University of Ljubljana
Institute of Mathematics, Physics and Mechanics
Department of Mathematics
Jadranska 19, 1 111 Ljubljana, Slovenia

Preprint series, Vol. 43 (2005), 989

DISTANCE-REGULAR CAYLEY GRAPHS ON DIHEDRAL GROUPS

Štefko Miklavič Primož Potočnik

ISSN 1318-4865

September 8, 2005

Ljubljana, September 8, 2005

Distance-Regular Cayley Graphs on Dihedral Groups

Štefko Miklavič
Department of Mathematics and Computer Science
Faculty of Education, University of Primorska
6000 Koper, Slovenia

Primož Potočnik[1]
Institute of Mathematics, Physics and Mechanics
Jadranska 19, SI-1000 Ljubljana
Slovenia

Abstract

The main result of this article is a classification of distance-regular Cayley graphs on dihedral groups. There exist four obvious families of such graphs, which are called *trivial*. These are: complete graphs, complete bipartite graphs, complete bipartite graphs with the edges of a 1-factor removed, and cycles. It is proved that every non-trivial distance-regular Cayley graph on a dihedral group is bipartite, non-antipodal, has diameter 3 and arises either from a cyclic difference set, or possibly (if any such exists) from a dihedral difference set satisfying some additional conditions. Finally, all distance-transitive Cayley graphs on dihedral groups are determined. It transpires that a Cayley graph on a dihedral group is distance-transitive if and only if it is trivial, or isomorphic to the incidence or to the non-incidence graph of a projective space $\mathrm{PG}_{d-1}(d,q)$, $d \geq 2$, or the unique pair of complementary symmetric designs on 11 vertices.

Key words: Cayley graph, distance-regular graph, distance-transitive graph, dihedral group, dihedrant, difference set.

[1]Supported in part by "Ministrstvo za šolstvo znanost in šport Republike Slovenije", proj. no. Z1–3124 and Z1–4186

1 Introduction

A connected finite graph is *distance-regular* if the cardinality of the intersection of two spheres depends only on their radii and the distance between their centres. Even though this condition is purely combinatorial, the notion of distance-regular graphs is closely related to certain topics in algebra, and has motivated a development of various new algebraic notions, as well as shed a new light on the existing ones (see, for example, [1, 5, 17]). This interplay of concepts proves to be especially intimate when a subclass of distance-regular *Cayley graphs* is considered. (The *Cayley graph* $\mathrm{Cay}(G;S)$ on a finite group G relative to an *inverse-closed* subset S of $G\setminus\{1\}$, that is, a subset $S\subseteq G\setminus\{1\}$ such that $s\in S\Leftrightarrow s^{-1}\in S$, is the graph with vertex set G and the adjacency relation given by $g\sim h\Leftrightarrow h^{-1}g\in S$.) As it may be deduced from Proposition 5.1, distance-regular Cayley graphs generalize the notion of *difference sets* in abelian groups, and are also closely related to *relative difference sets* in general. (A *relative difference set in a group G with respect to a subgroup $N\leq G$* is a subset D of G, such that the number of pairs $(r_1,r_2)\in D\times D$ satisfying $r_2r_1^{-1}=g$ is constant for all $g\in G\setminus N$, and equals 0 for all $g\in N\setminus\{1\}$. A *difference set* is a relative difference set with respect to the trivial subgroup $N=\{1\}$.) It is well known that relative difference sets in a group G are nothing but solutions of certain equations in the corresponding group ring $\mathbb{Z}G$ (see, for example, [18, Section 1.4]). Surprisingly, known techniques for solving such equations are not sufficient even to deal with the case where G is a dihedral group. Namely, the question whether or not there are any difference sets in dihedral groups (other than empty sets, singletons and their complements) is one of the oldest open problems in the theory of difference sets (see, for example, [11]).

The aim of this article is twofold. Firstly, to classify all distance-regular Cayley graphs on dihedral groups, and thus to continue the project of classification of distance-regular Cayley graphs initiated in [15]. And secondly, to show how classical tools of algebraic number theory can be engaged to tackle questions about distance-regular Cayley graphs.

We start with presenting four obvious families of distance-regular Cayley graphs, which will be called *trivial* for the purpose of this article. These are: complete graphs K_n (of diameter 1), complete multipartite graphs $K_{t\times m}$ (of diameter 2), complete bipartite graphs without a 1-factor $K_{m,m}-mK_2$ (of diameter 3), and cycles C_n (of diameter $\lfloor n/2\rfloor$). All these distance-regular graphs are Cayley graphs. For example, the complete graph K_n is a Cayley graph on any group G of order n relative to $S=G\setminus\{1\}$. The complete multi-partite graph $K_{t\times m}$ is a Cayley graph on any group G of order tm which contains a subgroup L of order m, relative to $S=G\setminus L$. The graph $K_{m,m}-mK_2$ can be obtained as a Cayley graph on the dihedral group $D_m=\langle\rho,\tau\mid\rho^m,\tau^2,(\rho\tau)^2\rangle$, relative to $S=\{\rho^i\tau\mid i\in\{1,\dots,m-1\}\}$. Finally, the cycle C_n is a Cayley graph on the cyclic group $\langle\rho\mid\rho^n\rangle$ relative to $S=\{\rho,\rho^{-1}\}$, or if $n=2m$ is even, C_n is also a Cayley graph on the dihedral group D_m relative to $S=\{\tau,\rho\tau\}$. In particular, all trivial distance-regular graphs with even number of vertices are Cayley graphs on dihedral groups. (Cayley graphs on dihedral groups are also called *dihedrants*.)

Further examples of non-trivial distance-regular Cayley graphs are provided by the following construction. For an integer $q=p^m$, p a prime, $q\equiv 1\,(\mathrm{mod}\ 4)$, let $\mathbb{F}_q$ denote the finite field of cardinality q, let S denote the set of all squares in the multiplicative group of $\mathbb{F}_q$, and let $H\cong\mathbb{Z}_p^m$ denote the additive group of $\mathbb{F}_q$. The *Paley graph* $\mathrm{P}(q)$ *of order* q is defined as the Cayley graph $\mathrm{Cay}(H;S)$. It is easy to see that Paley graphs are distance-regular graphs of diameter 2.

Non-trivial distance-regular Cayley graphs on non-abelian groups seem to be more difficult to find. The smallest such graph is the *graph of the icosahedron*, which can be repre-

sented as a Cayley graph on the non-abelian non-dihedral group of order 12. The *Heawood graph* and its *bipartite complement* are distence-regular Cayley graphs on the dihedral group of order 14, and as it was pointed out in [15], the *Shrikhande graph* can be represented as a Cayley graph on three non-isomorphic non-abelian groups of order 16, as well as a Cayley graph on $\mathbb{Z}_4 \times \mathbb{Z}_4$ (see [15]). To our best knowledge, there is only one known example of a distance-regular Cayley graph on a non-solvable group (see [6]). It is the antipodal distance-regular Cayley graph on the alternating group A_5, with diameter 3 and valency 29. At this point, the following general problem arises naturally.

Problem 1.1 *For a class of groups $\mathcal{G}$, determine all distance-regular graphs, which are Cayley graphs on a group in $\mathcal{G}$.*

In [15] this problem was solved for the class of cyclic groups. (Cayley graphs on cyclic groups are also called *circulants*.)

Theorem 1.2 ([15], Theorem 1.2) *Let X denote an arbitrary circulant with n vertices. Then X is distance-regular if and only if it is isomorphic to one of the following graphs:*

(i) *the cycle C_n,*

(ii) *the complete graph K_n,*

(iii) *the complete multipartite graph $K_{t\times m}$, where $tm = n$,*

(iv) *the complete bipartite graph without a 1-factor $K_{m,m} - mK_2$, where $2m = n$, m odd,*

(v) *the Paley graph $\mathrm{P}(n)$, where $n \equiv 1 \pmod 4$ is prime.*

The main result of this article is a similar classification of distance-regular Cayley graphs on dihedral groups. As it has already been noted, all trivial distance-regular graphs with an even number of vertices are dihedrants, and as we shall prove, all non-trivial distance-regular dihedrants are bipartite, non-antipodal, have diameter 3, and are associated with certain difference sets in cyclic or (possibly) dihedral groups.

Throughout this article, the following notation will be used. For a positive integer n, D_n will denote the dihedral group with $2n$ elements, generated by an element ρ of order n and an involution τ satisfying the relation $\tau\rho\tau = \rho^{-1}$. For subsets $R, T \subseteq \mathbb{Z}_n$ we let $\rho^R = \{\rho^i \mid i \in R\}$ and $\rho^T\tau = \{\rho^i\tau \mid i \in T\}$. Finally, by $\mathrm{Dih}\,(n; R, T)$ we denote the Cayley graph $\mathrm{Cay}(D_n; \rho^R \cup \rho^T\tau)$. (It should be noted that the notation $\mathrm{Dih}\,(2n, R, T)$ was used in [13] instead of $\mathrm{Dih}\,(n; R, T)$, as well as D_{2n} instead of D_n.) A difference set D in a group G is called *trivial*, if $|D| \in \{|G|, |G| - 1, 1, 0\}$, otherwise it is called *non-trivial*. For a subset $A \subseteq \mathbb{Z}_n$ and an element $i \in \mathbb{Z}_n$, we let $i + A = \{i + a \mid a \in A\}$ and $iA = \{ia \mid a \in A\}$. We are now ready to state the main theorem of this article.

Theorem 1.3 *Let X be a dihedrant on $2n$ vertices other than the cycle C_{2n}, the complete graph K_{2n}, the complete multipartite graph $K_{t\times m}$, where $tm = 2n$, or the complete bipartite graph without a 1-factor $K_{n,n} - nK_2$. Then X is distance-regular if and only if one of the following holds:*

(i) *$X \cong \mathrm{Dih}\,(n; \emptyset, T)$, where T is a non-trivial difference set in the group $\mathbb{Z}_n$.*

(ii) *n is even and $X \cong \mathrm{Dih}\,(n; R, T)$, where R and T are non-empty subsets of $1 + 2\mathbb{Z}_n$ such that $\rho^{-1+R} \cup \rho^{-1+T}\tau$ is a non-trivial difference set in the dihedral group $\langle \rho^2, \tau\rangle$ of order n.*

If either (i) *or* (ii) *holds, then X is bipartite, non-antipodal, and has diameter* 3.

Let us remark that since there are many non-trivial difference sets in cyclic groups, there are also many distance-regular dihedrants arising from case (i). However, since there are no known examples of non-trivial difference sets in dihedral groups, there are also no known examples of distance-regular dihedrants arising from case (ii). Moreover, not every non-trivial difference set in a dihedral group would necessarily give rise to a distance-regular dihedrant since it might not be imbeddable into a larger dihedral group as indicated in case (ii). It is therefore very likely that the graphs arising in case (i) are the only non-trivial distance-regular dihedrants. Further discussion on examples of non-trivial distance-regular dihedrants is postponed until Section 5, where some further implications of Theorem 1.3 are proved. All distance-transitive dihedrants are explicitely constructed in Subsection 5.4. In Section 2 we summarize some definitions and results on distance-regular graphs and Cayley graphs. In Section 3 we introduce the Fourier transformation, which is a usual vehicle for the study of difference sets and has been successfully used also in the investigation of strongly regular circulants, bicirculants and tricirculants as well as 2-arc-transitive dihedrants undertaken in [13, 12, 14]. Finally, in Section 4 a detailed version of Theorem 1.3 is given and proved.

2 Preliminaries

In this section, we review some definitions and facts about distance-regular graphs, Cayley graphs and group actions on graphs. More background information on distance-regular graphs can be found in [4]. For the group theoretical concepts not defined here we refer the reader to [7].

2.1 Distance-regular graphs – intersection numbers

Throughout this paper all graphs are assumed to be finite, undirected and without loops or multiple edges. For a graph X we let $V(X)$, $E(X)$ and ∂_X (or just ∂) denote the *vertex set*, the *edge set* and the *path length distance function*, respectively. The *diameter* $\max\{\partial(x,y)|x,y\in V(X)\}$ of X will be denoted by d_X (or just d, when the graph X is clear form the context). For a vertex $x\in V(X)$ and an integer i, we let $S_i(x)=\{y \mid \partial(x,y)=i\}$ denote the i-th sphere centred in x. We abbreviate $S(x)=S_1(x)$. A connected graph X is said to be *distance-regular* whenever, for all integers $h,i,j,\ (0\le h,i,j\le d)$ and all $x,y\in V(X)$ with $\partial(x,y)=h$, the number

$$p_{ij}^h=|\{z\,|\,z\in V\Gamma,\,\partial(x,z)=i,\,\partial(y,z)=j\}| \tag{1}$$

is independent of the choice of x and y. The constants p_{ij}^h $(0\le h,i,j\le d)$ are known as the *intersection numbers* of X.

For notational convenience we define $c_i=p_{1,i-1}^i\,(1\le i\le d)$, $a_i=p_{1,i}^i\,(0\le i\le d)$, $b_i=p_{1,i+1}^i\,(0\le i\le d-1), k_i=p_{i,i}^0\,(0\le i\le d)$, and set $c_0=b_d=0$. We observe $a_0=0$ and $c_1=1$. Moreover, $a_i+b_i+c_i=k$ $(0\le i\le d)$, where $k=k_1$. Following convention, we abbreviate $\lambda=a_1$ and $\mu=c_2$. Observe also that $k_i=|S_i(x)|$ for every $x\in V(X)$. The array

$$\{b_0,b_1,\ldots,b_{d-1};c_1,c_2,\ldots,c_d\} \tag{2}$$

is called the *intesection array* of X.

2.2 Automorphisms, blocks of imprimitivity, and quotients of graphs

An *automorphism of a graph* X is a permutation on $V(X)$ which preserves the adjacency relation. The group of all automorphisms of X is denoted by $\mathrm{Aut}X$. We shall assume that $\mathrm{Aut}X$ acts on $V(X)$ on left and thus write $g(v)$ to denote the image of $v \in V(X)$ with respect to some $g \in \mathrm{Aut}X$. In this way $\mathrm{Aut}X$ becomes a permutation group on $V(X)$.

A permutation group G on a set V is called *transitive* if for each pair $u, v \in V$ there exists $g \in G$ such that $g(u) = v$. If, in addition, such g is unique for each (ordered) pair (u, v), then the permutation group G is called *regular*. A graph with a transitive automorphism group is called *vertex-transitive*. An *imprimitivity system* for a transitive permutation group G on a set V is a G-invariant partition of V. Clearly, the partition of V into singletons and the partition into one set are imprimitivity systems for any permutation group on V, and are hence called *trivial imprimitivity systems*. Members of (non-trivial) imprimitivity systems are called (non-trivial) *blocks of imprimtivity*. A transitive permutation group is called *primitive* if it admits no non-trivial imprimitivity systems.

If $\mathcal{B}$ is a partition of the vertex set V of a graph X, then we define the *quotient graph of X with respect to $\mathcal{B}$* (denoted by $X_{\mathcal{B}}$) to be the graph with vertex set $\mathcal{B}$ and two different members $B_1, B_2 \in \mathcal{B}$ being adjacent whenever there exists an edge in X between a vertex in B_1 and a vertex in B_2. If $\mathcal{B}$ is an imprimitivity system for a group of automorphisms $G \leq \mathrm{Aut}X$ and K the maximal subgroup of G preserving the partition $\mathcal{B}$ (note that K is normal in G and is usually referred to as the *kernel*), then $X_{\mathcal{B}}$ admits a natural (faithful) action of G/K as a group of automorphisms. Moreover, if G is transitive on $V(X)$, then G/K is transitive on $V(X_{\mathcal{B}})$. An important class of such quotient graphs arises when $\mathcal{B}$ is the set of H-orbits for an intransitive subgroup $H \leq \mathrm{Aut}X$. Then $\mathcal{B}$ is an imprimitivity system for the normalizer G of H in $\mathrm{Aut}X$ and H is contained in the kernel $K \lhd G$. Hence, if G is transitive on $V(X)$, then $G/K \leq \mathrm{Aut}X_{\mathcal{B}}$ is transitive on $V(X_{\mathcal{B}})$.

2.3 Antipodal quotients and halved graphs

For a distance-regular graph X let the *r-th distance graph* X_r be the graph with the same vertex set as X, and with two vertices adjacent if and only if they are at distance r in X. If X_r is connected for all r, $1 \leq r \leq d$, then X is called *primitive*. Otherwise, X is *imprimitive*. Clearly, if G is a vertex-transitive subgroup of $\mathrm{Aut}X$, then connected components of X_r form an imprimitivity system for G. Therefore, if a vertex-transitive distance-regular graph is imprimitive, then each transitive subgroup of $\mathrm{Aut}X$ is imprimitive. The converse is not true in general. However, if G is *distance-transitive* (that is, if for each r, $0 \leq r \leq d_X$, G acts transitively on the set of ordered pairs of vertices at distance r), then the imprimitivity of G yields the imprimitivity of X.

