UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

DOKTORSKA DISERTACIJA
(DOCTORAL THESIS)

O PROBLEMU IZOMORFNOSTI BI-CAYLEYJEVIH GRAFOV

(ON THE ISOMORPHISM PROBLEM OF BI-CAYLEY GRAPHS)

SERGIO HIROKI KOIKE QUINTANAR

KOPER, 2015

UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

DOKTORSKA DISERTACIJA
(DOCTORAL THESIS)

O PROBLEMU IZOMORFNOSTI BI-CAYLEYJEVIH GRAFOV

(ON THE ISOMORPHISM PROBLEM OF BI-CAYLEY GRAPHS)

SERGIO HIROKI KOIKE QUINTANAR

KOPER, 2015

MENTOR: IZR. PROF. DR. ISTVÁN KOVÁCS

Acknowledgements

I would like to express all my gratitude to my PhD. supervisor István Kovács for all the help, support and patience he showed towards me, and all time he invested on me throughout all these years.

I would like to show all my gratitude to Dr. Alexander Malnič for accepting me as a young researcher under his supervision.

I also would like to thank Dr. Dragan Marušič and Dr. Klavdija Kutnar for their support throughout my studies in the University of Primorska. I would like to thank all the staff in the Faculty of Mathematics, Natural Sciences and Information Technologies and the Andrej Marušič Institute, specially to Monika Marinko, for their help during my stay in Slovenia, to Dr. Daniel Pellicer for encouraging me to enrol in the University of Primorska, to Dr. Boštjan Frelih for the translation to Slovene, to my family and to all my friends for their support, love and friendship.

Contents

Abstract

ON THE ISOMORPHISM PROBLEM OF BI-CAYLEY GRAPHS

In this PhD thesis we study the isomorphism problem of bi-Cayley graphs and the related question of classifying finite BCI-groups. More precisely, the following questions/problems are considered:

(i) Find effective sufficient and necessary conditions for the isomorphism of two cyclic bi-Cayley graphs.

(ii) Which groups are 3-BCI-groups?

(iii) Which cubic bi-Cayley graphs are BCI-graphs?

(iv) Which cyclic balanced configurations have the CI-property?

(v) Analytical enumeration of balanced cyclic configurations.

Problem (i) is solved for tetravalent graphs. Problem (ii) is solved for nilpotent groups. We contribute to Problem (iii) by proving that all connected cubic arc-transitive bi-Cayley graphs over abelian groups are BCI-graphs. Regarding Problem (iv), we prove that all cyclic balanced configurations have the CI-property for which the number of points is either a product of two distinct primes, or a prime power. Regarding Problem (v), we derive a close formula for the number of connected cyclic configurations of type (v_3).

Math. Subj. Class (2010): 20B25, 05C25, 05C60, 51E30.

Key words: graph isomorphism, bi-Cayley graph, BCI-graph, BCI-group, n-BCI-group, arc-transitive graph, cyclic configuration, cyclic object.

Izvleček

O PROBLEMU IZOMORFNOSTI BI-CAYLEYJEVIH GRAFOV

V doktorski disertaciji obravnavamo problem izomorfnosti bi-Cayleyjevih grafov in z njim povezano vprašanje klasifikacije končnih BCI-grup. Obravnavani so naslednji konkretni problemi oz. vprašanja:

(i) Poiskati učinkovite potrebne in zadostne pogoje za izomorfnost dveh cikličnih bi-Cayleyjevih grafov.

(ii) Katere grupe so 3-BCI-grupe?

(iii) Kateri kubični bi-Cayleyjevi grafi so BCI-grafi?

(iv) Katere ciklične uravnotežene konfiguracije imajo CI-lastnost?

(v) Analitično oštevilčenje uravnoteženih cikličnih konfiguracij.

V doktorski disertaciji je Problem (i) rešen za tetravalentne grafe, Problem (ii) pa za nilpotentne grupe. Prispevek k rešitvi Problema (iii) je dokaz, da je vsak povezan kubičen ločno-tranzitiven bi-Cayleyjev graf nad abelsko grupo BCI-graf. Kar se tiče Problema (iv), je v doktorski disertaciji dokazano, da ima CI-lastnost vsaka ciklična uravnotežena konfiguracija, katere število točk je bodisi enako produktu dveh različnih praštevil ali pa je enako potenci nekega praštevila. Za Problem (v) je izpeljana formula za število povezanih cikličnih konfiguracij tipa (v_3).

Math. Subj. Class (2010): 20B25, 05C25, 05C60, 51E30.

Ključne besede: isomorfia grafov, bi-Cayleyjey graf, BCI-graf, BCI-grupa, n-BCI-grupa, ločno tranzitiven graf, ciklična c configuracija, cikličen objekt.

Chapter 1

Introduction

The central objects in this PhD Thesis are the so called *bi-Cayley graphs*. These graphs are natural generalizations of Cayley graphs in the following sense: while the latter graphs can be described as those with a regular subgroup in their automorphism group, the former graphs are those having a semiregular group with two orbits. In this thesis we are interested in the case when each edge has endpoints in different orbits. More formally, for a group G and a subset S of G, the *bi-Cayley graph* $BCay(G, S)$ has vertex set $G \times \{0, 1\}$, and the edges are in the form $(x, 0)(sx, 1)$, where $x \in G$ and $s \in S$. Bi-Cayley graphs have been studied from various aspects, e. g., they have been used for constructions of strongly regular graphs [17, 49] and semisymmetric graphs [21, 60]. In this thesis we focus on their isomorphism problem and the related question of classifying finite BCI-groups. The latter problem is a natural analogue to the well-known problem of classifying finite CI-groups which has attracted considerable attention over the last 45 years and which is still wide open (see, e. g., [20, 53, 54]).

In 2008, motivated by the concepts CI-graph, m-CI-group and CI-group, Xu et al. [77] introduced the concepts BCI-graph, m-BCI-group and BCI-group, respectively. We say that a bi-Cayley graph $\mathrm{BCay}(G, S)$ is a *BCI-graph* if whenever $\mathrm{BCay}(G, S) \cong \mathrm{BCay}(G, T)$ for some subset T of G, the set $T = gS^\sigma$ for some $g \in G$ and automorphism $\sigma \in \mathrm{Aut}(G)$. The group G is an *m-BCI-group* if every bi-Cayley graph over G of valency at most m is a BCI-graph, and G is a *BCI-group* if every bi-Cayley graph over G is a BCI-graph. The theory of BCI-graphs and BCI-groups is less developed as in the case of CI-graphs and CI-groups. Several basic properties have been obtained by Jin and Liu in a series of papers [34, 35, 36, 37], and very recently, by Arezoomand and Taeri [2, 3]. We will review these results in Chapter 3. We also give several examples, and most importantly, discuss in details the relation between BCI-groups and CI-groups. In fact, our primary motivation by studying BCI-graphs and BCI-groups is that these objects can bring new insight into the old problem of classifying CI-groups.

