systems are considered in [6, Section 5].

PROPOSITION 6.5. *Led* $\mathbf{D}$ *be any Steiner system* $S(2, s+1, 2s^2 + 2s + 1)$*. Then the complement* Γ *of the line graph of* $\mathbf{D}$ *is strongly regular with parameters (4.1). If* $\mathbf{D}$ *actually belongs to a* $(2s^2 + 2s + 1, s + 1, 1)$*-difference family over a group* G*, then* Γ *is a semi-Cayley graph with respect to* G*.*

Proof. By a result of Bose [3], the line graph of any Steiner system $\mathbf{D}$ is strongly regular. If $\mathbf{D}$ is an $S(2, s+1, 2s^2+2s+1)$, one easily checks that the parameters of the line graph are given by

$$v = 2n,\ n = 2s^2 + 2s + 1,\ k = 2s^2 + 3s + 1,\ \lambda = s^2 + 2s,\ \mu = s^2 + 2s + 1. \tag{6.4}$$

(Alternatively, one may obtain these values by substituting in Proposition (5.2) of [6].) Hence the complementary graph Γ has parameters (4.1); see, for

instance, Proposition (2.7) of [6]. Now assume that **D** actually belongs to a $(2s^2 + 2s + 1, s + 1, 1)$-difference family over G. Then G has two orbits on the line set of **D** (and acts regularly on each of these orbits), and so Γ is a semi-Cayley graph in this case. □

Example 6.6. There exists a (25, 4, 1)-difference family in $G = \mathbf{Z}_5 \oplus \mathbf{Z}_5$ (see, for instance, [2, p. 311]); this gives a (noncyclic) semi-Cayley graph with parameters (4.1) for $s = 3$. (Note that there is no cyclic (25, 4, 1)-difference family; see [2, Table VII.3.8]). Similarly, one can use a cyclic (41, 5, 1)-difference family (see, e.g., [2, p. 326]) to obtain a cyclic example for $s = 4$.

Unfortunately, no $(2s^2 + 2s + 1, s + 1, 1)$-difference family is known for any $s \geq 5$. Indeed, according to the tables given by Mathon and Rosa [20], the existence of any $S(2, s+1, 2s^2+2s+1)$ is still undecided in the range $5 \leq s \leq 20$.

Acknowledgment

We thank Tilla Schade for her careful reading of the original manuscript and for her helpful comments. We are also indebted to the referees for their valuable suggestions.

References

1. G.M. Adel'son-Vel'skii, B.Ju. Veisfeiler, A.A. Leman, and I.A. Faradzev, "Example of a graph without a transitive automorphism group," *Soviet Math. Dokl.* **10** (1969), 440–441.
2. T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, 1986.
3. R.C. Bose, "Strongly regular graphs, partial geometries, and partially balanced designs," *Pacific J. Math.* **13** (1963), 389–419.
4. W.G. Bridges and R.A. Mena, "Rational circulants with rational spectra and cyclic strongly regular graphs," *Ars Combin.* **8** (1979), 143–161.
5. W.G. Bridges and R.A. Mena, "Rational G-matrices with rational eigenvalues," *J. Combin. Theory Ser. A* **32** (1982), 264–280.
6. P.J. Cameron and J.H. van Lint, *Designs, Graphs, Codes and Their Links*, Cambridge University Press, Cambridge, 1991.
7. J.E.H. Elliott and A.T. Butson, "Relative difference sets," *Illinois J. Math.* **10** (1966), 517–531.
8. D. Gorenstein, *Finite Groups*, Harper and Row, New York, 1968.
9. A.J. Hoffman and R.R. Singleton, "On Moore graphs of diameters 2 and 3," *IBM J. Res. Develop.* **4** (1960), 497–504.
10. D.R. Hughes, J.H. van Lint, and R.M. Wilson, Unpublished Manuscript (announcement at the 7th British Combinatorial Conference, Cambridge, 1979).
11. B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.
12. D. Jungnickel, "On automorphism groups of divisible designs," *Canad. J. Math.* **34** (1982), 257–297.
13. D. Jungnickel, "On automorphism groups of divisible designs II: group invariant generalized conference matrices," *Arch. Math.* **54** (1990), 200–208.

14. D. Jungnickel, "Difference sets," in *Contemporary Design Theory: A Collection of Surveys*, J.H. Dinitz and D.R. Stinson, eds., Wiley Interscience, New York, 1992, pp. 241–324.
15. W.M. Kantor, "k-homogeneous groups," *Math. Z.* **124** (1972), 261–265.
16. S.L. Ma, "Partial differences sets," *Discrete Math.* **72**, (1984), 75–89.
17. S.L. Ma, "Partial difference sets in dihedral groups," *South East Asian Bull. Math.* **11** (1987), 53–59.
18. S.L. Ma, "On association schemes, Schur rings, strongly regular graphs and partial difference sets," *Ars Combin.* **27** (1989), 211–220.
19. D. Marusic, "Strongly regular bicirculants and tricirculants," *Ars Combin.* **25-C** (1988), 11–15.
20. R. Mathon and A. Rosa, "Tables of parameters of BIBDs with $r \leq 41$ including existence, enumeration and resolvability results: an update," *Ars Combin.* **30** (1990), 65–96.
21. T. Schade, "Stark reguläre Graphen mit Singergruppe," Diplomarbeit, Universität Giessen, 1989.
22. M. Suzuki, *Group Theory I*, Springer, Berlin, 1982.
23. H.P. Yap, *Some Topics in Graph Theory*, Cambridge University Press, Cambridge, 1986.