A distance-regular graph X is called *antipodal*, if the relation R on $V(X)$ defined by $xRy \Leftrightarrow \partial_X(x, y) \in \{0, d\}$ is an equivalence relation. By [4, Theorem 4.2.1], an imprimitive distance-regular graph with valency $k > 2$ is either bipartite, antipodal, or both. If X is bipartite distance-regular graph, then X_2 has two connected components, called the *halved* graphs of X and denoted by X^+ and X^-. The symbol $\frac{1}{2}X$ is used to denote an arbitrary one of these two graphs. Note also that if X is not vertex-transitive, X^+ and X^- may not be isomorphic graphs.

If X is an antipodal distance-regular graph of diameter d, then the relation R on $V(X)$ gives rise to a partition of $V(X)$ into equivalence classes, called fibres. The quotient graph of X relative to this partition is called the *antipodal quotient* of X and is denoted by $\overline{X}$. If the diameter of X is at least 3, then for any two adjacent fibres F_1, F_2 and any vertex $v \in F_1$, there exists exactly one vertex in F_2 which is adjacent to v in X. Moreover, all the

fibres have the same cardinality r, called the *index* of X. In this case, the graph X is also called an *r-fold antipodal cover* of $\overline{X}$. Finally, note that the only antipodal distance-regular graphs of diameter 2 are the complete multipartite graphs.

We summarize some well known facts about imprimitive distance-regular graphs in the following lemma.

Lemma 2.1 ([4, page 141, Proposition 4.2.2]) *Let X denote an imprimitive distance-regular graph with diameter d and valency $k \geq 3$. Then the following hold.*

(i) *If X is bipartite, then the halved graphs of X are non-bipartite distance-regular graphs with diameter $\lfloor \frac{d}{2} \rfloor$.*

(ii) *If X is antipodal, then $\overline{X}$ is a distance-regular graph with diameter $\lfloor \frac{d}{2} \rfloor$.*

(iii) *If X is antipodal, then $\overline{X}$ is not antipodal, except when $d \leq 3$ (in that case $\overline{X}$ is a complete graph), or when X is bipartite with $d = 4$ (in that case $\overline{X}$ is a complete bipartite graph).*

(iv) *If X is antipodal and has odd diameter or is not bipartite, then $\overline{X}$ is primitive.*

(v) *If X is bipartite and has odd diameter or is not antipodal, then the halved graphs of X are primitive.*

(vi) *If X has even diameter and is both bipartite and antipodal, then $\overline{X}$ is bipartite. Moreover, if $\frac{1}{2}X$ is a halved graph of X, then it is antipodal, and $\overline{\frac{1}{2}X}$ is primitive and isomorphic to $\frac{1}{2}\overline{X}$.*

Lemma 2.2 *Let X denote a bipartite distance-regular graph. If one of the halved graphs of X is a cycle, then X is either a cycle, or the complete bipartite graph $K_{3,3}$.*

PROOF. Let $\{b_0, b_1, \ldots, b_{d-1}; 1, c_2, \ldots, c_d\}$ be the intersection array of X. Since X is bipartite we have $b_1 = b_0 - 1$. If $b_0 = 2$, then X is clearly a cycle, so assume $b_0 > 2$. Suppose that a halved graph $\frac{1}{2}X$ is a cycle. Then by [4, Proposition 4.2.2], $b_0 b_1 / c_2 = 2$, implying $b_0(b_0 - 1) = 2c_2$. Since $c_2 \leq b_0$ and $2 \leq b_0 - 1$ we obtain $b_0 = c_2 = 3$. So X is a distance-regular graph with diameter $d = 2$ and intersection array $\{3, 2; 1, 3\}$, hence the complete bipartite graph on 6 vertices. ∎

2.4 Cayley graphs and dihedrants

In this subsection we prove some auxiliary results, the first two dealing with the quotients of Cayley graphs.

Lemma 2.3 *Let $X = \mathrm{Cay}(G; S)$ denote a Cayley graph with the group G acting regularly on the vertex set of X by left multiplication. Suppose there exists an imprimitivity system $\mathcal{B}$ for G. Then the block $B \in \mathcal{B}$ containing the identity element $1 \in G$ is a subgroup in G. Morover,*

(i) *if B is normal in G, then $X_{\mathcal{B}} = \mathrm{Cay}(G/B, S/B)$ where $S/B = \{sB \mid s \in S \setminus B\}$;*

(ii) *if there exists an abelian subgroup A in G such that $G = AB$, then $X_{\mathcal{B}}$ is isomorphic a Cayley graph on the group $A/(A \cap B)$.*

PROOF. The proof of the fact that B is a subgroup of G and the proof of part (i) are straightforward and left to the reader. To prove part (ii), observe that the vertex set $\mathcal{B}$ of the graph $X_{\mathcal{B}}$ is the set $\{gB \mid g \in G\}$ of right cosets of B in G. Since $G = AB$, the latter, however, equals $\{aB \mid a \in A\}$, showing that the subgroup A of G acts by left multiplication transitively (and possibly unfaithfully) on the vertex set $\mathcal{B}$ of X. The kernel of this action consists of those elements $g \in A$ for which $gaB = aB$ for all $a \in A$. Since A is abelian, this condition is equivalent to the condition $g \in B$, showing that the kernel of the action of A on $\mathcal{B}$ is $A \cap B$. Hence, $A/(A \cap B)$ is a transitive subgroup of $\mathrm{Aut}X_{\mathcal{B}}$, which (being abelian) acts regularly on $V(X_{\mathcal{B}})$. ∎

Corollary 2.4 *Let X denote a distance-regular dihedrant. Then:*

(i) *if X is antipodal, then the antipodal quotient $\overline{X}$ is a distance-regular circulant or a distance-regular dihedrant;*

(ii) *if X is bipartite, then the halved graphs X^+ and X^- are distance-regular circulants or distance-regular dihedrants.*

PROOF. Let $X = \mathrm{Cay}(D_n; S)$ and let ρ be an element of D_n with order n. Assume first that X is antipodal and let $H \subseteq D_n$ be the antipodal class of X containing the identity of D_n. By Lemma 2.3, H is a subgroup in D_n. If $H \leq \langle\rho\rangle$, then H is normal in D_n, and by part (i) of Lemma 2.3, $\overline{X}$ is a dihedrant. On the other hand, if $H \not\leq \langle\rho\rangle$, then $D_n = \langle\rho\rangle H$. Thus, by part (ii) of Lemma 2.3, $\overline{X}$ is a Cayley graph on the group $\langle\rho\rangle/(\langle\rho\rangle \cap H)$, which is clearly cyclic.

Suppose now that X is bipartite. Let X^+ be the halved graph of X containing the identity of D_n. Since the vertices of a bipartition set form a block of imprimitivity, by Lemma 2.3, the vertex set of X^+ is a subgroup of D_n, which clearly acts regularly on itself by left multiplication as a subgroup of $\mathrm{Aut}X^+$. Since any subgroup of a dihedral group is cylic or dihedral, X^+ is a circulant or a dihedrant. Moreover, since X is vertex-transitive, X^+ and X^- are isomorphic, hence also X^- is a circulant or a dihedrant. To complete the proof observe that by Lemma 2.1 the antipodal quotient of an antipodal distance-regular graph and halved graphs of a bipartite distance-regular graph are distance-regular. ∎

Lemma 2.5 *Let $R, T \subseteq \mathbb{Z}_n$, $0 \notin R, -R = R$, and let $X = \mathrm{Dih}\,(n; R, T)$. Then $S(\rho^i) = \rho^{i+R} \cup \rho^{i+T}\tau$ and $S(\rho^i\tau) = \rho^{i-T} \cup \rho^{i+R}\tau$.*

PROOF. Since, by definition, $\mathrm{Dih}\,(n; R, T) = \mathrm{Cay}(D_n; \rho^R \cup \rho^T\tau)$, we have $S(\rho^i) = \rho^i(\rho^R \cup \rho^T\tau) = \rho^{i+R} \cup \rho^{i+T}\tau$, and $S(\rho^i\tau) = \rho^i\tau(\rho^R \cup \rho^T\tau) = \rho^{i-R}\tau \cup \rho^{i-T}$. The result now follows from the fact that $R = -R$. ∎

Lemma 2.6 *If $\mathrm{Dih}\,(n; R, T)$ is an arbitrary dihedrant, $a \in \mathbb{Z}_n^*$ and $b \in \mathbb{Z}_n$, then the graphs $\mathrm{Dih}\,(n; aR, b + aT)$ and $\mathrm{Dih}\,(n; R, T)$ are isomorphic.*

PROOF. We leave it to the reader to check that the mapping $g\colon D_n \to D_n$ defined by $g(\rho^i) = \rho^{ai}$, $g(\rho^i\tau) = \rho^{ai+b}$, is an isomorphism of groups, and therefore induces an isomorphism of graphs $\mathrm{Dih}\,(n; R, T)$ and $\mathrm{Dih}\,(n; aR, b + aT)$. ∎

Lemma 2.7 *Let $X = Dih(n; R, T)$ denote a distance-regular dihedrant, and let $T_2 = \{i \in \mathbb{Z}_n \mid \partial(\rho^i\tau, 1) = 2\}$. Then λ is even and $|S(\rho^i\tau) \cap \rho^R| = |S(\rho^i\tau) \cap \rho^T\tau| = \frac{\lambda}{2}$ for each $i \in T$. Morover, if $T_2 \neq \emptyset$, then μ is even and $|S(\rho^i\tau) \cap \rho^R| = |S(\rho^i\tau) \cap \rho^T\tau| = \frac{\mu}{2}$ for each $i \in T_2$.*

PROOF. By Lemma 2.5, $S(\rho^i\tau) \cap S(1) = (\rho^{i-T} \cap \rho^R) \cup (\rho^{i-R}\tau \cap \rho^T\tau)$. But $|(i-T) \cap R| = |T \cap (i-R)|$ and so $|S(\rho^i\tau) \cap S(1)|$ is even. On the other hand, $|S(\rho^i\tau) \cap S(1)| = \lambda$ if $i \in T$ and $|S(\rho^i\tau) \cap S(1)| = \mu$, if $i \in T_2$. ∎

2.5 Distance-regular Cayley graphs and difference sets

In this subsection we will prove two auxiliary results, which will reveal a close relationship between distance-regular Cayley graphs and difference sets. This relationship will be pursued further in a separate article. The results and proofs are stated in the language of group algebras. We shall abuse the notation and use the same symbol to denote a subset S of a group G and the corresponding element $S = \sum_{a \in S} a$ of the group algebra $\mathbb{Z}G$. For $S \subseteq G$ we let $S^{(-1)}$ denote the set $\{s^{-1} \mid s \in S\}$ (as well as the corresponding element of $\mathbb{Z}G$). The notion of a difference set can then be defined as follows.

Definition 2.8 Let ν, k and μ be non-negative integers, let G be a group of order ν, and let D be a k-subset of G. Then D is a (ν, k, μ)-difference set if and only if $DD^{(-1)} = (k - \mu)1_G + \mu G$.

It is not difficult to see that this definition of a difference set is equivalent to the one in Section 1 (see also [18]).

Lemma 2.9 *A Cayley graph* $\mathrm{Cay}(G; S)$ *is a bipartite distance-regular graph with diameter* 3 *and intersection array* $\{k, k-1, k-\mu; 1, \mu, k\}$ *if and only if there exist disjoint subsets* $N_2, N_3 \subseteq G \setminus (\{1\} \cup S)$ *such that* $\{\{1\}, S, N_2, N_3\}$ *is a partition of* G *and the equalities*

$$S^2 = k1_G + \mu N_2, \qquad N_2 S = (k-1)S + kN_3 \tag{3}$$

hold in the group algebra $\mathbb{Z}G$*. In this case,* N_2 *and* N_3 *are exactly the sets of vertices at distance* 2 *and* 3 *from* 1_G*, respectively.*

Proof. Observe first that the equality

$$N\,S = \sum_{g \in G} \alpha_g g \tag{4}$$

holds in $\mathbb{Z}G$ for a subset $N \subseteq G$ if and only if every vertex $g \in G$ of $\mathrm{Cay}(G; S)$ has exactly α_g neighbours in the set N. If $\mathrm{Cay}(G; S)$ is a bipartite distance-regular graph with diameter 3 and intersection array $\{k, k-1, k-\mu; 1, \mu, k\}$, then (4) immediately implies (3). Conversely, suppose that (3) holds for disjoint subsets $N_2, N_3 \subseteq G \setminus (\{1\} \cup S)$. Note that $k = |S|$ is the valency of $\mathrm{Cay}(G; S)$. Since $\mathrm{Cay}(G; S)$ is a vertex-transitive graph it sufficies to prove the following:

(a) elements of S have no neighbours in S;

(b) N_2 is the set of vertices at distance 2 from 1_G in $\mathrm{Cay}(G; S)$ and every element in N_2 has μ neighbours in S and no neighbours in N_2;

(c) N_3 is the set of vertices at distance 3 from 1_G in $\mathrm{Cay}(G; S)$ and all the neighbours of every element of N_3 belong to N_2.

Let g be an arbitrary vertex of $\mathrm{Cay}(G; S)$. If g is at distance 1 from 1_G (that is, $g \in S$), then, by (3) and (4), it has no neighbours in S. This proves (a). Further, if $g \in N_2$, then by (3) and (4), g has μ neighbours in S and no neighbours in N_2. In particular, every element of N_2 is at distance 2 from 1_G. On the other hand, every element $x \in G$ at distance 2 from 1_G has to appear in the expansion of S^2 in (3) with a positive coefficient, and thus belongs to N_2. This implies that N_2 is the set of all vertices at distance 2 from 1_G, and proves (b). Finally, if $g \in N_3$, then all of its k neighbours belong to N_2. In particular, every vertex in N_3 is at distance at most 3 from 1_G. On the other hand, every element $x \in G$ at distance

3 from 1_G has to have a neighbour in N_2 and thus appears in the expansion of $N_2 S$ in (3) with a positive coefficient. Therefore, every vertex which is at distance 3 from 1_G belongs to N_3. This proves (c) and completes the proof of the lemma. ∎

Lemma 2.10 *Let G be a group of order $2n$ and S a subset of G. Then the following statements are equivalent.*

(i) *$S \subseteq G \setminus \{1\}$, $S = S^{(-1)}$ and $\mathrm{Cay}(G;S)$ is a bipartite non-trivial distance-regular graph with diameter 3 and intersection array $\{k, k-1, k-\mu; 1, \mu, k\}$;*

(ii) *there is a subgroup H of index 2 in G such that for every $a \in G \setminus H$, the set $D = a^{-1}S$ is a non-trivial (n,k,μ)-difference set in H satisfying $D^{(-1)} = aDa$;*

(iii) *there are a subgroup H of index 2 in G and an element $a \in G \setminus H$ such that the set $D = a^{-1}S$ is a non-trivial (n,k,μ)-difference set in H satisfying $D^{(-1)} = aDa$.*

Moreover, if (i), (ii) *and* (iii) *hold, then $H \setminus \{1\}$ is exactly the set of vertices of $\mathrm{Cay}(G;S)$ which are at distance 2 from the vertex 1.*

Proof. Suppose that (i) holds. For $i \in \{0,1,2,3\}$ let N_i denote the set of vertices at distance i from 1_G in $\mathrm{Cay}(G;S)$. By Lemma 2.3 the bipartition set $H = N_0 \cup N_2$ is a subgroup of index 2 in G. Let a be an arbitrary element of $G \setminus H$ and let $D = a^{-1}S$. Then $D^{(-1)} = S^{(-1)}a = Sa = aDa$. Moreover, by Lemma 2.9, $DD^{(-1)} = a^{-1}SS^{(-1)}a = a^{-1}(k1_G + \mu N_2)a = k1_G + \mu N_2 = (k-\mu)1_G + \mu H$. Whence, D is a (n,k,μ)-difference set in H, showing that (ii) holds. Clearly, (ii) implies (iii), therefore it remains to prove that (iii) implies (i). Assume that (iii) holds. Since $a \in G \setminus H$ and $D \subseteq H$, we obtain $S \cap H = \emptyset$. In particular, $S \subseteq G \setminus \{1\}$. Moreover, it follows from $D^{(-1)} = aDa$ that $S^{(-1)} = D^{(-1)}a^{-1} = aD = S$. Let $N_2 = H \setminus \{1\}$ and let $N_3 = G \setminus (H \cup S)$. Clearly $\{\{1\}, S, N_2, N_3\}$ is a partition of G. Further, $S^2 = SS^{(-1)} = aDD^{(-1)}a^{-1} = a((k-\mu)1_G + \mu H)a^{-1} = k1_G + \mu N_2$, and $N_2 S = HS - S = aHD - S = kaH - S = k(G \setminus H) - S = kN_3 + kS - S = (k-1)S + kN_3$. Whence, by Lemma 2.9, (i) holds. ∎

2.6 Miscellanea

In what follows, an element of the ring $\mathbb{Z}_n$ (and therefore also of its group of units $\mathbb{Z}_n^*$) will be sometimes considered also as the corresponding element of $\mathbb{Z}$ contained in the set $\{0, 1, \ldots, n-1\}$. This abuse of notation should not cause any ambiguities.