The isomorphism problem for circulant graphs was investigated by many researchers, and finally, a complete solution was given by Muzychuk [64]. In Chapter 4, we consider the same problem in the class of *cyclic bi-Cayley graphs* (i. e., bi-Cayley graphs over cyclic groups). As far as we know, the only result in this direction is due to Wiedemann and Zieve [76], who proved that every cyclic bi-Cayley graph

of valency at most 3 is a BCI-graph. Furthermore, they also gave examples of non-BCI-graphs of valency 4, and thus the tetravalent bi-Cayley graphs represent the first non-trivial case to be considered. In Chapter 4, we solve this case (see Theorem 4.1). Interestingly, the arithmetic conditions that appear in our solution coincide entirely with those in the solution for cubic circulant graphs that can be retrieved from the general algorithm of Muzychuk [64].

In Chapters 5 and 6 we consider cubic BCI-graphs and also 3-BCI-groups. It is a trivial observation that every group is a 1-BCI-group, while the 2-BCI-groups were described in purely group theoretical terms in [77]. In this PhD Thesis we are interested in 3-BCI-groups. The classification of these groups is still an open problem, some partial solutions can be found in [34, 35, 36]. In the theory of CI-groups the counterpart problem is [53, Problem 9.6]. In Chapter 5, we contribute to this problem by classifying the nilpotent 3-BCI-groups (see Theorem 5.1). In Chapter 6, we give further examples of cubic BCI-graphs. Namely, we prove that every connected arc-transitive cubic bi-Cayley graph over an abelian group is a BCI-graph (see Theorem 6.2). In addition to this, we also derive a complete description of these graphs which is of independent interest. This result is comparable with the recent classification of vertex-transitive cubic bi-Cayley graphs over abelian groups obtained by Feng and Zhou [25]. Our interest in connected arc-transitive cubic abelian bi-Cayley graphs came from the classification of connected arc-transitive cubic graphs of girth 6 obtained by Kutnar and Marušič [47]. It turns out that each of the latter graphs has a semiregular abelian automorphism group with two orbits.

In Chapter 7, we change the subject and turn to configurations. A *cyclic configuration* $(P, \mathcal{B})$ consists of a point set P and a line set $\mathcal{B}$, which consists of certain subsets of P, and it is also assumed that a cyclic automorphism group G is regular on P. In this case there is a canonical way to identify P with G, and thus $(P, \mathcal{B})$ can be regarded as a *Cayley-object* of G. Furthermore, if the configuration $(G, \mathcal{B})$ is also *balanced* (i. e., $|G| = |\mathcal{B}|$), then the incidence graph of $(G, \mathcal{B})$ is a bi-Cayley graph over G, and $(G, \mathcal{B})$ has the CI-property exactly when the corresponding bi-Cayley graph is a BCI-graph. Using also this observation, we prove that every balanced cyclic configuration has the CI-property for which the number of points is either a product of two distinct primes, or it is a prime power (see Theorem 7.2). As an application, we also derive a close formula for the number of non-isomorphic connected cyclic configurations of type (v_3) (see Theorem 7.3).

The results presented in this PhD Thesis are from the following articles:

- H. Koike, I.Kovács, Isomorphic tetravalent circulant Haar graphs, *Ars Math. Contemporanea* **7** (2014), 215–235.
- H. Koike, I. Kovács, T. Pisanski, The number of cyclic configurations of type (v_3) and the isomorphism problem, *J. Combin. Designs* **22** (2014), 216–229.
- H. Koike, I. Kovács, Arc-transitive cubic abelian bi-Cayley graphs and BCI-graphs, *Filomat*, in press.
- H. Koike, I. Kovács, A classification of nilpotent 3-BCI groups, submitted.

Chapter 2

Preliminaries

The purpose of this chapter is to familiarize the reader with the concepts, terminology and notation, and to review the results that we shall use in the thesis.

2.1 Groups

In this thesis we will consider finite groups. If it is not specified otherwise we use multiplicative notation for the group operation and denote by 1_G the identity element of a given group G. For group theoretical terms not defined here we refer the reader to [18, 70, 72].

The following list presents the notation and definitions of special classes of groups that will appear throughout the thesis.

- $\mathbb{Z}_n$. The ring of residue classes of integers module n, and parallel, it will denote its additive group, representing the cyclic group of order n. We let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$.
- $\mathbb{Z}_n^*$. The multiplicative group of units of the ring $\mathbb{Z}_n$.
- $\mathrm{AGL}(1, n)$. The group of all permutations of $\mathbb{Z}_n$ of the form $x \mapsto ax + b$, where $a \in \mathbb{Z}_n^*$ and $b \in \mathbb{Z}_n$. These will be also called the affine transformations of $\mathbb{Z}_n$.
- $\mathrm{Dih}(A)$. The generalized dihedral group defined as the semidirect product of the abelian group A with $\mathbb{Z}_2 = \langle \eta \rangle$ where η acts on A as $a^\eta = a^{-1}$ for every $a \in A$.
- D_{2n}. The dihedral group of order $2n$, i. e., the group $Dih(\mathbb{Z}_n)$.
- Q_8. The usual quaternion group given as $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$.
- $\mathrm{GL}(n, F)$. The general linear group, i. e., the group of all $n \times n$ invertible matrices with elements from the field F.
- $\mathrm{SL}(n, F)$. The special linear group, i. e., the group of all $n \times n$ matrices with elements from the field F whose determinants are equal to 1.

- $\mathrm{PGL}(n, F)$ and $\mathrm{PSL}(n, F)$. The projective linear group and projective special linear group, respectively, i. e., the quotients groups of $\mathrm{GL}(n, F)$ and $\mathrm{SL}(n, F)$ by their respective centers.

If F is a finite field with q elements, where q is a prime power, we write $\mathrm{GL}(n, q)$, $\mathrm{SL}(n, q)$, $\mathrm{PGL}(n, q)$ and $\mathrm{PSL}(n, q)$ instead of $\mathrm{GL}(n, F)$, $\mathrm{SL}(n, F)$, $\mathrm{PGL}(n, F)$ and $\mathrm{PSL}(n, F)$.

2.1.1 Nilpotent and solvable groups

A series of subgroups

$$\{1_G\} = G_0 \leq G_1 \leq \cdots \leq G_n = G$$

of a group G is called a *subnormal series* of G if $G_i \trianglelefteq G_{i+1}$ for every $i \in \{0, 1, \ldots, n-1\}$. A subnormal series is called a *normal series* if, in addition, $G_i \trianglelefteq G$ holds for every $i \in \{0, 1, \ldots, n-1\}$. A group G is called *nilpotent* if it has a *central series*, i. e., a normal series $\{1_G\} = G_0 \leq G_1 \leq \cdots \leq G_n = G$, such that G_{i+1}/G_i is contained in the center of G/G_i for every $i \in \{0, 1, \ldots, n-1\}$. There are several group theoretical properties which are equivalent to nilpotency for finite groups. We summarize some of them in the following theorem (cf. [70, Theorem 5.2.4]):

Theorem 2.1. *Let G be a finite group. Then the following properties are equivalent:*

(i) G is nilpotent.

(ii) Every proper subgroup of G is properly contained in its normalizer.

(iii) Every maximal subgroup of G is normal.

(iv) G is the direct product of its Sylow subgroups.

A group G is *solvable* if it has an *abelian series*, by which we mean a subnormal series $1_G = G_0 \leq G_1 \leq \cdots \leq G_n = G$ in which each factor G_{i+1}/G_i is abelian. The following theorem is due to Huppert and Itô (cf. [72, Theorem 13.10.1]):

Theorem 2.2. *If a finite group $G = AB$, where A is nilpotent, and B contains a cyclic subgroup of index 2, then G is solvable.*

2.1.2 Group actions

Let X be a nonempty set. We shall denote by $\mathrm{Sym}(X)$ the group of all permutations of X. In this thesis we let permutations act on the right, i. e., if π and ρ are permutations in $\mathrm{Sym}(X)$, then by their product $\pi\rho$ we apply first π and then ρ. In consistence with this, we denote by x^π the image of $x \in X$ under π.

An *action* of a group G on the set X is a function $X \times G \to X$ which satisfies the following axioms:

- $x^{1_G} = x$ for every $x \in X$, and
- $(x^g)^h = x^{gh}$ for every $x \in X$ and for all $g, h \in G$,

where, for $x \in X$ and $g \in G$, the symbol x^g denotes the image of $(x, g) \in X \times G$ under this function.

For every $g \in G$, the mapping $\pi_g : X \to X$ defined by $x \mapsto x^g$ is a permutation of X. The mapping $\varphi : g \mapsto \pi_g$ defines a homomorphism from G to $\mathrm{Sym}(X)$, this is called *the permutation representation* of G induced by the action. The *kernel* $\mathrm{Ker}(\varphi) = \{g \in G \,|\, x^g = x, x \in X\}$ is also called the kernel of the action, and if this is trivial then the action is called *faithful*.

For an element $x \in X$, we denote by x^G the *orbit* of x under G, and by G_x the *stabilizer* of x in G. The set of all orbits under G, or in other words, the set of all *G-orbits* will be denoted by $\mathrm{Orb}(G, X)$. If the whole set X is a G-orbit, then we say that G is *transitive* on X. We say that G is *semiregular* on X if G_x is trivial for every element $x \in X$, and that G is *regular* on X if it is both transitive and semiregular. The following basic relation holds between orbits and stabilizers (cf. [18, Theorem 1.4A]):

Lemma 2.3. (The Orbit Stabilizer Property) *Let G be a finite group acting on a finite set X and let $x \in X$. Then $|G| = |x^G| \cdot |G_x|$.*

For $g \in G$, we define

$$\mathrm{fix}(g) = \{x \in X \,|\, x^g = x\}.$$

The next lemma essentially says that number $|\mathrm{Orb}(G, X)|$ of orbits is equal to the the average number of points fixed by elements of G (cf. [18, Theorem 1.7A]):

Lemma 2.4. (The Orbit Counting Lemma) *Let G be a finite group acting on a finite set X. Then*

$$|\mathrm{Orb}(G, X)| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{fix}(g)|.$$

Let $\Delta \subseteq X$ and define $\Delta^g = \{x^g \,|\, x \in \Delta\}$. Suppose that G is transitive on X. A nonempty subset Δ of X is called a *block* if for each $g \in G$, either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$. It follows from the definition that the whole set X and the singletons $\{x\}$, $x \in X$, are blocks, these are called *trivial* blocks and any other block is called *nontrivial*. We say that G is *primitive* if it has no nontrivial blocks, otherwise it is *imprimitive*. If Δ is a block for G, then the set $\delta = \{\Delta^g \,|\, g \in G\}$ is a partition of the set X. This partition is called the *system of blocks* induced by Δ. The following theorem is a special case of [18, Theorem 1.5A]:

Theorem 2.5. *Let G be a group which acts transitively on a set X, $x \in X$, and $H \leq G$ be a subgroup for which $G_x \leq H$. Then the orbit x^H is a block for G.*

Let G be a group acting on a set X and let Δ be a subset of X. Then the *pointwise stabilizer* of Δ in G is:

$$G_\Delta = \{g \in G \,|\, x^g = x, x \in \Delta\},$$

and the *setwise stabilizer* of Δ in G is:

$$G_{\{\Delta\}} = \{g \in G \,|\, \Delta^g = \Delta\}.$$

We say that Δ is *G-invariant* if $\Delta^g = \Delta$ for every $g \in G$. Clearly, Δ is G-invariant if and only if it is an union of G-orbits. In this case we can consider the *restriction of the action* to Δ, and denote by G^Δ the image of the latter restriction (note that, $G^\Delta \leq \mathrm{Sym}(\Delta)$). Two permutation groups $G \leq \mathrm{Sym}(X)$ and $H \leq \mathrm{Sym}(Y)$ are called *permutation isomorphic* if there exist a bijection $\lambda : X \to Y$ and a group isomorphism $\phi : G \to H$ such that:

$$\lambda(x^g) = \lambda(x)^{\phi(g)} \text{ for all } x \in X \text{ and } g \in G.$$

The next theorem is [18, Theorem 1.6A]:

Theorem 2.6. *Let G be a group acting transitively on a set X, and let N be a normal subgroup of G.*

(i) The N-orbits form a system of blocks for G.

(ii) If Δ and Δ' are two N-orbits, then the permutation groups N^Δ and $N^{\Delta'}$ are permutation isomorphic.

(iii) If any point of X is fixed by all elements of N, then N lies in the kernel of the action.

(iv) The group N has at most $|G : N|$ orbits. If the index $|G : N|$ is finite, then the number of N-orbits divides $|G : N|$.

(v) If G is primitive on X then either N is transitive, or it lies in the kernel of the action.

2.1.3 The holomorph

The *right regular representation* of G is the permutation representations ρ of G induced by its action on itself by multiplying from the right, i. e., $g^\rho : x \mapsto xg$ for all $g, x \in G$. The image of ρ will be denoted by G_{right}. The *left regular representation* of G is the permutation representations λ of G induced by its action on itself defined by $g^\lambda : x \mapsto g^{-1}x$ for all $g, x \in G$. The image of λ will be denoted by G_{left}.

Now, the product $g^\lambda g^\rho$ maps an element x in G to the conjugate $g^{-1}xg$, so $g^\lambda g^\rho$ is equal to the inner automorphism of G induced by g. Consequently,

$$\langle\, G_{\mathrm{left}}, \mathrm{Aut}(G) \,\rangle = \langle\, G_{\mathrm{right}}, \mathrm{Aut}(G) \,\rangle.$$

This group is called the *holomorph* of G, and it is denoted by $\mathrm{Hol}(G)$. Moreover, if $\alpha \in \mathrm{Aut}(G)$ and $g \in G$, then $\alpha^{-1} g^\rho \alpha$ maps an element x of G to $(x^{\alpha^{-1}} g)^\alpha = xg^\alpha$. Consequently, $\alpha^{-1} g^\rho \alpha = (g^\alpha)^\rho$, and thus $G_{\mathrm{right}} \lhd \mathrm{Hol}(G)$. Since the group G_{right} is regular, $G_{\mathrm{right}} \cap \mathrm{Aut}(G)$ is trivial, and we can write $\mathrm{Hol}(G)$ as the semidirect product

$$\mathrm{Hol}(G) = G_{\mathrm{right}} \rtimes \mathrm{Aut}(G).$$

Notice that, the holomorph $\mathrm{Hol}(\mathbb{Z}_n)$ coincides with the group $\mathrm{AGL}(1, n)$ defined in page 7.