Lemma 2.11 *Let n denote a positive integer, and let p be an odd prime divisor of n. Then there exists $m \in \mathbb{Z}_n^* \setminus \{1\}$ such that $p \equiv mp \pmod{\frac{n}{p}}$.*

Proof. Let $n = p^a q_1^{b_1} \cdots q_s^{b_s}$ be a prime decomposition of n. If $a \geq 2$, then $m = \frac{n}{p} + 1 \in \mathbb{Z}_n^* \setminus \{1\}$ is coprime with n, does not equal 1, and $mp \equiv p \pmod{\frac{n}{p}}$. Whence, we may assume that $a = 1$. Let $m_i = i\frac{n}{p} + 1$, for $i = 1, 2$, and observe that $m_i p \equiv p \pmod{\frac{n}{p}}$. Clearly, m_i is coprime with every prime divisor of n, except possibly with p. Moreover, at least one of the integers m_1, m_2, is coprime with p, since p would otherwise divide $m_2 - m_1 = \frac{n}{p}$, contradicting our assumption that $a = 1$. Therefore, at least one of the numbers m_1 and m_2, call it m, is coprime with n. Hence, $m \in \mathbb{Z}_n^* \setminus \{1\}$ and $mp \equiv p \pmod{\frac{n}{p}}$. ∎

Corollary 2.12 *Let n denote a positive integer, and let p be an odd prime divisor of n. Then for every pair $\alpha, \beta \in \{1, 2, \ldots, p-1\}$ and for every $\ell \in \mathbb{Z}$, there exists $m \in \mathbb{Z}_n^* \setminus \{1\}$ such that*

$$(\alpha\frac{n}{p} + \ell p) \equiv m(\beta\frac{n}{p} + \ell p) \pmod{\frac{n}{p}}.$$

PROOF. By Lemma 2.11, there exists $m \in \mathbb{Z}_n^* \setminus \{1\}$ such that $mp \equiv p \,(\mathrm{mod}\, \frac{n}{p})$. But then also $(\alpha\frac{n}{p} + \ell p) \equiv m(\beta\frac{n}{p} + \ell p) \,(\mathrm{mod}\, \frac{n}{p})$. ∎

A *transversal* of a subgroup H in a group G is a subset of G which contains exactly one element from each of the right cosets of H in G.

Lemma 2.13 *Let n denote a positive integer, let p denote a prime divisor of n, and let A denote a transversal of the subgroup $\frac{n}{p}\mathbb{Z}_n$ in $\mathbb{Z}_n$. If A is a union of orbits of the action of $\mathbb{Z}_n^*$ on $\mathbb{Z}_n$ by multiplication, then $p = 2$ or $A = p\mathbb{Z}_n$.*

PROOF. Suppose that $p > 2$. Let $\ell \in \{0, 1, \ldots, \frac{n}{p} - 1\}$ and suppose $\ell p \notin A$. Since A is a transversal of $\frac{n}{p}\mathbb{Z}_n$, there exists $\alpha \in \{1, \ldots, p-1\}$ such that $\ell p + \alpha\frac{n}{p} \in A$. Let $\beta \in \{1, \ldots, p-1\} \setminus \{\alpha\}$. By Corollary 2.12 there exist $m \in \mathbb{Z}_n^* \setminus \{1\}$ such that $(\ell p + \alpha\frac{n}{p}) \equiv m(\ell p + \beta\frac{n}{p}) \,(\mathrm{mod}\, \frac{n}{p})$. Since A is a union of orbits of the action of $\mathbb{Z}_n^*$ on $\mathbb{Z}_n$ by multiplication, we have $\ell p + \beta\frac{n}{p} \in A$. But then A contains two different elements from $\ell p + \frac{n}{p}\mathbb{Z}_n$, a contradiction. ∎

3 Fourier transformation

Throughout this section n will denote a fixed positive integer, $\mathbb{Z}_n^*$ the multiplicative group of units in the ring $\mathbb{Z}_n$, ω a fixed primitive n-th root of unity, and $\mathbb{F} = \mathbb{Q}[\omega]$ the n-th cyclotomic field over the rationals. For a subset $A \subseteq \mathbb{Z}_n$, an element $i \in \mathbb{Z}_n$ and a unit $c \in \mathbb{Z}_n^*$, let $\Delta_A \colon \mathbb{Z}_n \to \mathbb{F}$ denote the characteristic function of A, let $cA = \{ca \mid a \in A\}$, let $i + A = \{i + a \mid a \in A\}$, and let $i - A = i + (-1)A$. In a special case when $A = \{c\}$ is a singleton, we write Δ_c instead of Δ_A. Further, let $\mathbb{F}^{\mathbb{Z}_n}$ be the $\mathbb{F}$-vector space of all functions $f \colon \mathbb{Z}_n \to \mathbb{F}$ mapping from the residue class ring $\mathbb{Z}_n$ to the field $\mathbb{F}$ (with the scalar multiplication and addition defined point-wise). The $\mathbb{F}$-algebra obtained from $\mathbb{F}^{\mathbb{Z}_n}$ by defining the multiplication point-wise will be denoted by $(\mathbb{F}^{\mathbb{Z}_n}, \cdot)$, while $(\mathbb{F}^{\mathbb{Z}_n}, *)$ will denote the $\mathbb{F}$-algebra obtained from $\mathbb{F}^{\mathbb{Z}_n}$ by defining the multiplication as the *convolution*:

$$(f * g)(z) = \sum_{i \in \mathbb{Z}_n} f(i)g(z - i)\,, \quad f, g \in \mathbb{F}^{\mathbb{Z}_n}. \tag{5}$$

Note that for any subsets $A, B \subseteq \mathbb{Z}_n$ and any $i \in \mathbb{Z}_n$ the following holds:

$$|(i - A) \cap B| = |A \cap (i - B)| = (\Delta_A * \Delta_B)(i). \tag{6}$$

The *Fourier transformation*

$$\mathcal{F} \colon (\mathbb{F}^{\mathbb{Z}_n}, *) \to (\mathbb{F}^{\mathbb{Z}_n}, \cdot)\,, \qquad (\mathcal{F}f)(z) = \sum_{i \in \mathbb{Z}_n} f(i)\omega^{iz}, \tag{7}$$

is an isomorphism of $\mathbb{F}$-algerbas $(\mathbb{F}^{\mathbb{Z}_n}, *)$ and $(\mathbb{F}^{\mathbb{Z}_n}, \cdot)$. It obeys the *inversion formula*

$$\mathcal{F}(\mathcal{F}(f))(z) = nf(-z). \tag{8}$$

The Fourier transform of characteristic functions of subgroups in $\mathbb{Z}_n$ can be easily computed. For a positive divisor r of n let $r\mathbb{Z}_n = \{0, r, 2r, \ldots, n - r\}$ be the subgroup of the additive group of $\mathbb{Z}_n$ of order $\frac{n}{r}$. Then:

$$\mathcal{F}\Delta_{r\mathbb{Z}_n} = \frac{n}{r}\Delta_{\frac{n}{r}\mathbb{Z}_n}, \text{ in particular, } \mathcal{F}1 = \mathcal{F}\Delta_{\mathbb{Z}_n} = n\Delta_0, \text{ and } \mathcal{F}\Delta_0 = \Delta_{\mathbb{Z}_n} = 1. \tag{9}$$

For an element $c \in \mathbb{Z}_n^*$, let σ_c be the element of the Galois group $\mathrm{Gal}\,[\mathbb{F} : \mathbb{Q}]$ mapping ω to ω^c. Further, for each $f \in \mathbb{F}^{\mathbb{Z}_n}$ let $f^{(c)}$ and f^{σ_c} be the elements of $\mathbb{F}^{\mathbb{Z}_n}$ defined by $f^{(c)}(z) = f(c^{-1}z)$ and $f^{\sigma_c}(z) = f(z)^{\sigma_c}$. A straightforward computation shows that the following holds for each $c \in \mathbb{Z}_n^*$ and each $f \in \mathbb{F}^{\mathbb{Z}_n}$:

$$(\mathcal{F}f)^{\sigma_c} = \mathcal{F}((f^{\sigma_c})^{(c)}) = (\mathcal{F}(f^{\sigma_c}))^{(c^{-1})}. \tag{10}$$

Since the set of elements of $\mathbb{F}$ which are fixed by every element of the Galois group $\mathrm{Gal}\,[\mathbb{F} : \mathbb{Q}]$ is exactly $\mathbb{Q}$, it easily follows that $f^{\sigma_c} = f$ for every $c \in \mathbb{Z}_n^*$ if and only if $\mathrm{Im}(f) \subseteq \mathbb{Q}$. Whence, by formula (10),

$$\mathrm{Im}(f) \subseteq \mathbb{Q} \;\Rightarrow\; (\mathcal{F}f)^{\sigma_c} = \mathcal{F}(f^{(c)}) = (\mathcal{F}f)^{(c^{-1})}. \tag{11}$$

Moreover, if $f = \Delta_A$ for some $A \subseteq \mathbb{Z}_n$, then

$$(\mathcal{F}\Delta_A)^{\sigma_c} = \mathcal{F}({\Delta_A}^{(c)}) = \mathcal{F}\Delta_{cA}. \tag{12}$$

On the other hand, $f^{(c)} = f$ holds for each $c \in \mathbb{Z}_n^*$ if and only if f is constant on each orbit of the action of $\mathbb{Z}_n^*$ on $\mathbb{Z}_n$ by multiplication. Note that every such orbit consits of all elements of a given order in the additive group $\mathbb{Z}_n$. If r is a positive divisor of n, then the $\mathbb{Z}_n^*$-orbit containing all elements of order r will be denoted by O_r. Hence,

$$O_r = \{z \mid z \in \mathbb{Z}_n,\, r\gcd(n,z) = n\} = \{\frac{cn}{r} \mid c \in \mathbb{Z}_n^*\}. \tag{13}$$

The following lemma now follows easily from (11).

Lemma 3.1 *Suppose that* $f\colon \mathbb{Z}_n \to \mathbb{F}$ *is a function such that* $\mathrm{Im}(f) \subseteq \mathbb{Q}$. *Then* $\mathrm{Im}(\mathcal{F}f) \subseteq \mathbb{Q}$ *if and only if* $f = \sum_{r|n} \alpha_r \Delta_{O_r}$ *for some* $\alpha_r \in \mathbb{Q}$.

The Fourier transform of the characteristic function of an orbit O_r plays an important role in the theory of arithmetic functions and its values are also known as the Ramanujan's sums. It can be expressed in terms of the Euler function ϕ and the Möbius function μ (see, for example, [20, Chapter IX]):

$$(\mathcal{F}\Delta_{O_r})(z) = \frac{\mu(m)\,\phi(r)}{\phi(m)} \in \mathbb{Z}, \quad \text{where } m = \frac{r}{\gcd(z,r)}. \tag{14}$$

The above equation together with Lemma 3.1 has the following interesting corollary:

Corollary 3.2 *If* A *is a subset of* $\mathbb{Z}_n$ *and* $\mathrm{Im}(\mathcal{F}\Delta_A) \subseteq \mathbb{Q}$, *then* A *is a union of orbits* O_r, *and* $\mathrm{Im}(\mathcal{F}\Delta_A) \subseteq \mathbb{Z}$.

Lemma 3.3 *Let* A *be a subset of* $\mathbb{Z}_n$, *let* r *be a positive divisor of* n, *and let* $\xi = \omega^{\frac{n}{r}}$ *be a primitive* r*-th root of unity. Then:*

(i) $\mathcal{F}\Delta_{(\frac{n}{r}+A)} = \mathcal{F}\Delta_A\left(\Delta_{r\mathbb{Z}_n} + \xi\Delta_{(1+r\mathbb{Z}_n)} + \ldots + \xi^{r-1}\Delta_{(r-1+r\mathbb{Z}_n)}\right)$,

(ii) $\mathcal{F}\Delta_A(\frac{n}{r}) = \alpha_0 + \alpha_1\xi + \ldots + \alpha_{r-1}\xi^{r-1}$, *where* $\alpha_i = |A \cap (i + r\mathbb{Z}_n)|$.

Proof. To prove part (i) suppose that $z \in i + r\mathbb{Z}_n$ for some $i \in \{0, 1, \ldots, r-1\}$. Then $z = i + rm$ for some $m \in \mathbb{Z}_n$, and

$$(\mathcal{F}\Delta_{(\frac{n}{r}+A)})(z) = \sum_{j \in \frac{n}{r}+A} \omega^{jz} = \sum_{\ell \in A} \omega^{(\ell+\frac{n}{r})z} = \omega^{\frac{n}{r}(i+mr)} \sum_{\ell \in A} \omega^{\ell z} = \xi^i(\mathcal{F}\Delta_A)(z).$$

To prove part (ii) observe that $\omega^{j\frac{n}{r}} = \xi^i$ if and only if $j \in i + r\mathbb{Z}_n$. ∎

Lemma 3.4 *Let r be a positive divisor of n, and let A be a transversal of $r\mathbb{Z}_n$ in $\mathbb{Z}_n$. If $z = m\frac{n}{r}$ $(m \notin r\mathbb{Z}_n)$ is an arbitrary element of $\frac{n}{r}\mathbb{Z}_n \setminus \{0\}$, then $\mathcal{F}\Delta_A(z) = 0$.*

Proof. Observe that

$$\mathcal{F}\Delta_A(z) = \sum_{i\in A} \omega^{im\frac{n}{r}} = \sum_{j=0}^{r-1} \omega^{jm\frac{n}{r}} = 0.$$

■

The following technical lemma deals with a very special situation, which will occur in Section 4.

Lemma 3.5 *Let d is an odd positive integer, let $n = 2d$, and let $A \subseteq \mathbb{Z}_n$ be a transversal of the subgroup $d\mathbb{Z}_n \leq \mathbb{Z}_n$. If $\mathrm{Im}(\mathcal{F}\Delta_A) \subseteq \mathbb{Q}$, then $(\mathcal{F}\Delta_A)(z)$ is an even integer for every $z \in \mathbb{Z}_n \setminus \{0, d\}$.*

Proof. Let $\{r_1, r_2, \ldots, r_t\}$ be the set of positive divisors of d. Since the elements of the orbits O_{r_i}, $i \in \{1, \ldots, t\}$, belong to the subgroup $2\mathbb{Z}_n \leq \mathbb{Z}_n$, we call these orbits *even*. Further, since the union of all even orbits is the set $2\mathbb{Z}_n$, we call the rest of the orbits O_r, $r \mid n$, *odd*. Since $cd = d$ for every element $c \in \mathbb{Z}_n^*$, the set $d + O_r$ is also an orbit of the action of $\mathbb{Z}_n^*$ on $\mathbb{Z}_n$. Therefore the set of odd orbits is $\{d + O_{r_i} \mid i \in \{1, \ldots, t\}\}$. The assumption $\mathrm{Im}(\mathcal{F}\Delta_A) \subseteq \mathbb{Q}$, together with Corollary 3.2, implies that A is a union of orbits O_r. We can assume without loss of generality that there exists an index $s \in \{0, 1, \ldots, t\}$ such that $O_{r_i} \subseteq A$ for all $i \in \{1, 2, \ldots, s\}$ and that $O_{r_i} \cap A = \emptyset$ for all $i \in \{s+1, s+2, \ldots, t\}$. Since A is a transversal of $d\mathbb{Z}_n \leq \mathbb{Z}_n$, this amounts to:

$$A = \big(O_{r_1} \cup O_{r_2} \cup \ldots \cup O_{r_s}\big) \cup \big((d + O_{r_{s+1}}) \cup (d + O_{r_{s+2}}) \cup \ldots \cup (d + O_{r_t})\big).$$

Part (i) of Lemma 3.3 implies that $(\mathcal{F}\Delta_{(d+O_r)})(z) = -(\mathcal{F}\Delta_{O_r})(z)$ for each $z \in 1 + 2\mathbb{Z}_n$. But then by (9), for $z \in 1 + 2\mathbb{Z}_n \setminus \{d\}$, we get:

$$(\mathcal{F}\Delta_A)(z) = \sum_{i=1}^{s} (\mathcal{F}_{\Delta_{O_{r_i}}})(z) - \sum_{i=s+1}^{t} (\mathcal{F}_{\Delta_{O_{r_i}}})(z) =$$

$$= \sum_{i=1}^{t} (\mathcal{F}_{\Delta_{O_{r_i}}})(z) - 2\sum_{i=s+1}^{t} (\mathcal{F}_{\Delta_{O_{r_i}}})(z) = (\mathcal{F}\Delta_{2\mathbb{Z}_n})(z) - 2\sum_{i=s+1}^{t} (\mathcal{F}_{\Delta_{O_{r_i}}})(z) =$$

$$d(\Delta_{d\mathbb{Z}_n})(z) - 2\sum_{i=s+1}^{t} (\mathcal{F}_{\Delta_{O_{r_i}}})(z) = -2\sum_{i=s+1}^{t} (\mathcal{F}_{\Delta_{O_{r_i}}})(z),$$

which is an even integer by (14). Observe also that for $z \in 2\mathbb{Z}_n \setminus \{0\}$ it follows from Lemma 3.4 that $(\mathcal{F}\Delta_A)(z) = 0$. ■

4 The proof of Theorem 1.3

After preparing necessary prerequisites, we are now ready to carry out the proof of Theorem 1.3. In fact, we are going to prove the following, slightly stronger theorem.

Theorem 4.1 *Let $X = \mathrm{Dih}\,(n; R, T)$ be a connected dihedrant other than C_{2n}, K_{2n}, $K_{t\times m}$ (where $tm = 2n$), or $K_{n,n} - nK_2$. Then X is distance-regular if and only if one of the following occurs:*

(i) $R = \emptyset$ *and* T *is a non-trivial difference set in* $\mathbb{Z}_n$*;*

(ii) n *is even,* R *is a non-empty subset of* $1 + 2\mathbb{Z}_n$*, and either*

  (a) $T \subseteq 1 + 2\mathbb{Z}_n$ *and* $\rho^{-1+R} \cup \rho^{-1+T}\tau$ *is a non-trivial difference set in the dihedral group* $\langle \rho^2, \tau \rangle$*, or*

  (b) $T \subseteq 2\mathbb{Z}_n$ *and* $\rho^{-1+R} \cup \rho^{T}\tau$ *is a non-trivial difference set in the dihedral group* $\langle \rho^2, \tau \rangle$*.*

Moreover, if either (i) *or* (ii) *occurs, then* X *is bipartite, non-antipodal, and has diameter* 3*.*

In view of Lemma 2.6, a dihedrant $\mathrm{Dih}\,(n; R, T)$ is isomorphic to $\mathrm{Dih}\,(n; R, 1+T)$. Therefore, if $X = \mathrm{Dih}\,(n; R, T)$ in the above theorem is such that $\rho^{-1+R} \cup \rho^{T}\tau$ is a non-trivial difference set in the dihedral group $\langle \rho^2, \tau \rangle$, then $X \cong \mathrm{Dih}\,(n; R, T')$, where $T' = 1 + T$, and $\rho^{-1+R} \cup \rho^{-1+T'}\tau$ is a non-trivial difference set in the dihedral group $\langle \rho^2, \tau \rangle$. Whence, Theorem 4.1 indeed implies Theorem 1.3.

Throughout this section we shall use the following generic notation. For a positive integer n, D_n will denote the dihedral group with $2n$ elements, generated by an element ρ of order n and an involution τ satisfying the relation $\tau\rho\tau = \rho^{-1}$. With k, λ, μ and d, we shall respectively denote the valency, the number of common neighbours of two adjacent vertices, the number of common neighbours of two vertices at distance 2, and the diameter of the distance-regular dihedrant $X = \mathrm{Dih}\,(n; R, T)$ under consideration. For every $j \in \{0, 1, \ldots, d\}$, let N_j denote the set of vertices in X at distance j from the vertex $1 \in D_n$, and let $R_j = \{i \in \mathbb{Z}_n \mid \rho^i \in N_j\}$ and $T_j = \{i \in \mathbb{Z}_n \mid \rho^i\tau \in N_j\}$. Note that $R = R_1$ and $T = T_1$. Finally, let $\rho^{R_j} = \{\rho^i \mid i \in R_j\} = N_j \cap \langle \rho \rangle$ and $\rho^{T_j}\tau = \{\rho^i\tau \mid i \in T_j\} = N_j \cap \langle \rho \rangle\tau$.

The Fourier transforms (relative to a fixed primitive n-th root of unity ω) $\mathcal{F}\Delta_{R_j}$ and $\mathcal{F}\Delta_{T_j}$ will be denoted by $\underline{\mathbf{r}}_j$ and $\underline{\mathbf{t}}_j$, respectively. That is,

$$\underline{\mathbf{r}}_j(z) = \sum_{i \in R_j} \omega^{iz}, \qquad \underline{\mathbf{t}}_j(z) = \sum_{i \in T_j} \omega^{iz}. \tag{15}$$

In particular, we let $\underline{\mathbf{r}} = \underline{\mathbf{r}}_1 = \mathcal{F}\Delta_R$, and $\underline{\mathbf{t}} = \underline{\mathbf{t}}_1 = \mathcal{F}\Delta_T$. The following lemma is crucial for our analisys of distance-regular dihedrants.

Lemma 4.2 *If* $X = \mathrm{Dih}\,(n; R, T)$ *is distance-regular, then*

$$\begin{aligned} \underline{\mathbf{r}}^2 + |\underline{\mathbf{t}}|^2 &= k + \lambda\underline{\mathbf{r}} + \mu\underline{\mathbf{r}}_2 \\ 2\underline{\mathbf{r}}\underline{\mathbf{t}} &= \lambda\underline{\mathbf{t}} + \mu\underline{\mathbf{t}}_2. \end{aligned}$$

Proof. Observe that by (6) and Lemma 2.5, $(\Delta_R * \Delta_R)(i) + (\Delta_T * \Delta_{-T})(i) = |R \cap (i - R)| + |T \cap (i+T)| = (k\Delta_0 + \lambda\Delta_R + \mu\Delta_{R_2})(i)$, and $2(\Delta_R * \Delta_T)(i) = |R \cap (i-T)| + |T \cap (i-R)| = (\lambda\Delta_T + \mu\Delta_{T_2})(i)$. The result now follows by applying the Fourier transformation on these two equalities. ∎

We shall now prove two lemmas, dealing with two possible types of counter-examples to Theroem 4.1 which proved to be the most difficult to exclude. These are: an antipodal non-bipartite distance-regular dihedrant with diameter 3, and an antipodal, bipartite distance-regular dihedrant with diameter 4. After that, a proof of Theorem 4.1 will follow.

Lemma 4.3 *There are no antipodal non-bipartite distance-regular dihedrants with diameter* 3*.*

PROOF. Suppose that this is not true and let $X = \mathrm{Dih}\,(n; R, T)$ be the smallest (with respect to the size of the vertex set) antipodal non-bipartite distance-regular dihedrant with diameter 3. The antipodal class of X containing the identity element of the group D_n is the set $H = N_3 \cup \{1\}$. Since antipodal classes of X are blocks of imprimitivity for the group $\mathrm{Aut}(X)$, by Lemma 2.3, H is a subgroup of the regular dihedral group D_n. Let p denote the size of H. If p were not a prime number, H would contain a proper non-trivial subgroup $K \subseteq \langle\rho\rangle$, $K \lhd D_n$. Let $\mathcal{B}$ denote the set of K-orbits on $V(X)$. Then in view of Lemma 2.3(i), the quotient graph $X_{\mathcal{B}}$ is a dihedrant. On the other hand, by [8, Theorem 6.2] (and since the orbits of a subgroup in $\mathrm{Aut}(X)$ always form an equitable partition of a graph), $X_{\mathcal{B}}$ would be an antipodal distance-regular graph with diameter 3. If $X_{\mathcal{B}}$ were bipartite, then so would be X. Whence, $X_{\mathcal{B}}$ is an antipodal non-bipartite distance-regular dihedrant with diameter 3 with fewer vertices than X. But this contradicts the minimality of X, and shows that p is prime. Since X is an antipodal cover of the complete graph on $2n/p$ vertices, we have

$$k + 1 = \frac{2n}{p}. \tag{16}$$

Also, by [4, p. 431], graph X has the intersection array

$$\{k, \mu(p-1), 1; 1, \mu, k\} \tag{17}$$

and eigenvalues $k, \theta_1, -1, \theta_3$, where

$$\theta_1 = \frac{\lambda-\mu}{2} + \delta, \quad \theta_3 = \frac{\lambda-\mu}{2} - \delta; \qquad \delta = \sqrt{k + (\frac{\lambda-\mu}{2})^2}. \tag{18}$$

We shall now divide our analysis into two subcases, with respect to whether the intersection $N_3 \cap \langle\rho\rangle\tau$ is empty or not.

Case A: $N_3 \cap \langle\rho\rangle\tau \neq \emptyset$. Note that in this case the group H is dihedral, and since it is of prime order, its size is 2. Whence, $N_3 = \{\rho^c\tau\}$ for some $c \in \mathbb{Z}_n$. Since $X \cong \mathrm{Dih}\,(n; R, -c+T)$ by Lemma 2.6, we may in fact assume that $N_3 = \{\tau\}$.

By (16) and (17), $n = k + 1$ and the intersection array of X is $\{k, \mu, 1; 1, \mu, k\}$. Since $k = \lambda + \mu + 1$ and since, by Lemma 2.7, λ and μ are even (observe that since X is not bipartite we have $T_2 \neq \emptyset$), k is odd and thus n is even. By Lemma 2.5, $S(\tau) = \rho^{-T} \cup \rho^R\tau$. On the other hand, $S(\tau) = N_2 = \rho^{R_2} \cup \rho^{T_2}\tau$, hence $T = -R_2 = R_2$ and $T_2 = -R = R$. In particular, $T = -T$ and so $|\underline{\mathbf{t}}|^2 = \underline{\mathbf{t}}^2$. Now, by Lemma 4.2,

$$\underline{\mathbf{r}}^2 + \underline{\mathbf{t}}^2 = k + \lambda\underline{\mathbf{r}} + \mu\underline{\mathbf{t}}, \qquad 2\underline{\mathbf{r}}\underline{\mathbf{t}} = \lambda\underline{\mathbf{t}} + \mu\underline{\mathbf{r}}. \tag{19}$$

Let $\underline{\mathbf{x}} = \underline{\mathbf{r}} - \underline{\mathbf{t}}$ and observe that by (19), $\underline{\mathbf{x}}^2 - (\lambda-\mu)\underline{\mathbf{x}} - k = 0$. The solutions of this quadratic equation in $\mathbb{C}$ are θ_1 and θ_3, showing that $\mathrm{Im}(\underline{\mathbf{x}}) \subseteq \{\theta_1, \theta_3\}$. In particular, $|R| - |T| = \underline{\mathbf{x}}(0) = \theta_1$, if $|R| > |T|$, and $|R| - |T| = \underline{\mathbf{x}}(0) = \theta_3$, if $|R| < |T|$. This shows that $\theta_1, \theta_3 \in \mathbb{Z}$ and so also $\delta \in \mathbb{Z}$. In view of [4, p. 431], the second distance graph X_2 is also an antipodal non-bipartite distance-regular graph with diameter 3 (in fact, it has the same intersection array as X). On the other hand, $X_2 = \mathrm{Dih}\,(n; R_2, T_2) = \mathrm{Dih}\,(n; T, R)$. This allows us to assume without any loss of generality that $|R| > |T|$. Namely, if this were not the case, we could consider the graph X_2 instead of X. In particular, we may assume that

$$|R| - |T| = \theta_1. \tag{20}$$

Since $R_2 = T$ and since $\{R, R_2\}$ is a partition of the set $\mathbb{Z}_n \setminus \{0\}$, we have $\underline{\mathbf{t}} = n\Delta_0 - 1 - \underline{\mathbf{r}}$. Using this together with (19), we obtain the following formulae

$$\underline{\mathbf{r}}(z) = \begin{cases} |R|; & z = 0 \\ \frac{\theta_1 - 1}{2}; & z \in B \\ \frac{\theta_3 - 1}{2}; & z \in C \end{cases}, \quad \underline{\mathbf{t}}(z) = \begin{cases} |T|; & z = 0 \\ \frac{-\theta_1 - 1}{2}; & z \in B \\ \frac{-\theta_3^{-1}}{2}; & z \in C \end{cases}, \tag{21}$$

for some disjoint subsets $B, C \subseteq \mathbb{Z}_n$, satisfying $B \cup C = \mathbb{Z}_n \setminus \{0\}$. Recall that $\theta_1, \theta_3 \in \mathbb{Z}$, hence $\mathrm{Im}(\underline{\mathbf{r}}) \subseteq \mathbb{Q}$, $\mathrm{Im}(\underline{\mathbf{t}}) \subseteq \mathbb{Q}$, and thus, by Corollary 3.2, R and T are unions of $\mathbb{Z}_n^*$-orbits on $\mathbb{Z}_n$, and $\mathrm{Im}(\underline{\mathbf{r}}) \subseteq \mathbb{Z}$, $\mathrm{Im}(\underline{\mathbf{t}}) \subseteq \mathbb{Z}$. Applying the Fourier transformation on (21), using (8), and solving the transformed system of equations on $\mathcal{F}(\Delta_B)$ and $\mathcal{F}(\Delta_C)$ (taking into account (20)), we deduce that

$$\mathcal{F}\Delta_B(z) = \begin{cases} |B|; & z = 0 \\ \frac{n}{2\delta} - 1; & z \in R \\ -\frac{n}{2\delta} - 1; & z \in T \end{cases}, \quad \mathcal{F}\Delta_C(z) = \begin{cases} |C|; & z = 0 \\ -\frac{n}{2\delta}; & z \in R \\ \frac{n}{2\delta}; & z \in T \end{cases}. \tag{22}$$

Note that $\mathrm{Im}(\mathcal{F}\Delta_B) \subseteq \mathbb{Q}$, $\mathrm{Im}(\mathcal{F}\Delta_C) \subseteq \mathbb{Q}$, hence, by Corollary 3.2, B and C are unions of $\mathbb{Z}_n^*$-orbits on $\mathbb{Z}_n$ and $\mathrm{Im}(\mathcal{F}\Delta_B) \subseteq \mathbb{Z}$, $\mathrm{Im}(\mathcal{F}\Delta_C) \subseteq \mathbb{Z}$. In particular, $B = -B$ and $C = -C$. By (8), (6) and (22), we have

$$|(i - C) \cap C| = (\Delta_C * \Delta_C)(i) = \frac{1}{n}\mathcal{F}((\mathcal{F}(\Delta_C))^2)(i) =$$

$$= \frac{1}{n}\mathcal{F}(|C|^2\Delta_0 + \frac{n^2}{4\delta^2}\Delta_{\mathbb{Z}_n \setminus \{0\}})(i) = \frac{1}{n}(|C|^2 + \frac{n^2}{4\delta^2}(n\Delta_0(i) - 1)).$$

This implies that the Cayley graph $\mathrm{Cay}(\mathbb{Z}_n; C)$ is a strongly regular circulant with parameters $(n, |C|, \lambda', \mu')$ where $\lambda' = \mu' = \frac{1}{n}(|C|^2 - \frac{n^2}{4\delta^2})$, or the complete graph (if $C = \mathbb{Z}_n \setminus \{0\}$), or it is isomorphic to $\frac{n}{2}K_2$ (if $C = \{\frac{n}{2}\}$). By [3] (cf. Theorem 1.2), the only strongly regular circulants are the complete multipartite graphs, and the Paley graphs on prime number of vertices. But none of these satisfies the condition $\lambda' = \mu'$. If $\mathrm{Cay}(\mathbb{Z}_n; C)$ is a complete graph (and hence $C = \mathbb{Z}_n \setminus \{0\}$), then $B = \emptyset$, contradicting (22). Finally, if $\mathrm{Cay}(\mathbb{Z}_n; C) \cong \frac{n}{2}K_2$ (and $C = \{\frac{n}{2}\}$), then $\mathcal{F}\Delta_C = 2\Delta_{2\mathbb{Z}_n} - 1$, and by (22), $R = \emptyset$, contradicting the assumption that X is not bipartite.