2.2 Graphs

In this thesis every graph will be finite and simple. For graph theoretical terms not defined below we refer the reader to [27].

2.2.1 Action of groups on graphs

For a graph Γ, we denote by $V(\Gamma)$, $E(\Gamma)$, $A(\Gamma)$ and $\mathrm{Aut}(\Gamma)$ its vertex set, edge set, arc set and full automorphism group, respectively. An edge $\{u, v\} \in E(\Gamma)$ will be also written as uv, and the ordered pairs (u, v) and (v, u) will be called the *arcs* of Γ induced by the edge uv. For a vertex $v \in V(\Gamma)$, we let $N_\Gamma(v)$ denote the set of all vertices adjacent to v. In what follows we also use the terms *cubic* and *tetravalent*, respectively, for a regular graph of valency 3 and 4, respectively.

We say that Γ is *vertex-transitive*, *edge-transitive* and *arc-transitive*, respectively, if $\mathrm{Aut}(\Gamma)$ acts transitively on the vertex set $V(\Gamma)$, edge set $E(\Gamma)$ and arc set $A(\Gamma)$, respectively. A *k-arc* of a graph Γ is a sequence of $k+1$ vertices, such that any two consecutive vertices are adjacent, and with any repeated vertices being more than 2 steps apart. More formally, it is an ordered $(k+1)$-tuple $(v_0, v_1, \ldots, v_k)$ of vertices of Γ such that, for every $i \in \{1, \ldots, k\}$, v_{i-1} is adjacent to v_i, and for every $i \in \{1, \ldots, k-1\}$, $v_{i-1} \neq v_{i+1}$. Let $G \leq \mathrm{Aut}(\Gamma)$. Then the graph Γ is called *(G, k)-arc-transitive* (*(G, k)-arc-regular*) if G is transitive (regular) on the set of k-arcs of Γ. If $G = \mathrm{Aut}(\Gamma)$, then a (G, k)-arc-transitive ((G, k)-arc-regular) graph is simply called *k-transitive* (*k-regular*).

2.2.2 Connected arc-transitive cubic graphs

In this subsection we review some results on connected arc-transitive cubic graphs. Perhaps the most important among these was proved by Tutte in 1947:

Theorem 2.7 (Tutte [74])**.** *Every connected arc-transitive cubic graph is k-regular for some $k \leq 5$.*

In this thesis we will occasionally need information about connected arc-transitive cubic graphs of small order. For this purpose we use the catalogue [14, Table] due to Conder and Dobcsányi which contains all such graphs of order up to 768 (let us remark that, this has completed and extended the earlier list of these graphs up to 512 vertices which was compiled by Foster [26]). For an update of the catalogue [14, Table], we refer to the homepage of Marston Conder [13]. Following [14], we denote by FnA, $FnB, \ldots$, etc. the connected arc-transitive cubic graphs on n points, and simply write Fn if the graph is uniquely determined by n.

We will use the following description of connected arc-transitive cubic graphs of girth 6:

Theorem 2.8. *Let Γ be a connected arc-transitive cubic graph of girth 6. Then one of the following holds:*

(i) Γ is 1-regular, and $\mathrm{Aut}(\Gamma)$ contains a regular normal subgroup isomorphic to the generalized dihedral group $\mathrm{Dih}(L)$, where $L \cong \mathbb{Z}_{rm} \times \mathbb{Z}_m$, $r = 3^s p_1^{e_1} \cdots p_t^{e_t}$, $r > 3$ and $r \geq 11$ if $m = 1$, $s \in \{0, 1\}$, and every $p_i \equiv 1 (\mathrm{mod}\ 3)$.

(ii) Γ *is* 2*-regular, and* $\Gamma \cong GP(8,3)$, *or* $\mathrm{Aut}(\Gamma)$ *contains a regular normal subgroup isomorphic to the generalized dihedral group* $\mathrm{Dih}(L)$, *where* $L \cong \mathbb{Z}_{rm} \times \mathbb{Z}_m$, $r \in \{1,3\}$, $m > 1$, *and if* $r = 1$, *then* $m \neq 3$.

(iii) Γ *is* 3*-regular, and* $\Gamma \cong F18$ *(the Pappus graph) or* $GP(10,3)$ *(the Desargues graph).*

(iv) Γ *is* 4*-regular, and* $\Gamma \cong F14$ *(the Heawood graph).*

In fact, part (i) is deduced from [47, Theorem 1.2], part (ii) from [47, Theorem 1.1], and parts (iii)-(iv) from [24, Corollary 6.3] (see also [15, Theorem 2.3]).

2.2.3 Normal quotients, covers and voltage graphs

Let Γ be an arbitrary graph and $G \leq \mathrm{Aut}(\Gamma)$ which is transitive on $V(\Gamma)$. For a normal subgroup $N \triangleleft G$ which is not transitive on $V(\Gamma)$, the *normal quotient* Γ_N is the graph whose vertices are the N-orbits on $V(\Gamma)$, and two N-orbits Δ_1 and Δ_2 are adjacent if and only if there exist vertices $v_1 \in \Delta_1$ and $v_2 \in \Delta_2$ such that v_1 is adjacent to v_2 in Γ.

Example 2.9. Let Γ be the graph on 15 vertices shown on Fig. 2.1.

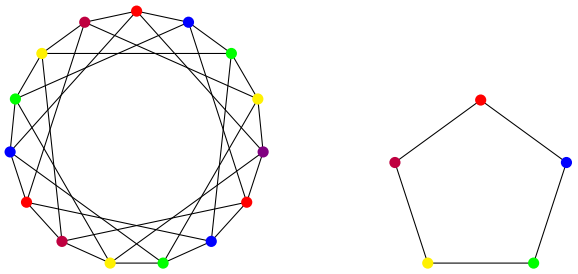

Figure 2.1: The graph Γ (left) and its normal quotient Γ_N (right).

It is easily seen that Γ has an automorphism group $G \cong \mathbb{Z}_{15}$ which is regular on $V(\Gamma)$. Now, take N to be the subgroup of G of order $|N| = 3$. Then $N \triangleleft G$, and the normal quotient Γ_N is isomorphic to the 5-cycle (see Fig. 2.1, where each colour represents one N-orbit on $V(\Gamma)$). □

Let Γ be a finite simple graph and K be a finite group whose identity element is denoted by 1_K. For an arc $x = (w, w') \in A(\Gamma)$ we set $x^{-1} = (w', w)$. A *K-voltage assignment* of Γ is a mapping $\zeta : A(\Gamma) \to K$ with the property that $\zeta(x^{-1}) = \zeta(x)^{-1}$ for every $x \in A(\Gamma)$. The values of ζ are called *voltages* and K is called the *voltage group*. Voltages are naturally extended to a directed walk $\vec{W} = (w_1, \ldots, w_n)$ by letting $\zeta(\vec{W}) = \prod_{i=1}^{n-1} \zeta((w_i, w_{i+1}))$. Fix a spanning tree T of Γ. Then every edge not in $E(T)$ together with the edges in $E(T)$ span a unique circuit of Γ, and we shall refer to the circuits obtained in this manner as the *base circuits of* Γ *relative to* T. The K-voltage assignment ζ is called *T-reduced* if $\zeta(x) = 1_K$ whenever x is an arc belonging to $A(T)$.