Case B: $N_3 \cap \langle\rho\rangle\tau = \emptyset$. In this case $H = N_3 \cup \{1\}$ is the subgroup of $\langle\rho\rangle$ order p, and therefore $N_3 = \{\rho^{i\frac{n}{p}} \mid i \in \{1, \ldots, p-1\}\}$. We shall first prove that the sets T and $R \cup \{0\}$ are transversals of the subgroup $\frac{n}{p}\mathbb{Z}_n$ in $\mathbb{Z}_n$ (that is, each of them contains exactly one element from every coset of $\frac{n}{p}\mathbb{Z}_n$ in $\mathbb{Z}_n$). Observe that $R \cap \frac{n}{p}\mathbb{Z}_n = \emptyset$, so $R \cup \{0\}$ contains exactly one element of $\frac{n}{p}\mathbb{Z}_n$. Suppose that T (or $R \cup \{0\}$) contains two distinct elements in a coset $l + \frac{n}{p}\mathbb{Z}_n$. Then $T - T$ (or $R - R$) contains a non-zero element of $\frac{n}{p}\mathbb{Z}_n$, say $s\frac{n}{p}$. But then $\rho^{s\frac{n}{p}} \in N_0 \cup N_1 \cup N_2$, contradicting the fact that $N_3 = \{\rho^{i\frac{n}{p}} \mid i \in \{1, \ldots, p-1\}\}$. Suppose now that T has empty intersection with a coset $l + \frac{n}{p}\mathbb{Z}_n$. Then $l + \frac{n}{p}\mathbb{Z}_n \subseteq T_2$. Since each element in N_2 has a neighbour in N_3, there exists $i \in \{1, \ldots, p-1\}$ such that $\rho^{l+\frac{n}{p}}\tau$ is adjacent to $\rho^{i\frac{n}{p}}$, and so $l + (1-i)\frac{n}{p} \in T$. But then $T \cap T_2 \neq \emptyset$, which is a contradiction. Similarly, if $R \cup \{0\}$ has empty intersection with a coset $l + \frac{n}{p}\mathbb{Z}_n$, then $l + \frac{n}{p}\mathbb{Z}_n \subseteq R_2$, and there exists $i \in \{1, \ldots, p-1\}$ such that $\rho^{l+\frac{n}{p}}$ is adjacent to $\rho^{i\frac{n}{p}}$. But then $l + (1-i)\frac{n}{p} \in R$, which is again a contradiction. This shows that $R \cup \{0\}$ and T are indeed transversals of the subgroup $\frac{n}{p}\mathbb{Z}_n$. In particular, $|T| = \frac{n}{p}$, $|R| = \frac{n}{p} - 1$, $|R_2| = (p-1)|R|$ and $|T_2| = (p-1)|T|$.

Since $R_2 = \mathbb{Z}_n \setminus (\frac{n}{p}\mathbb{Z}_n \cup R)$ and $T_2 = \mathbb{Z}_n \setminus T$, we have that $\underline{\mathbf{r}}_2 = n\Delta_0 - p\Delta_{p\mathbb{Z}_n} - \underline{\mathbf{r}}$ and $\underline{\mathbf{t}}_2 = n\Delta_0 - \underline{\mathbf{t}}$. By Lemma 4.2,

$$\underline{\mathbf{r}}^2 + |\underline{\mathbf{t}}|^2 = k + (\lambda - \mu)\underline{\mathbf{r}} - p\mu\Delta_{p\mathbb{Z}_n} + n\mu\Delta_0, \quad 2\underline{\mathbf{r}}\underline{\mathbf{t}} = (\lambda - \mu)\underline{\mathbf{t}} + \mu n\Delta_0. \tag{23}$$

Clearly $\underline{\mathbf{r}}(0) = |R| = \frac{n}{p} - 1$ and $\underline{\mathbf{t}}(0) = |T| = \frac{n}{p}$. Since T and $R \cup \{0\}$ are transversals of the subgroup $\frac{n}{p}\mathbb{Z}_n \leq \mathbb{Z}_n$, it follows from Lemma 3.4, that $\underline{\mathbf{r}}(z) = -1$ and $\underline{\mathbf{t}}(z) = 0$, for every $z \in p\mathbb{Z}_n \setminus \{0\}$. Suppose now that $z \notin p\mathbb{Z}_n$. By (23), if $\underline{\mathbf{t}}(z) \neq 0$, then $\underline{\mathbf{r}}(z) = \frac{\lambda-\mu}{2}$, and $|\underline{\mathbf{t}}(z)| = \delta$. On the other hand, if $\underline{\mathbf{t}}(z) = 0$, then (23) implies that $\underline{\mathbf{r}}(z) \in \{\theta_1, \theta_3\}$. Let $B = \{z \mid z \notin p\mathbb{Z}_n, \underline{\mathbf{t}}(z) = 0, \underline{\mathbf{r}}(z) = \theta_1\}$, $C = \{z \mid z \notin p\mathbb{Z}_n, \underline{\mathbf{t}}(z) = 0, \underline{\mathbf{r}}(z) = \theta_3\}$, and $D = \mathbb{Z}_n \setminus (B \cup C \cup p\mathbb{Z}_n)$. Then

$$\underline{\mathbf{r}}(z) = \begin{cases} \frac{n}{p} - 1; & z = 0 \\ -1; & z \in p\mathbb{Z}_n \setminus \{0\} \\ \theta_1; & z \in B \\ \theta_3; & z \in C \\ \frac{\lambda-\mu}{2}; & z \in D \end{cases}, \quad |\underline{\mathbf{t}}(z)| = \begin{cases} \frac{n}{p}; & z = 0 \\ 0; & z \in p\mathbb{Z}_n \setminus \{0\} \\ 0; & z \in B \\ 0; & z \in C \\ \delta; & z \in D \end{cases}. \tag{24}$$

We split the analysis into two subcases with respect to whether δ is a rational number or not.

Subcase B.1: Assume that $\delta \in \mathbb{Q}$. Then $\mathrm{Im}(\underline{\mathbf{r}}) \subseteq \mathbb{Q}$, and Corollary 3.2 implies that R is a union of $\mathbb{Z}_n^*$-orbits. But then also $R \cup \{0\}$ is a union of $\mathbb{Z}_n^*$-orbits. On the other hand, $R \cup \{0\}$ is a transversal of the subgroup $\frac{n}{p}\mathbb{Z}_n$ in $\mathbb{Z}_n$. Hence, by Lemma 2.13, $p = 2$ or $R = p\mathbb{Z}_n \setminus \{0\}$. If $R = p\mathbb{Z}_n \setminus \{0\}$, then $S(\rho^i) \cap \rho^{R_2} = \emptyset$ for every $i \in R$, implying $S(\rho^i) \cap N_2 \subseteq \rho^{T_2}\tau$ for every $i \in R$. On the other hand, by Lemma 2.7, $|S(\rho^i\tau) \cap \rho^R| = \frac{\mu}{2}$ for every $i \in T_2$. Whence, by counting edges between ρ^R and $\rho^{T_2}\tau$ and by (17), we get $|R|\mu(p-1) = |T_2|\frac{\mu}{2}$. Since $|R| = \frac{n}{p} - 1$ and $|T_2| = n - |T| = \frac{n}{p}(p-1)$, the latter implies $\frac{n}{p} = 2$. Hence, $|R| = 1$, $|T| = 2$, and so $k = |R| + |T| = 3$. By Lemma 2.7, μ is an even integer, and is clearly positive and smaller than k. Therefore, $\mu = 2$. By (17), $\mu(p-1) < k$, implying that $p = 2$, and the intersection array of X is $\{3, 2, 1; 1, 2, 3\}$. But this would only be possible if X were bipartite. Whence, $R \neq p\mathbb{Z}_n \setminus \{0\}$. But then $p = 2$, and $R_3 = \{\frac{n}{2}\}$. Therefore, R contains no elements of $\mathbb{Z}_n$ of order 2 ($\frac{n}{2}$ being the only one), and since $R = -R$, it follows that $|R| = \frac{n}{2} - 1$ is an even integer, and $\frac{n}{2}$ is an odd integer. By part (ii) of Lemma 3.3, $\underline{\mathbf{t}}(\frac{n}{2}) = |T \cap 2\mathbb{Z}_n| - |T \cap (1 + 2\mathbb{Z}_n)|$. Since $|T| = \frac{n}{2}$ is odd, also $\underline{\mathbf{t}}(\frac{n}{2})$ is odd. But then, in view of (24), $\frac{n}{2} \in D$. Similarly, since $|R|$ is even, $\underline{\mathbf{r}}(\frac{n}{2})$ is also even. Therefore, $\frac{\lambda-\mu}{2}$ is even. By Lemma 3.5, $\underline{\mathbf{r}}(z) + 1 = \mathcal{F}\Delta_{R\cup\{0\}}(z)$ is an even integer for every $z \in \mathbb{Z}_n \setminus \{0, \frac{n}{2}\}$, hence $D = \{\frac{n}{2}\}$. This implies that $\underline{\mathbf{t}}(z) = \frac{n}{2}\Delta_0 + \alpha\Delta_{\{n/2\}} = (\frac{n}{2} - \alpha)\Delta_0 + \alpha\Delta_{\frac{n}{2}\mathbb{Z}_n}$, where $\alpha \in \{\delta, -\delta\}$. By applying (8), we obtain

$$\Delta_{-T} = \frac{1}{n}(\frac{n}{2} - \alpha + \alpha 2\Delta_{2\mathbb{Z}_n}). \tag{25}$$

Evaluating (25) at 0, we conclude that $\alpha = \frac{n}{2}$ if $0 \in T$, and $\alpha = -\frac{n}{2}$ if $0 \notin T$. Hence,

$$\sqrt{(\frac{\lambda-\mu}{2})^2 + k} = \delta = |\delta| = |\alpha| = \frac{n}{2}. \tag{26}$$

Since $n = k + 1$ and $k = \lambda + \mu + 1$, (26) implies $\mu = k - 1$, and therefore $\lambda = 0$. But then X is bipartite, which contradicts our assumptions. This completes the analysis of Subcase B.1.

Subcase B.2: Assume now that $\delta \notin \mathbb{Q}$. Then by [4, p. 431], $\lambda = \mu$. By (24), $k = |R| + |T| = 2\frac{n}{p} - 1$. On the other hand, it follows from (17) that $k = 1 + \mu p$. Since, by Lemma 2.7, μ is an even integer, this implies that

$$p \mid (\frac{n}{p} - 1). \tag{27}$$

Since $\mu = \lambda$, formula (24) implies that

$$\underline{\mathbf{r}} = \frac{n}{p}\Delta_0 - \Delta_{p\mathbb{Z}_n} + \delta(\Delta_B - \Delta_C). \tag{28}$$

Now, let c be an arbitrary element of $\mathbb{Z}_n^*$, and let (as in Section 3) σ_c denote the element of the Galois group $\mathrm{Gal}\,[\mathbb{Q}[\omega] : \mathbb{Q}]$ mapping ω to ω^c. By applying σ_c on (28) and using (11), we obtain

$$\underline{\mathbf{r}}^{(c^{-1})} = \underline{\mathbf{r}}^{\sigma_c} = \frac{n}{p}\Delta_0 - \Delta_{p\mathbb{Z}_n} + \delta^{\sigma_c}(\Delta_B - \Delta_C), \tag{29}$$

which implies

$$\underline{\mathbf{r}} = \frac{n}{p}\Delta_0 - \Delta_{p\mathbb{Z}_n} + \delta^{\sigma_c}(\Delta_{cB} - \Delta_{cC}). \tag{30}$$

Comparing (28) with (30), we see that either $cB = B$, $cC = C$ and $\delta^{\sigma_c} = \delta$, or $cB = C$, $cC = B$ and $\delta^{\sigma_c} = -\delta$. Since $\delta \notin \mathbb{Q}$, there exists an element σ_{c_0} of the Galois group $\mathrm{Gal}\,[\mathbb{Q}[\omega] : \mathbb{Q}]$ which does not fix δ. By the preceding argument, $\delta^{\sigma_{c_0}} = -\delta$, and thus $c_0 B = C$, $c_0 C = B$. In particular, $|B| = |C|$. Now, apply the Fourier transformation on (28), use (8), and solve the equation on $g = \mathcal{F}(\Delta_B - \Delta_C)$.

$$g = \mathcal{F}(\Delta_B - \Delta_C) = \frac{n}{\delta}(\Delta_R + \frac{1}{p}(\Delta_{\frac{n}{p}\mathbb{Z}_n} - 1)). \tag{31}$$

Next, apply σ_c on (31) and use (12).

$$g^{\sigma_c} = \mathcal{F}(\Delta_{cB} - \Delta_{cC}) = \frac{n}{\delta^{\sigma_c}}(\Delta_R + \frac{1}{p}(\Delta_{\frac{n}{p}\mathbb{Z}_n} - 1)). \tag{32}$$

Finally, compare (31) and (32), and observe that either

$$g^{\sigma_c} = g, \text{ if } \delta^{\sigma_c} = \delta, \quad \text{or} \quad g^{\sigma_c} = -g, \text{ if } \delta^{\sigma_c} = -\delta. \tag{33}$$

In particular, for $c = c_0$, we have

$$-g^{\sigma_c}(z) = g(z) = \begin{cases} 0; & z \in \frac{n}{p}\mathbb{Z}_n \\ \frac{n(p-1)}{\delta p}; & z \in R \\ -\frac{n}{\delta p}; & z \in \mathbb{Z}_n \setminus (R \cup \frac{n}{p}\mathbb{Z}_n) \end{cases}. \tag{34}$$

On the other hand, in view of (11), $g^{\sigma_c}(z) = g(cz)$, for every $z \in \mathbb{Z}_n$. Note that if $z \in R$, then either $cz \in R$ or $cz \in \mathbb{Z}_n \setminus (R \cup \frac{n}{p}\mathbb{Z}_n)$. In the former case, (34) implies $\frac{n(p-1)}{\delta p} = g(cz) = -g(z) = -\frac{n(p-1)}{\delta p}$, which is clearly impossible. In the latter case, (34) gives $-\frac{n}{\delta p} = g(cz) = -g(z) = -\frac{n(p-1)}{\delta p}$, implying that $p = 2$. However, if $p = 2$, the integer n is even and $n/2$ is odd, by (27). In view of Lemma 3.3, $\underline{\mathbf{t}}(\frac{n}{2}) = |T \cap 2\mathbb{Z}_n| - |T \cap (1 + 2\mathbb{Z}_n)| \in \mathbb{Q}$. Since $\delta \notin \mathbb{Q}$, (24) implies that $\frac{n}{2} \notin D$, and thus $\underline{\mathbf{t}}(\frac{n}{2}) = 0$. This shows that $|T|$ is even. On the other hand, $|T| = \frac{n}{2}$, which is an odd integer. This contradiction closes the subcase B.2, and concludes the proof of Lemma 4.3 ∎

Lemma 4.4 *The cycle C_8 is the only antipodal bipartite distance-regular dihedrant with diameter* 4.

PROOF. Suppose that the assertion of the lemma is not true. Choose a minimal antipodal bipartite distance-regular dihedrant $X = \mathrm{Dih}\,(n; R, T)$ with diameter 4 which is not isomorphic to C_8. Since C_8 is the only bipartite cycle with diameter 4, X is not a cycle. Whence, the valency of X is at least 3. Since X is bipartite, $\lambda = 0$. By Lemma 2.3, the antipodal class $H = \{1\} \cup N_4$ is a subgroup of D_n. Similiraly as in the proof of Lemma 4.3, in view of [8, Theorem 6.2], the minimality of X implies that the order p of H is prime. Whence, either $N_4 = \rho^{\frac{n}{p}\mathbb{Z}_n \setminus \{0\}}$, or $p = 2$ and $N_4 = \{\rho^c\tau\}$, for some $c \in \mathbb{Z}_n$. By [4, p. 425],

$$n = p^2\mu, \qquad k = \mu p. \tag{35}$$

The bipartition set $N_0 \cup N_2 \cup N_4$ is a subgroup of index 2 in D_n. Whence, either $N_0 \cup N_2 \cup N_4 = \langle\rho\rangle$, or n is even and $N_0 \cup N_2 \cup N_4 \in \{\rho^{2\mathbb{Z}_n} \cup \rho^{2\mathbb{Z}_n}\tau, \rho^{2\mathbb{Z}_n} \cup \rho^{1+2\mathbb{Z}_n}\tau\}$. The rest of the proof is split into several cases, depending on what the bipartition set $N_0 \cup N_2 \cup N_4$ and the antipodal class $N_0 \cup N_4$ are.

Case A: Suppose that n is even, $N_0 \cup N_2 \cup N_4 \in \{\rho^{2\mathbb{Z}_n} \cup \rho^{2\mathbb{Z}_n}\tau, \rho^{2\mathbb{Z}_n} \cup \rho^{1+2\mathbb{Z}_n}\tau\}$, and $N_0 \cup N_4 = \rho^{\frac{n}{p}\mathbb{Z}_n}$. Since $\mathrm{Dih}\,(n; R, T) \cong \mathrm{Dih}\,(n; R, 1 + T)$, we may in fact assume that $N_0 \cup N_2 \cup N_4 = \rho^{2\mathbb{Z}_n} \cup \rho^{2\mathbb{Z}_n}\tau$. Then $T_2 = 2\mathbb{Z}_n$, and by Lemma 2.7, μ is even. Also, $T \cup T_3 = R \cup R_3 = 1 + 2\mathbb{Z}_n$. In particular, in view of (35), $|R_3| = \frac{n}{2} - |R| = \frac{p^2\mu}{2} - |R|$. Observe that, since any two vertices in N_4 are at distance 4, the set ρ^{R_3} partitions into subsets ρ^{i+R}, $i \in R_4$, hence $|R_3| = (p-1)|R|$, implying $|R| = \frac{p\mu}{2}$. Similarly, $|T_3| = (p-1)|T|$, and thus $|T| = \frac{p\mu}{2}$. Therefore, $k = |R| + |T| = \mu p = \frac{n}{p}$. Using $R_2 = 2\mathbb{Z}_n \setminus \frac{n}{p}\mathbb{Z}_n$ and $T_2 = 2\mathbb{Z}_n$, and applying Lemma 4.2, we deduce that

$$\underline{\mathbf{r}}^2 + |\underline{\mathbf{t}}|^2 = k + \frac{k^2}{2}\Delta_{\frac{n}{2}\mathbb{Z}_n} - k\Delta_{p\mathbb{Z}_n}, \qquad 2\underline{\mathbf{r}}\underline{\mathbf{t}} = \frac{k^2}{2}\Delta_{\frac{n}{2}\mathbb{Z}_n}. \tag{36}$$

For $z \in p\mathbb{Z}_n \setminus \{0, \frac{n}{2}\}$, (36) implies that $\underline{\mathbf{r}}(z) = \underline{\mathbf{t}}(z) = 0$. On the other hand, if $z \notin p\mathbb{Z}_n$, then $\underline{\mathbf{r}}(z) = 0$ or $\underline{\mathbf{t}}(z) = 0$. In the first case, $|\underline{\mathbf{t}}(z)| = \sqrt{k}$, and in the second case, $\underline{\mathbf{r}}(z) \in \{\sqrt{k}, -\sqrt{k}\}$. Define $B = \{z | z \notin p\mathbb{Z}_n, \underline{\mathbf{t}}(z) = 0, \underline{\mathbf{r}}(z) = \sqrt{k}\}$, $C = \{z | z \notin p\mathbb{Z}_n, \underline{\mathbf{t}}(z) = 0, \underline{\mathbf{r}}(z) = -\sqrt{k}\}$, and $D = \mathbb{Z}_n \setminus (p\mathbb{Z}_n \cup B \cup C)$. Then

$$\underline{\mathbf{r}}(z) = \begin{cases} \frac{k}{2}; & z = 0 \\ -\frac{k}{2}; & z = n/2 \\ 0; & z \in p\mathbb{Z}_n \setminus \{0, \frac{n}{2}\} \\ \sqrt{k}; & z \in B \\ -\sqrt{k}; & z \in C \\ 0; & z \in D \end{cases}, \quad |\underline{\mathbf{t}}(z)| = \begin{cases} \frac{k}{2}; & z = 0 \\ \frac{k}{2}; & z = n/2 \\ 0; & z \in p\mathbb{Z}_n \setminus \{0, \frac{n}{2}\} \\ 0; & z \in B \\ 0; & z \in C \\ \sqrt{k}; & z \in D \end{cases}. \tag{37}$$

Observe that the antipodal class of an element ρ^i, $i \in R$, is $\rho^{i+(R_4 \cup \{0\})} = \rho^{i+\frac{n}{p}\mathbb{Z}_n}$. Since any two vertices in ρ^R are at distance 2, $\rho^{i+(R_4\cup\{0\})}$ meets ρ^R in exactly one element, namely ρ^i. Since X is bipartite, the rest of $\rho^{i+(R_4\cup\{0\})}$ lies in ρ^{R_3}. Whence, R_3 contains the disjoint union of sets $i + \frac{n}{p}\mathbb{Z}_n \setminus \{0\}$, $i \in R$, each of size $p - 1$. However, $|R_3| = (p-1)|R|$, therefore the above sets form a partition of R_3. Since $R \cup R_3 = 1 + 2\mathbb{Z}_n$, this implies that

$$|R \cap (i + \frac{n}{p}\mathbb{Z}_n)| = 1 \text{ and } |R_3 \cap (i + \frac{n}{p}\mathbb{Z}_n)| = p - 1, \text{ for every } i \in 1 + 2\mathbb{Z}_n. \tag{38}$$

In what follows, we distinguish two subcases, $p = 2$ and $p > 3$.

Subcase A.1: Suppose $p = 2$. For $E \in \{R, T\}$, let $\underline{\mathbf{e}} = \mathcal{F}\Delta_E$. Furthermore, for a positive integer t such that $2^t \mid n$ and $i \in \{0, 1, \ldots, 2^t - 1\}$, let $E_i(t) = E \cap (i + 2^t\mathbb{Z}_n)$ and $\alpha_i(t) = |E_i(t)|$. Since $R, T \subseteq 1 + 2\mathbb{Z}_n$, also $E \subseteq 1 + 2\mathbb{Z}_n$, and thus

$$\alpha_0(t) = \alpha_2(t) = \ldots = \alpha_{2^t-2}(t) = 0. \tag{39}$$

We shall now prove that for any integer t, $t \geq 2$, the following implication holds.

$$\underline{\mathbf{e}}(\frac{n}{2^i}) = 0, \text{ for all } i \in \{2, 3, \ldots, t\} \quad \Rightarrow \quad \alpha_1(t) = \alpha_3(t) = \ldots = \alpha_{2^t-1}(t). \tag{40}$$

The proof is by induction on t. Suppose first that $t = 2$ and $\underline{\mathbf{e}}(\frac{n}{4}) = 0$. Then, by Lemma 3.3(ii) and (39), $\underline{\mathbf{e}}(\frac{n}{4}) = (\alpha_1(2) - \alpha_3(2))i$, where $i^2 = -1$, whence $\alpha_1(2) = \alpha_3(2)$. Assume now that $t \geq 3$ and that (40) holds for any t', $2 \leq t' \leq t-1$, in place of t. Suppose that $\underline{\mathbf{e}}(\frac{n}{2^i}) = 0$, for all $i \in \{2, 3, \ldots, t\}$. In view of Lemma 3.3(ii),

$$0 = \underline{\mathbf{e}}(\frac{n}{2^t}) = \sum_{i=0}^{2^{t-1}-1} (\alpha_i(t) - \alpha_{i+2^{t-1}}(t))\, \xi^i, \tag{41}$$

where $\xi = \omega^{\frac{n}{2^t}}$ is a 2^t-th root of unity. Since the degree of the minimal polynomial for ξ over $\mathbb{Q}$ is $\phi(2^t) = 2^{t-1}$, (41) implies that

$$\alpha_i(t) = \alpha_{i+2^{t-1}}(t), \quad \text{for every } i \in \{0, 1, \ldots, 2^{t-1} - 1\}. \tag{42}$$

Furthermore, by the induction assumption, there exists an integer c such that

$$\alpha_1(t-1) = \alpha_3(t-1) = \ldots = \alpha_{2^{t-1}-1}(t-1) = c. \tag{43}$$

Since the set $2^{t-1}\mathbb{Z}_n$ is a disjoint union of the sets $2^t\mathbb{Z}_n$ and $2^{t-1} + 2^t\mathbb{Z}_n$, also $E_i(t-1)$ is a disjoint union of $E_i(t)$ and $E_{i+2^{t-1}}(t)$. Whence, $\alpha_i(t-1) = \alpha_i(t) + \alpha_{i+2^{t-1}}(t)$. The latter, however, combined with (42) and (43) implies that

$$\alpha_1(t) = \alpha_3(t) = \ldots = \alpha_{2^t-1}(t) = \frac{c}{2}, \tag{44}$$

completing the proof of (40). In view of the fact that $4|R| = 4|T| = n$, (39) and (40) imply that

$$2^{t+1} \mid n, \qquad \text{whenever } \underline{\mathbf{e}}(\frac{n}{2^i}) = 0, \text{ for all } i \in \{2, 3, \ldots, t\}. \tag{45}$$

Let s be the largest integer such that $2^s \mid n$. Since $n = 4\mu$ and $\mu = |R|$ is even, $s \geq 3$. By (37), $\underline{\mathbf{r}}(\frac{n}{2^i}) = \underline{\mathbf{t}}(\frac{n}{2^i}) = 0$, for all $i \in \{2, 3, \ldots, s-1\}$. Moreover, since $\frac{n}{2^s} \notin \{0, \frac{n}{2}\}$, either $\underline{\mathbf{r}}(\frac{n}{2^s}) = 0$ or $\underline{\mathbf{t}}(\frac{n}{2^i}) = 0$, and by (45), $2^{s+1} \mid n$, contradicting the maximality of s.

Subcase A.2: Suppose now that $p > 2$. Then $\frac{n}{p}$ is even. If $\sqrt{k} \in \mathbb{Q}$, then, by Corollary 3.2, R is a union of $\mathbb{Z}_n^*$-orbits on $\mathbb{Z}_n$. On the other hand, in view of (38), R consists of exactly one element from each of the cosets $i + \frac{n}{p}\mathbb{Z}_n$, $i \in 1 + 2\mathbb{Z}_n$. Whence, it contains an element from $1 + \frac{n}{p}\mathbb{Z}_n$. Since $n = p^2\mu$, then $1 + \frac{n}{p}\mathbb{Z}_n \subseteq \mathbb{Z}_n^*$. Hence R contains an element of $\mathbb{Z}_n^*$. However, R is a union of $\mathbb{Z}_n^*$-orbits, therefore $\mathbb{Z}_n^* \subseteq R$, and thus $1 + \frac{n}{p}\mathbb{Z}_n \subseteq R$. But $|(1 + \frac{n}{p}\mathbb{Z}_n) \cap R| = 1$, implying that $|\frac{n}{p}\mathbb{Z}_n| = 1$, which is clearly a contradiction.

If $\sqrt{k} \notin \mathbb{Q}$, then there exists an element σ_c, $c \in \mathbb{Z}_n^*$, of the Galois group $\mathrm{Gal}\,[\mathbb{Q}(\omega) : \mathbb{Q}]$ such that $\sqrt{k}^{\sigma_c} = -\sqrt{k}$. It follows from (37) that

$$\underline{\mathbf{r}} = \frac{k}{2}(2\Delta_0 - \Delta_{\frac{n}{2}\mathbb{Z}_n}) + \sqrt{k}(\Delta_B - \Delta_C), \tag{46}$$

and from (12) that

$$\underline{\mathbf{r}}^{\sigma_c} = \mathcal{F}(\Delta_{cR}) = \frac{k}{2}(2\Delta_0 - \Delta_{\frac{n}{2}\mathbb{Z}_n}) - \sqrt{k}(\Delta_B - \Delta_C). \tag{47}$$

Applying (8) on (46) and (47), we deduce that

$$n\Delta_R = k(1 - \Delta_{2\mathbb{Z}_n}) + \sqrt{k}\, g, \qquad n\Delta_{cR} = k(1 - \Delta_{2\mathbb{Z}_n}) - \sqrt{k}\, g, \tag{48}$$

where $g = \mathcal{F}(\Delta_B - \Delta_C)$. Having in mind that $n = p^2\mu$ and $k = p\mu$, we deduce from (48) that

$$p(\Delta_R + \Delta_{cR}) = 2(1 - \Delta_{2\mathbb{Z}_n}). \tag{49}$$

Evaluting the latter at any $z \in R$, we deduce that $p = 2$, contradicting our assumption $p > 2$.

Case B: Suppose that n is even, $N_0 \cup N_2 \cup N_4 \in \{\rho^{2\mathbb{Z}_n} \cup \rho^{2\mathbb{Z}_n}\tau, \rho^{2\mathbb{Z}_n} \cup \rho^{1+2\mathbb{Z}_n}\tau\}$, and $N_4 = \{\rho^c\tau\}$, for some $c \in \mathbb{Z}_n$. Since $X \cong \mathrm{Dih}\,(n; R, -c + T)$, we may assume without loss of generality that $N_4 = \{\tau\}$, implying also that $N_0 \cup N_2 \cup N_4 = \rho^{2\mathbb{Z}_n} \cup \rho^{2\mathbb{Z}_n}\tau$. Clearly, $p = 2$, and by (35), $n = 4\mu$ and $k = 2\mu$. Observe that $R_2 = T_2 = 2\mathbb{Z}_n \setminus \{0\}$, and therefore $\underline{\mathbf{r}}_2 = \underline{\mathbf{t}}_2 = \frac{n}{2}\Delta_{\frac{n}{2}\mathbb{Z}_n} - 1$. Furthermore, $N_3 = S_1(\tau)$, and in view of Lemma 2.5, $R_3 = -T$ and $T_3 = R$. In particular, $T = -T$, hence $\mathrm{Im}(\underline{\mathbf{t}}) \subseteq \mathbb{R}$. Now, by Lemma 4.2,

$$\underline{\mathbf{r}}^2 + \underline{\mathbf{t}}^2 = 2\mu^2\Delta_{\frac{n}{2}\mathbb{Z}_n} + \mu, \qquad 2\underline{\mathbf{r}}\underline{\mathbf{t}} = 2\mu^2\Delta_{\frac{n}{2}\mathbb{Z}_n} - \mu, \tag{50}$$

Evaluating (50) at $\frac{n}{4}$ we deduce that $\underline{\mathbf{r}}(\frac{n}{4}) \in \{\sqrt{\frac{\mu}{2}}, -\sqrt{\frac{\mu}{2}}\}$. But in view of Lemma 3.3(ii) and the fact that $R \subseteq 1 + 2\mathbb{Z}_n$, the real part of $\underline{\mathbf{r}}(\frac{n}{4})$ is 0, which is a clear contradiction.

Case C: $N_0 \cup N_2 \cup N_4 = \langle\rho\rangle$ and $N_0 \cup N_4 = \rho^{\frac{n}{p}\mathbb{Z}_n}$. In this case, $R_2 = \mathbb{Z}_n \setminus \frac{n}{p}\mathbb{Z}_n$, and therefore for every $i \in \mathbb{Z}_n \setminus \frac{n}{p}\mathbb{Z}_n$, there exist exactly μ pairs $(j, j') \in T \times T$ such that $i = j - j'$. On the other hand, an element $i \in \frac{n}{p}\mathbb{Z}_n \setminus \{0\}$ cannot be represented as $j - j'$, $j, j' \in T$, since in this case, $\rho^i = \rho^j\tau\rho^{j'}\tau$ would be in R_2. A set T with this property is known as a *relative* $(\frac{n}{p}, p, k, \mu)$*-difference set in* $\mathbb{Z}_n$ *relative to the forbidden subgroup* $\frac{n}{p}\mathbb{Z}_n$ (see, for example [17]). Since $\frac{n}{p} = k$ and $\mu = \frac{k}{p}$, T is a relative $(k, p, k, \frac{k}{p})$ difference set in $\mathbb{Z}_n$ relative to the forbidden subgroup $\frac{n}{p}\mathbb{Z}_n$. In view of [17, Theorem 4.1.1], such relative difference set exists if and only if $p = 2$ and $n = 4$. In this case $X \cong C_8$. ∎

Proof of Theorem 4.1. Let us first prove that the graphs satisfying (i) or (ii) are indeed distance-regular. If $R = \emptyset$ and T is a non-trivial difference set in $\mathbb{Z}_n$, then also $-T$ is a non-trivial difference set in $\mathbb{Z}_n$, and hence ρ^{-T} is a non-trivial difference set in $\langle\rho\rangle$. Observe that $\rho^T = \tau\rho^{-T}\tau$. Then by Lemma 2.10, the Cayley graph $\mathrm{Cay}(D_n; S) = \mathrm{Dih}\,(n; \emptyset, T)$, $S = \tau\rho^{-T} = \rho^T\tau$, is a non-trivial bipartite distance-regular graph with diameter 3.