The *voltage graph* $\Gamma \times_\zeta K$ is defined to have vertex set $V(\Gamma) \times K$, and edge set

$$E(\Gamma \times_\zeta K) = \Big\{(w,k)(w',\zeta(x)k) \mid x = (w,w') \in A(\Gamma) \text{ and } k \in K\Big\}. \tag{2.1}$$

The voltage group K induces an automorphism group of $\Gamma \times_\zeta K$ through the action defined by

$$(w,l)^k = (w,lk),\ w \in V(\Gamma) \text{ and } k,l \in K.$$

We denote $\hat{k}$ the permutation of $V(\Gamma)$ induced by k with respect to the above action, and let $\widehat{K} = \{\hat{k} : k \in K\}$. Let $g \in \mathrm{Aut}(\Gamma \times_\zeta K)$ such that it normalizes $\widehat{K}$. This implies that, if $(w,k) \in V(\Gamma \times_\zeta K)$ and $(w,k)^g = (w',k')$, then w' does not depend on the choice of $k \in K$, and the mapping $w \mapsto w'$ is a well-defined permutation of $V(\Gamma)$. The latter permutation is called the *projection* of g which belongs to $\mathrm{Aut}(\Gamma)$. On the other hand, we say that an automorphism of $\mathrm{Aut}(\Gamma)$ *lifts* to an automorphism $h \in \mathrm{Aut}(\Gamma \times_\zeta K)$ if it is equal to the projection of h. The following "Lifting Lemma" is a special case of [59, Theorem 4.2]:

Theorem 2.10 (Malnič [59]). *Let $\Gamma \times_\zeta K$ be a connected voltage graph, where K is an abelian group, and ζ is a T-reduced K-voltage assignment. Then $\sigma \in \mathrm{Aut}(\Gamma)$ lifts to an automorphism of $\Gamma \times_\zeta K$ if and only if there exists some $\sigma_* \in \mathrm{Aut}(K)$ such that for every directed base circuit $\vec{C}$ relative to T, $\sigma_*(\zeta(\vec{C})) = \zeta(\vec{C}^\sigma)$.*

For more information on voltage graphs the reader is referred to [28, 59].

2.2.4 Cayley graphs and the CI-property

Let G be a group and $S \subseteq G \setminus \{1_G\}$. The *Cayley graph* $\mathrm{Cay}(G,S)$ is the graph whose vertex set is G and arc set is $\{(x,sx) \mid x \in G, s \in S\}$. Observe that, if $S = S^{-1}$, then $\mathrm{Cay}(G,S)$ is in fact an undirected graph. By definition, $\mathrm{Cay}(G,S)$ has out-valency $|S|$, and it is connected if and only if $\langle S\rangle = G$, i. e., S generates G. In general, $\mathrm{Cay}(\langle S\rangle, S)$ is a connected component of $\mathrm{Cay}(G,S)$, and $\mathrm{Cay}(G,S)$ is isomorphic to the union of $|G : \langle S\rangle|$ disjoint copies of $\mathrm{Cay}(\langle S\rangle, S)$. For every Cayley graph $\mathrm{Cay}(G,S)$, the group G_{right} (see Subsection 2.1.3) acts as an automorphism group of the graph, implying that $\mathrm{Cay}(G,S)$ is vertex-transitive. In fact, Sabidussi [71] characterized Cayley graphs over a group G as those (di)graphs whose automorphism groups contain a regular subgroup isomorphic to G.

A fundamental problem about Cayley graphs is the so called *isomorphism problem,* that is, given two Cayley graphs $\mathrm{Cay}(G,S)$ and $\mathrm{Cay}(H,T)$ determine whether or not $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(H,T)$. It follows quickly from the definition that for any automorphism $\alpha \in \mathrm{Aut}(G)$, the graphs $\mathrm{Cay}(G,S)$ and $\mathrm{Cay}(G,S^\alpha)$ are isomorphic, namely, α induces an isomorphism between these graphs. Such an isomorphism is also called a *Cayley isomorphism.* In 1967, Ádám [1] conjectured that two Cayley graphs over the cyclic group $\mathbb{Z}_n$ are isomorphic if and only if there is a Cayley isomorphism which maps one to the other. Soon afterwards, Elpas and Turner [22] found the counterexample shown in Fig. 2.2. The graphs $\mathrm{Cay}(\mathbb{Z}_8, \{1,2,5\})$ and $\mathrm{Cay}(\mathbb{Z}_8, \{1,6,5\})$ are isomorphic but there is no Cayley isomorphism between them.

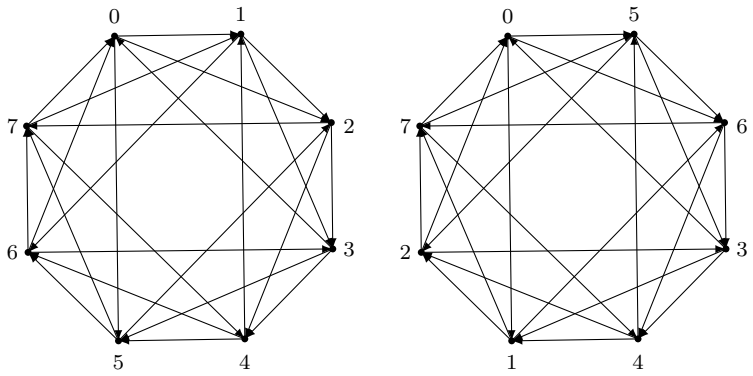

Figure 2.2: The Cayley graphs $\mathrm{Cay}(\mathbb{Z}_8, \{1,2,5\})$ and $\mathrm{Cay}(\mathbb{Z}_8, \{1,6,5\})$.

This also motivated the following definition. A Cayley graph $\mathrm{Cay}(G,S)$ has the *CI-property* (for short, it is a *CI-graph*) if for any Cayley graph $\mathrm{Cay}(G,T)$, $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$ implies that $T = S^\alpha$ for some $\alpha \in \mathrm{Aut}(G)$. A group G is called a *DCI-group* if every Cayley graph over G is a CI-graph, and it is called a *CI-group* if every undirected Cayley graph over G is a CI-graph. Finite DCI-groups and CI-groups have attracted considerable attention over the last 45 years. In [61, 62], Muzychuk gave a complete classification of cyclic CI-groups and DCI-groups.

Theorem 2.11 (Muzychuk [61, 62])**.**

(i) A cyclic group of order n is a DCI-group if and only if $n = k$, $2k$ or $4k$ where k is an odd square-free number.

(ii) A cyclic group of order n is a CI-group if and only if either $n \in \{8, 9, 18\}$ or $n = k$, $2k$ or $4k$ where k is an odd square-free number.