Next, suppose that $T \subseteq 1 + 2\mathbb{Z}_n$ and $D = \rho^{-1+R} \cup \rho^{-1+T}\tau$ is a non-trivial difference set in $\langle\rho^2, \tau\rangle$. Then $S = \rho^R \cup \rho^T\tau = \rho D$, and therefore $D^{(-1)} = S^{(-1)}\rho = S\rho = \rho D\rho$. By Lemma 2.10, $\mathrm{Cay}(D_n; S) = \mathrm{Dih}\,(n; R, T)$ is a non-trivial bipartite distance-regular graph with diameter 3.

Finally, if $T \subseteq 2\mathbb{Z}_n$ and $D = \rho^{-1+R} \cup \rho^T\tau$ is a non-trivial difference set in $\langle\rho^2, \tau\rangle$, then let $S' = \rho D = \rho^R \cup \rho^{1+T}\tau$. Observe that $S'^{(-1)} = S'$ and so $D^{(-1)} = \rho D\rho$. By Lemma 2.10, $\mathrm{Cay}(D_n; S') = \mathrm{Dih}\,(n; R, 1 + T)$ is a non-trivial bipartite distance-regular graph with diameter 3. But by Lemma 2.6, $\mathrm{Dih}\,(n; R, 1 + T)$ is isomorphic to $\mathrm{Dih}\,(n; R, T)$, and thus $\mathrm{Dih}\,(n; R, T)$ is distance-regular. This completes the proof of sufficiency of the conditions in Theorem 4.1.

Suppose now that $X = \mathrm{Dih}\,(n; R, T)$ is a connected non-trivial distance-regular dihedrant. It was observed in [15, Corollary 3.7] that an old result of Wielandt [21] implies that there are no primitive distance-regular dihedrants other than the complete graphs. This shows that the graph X has to be of one of the following types: *antipodal but not bipartite*, *antipodal and bipartite*, or *bipartite but not antipodal*. We shall now scrutinize these three possibilities and show that each of them leads to a contradiction.

Case 1. Suppose X is an *antipodal non-bipartite distance-regular graph*. By Lemma 2.1, the antipodal quotient $\overline{X}$ is a primitive distance-regular graph. Moreover, by Corollary 2.4, $\overline{X}$ is a dihedrant or a circulant. Thus, by [15, Corollary 3.7] and Theorem 1.2, $\overline{X}$ is either a complete graph, or a Paley graph on a prime number of vertices. By [4, p. 180], a Paley graph cannot be covered by an antipodal distance-regular graph, hence $\overline{X}$ is a complete graph. In particular, $d \in \{2, 3\}$. By Lemma 4.3, $d \neq 3$, whence $d = 2$. However, the only antipodal distance-regular graphs with diameter 2 are the complete multipartite graphs. We can therefore conclude, that there are no non-trivial distance-regular dihedrants which are antipodal but not bipartite.

Case 2. Let X be a bipartite antipodal distance-regular graph. By Corollary 2.4, the antipodal quotient $\overline{X}$ and a halved graph $\frac{1}{2}X$ are dihedrants or circulants. Suppose that the diameter d of X is odd. Then, by Lemma 2.1, $\overline{X}$ is primitive distance-regular graph. As in Case 1, in view of [15, Corollary 3.7], Theorem 1.2 and [4, p. 180], $\overline{X}$ is a complete graph. Whence, $d = 3$. But then X would be isomorphic to $K_{n,n} - nK_2$. Therefore, we may assume that d is even. Then, by Lemma 2.1, $\frac{1}{2}X$ is a non-bipartite antipodal distance-regular dihedrant or a circulant, with $d_{\frac{1}{2}X} = \frac{1}{2}d$. Clearly, $d \neq 2$. By Lemma 4.4, $d \neq 4$. Therefore, we may assume that $d_{\frac{1}{2}X} \geq 3$. In view of Case 1 above, $\frac{1}{2}X$ is not a dihedrant, hence it is a circulant. But then Theorem 1.2 implies that $\frac{1}{2}X$ is a cycle, and by Lemma 2.2, X is a cycle, contradicting our assumptions on X.

Case 3. Let X be a bipartite non-antipodal distance-regular graph. By Lemma 2.1, Corollary 2.4 and Theorem 1.2, $\frac{1}{2}X$ is either a complete graph, or a Paley graph on a prime number of vertices. Since, by [4, p. 180], a Paley graph cannot be isomorphic to a halved graph of a distance-regular graph, $\frac{1}{2}X$ is a complete graph. By Lemma 2.1, the diameter d of X is either 2 or 3. If $d = 2$ then X is a complete bipartite graph, which is antipodal. Hence X is isomorphic to a bipartite non-antipodal distance-regular graph with diameter 3. Recall that $X = \mathrm{Cay}(D_n; S)$, where $S = \rho^R \cup \rho^T\tau$. Let H be the bipartition set of X containing the element 1. Note that $H = N_0 \cup N_2$. On the other hand, by Lemma 2.3, H is a subgroup of index 2 in D_n. Moreover, if $a \in D_n \setminus H$, then, in view of Lemma 2.10, $D = a^{-1}S$ is a difference set in H. Observe that the dihedral group D_n has a unique subgroup of index 2, namely $\langle\rho\rangle$, if n is odd, and has two more subgroups of index 2, namely $\langle\rho^2, \tau\rangle$ and $\langle\rho^2, \rho\tau\rangle$, if n is even. We shall now split the proof into three subcases with respect to which of these subgroups H is.

Subcase 3.1. If $H = \langle\rho\rangle$, then $S = \rho^T\tau$ and by letting $a = \tau$ we may conclude that $D = a^{-1}S = \tau\rho^T\tau = \rho^{-T}$ is a non-trivial difference set in $\langle\rho\rangle$. But then also ρ^T is a difference set in $\langle\rho\rangle$, and since $\langle\rho\rangle$ is isomorphic to $\mathbb{Z}_n$, T is a non-trivial difference set in $\mathbb{Z}_n$.

Subcase 3.2. If n is even and $H = \langle\rho^2, \tau\rangle$, then clearly $T \cap 2\mathbb{Z}_n = \emptyset$ and thus $T \subseteq 1 + 2\mathbb{Z}_n$. Furthermore, for $a = \rho$, $D = a^{-1}S = \rho^{-1}(\rho^R \cup \rho^T\tau) = \rho^{-1+R} \cup \rho^{-1+T}\tau$ is a non-trivial difference set in $\langle\rho^2, \tau\rangle$.

Subcase 3.3. If n is even and $H = \langle\rho^2, \rho\tau\rangle$, then $T \cap (1 + 2\mathbb{Z}_n) = \emptyset$, and thus $T \subseteq 2\mathbb{Z}_n$. Furthermore, for $a = \rho$, $D = a^{-1}S = \rho^{-1}(\rho^R \cup \rho^T\tau) = \rho^{-1+R} \cup \rho^{-1+T}\tau$ is a non-trivial

difference set in $\langle \rho^2, \rho\tau \rangle$. But since $f\colon \langle \rho^2, \rho\tau \rangle \to \langle \rho^2, \tau \rangle$ defined by $f(\rho^i) = \rho^i$ and $f(\rho^i\tau) = \rho^{i+1}\tau$ is a group homomorphism, $f(a^{-1}S) = \rho^{-1+R} \cup \rho^T\tau$ is a non-trivial difference set in $f(\langle \rho^2, \rho\tau \rangle) = \langle \rho^2, \tau \rangle$. ∎

5 Discussing non-trivial distance-regular dihedrants

In this section we will state some corollaries of the classification of distance-regular dihedrants proved in the previous sections and discuss their relation with other combinatorial objects, such as symmetric designs. In Subsection 5.4, a complete classification result for distance-transitive dihedrants is proved.

5.1 Distance-regular dihedrants and symmetric designs

According to Theorem 1.3 all non-trivial distance-regular dihedrants arise in the context of difference sets. On the other hand, difference sets are closely related to symmetric designs. If ν, k and μ are positive integers satisfying $\nu \geq k \geq 2$, then a *symmetric* (ν, k, μ)*-design* is an ordered pair $(\mathcal{P}, \mathcal{B})$ where $\mathcal{P}$ is a *point set* of size ν and $\mathcal{B}$ is a collection of ν k-subsets of $\mathcal{P}$ such that two distinct points in $\mathcal{P}$ are simultaneously contained in exactly μ elements of $\mathcal{B}$. (This then implies that the intersection of any two distinct elements of $\mathcal{B}$ has size μ.) The elements of $\mathcal{B}$ are usually referred to as *blocks* of the design. Note that if $(\mathcal{P}, \mathcal{B})$ is a symmetric (ν, k, μ)-design, then $(\mathcal{P}, \mathcal{B}^{\mathrm{C}})$, where $\mathcal{B}^{\mathrm{C}} = \{\mathcal{P} \setminus B \mid B \in \mathcal{B}\}$, is a symmetric $(\nu, \nu - k, \nu - 2k + \mu)$-design, which is called *the complement of* $(\mathcal{P}, \mathcal{B})$. An *automorphism* of a symmetric design $(\mathcal{P}, \mathcal{B})$ is a permutation of the set $\mathcal{P}$ which maps every block in $\mathcal{B}$ to a block in $\mathcal{B}$. A subgroup of the automorphism group of $(\mathcal{P}, \mathcal{B})$ which acts regularly on $\mathcal{P}$ is called a *point-regular* group of $(\mathcal{P}, \mathcal{B})$, or also a *Singer group* of $(\mathcal{P}, \mathcal{B})$. If G is a point-regular group of $(\mathcal{P}, \mathcal{B})$, then the induced action of G on $\mathcal{B}$ is also regular (see, for example, [18, Proposition 1.2.3]). For a (ν, k, μ)-difference set D in a group G, let $\mathcal{P}_D = G$ and $\mathcal{B}_D = \{gD \mid g \in G\}$. Then $(\mathcal{P}_D, \mathcal{B}_D)$ is a symmetric (ν, k, μ)-design with G acting by left multiplication point-regularly. Conversely, every symmetric (ν, k, μ)-design with a point-regular group isomorphic to G is isomorphic to the one obtained from a (ν, k, μ)-difference set in G as described above (see, for example, [18, Theorem 1.2.5]). Note that if D is a difference set in G and $D^{\mathrm{C}} = G \setminus D$ is its complementary difference set in G, then $(\mathcal{P}_D, \mathcal{B}_{D^{\mathrm{C}}}) = (\mathcal{P}_D, \mathcal{B}_D{}^{\mathrm{C}})$. *The incidence graph* of a symmetric design $(\mathcal{B}, \mathcal{P})$ is the bipartite graph with the vertex set $\mathcal{B} \cup \mathcal{P}$ and with $v \in \mathcal{P}$ adjacent to $B \in \mathcal{B}$ whenever $v \in B$. Similarly, the *non-incidence graph* of $(\mathcal{B}, \mathcal{P})$ is the bipartite graph with the same vertex set, but with $v \in \mathcal{P}$ adjacent to $B \in \mathcal{B}$ whenever $v \notin B$. Clearly, the non-incidence graph of $(\mathcal{P}, \mathcal{B})$ is the incidence graph of $(\mathcal{P}, \mathcal{B}^{\mathrm{C}})$. For a group H and a subgroup $A \leq \mathrm{Aut}(H)$, we let $A \ltimes H$ denote the *semidirect product* of H by A, that is, the set $A \times H$ with the product defined by $(\varphi, g)(\psi, h) = (\varphi\psi, \psi^{-1}(g)h)$, for every $\varphi, \psi \in A$, $g, h \in H$. For a subset $D \subseteq H$ and an element $\varphi \in A$, let $(\varphi, D) = \{(\varphi, h) \mid h \in D\} \subseteq A \ltimes H$. The following result will be used to prove that the graphs described in parts (i) and (ii) of Theorem 1.3 are in fact the incidence graphs of the corresponding difference sets. But since it bears some interest of its own, we state it as a separate proposition.

Proposition 5.1 *If H is a group with an automorphism φ of order 2, then the following statements are equivalent.*

(i) $\mathrm{Cay}(\langle \varphi \rangle \ltimes H; (\varphi, D))$ *is a non-trivial distance-regular graph with diameter 3 and intersection array $\{k, k-1, k-\mu; 1, \mu, k\}$;*

(ii) *D is a non-trivial $(|H|, k, \mu)$-difference set in H such that $D^{(-1)} = \varphi(D)$.*

Moreover, if (i) *and* (ii) *hold, then* $\mathrm{Cay}(\langle\varphi\rangle \ltimes H; (\varphi, D))$ *is isomorphic to the incidence graph of the symmetric design* $(\mathcal{P}_D, \mathcal{B}_D)$.

PROOF. To prove the equivalence of (i) and (ii), define $G = \langle\varphi\rangle \ltimes H$ and observe that the implication (i) $\Rightarrow$ (ii) follows immediately from the implication (i) $\Rightarrow$ (ii) in Lemma 2.10, while the implication (ii) $\Rightarrow$ (i) follows from the implication (iii) $\Rightarrow$ (i) in Lemma 2.10. Now, suppose that (i) and (ii) hold. Recall that $\mathcal{P}_D = H$ and $\mathcal{B}_D = \{hD \mid h \in H\}$, and let $f\colon \langle\varphi\rangle \ltimes H \to \mathcal{P}_D \cup \mathcal{B}_D$ be the function defined by $f(\mathrm{id}_H, h) = h \in \mathcal{P}_D$ and $f(\varphi, h) = \varphi(h)D \in \mathcal{B}_D$, for every $h \in H$. Note that f is bijective. Next, observe that two vertices $x, y \in \mathcal{P}_D \cup \mathcal{B}_D$ are adjacent in the incidence graph X of $(\mathcal{P}_D, \mathcal{B}_D)$ if and only if there exist $h \in H$ and $g \in D^{(-1)}$ such that $\{x, y\} = \{h, hgD\}$. Furthermore, for arbitrary vertices u, v of $\mathrm{Cay}(\langle\varphi\rangle \ltimes H; (\varphi, D))$ and $r, h \in H$, the following equivalences hold:

$$\{u, v\} = \{(\mathrm{id}_H, h), (\mathrm{id}_H, h)(\varphi, r)\} \Leftrightarrow \{u, v\} = \{(\mathrm{id}_H, h), (\varphi, \varphi(h\varphi(r)))\} \Leftrightarrow$$

$$\{f(u), f(v)\} = \{h, h\varphi(r)D\}.$$

Now, since u and v are adjacent in $\mathrm{Cay}(\langle\varphi\rangle \ltimes H; (\varphi, D))$ if and only if $\{u, v\} = \{(\mathrm{id}_H, h), (\mathrm{id}_H, h)(\varphi, r)\}$ for some $h \in H$ and $r \in D$, the above equivalences show that u and v are adjacent in $\mathrm{Cay}(\langle\varphi\rangle \ltimes H; (\varphi, D))$ if and only if $\{f(u), f(v)\} = \{h, h\varphi(r)D\}$ for some $h \in H$ and $r \in D$. However, $D^{(-1)} = \varphi(D)$, hence $\varphi(r) \in D^{(-1)}$ whenever $r \in D$. Therefore, vertices u and v of $\mathrm{Cay}(\langle\varphi\rangle \ltimes H; (\varphi, D))$ are adjacent if and only if $f(u), f(v)$ are adjacent in X. Since f is a bijection, this implies that $\mathrm{Cay}(\langle\varphi\rangle \ltimes H; (\varphi, D))$ and X are isomorphic. ∎

Corollary 5.2 *A connected graph X is a non-trivial distance-regular dihedrant on $2n$ vertices with intersection array $\mathcal{R}$ if and only if $d_X = 3$, $\mathcal{R} = \{k, k-1, k-\mu; 1, \mu, k\}$, X is isomorphic to the incidence graph of the symmetric design $(\mathcal{P}_D, \mathcal{B}_D)$ where D is a non-trivial (n, k, μ)-difference set in a group G, and one of the following holds:*

(i) *$G = \mathbb{Z}_n$;*

(ii) *$n = 2m$ for an integer m, $G = \langle r, t \mid r^m = t^2 = (rt)^2 = 1\rangle \cong D_m$, and $D^{(-1)} = \varphi(D)$, where φ is the automorphism of G defined by $\varphi(r^i) = r^{-i}$, $\varphi(r^i t) = r^{-i+1}t$.*

PROOF. Let ψ be the automorphism of the additive group of $\mathbb{Z}_n$ defined by $\psi(i) = -i$. Further, if $n = 2m$ for an integer m, let $D_m = \langle r, t \mid r^m = t^2 = (rt)^2 = 1\rangle$, and let φ be the automorphism of D_m as defined in part (ii) above. Observe that the mappings

$$f\colon D_n \to \langle\psi\rangle \ltimes \mathbb{Z}_n, \quad f(\rho^i) = (\mathrm{id}, i), \quad f(\rho^i\tau) = (\psi, -i), \tag{51}$$

and

$$g\colon D_n \to \langle\varphi\rangle \ltimes D_m, \quad g(\rho^{2i}\tau^\epsilon) = (\mathrm{id}, r^i t^\epsilon), \quad g(\rho^{2i+1}\tau^\epsilon) = (\varphi, r^{-i}t^{1-\epsilon}), \tag{52}$$

for $i \in \{0, \ldots, m-1\}$ and $\epsilon \in \{0, 1\}$, are group isomorphisms.

Suppose first that X is isomorphic to the incidence graph of the symmetric design $(\mathcal{P}_D, \mathcal{B}_D)$ where D is a non-trivial (n, k, μ)-difference set in the group $\mathbb{Z}_n$. By Proposition 5.1, X is isomorphic to $\mathrm{Cay}(\langle\psi\rangle \ltimes \mathbb{Z}_n; (\psi, D))$ and is a non-trivial distance-regular graph with diameter 3 and the intersection array $\{k, k-1, k-\mu; 1, \mu, k\}$. Since $\langle\psi\rangle \ltimes \mathbb{Z}_n \cong D_n$, X is also a dihedrant.

Suppose now that $n = 2m$ for an integer m, and that X is isomorphic to the incidence graph of the symmetric design $(\mathcal{P}_D, \mathcal{B}_D)$ where D is a non-trivial (n, k, μ)-difference set in the group D_m such that $D^{(-1)} = \varphi(D)$. Then by Proposition 5.1, X is isomorphic to $\mathrm{Cay}(\langle\varphi\rangle \ltimes D_m; (\varphi, D))$, and is a non-trivial distance-regular graph with diameter 3 and the intersection array $\{k, k-1, k-\mu; 1, \mu, k\}$. Since $\langle\varphi\rangle \ltimes D_m \cong D_n$, X is a dihedrant.

Conversely, suppose that X is a non-trivial distance-regular dihedrant on $2n$ vertices. Let $\mathcal{R}$ be its intersection array. Then, by Theorem 1.3, X is bipartite and has diameter 3. Hence, $\mathcal{R} = (k, k-1, k-\mu; 1, \mu, k)$ for some positive integers k, μ. Moreover, X is isomorphic to $\mathrm{Dih}\,(n; R, T)$ for some $R, T \subseteq \mathbb{Z}_n$ such that one of the following holds:

(a) $R = \emptyset$ and T is a non-trivial difference set in the group $\mathbb{Z}_n$;

(b) $n = 2m$ for an integer m, $R, T \subseteq 1 + 2\mathbb{Z}_n$, and $\rho^{-1+R} \cup \rho^{-1+T}\tau$ is a non-trivial difference set in $\langle\rho^2, \tau\rangle$.

If (a) occurs, we can apply the group isomorphism f on the vertex set of X to show that X is isomorphic to the Cayley graph $\mathrm{Cay}(\langle\psi\rangle \ltimes \mathbb{Z}_n; (\psi, -T))$. By Proposition 5.1, $D = -T$ is a non-trivial (n, k, μ)-difference set in $\mathbb{Z}_n$ and X is isomorhic to the incidence graph of the symmetric design $(\mathcal{P}_D, \mathcal{B}_D)$.

Suppose now that (b) occurs. Let $R' = \{i \mid i \in \{0, 1, \ldots, m-1\}, 2i \in -1 + R\}$ and $T' = \{i \mid i \in \{0, 1, \ldots, m-1\}, 2i \in -1 + T\}$. Since $R, T \subseteq 1 + 2\mathbb{Z}_n$, $R = \{2i + 1 \mid i \in R'\}$ and $T = \{2i + 1 \mid i \in T'\}$. This implies that $g(\rho^R \cup \rho^T\tau) = (\varphi, r^{-T'} \cup r^{-R'}t)$, and thus $X = \mathrm{Cay}(D_n; \rho^R \cup \rho^T\tau)$ is isomorphic to $\mathrm{Cay}(\langle\varphi\rangle \ltimes D_m; (\varphi, D))$ where $D = r^{-T'} \cup r^{-R'}t$. By Proposition 5.1, D is a non-trivial (n, k, μ)-difference set such that $D^{-1} = \varphi(D)$, and X is isomorhic to the incidence graph of the symmetric design $(\mathcal{P}_D, \mathcal{B}_D)$. ∎

5.2 Distance-regular dihedrants arising from cyclic difference sets

The study of *cyclic difference sets* (that is, difference sets in cyclic groups) dates back to 1938 when Singer [19] defined the concept and described an infinite family of cyclic difference sets. His family is in fact a subfamily of cyclic $(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1})$-difference sets giving rise to the *classical symmetric designs* $\mathrm{PG}_{d-1}(d, q)$, $d \geq 2$, q a prime power, with the point-set and block-set being the sets of points and hyperplanes of the finite projective geometry $\mathrm{PG}(d, q)$, respectively. Let us mention that the smallest two non-trivial distance-regular dihedrants arise as the incidence and the non-incidence graphs of symmetric design $\mathrm{PG}_1(2, 2)$, also known as *the Fanno plane*. The corresponding distance-regular dihedrants $\mathrm{Dih}\,(7; \emptyset, \{1, 2, 4\})$ and $\mathrm{Dih}\,(7; \emptyset, \{0, 3, 5, 6\})$ are isomorphic to the *Heawood graph* and its *bipartite complement*.

Another classical family of cyclic difference sets is essentially due to Paley [16] and can be described as follows. For a prime q congruent 3 modulo 4 let $\mathbb{F}_q$ denote the finite field of cardinality q and let $D = \{x^2 \mid x \in \mathbb{F}_q \setminus \{0\}\}$ be the set of all non-zero squares in $\mathbb{F}_q$. Then D is a difference set in the additive group of $\mathbb{F}_q$. The corresponding symmetric design is called the *Paley-Hadamard design* and denoted by $\mathrm{PalHad}(q)$. The smallest non-trivial distance-regular dihedrants arising from this familly are the incidence and the non-incidence graphs of the Paley-Hadamard design $\mathrm{PalHad}(7)$, and are isomorphic to the Hadamard graph and its bipartite complement. We remark that $\mathrm{PalHad}(11)$ is an exceptional symmetric design in many way. It is, among others, responsible for the existence of the Mathieu group M_{11}. The corresponding distance-regular dihedrants, $\mathrm{Dih}\,(11; \emptyset, \{1, 3, 4, 5, 9\})$ and its bipartite complement, also appear as exceptional distance-transitive dihedrants in Theorem 5.8. For other infinite families of cyclic difference sets we refer the reader to [9].

5.3 Distance-regular dihedrants arising from dihedral difference sets

In contrast with the situation of the previous subsection, the absence of any known non-trivial *dihedral difference sets* (that is, difference sets in dihedral groups) prevents us from giving any examples of distance-regular dihedrants which would arise from the situation described in part (ii) of Corollary 5.2 (or equivalently, part (ii) of Theorem 1.3 or Theorem 4.1). What is more, it is now a wide spread belief that there are no non-trivial dihedral difference sets at all, and a strong evidence for this can be found in very restricting conditions for the existence of such a difference sets proved in [11]. This encourages us to conjecture the following.

Conjecture 5.3 *A dihedrant* $\mathrm{Dih}\,(n; R, T)$ *is a non-trivial distance-regular graph if and only if* $R = \emptyset$ *and* T *is a difference set in* $\mathbb{Z}_n$.

As Corollary 5.2 shows, the statement of Conjecture 5.3 is equivalent to the claim that there are no non-trivial difference sets D in a dihedral group such that $D^{(-1)} = \varphi(D)$ where φ is the automorphism of the dihedral group described in Corollary 5.2. This fact motivates the following definition and conjecture. (Recall that a difference set D is *reversible* if $D = D^{(-1)}$.)

Definition 5.4 A difference set D in a group G is *skew-reversible with respect to an automorphism* $\varphi \in \mathrm{Aut}(G)$ if $D^{(-1)} = \varphi(D)$, and is *skew-reversible* if it is skew-reversible with respect to some automorphism of G.

Conjecture 5.5 *There are no non-trivial skew-reversible difference sets in dihedral groups.*

Note that the statement of Conjecture 5.5 implies the statement of Conjecture 5.3. Further study of skew-reversible difference sets is a topic of a separate article. Here we only state an immediate consequence of Theorem 1.2 and Theorem 1.3.

Proposition 5.6 *There are no non-trivial skew-reversible difference sets in cyclic or dihedral groups with respect to an automorphism of odd order. In particular, there are no non-trivial reversible difference sets in cyclic or dihedral groups.*

Proof. Observe first that if a difference set D in a group G satisfies $D^{(-1)} = \varphi(D)$ for some $\varphi \in \mathrm{Aut}(G)$ of odd order, then also $D^{(-1)} = D$, and thus D is reversible. If $1_G \notin D$, then let $D' = D$, and if $1_G \in D$, then let $D' = G \setminus D$. Note that D' is also a non-trivial reversible difference set. Whence, $\mathrm{Cay}(G; D')$ is a strongly regular graph with parameter $\lambda = S(1_G) \cap S(g)$ for $g \in D'$ and $\mu = S(1_G) \cap S(g)$ for $g \in G \setminus (D' \cup \{1_G\})$, coinciding. However, it follows from Theorem 1.2 and Theorem 1.3 that there are no such Cayley graphs on cyclic or dihedral groups. ∎

5.4 Distance-transitive dihedrants

Recall that a connected graph X with diameter d is said to be distance-transitive if for every integer i, $1 \le i \le d$, the automorphism group $\mathrm{Aut}(X)$ acts transitively on the set $\{(u, v) \mid \partial_X(u, v) = i\}$. Note that a connected vertex-transitive graph is distance-transitive if and only if the stabilizer $\mathrm{Aut}(X)_u$ of a vertex u in X acts transitively on each sphere $S_i(u)$, $1 \le i \le d$. The following lemma enables us to give an explicite description of all distance-transtive dihedrants. A group G is said to act *doubly transitively* on a set V if for

any two pairs of distinct vertices $(u_1, v_1), (u_2, v_2) \in V^2$, $u_1 \neq v_1$, $u_2 \neq v_2$, there exists an element $\alpha \in G$ such that $u_2 = \alpha(u_1)$ and $v_2 = \alpha(v_1)$. Note that a transitive permutation group G acts doubly transitively on V if and only if the vertex stabilizer G_u of a vertex $u \in V$ acts transitively on $G \setminus \{u\}$.

Lemma 5.7 *Suppose that the incidence graph X of a symmetric design $(\mathcal{P}, \mathcal{B})$ is vertex-transitive. Then X is distance-transitive if and only if the automorphism group of $(\mathcal{P}, \mathcal{B})$ acts doubly transitively on $\mathcal{P}$.*

PROOF. Observe first that $\mathrm{Aut}(X) = \langle G, \varphi \rangle$, where G is the automorphism group of $(\mathcal{P}, \mathcal{B})$ and φ is an automorphism of X interchanging the bipartition sets $\mathcal{P}$ and $\mathcal{B}$. Choose a vertex $u \in \mathcal{P}$ and observe that X is distance-transitive if and only if G_u acts transitively on each of the following three sets: $S_1 = \{B \in \mathcal{B} \mid u \in B\}$, $S_2 = \mathcal{P} \setminus \{u\}$, and $S_3 = \{B \in \mathcal{B} \mid u \notin B\}$. In particular, if X is distance-transitive, then G_u acts transitively on $\mathcal{P} \setminus \{u\}$, and hence G acts doubly transitively on $\mathcal{P}$. Conversely, assume that G acts doubly transitively on $\mathcal{P}$. Then G_u has 2 orbits on $\mathcal{P}$. By the well known *Orbit Theorem* (see [2, Theorem III.4.1]), G_u has exactly two orbits on $\mathcal{B}$, which must clearly be S_1 and S_3. Hence, X is distance-transitive. ∎

Corollary 5.2 now implies that every non-trivial distance-transitive dihedrant arises as an incidence graph of a symmetric design admitting an automorphism group acting doubly transitively on points and containing a point-regular cyclic or dihedral group. Symmetric designs with a doubly transitive point-group were classified in [10]. It transpires from this classification that none of these symmetric designs admit a point-regular action of a dihedral group, and that those with a point-regular cyclic group are precisely $\mathrm{PG}_{d-1}(d, q)$, $d \geq 2$, q a prime power, PalHad(11) and the complements of the above. Hence the following result.

Theorem 5.8 *A graph X is a non-trivial distance-transitive dihedrant if and only if it is isomorphic to the incidence or to the non-incidence graph of a symmetric design* $\mathrm{PG}_{d-1}(d, q)$*, $d \geq 2$, q a prime power, or the symmetric design* PalHad(11)*.*

Let us mention that the smallest non-trivial distance-regular dihedrant, which is not distance-transitive, is the incidence graph of the symmetric design PalHad(19). It can be represented as $\mathrm{Dih}\,(19; \emptyset, \{1, 4, 5, 6, 7, 9, 11, 16, 17\})$. According to [15], an abstract group H is called a *DT-group* if every distance-regular Cayley graph of H is distance-transitive. Whence, D_{19} is the smallest dihedral group which is not a DT-group.

References

[1] E. Bannai and T. Ito, "Algebraic Combinatorics I - Association schemes", The Benjamin/Cummings Publishing Company, Menlo Park, California, (1984).

[2] T. Beth, D. Jungnickel and H. Lenz, "Design Theory", Volume 1, Second Edition, *Encyclopedia of Mathematics and its Applications* **69**, Cambridge University Press (1999).

[3] W. G. Bridges and R. A. Mena, Rational circulants with rational spectra and cyclic strongly regular graphs, *Ars Combin.* **8** (1979), 143–161.

[4] A. E. Brouwer, A. M. Cohen and A. Neumaier, "Distance-regular graphs", Springer-Verlag, New York, (1998).

[5] P. J. Cameron, "Permutation Groups", London Mathematical Society Student Texts **45**, Cambrigde Universtity Press (1999).

[6] Y. Q. Chen and C. H. Li, Relative difference sets and distance-regular Cayley graphs, submitted.

[7] J. D. Dixon and B. Mortimer, "Permutation groups", Springer-Verlag (1996).

[8] C. D. Godsil and A. D. Hensel, Distance-Regular Covers of the Complete Graph, *J. Combin. Theory, Ser. B*, **56** (1992), 205–238.

[9] D. Jungnickel and A. Pott, Abelian difference sets, *The CRC Hanbook of Combinatorial Designs*, ed. C. J. Coulbourn and J. H. Dinitz, CRC Press New York (1996).

[10] W. Kantor, Classification of 2-transitive symmetric designs, *Graphs Combin.* **1** (1985), 165–166.

[11] K. H. Leung, S. L. Ma and Y. L. Wong, Difference Sets in Dihedral Groups, *Des. Codes Cryptogr.* **1** (1992), 333–338.

[12] D. Marušič, Strongly regular bicirculants and tricirculants, *Ars comb.* **25C** (1988), 11–15.

[13] D. Marušič, Strong regularity and circulant graphs, *Discrete math.* **78** (1989), 119–125.

[14] D. Marušič, On 2-arc-transitivity of Cayley graphs, *J. Combin. Theory Ser. B* **87** (2003), 162–196.

[15] Š. Miklavič and P. Potočnik, Distance-regular circulants, *Europ. J. Combin.* **24** (2003), 777-784.

[16] R. E. A. C. Paley, On orthogonal matrices, *J. Math. Phys. MIT* **12** (1933), 311–320.

[17] A. Pott, "Finite Geometry and Character Theory", Lecture Notes in Mathematics **1601**, Springer-Verlag (1995).

[18] B. Schmidt, "Characters and Cyclotomic Fields in Finite Geometry", Lecture Notes in Mathematics **1797**, Springer-Verlag (2002).

[19] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* **43** (1938), 377–385.

[20] R. Sivaramakrishnan, "Classical Theory of Arithmetic Functions", Pure and Applied Mathematics, **126**, Marcel Dekker, INC. (1989).

[21] H. Wielandt, Zur Theorie der Einfach Transitiven Permutationsgruppen II, *Math. Z.* **52** (1947), 384–393.