The best list of possible DCI-groups has been derived from the works of Li et al. [56, 57]. Before we recall this list, we need one more definition. Let M be an abelian group of odd order for which all Sylow subgroups are elementary abelian, and let $n \in \{2,3,4,8\}$ be such that $\gcd(|M|, n) = 1$. Now, let

$$E(M,n) = E \rtimes \langle z \rangle \tag{2.2}$$

such that z is of order n, and if n is even then z inverts all elements of M, that is, $x^z = x^{-1}$ for all $x \in M$; while if $n = 3$ then $x^z = x^l$ for all $x \in M$, where l is an integer satisfying $l^3 \equiv 1 (\mathrm{mod}\ \exp(M))$ and $\gcd(l(l-1), \exp(M)) = 1$.

Theorem 2.12 (Li, Praeger and Xu [53])**.** *If G is a DCI-group, then all Sylow subgroups of G are elementary abelian or isomorphic to $\mathbb{Z}_4$ or Q_8. Moreover, $G = U \times V$, where $\gcd(|U|, |V|) = 1$, U is abelian, and $V = 1, Q_8, A_4, E(M,2)$ or $E(M,4)$.*

The best list of CI-groups is due to Li et al. [54]. It should be mentioned that their proof was incomplete, but this was corrected recently by Dobson et al. [20]:

Theorem 2.13 (Li, Lu, Pálfy [54])**.** *Let G be a CI-group.*

(a) If G does not contain elements of order 8 or 9, then $G = H_1 \times H_2 \times H_3$, where the orders of H_1, H_2 and H_3 are pairwise coprime, and

(i) H_1 is an abelian group, and each Sylow subgroup of H_1 is elementary abelian or $\mathbb{Z}_4$;

(ii) H_2 is one of the groups $1, E(M,2), E(M,4)$ or Q_8;

(iii) H_3 is one of the groups $1, E(M,3)$ or A_4.

(b) If G contains elements of order 8, then $G \cong E(M,8)$ or $\mathbb{Z}_8$.

(c) If G contains elements of order 9, then G is one of the groups $\mathbb{Z}_9 \rtimes \mathbb{Z}_2, \mathbb{Z}_9 \rtimes \mathbb{Z}_4, \mathbb{Z}_2^2 \rtimes \mathbb{Z}_9$ or $\mathbb{Z}_9 \times \mathbb{Z}_2^n$ with $n \leq 5$.

However, the problem of determining whether or not a given group in the theorems above is really a DCI- or CI-group is difficult. For several results in these directions we refer the reader to the survey [53].

2.3 Cayley objects and the CI-property

In [5], Babai extended the CI-property of graphs to the CI-property of arbitrary relational structures (in fact, he used the language of categories). Given a finite set X, we define $\mathrm{Rel}(X)$ to be the set of all relations on X, and by a *relational structure* on X we simply mean an arbitrary subset $\mathcal{R} \subset \mathrm{Rel}(X)$. It should be mentioned that this definition includes such classical combinatorial objects as graphs, block-designs, configurations and codes.

The symmetric group $\mathrm{Sym}(X)$ acts naturally on the set $\mathrm{Rel}(X)$, namely, given a k-ary relation ρ and $g \in \mathrm{Sym}(X)$ we set

$$\rho^g = \{(x_1^g, \ldots, x_k^g) \mid (x_1, \ldots, x_k) \in \rho\}.$$

For any $g \in \mathrm{Sym}(X)$ and $\mathcal{R} \subset \mathrm{Rel}(X)$, we set $\mathcal{R}^g = \{\rho^g \mid \rho \in \mathcal{R}\}$. Two relational structures $\mathcal{R}$ and $\mathcal{S}$ are *isomorphic* if there exists $g \in \mathrm{Sym}(X)$ such that $\mathcal{R}^g = \mathcal{S}$. The *automorphism group* of $\mathcal{R}$, denoted by $\mathrm{Aut}(\mathcal{R})$, consists of all isomorphisms from $\mathcal{R}$ to itself. A relational structure with point set being equal to a group G is called a *Cayley object* of G, if $\mathrm{Aut}(\mathcal{R})$ contains G_{right}. In particular, it is called *cyclic* if G is a cyclic group.

Now, the *isomorphism problem for Cayley objects* reads as follows: given two Cayley objects $\mathcal{R}$ and $\mathcal{S}$, how do we check whether they are isomorphic or not? Let $\mathcal{K}$ be a class of Cayley objects of G, and let $X \in \mathcal{K}$. Following [5], we say that X has the *CI-property* (for short X is a *CI-object*) for G in the class $\mathcal{K}$ if, given any Cayley object $Y \in \mathcal{K}$, the isomorphism $X \cong Y$ implies that there exists some automorphism of G which maps X to Y. The group G is a *CI-group with respect to* $\mathcal{K}$ if every Cayley object of G in $\mathcal{K}$ has the CI-property. This generalizes the concept of a DCI- and CI-groups introduced in the previous section. In this context G is a DCI-group is equivalent to saying that it is a CI-group with respect to digraphs. Probably, the first result about CI-property of combinatorial objects is due to Bays [7] and Lambossy [48], who proved that the cyclic group $\mathbb{Z}_p$, p is a prime number,

has the CI-property with respect to Steiner triple systems. Babai [5] generalized the Bays-Lambossy Theorem to any class of Cayley objects:

Theorem 2.14 (Babai [5]). *$\mathbb{Z}_p$ is a CI-group with respect to any class of Cayley objects.*

In fact, this follows directly from the following lemma, which is typically the starting point when one studies CI-graphs:

Lemma 2.15 (Babai [5]). *The following are equivalent for every Cayley object X of G:*

(i) X is a CI-object.

(ii) Given a permutation $\pi \in \mathrm{Sym}(G)$ such that $\pi^{-1}G_{\mathrm{right}}\pi \leq \mathrm{Aut}(X)$, G_{right} and $\pi^{-1}G_{\mathrm{right}}\pi$ are conjugate in $\mathrm{Aut}(X)$.

The strongest result was obtained by Pálfy [65]. Let φ denote Euler's totient function.

Theorem 2.16 (Pálfy [65]). *A finite group G has the CI-property with respect to all relational structures if and only if $G \cong \mathbb{Z}_n$ with $\gcd(n, \varphi(n)) = 1$, or $|G| = 4$.*

In Chapter 7, we will consider the CI-property of cyclic groups with respect to balanced configurations. In particular, we will be interested in the special case when the number of points is either a product of two distinct primes or a prime power. We will make use of the results of Huffman [31] about isomorphic cyclic combinatorial objects on pq points, where p, q are distinct primes. In order to recall these results it is necessary to set a few definitions.

Let $\mathrm{Obj}(\mathbb{Z}_n)$ denote the set of all cyclic objects of the group $\mathbb{Z}_n$. Given a class $\mathcal{K}$ of cyclic objects in $\mathrm{Obj}(\mathbb{Z}_n)$, a *solving set* for $\mathcal{K}$ is a set Δ of permutations of $\mathbb{Z}_n$ satisfying the following property (see [63]):

$$(\forall X \in \mathcal{K})\ (\forall Y \in \mathrm{Obj}(\mathbb{Z}_n)\ (X \cong Y \iff X^\sigma = Y \text{ for some } \sigma \in \Delta).$$

Let p and q be distinct primes. In fact, for every cyclic object $X \in \mathrm{Obj}(\mathbb{Z}_{pq})$, a solving set for X was determined by Huffman [31]. For $j \in \mathbb{Z}_{pq}^*$, let μ_j be the permutation $\mu_j : x \mapsto jx$. For $i \in \{0, 1, ..., q-1\}$, define the permutation τ_i by

$$\tau_i : x \mapsto \begin{cases} x+q & \text{if } x \equiv i (\mathrm{mod}\ q) \\ x & \text{otherwise,} \end{cases}$$

and if in addition $j \in \mathbb{Z}_{pq}^*$ with $j \equiv 1 (\mathrm{mod}\ q)$, then define the permutation $\mu_{i,j}$ by

$$\mu_{i,j} : x \mapsto \begin{cases} jx & \text{if } x \equiv i (\mathrm{mod}\ q) \\ x & \text{otherwise.} \end{cases}$$

For the next two theorems suppose in addition that q divides $p-1$. Furthermore, fix an element $a \in \mathbb{Z}_{pq}^*$ of order $p-1$ for which $a \equiv 1 (\mathrm{mod}\ q)$, and put $b = a^{(p-1)/q}$. The next result is [31, Theorem 1.1]:

Theorem 2.17 (Huffman [31]). *Let $n = pq$, where p and q are primes such that q divides $p-1$, and let $X \in \mathrm{Obj}(\mathbb{Z}_n)$ such that $\mu_b \notin \mathrm{Aut}(X)$, where b is defined above. Then $\mathbb{Z}_n^*$ is a solving set for X.*

The powers $a, a^2, .., a^p$ are pairwise distinct modulo p. Let α be the positive integer in $\{1, 2, ..., p\}$ such that $a^\alpha \equiv -s (\mathrm{mod}\, p)$, where $s = (p-1)/q$. For $i \in \{0, 1, ..., q-1\}$, define $\nu_i = \prod_{j=0}^{q-1} \mu_{j, a^\alpha b^{-ij}}$. Notice that, $\nu_0 = \mu_{a^\alpha}$. The next theorem is [31, Theorem 1.2] which, for our convenience, is formulated slightly differently.

Theorem 2.18 (Huffman [31]). *Let $n = pq$, where p and q are primes such that q divides $p-1$, and let $X \in \mathrm{Obj}(\mathbb{Z}_n)$ such that $\mu_b \in \mathrm{Aut}(X)$ and $\tau_0 \notin \mathrm{Aut}(X)$, where b is defined above. Let β be the smallest positive integer such that $\mu_a^\beta \in \mathrm{Aut}(X)$. Then X admits a solving set Δ in the form:*

$$\Delta = \Big\{ \mu_a^i \, \nu_k \, \mu_j^{-1} \;\mid\; 0 \le i < \beta,\; 0 < j, k \le q-1,\; \prod_{l=0}^{q-1} \tau_l^{b^{(l+1)k}} \in \mathrm{Aut}(X) \Big\}. \qquad (2.3)$$

Remark 2.19. Theorems 2.16, 2.17 and 2.18 imply that every cyclic object in $\mathrm{Obj}(\mathbb{Z}_n)$ admits a solving set whose size is at most $\varphi(n)$ if $n = pq$. The same result was obtained by Huffman et al. [32] in the case when $n = p^2$, and finally, this was proved by Muzychuk [63] to be the case for any number n.

Chapter 3

BCI-graphs and BCI-groups

In this chapter we introduce the main concepts of the thesis: bi-Cayley graphs, BCI-graphs and BCI-groups.

A finite, simple and undirected graph Γ is called a *bi-Cayley graph* over a group G if it has a semiregular automorphism group, isomorphic to G, which has two orbits in the vertex set. Given such Γ, there exist subsets R, L, S of G such that $R^{-1} = R$, $L^{-1} = L$, $1_G \notin R \cup L$, and $\Gamma \cong \mathrm{BCay}(G, R, L, S)$, where the latter graph is defined to have vertex set $G \times \{0, 1\}$, the *right part* $G \times \{0\} = \{(g, 0) \mid g \in G\}$ and the *left part* $G \times \{1\} = \{(g, 1) \mid g \in G\}$; and the edge set consists of three sets:

$\{(x, 0)(y, 0) \mid yx^{-1} \in R\}$ (*right edges*),

$\{(x, 1)(y, 1) \mid yx^{-1} \in L\}$ (*left edges*),

$\{(x, 0)(y, 1) \mid yx^{-1} \in S\}$ (*spoke edges*).

In what follows we will also refer to $\mathrm{BCay}(G, R, L, S)$ as a *bi-Cayley representation* of Γ. As an example, we mention the well-known class of *generalized Petersen graphs* introduced by Coxeter [16], the name was given by Watkins [75]. These are the same as the bi-Cayley graphs $\mathrm{BCay}(\mathbb{Z}_n, \{1, -1\}, \{k, -k\}, \{0\})$, commonly denoted by $GP(n, k)$. Fig. 3.1 shows the graph $GP(12, 5)$ also known as the *Nauru graph*.

Bi-Cayley graphs are natural generalizations of Cayley graphs, they have attracted considerable attention in the last two decades. Unfortunately, the term "bi-Cayley" is not commonly accepted, they are also known as *semi-Cayley graphs* [17, 49], 2-*Cayley graphs* [4], referring to the two orbits of the semiregular group G, and *Haar graphs* [30] in the case when G is abelian and $L = R = \emptyset$. In this thesis we are interested exclusively in bi-Cayley graphs having only spoke edges. Formally, these are the graphs $\mathrm{BCay}(G, R, L, S)$ for which $L = R = \emptyset$. From now on we use the simplified notation $\mathrm{BCay}(G, S)$ for the graph $\mathrm{BCay}(G, \emptyset, \emptyset, S)$.

3.1 BCI-graphs

Let $\mathrm{BCay}(G, S)$ be a bi-Cayley graph of G, $\sigma \in \mathrm{Aut}(G)$ and $g \in G$. The graphs $\mathrm{BCay}(G, S)$ and $\mathrm{BCay}(G, gS^\sigma)$ are isomorphic, which can be easily checked by using

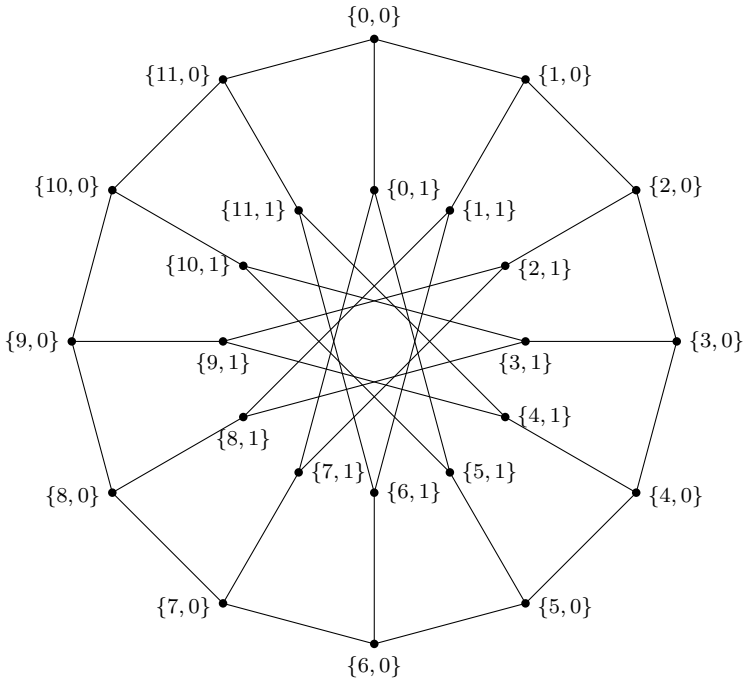

Figure 3.1: The generalized Petersen graph $GP(12,5)$.

the mapping $\varphi : G \times \{0,1\} \to G \times \{0,1\}$ defined by

$$(x,i)^\varphi = \begin{cases} (x^\sigma, 0) & \text{if } i = 0 \\ (gx^\sigma, 1) & \text{if } i = 1. \end{cases}$$

Clearly, φ is a bijection. Furthermore,

$$\begin{aligned} (x,0)(y,1) \in E(\mathrm{BCay}(G,S)) &\iff yx^{-1} \in S \\ &\iff gy^\sigma (x^\sigma)^{-1} \in gS^\sigma \\ &\iff (x,0)^\varphi (y,1)^\varphi \in E(\mathrm{BCay}(G, gS^\sigma)), \end{aligned}$$

hence it is also an isomorphism from $\mathrm{BCay}(G,S)$ to $\mathrm{BCay}(G,gS^\sigma)$. This isomorphism is called a *bi-Cayley isomorphism*. However, it is not always true that whenever two bi-Cayley graphs are isomorphic, there is a bi-Cayley isomorphism which maps one to the other.

Example 3.1. It is easy to see, by simply looking at their picture in Fig. 3.2, that the graphs $\mathrm{BCay}(\mathbb{Z}_8, \{0,1,2,5\})$ and $\mathrm{BCay}(\mathbb{Z}_8, \{0,1,6,5\})$ are isomorphic.

On the other hand, on can directly check that there are no $a \in \mathbb{Z}_8^*$ and $b \in \mathbb{Z}_8$ for which the mapping $x \mapsto ax + b$ maps the set $\{0,1,2,5\}$ to the set $\{0,1,6,5\}$. Therefore, $\mathrm{BCay}(\mathbb{Z}_8, \{0,1,2,5\})$ is not a BCI-graph. □

This motivates the following definitions which were first introduced by Xu et al. [77].

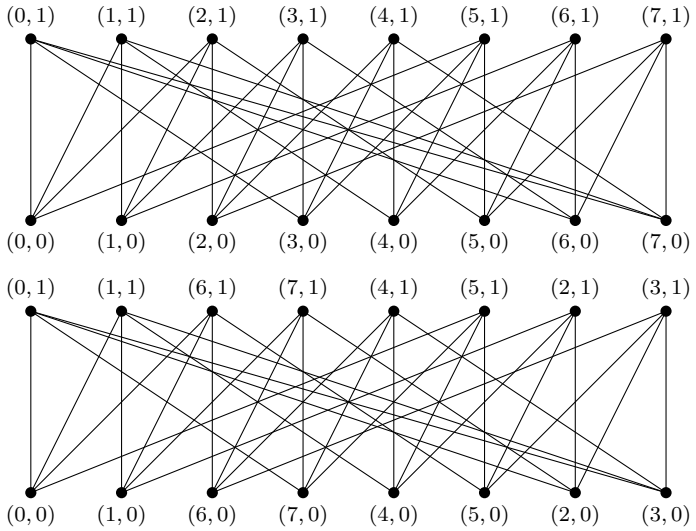

Figure 3.2: BCay($\mathbb{Z}_8, \{0,1,2,5\}$) (top) and BCay($\mathbb{Z}_8, \{0,1,6,5\}$) (bottom).

Definition 3.2.

1. A bi-Cayley graph BCay(G,S) is called a *BCI-graph* if for any BCay(G,T), BCay$(G,T) \cong$ BCay(G,S) implies that $T = gS^\sigma$ for some $g \in G$ and $\sigma \in \mathrm{Aut}(G)$.

2. A finite group G is called an *m-BCI-group* if every bi-Cayley graph over G of degree at most m is a BCI-graph, and it is called a *BCI-group* if it is an $|G|$-BCI-group.

The following simple lemma is useful for constructions of non-BCI-graphs:

Lemma 3.3. *If* BCay(G,S) *is a BCI-graph, then there exist* $g \in G$ *and* $\sigma \in \mathrm{Aut}(G)$ *which satisfy* $S^{-1} = gS^\sigma$.

Proof. In view of Definition 3.2, it is enough to prove that BCay(G,S) is isomorphic to BCay(G,S^{-1}). Define the mapping $\varphi : G \times \{0,1\} \to G \times \{0,1\}$ by $(x,0) \mapsto (x,1)$ and $(x,1) \mapsto (x,0), x \in G$. Now, $(x,0)(y,1) \in E(\mathrm{BCay}(G,S))$ if and only if $yx^{-1} \in S$, and this happens exactly when $xy^{-1} \in S^{-1}$, or equivalently, $(x,0)^\varphi(y,1)^\varphi \in E(\mathrm{BCay}(G,S^{-1}))$. □

We remark that, Lemma 3.3 can be applied only to non-abelian groups. Namely, if G is abelian, then for every subset S of G, the condition $S^{-1} = gS^\sigma$ holds by choosing $g = 1_G$ and σ to be the isomorphism $\sigma : x \mapsto x^{-1}, x \in G$. As an illustration of Lemma 3.3, we show below that there is no the dihedral BCI-group of order larger than 12.

Proposition 3.4. *The dihedral group* D_{2n} *is not a BCI-group if* $n > 6$.

Proof. Let $n > 4$, $G = D_{2n} = \langle a, b \mid a^n = b^2 = 1, bab = a^{-1} \rangle$ and let $S = \{1, a, a^3, b, ab, a^2b, a^4b\}$. Suppose that the graph BCay(G,S) is a BCI-graph. By

Lemma 3.3, there is $\sigma \in \mathrm{Aut}(D_{2n})$ and $g = a^i b^j \in D_{2n}$, where $i \in \mathbb{Z}_n$ and $j \in \{0,1\}$, such that $a^i b^j S^\sigma = S^{-1}$. Recall that $\mathrm{Aut}(D_{2n}) = \{\sigma_{s,t} : s \in \mathbb{Z}_n^*, t \in \mathbb{Z}_n\}$ where

$$(a^k b^m)^{\sigma_{s,t}} = \begin{cases} a^{ks} & if \quad m = 0 \\ a^{ks+t}b & if \quad m = 1. \end{cases}$$

Notice that $j = 0$ because the set S contains 4 involutions from $D_{2n} \setminus \langle a \rangle$ and 3 elements of $\langle a \rangle$. Then $a^i\{1, a, a^3, b, ab, a^2b, a^4b\}^{\sigma_{s,t}} = \{1, a^{-1}, a^{-3}, b, ab, a^2b, a^4b\}$. Thus

$$\begin{aligned} \{a^i, a^{s+i}, a^{3s+i}\} &= \{1, a^{-1}, a^{-3}\} \\ \{a^{i+t}b, a^{i+s+t}b, a^{i+2s+t}b, a^{i+4s+t}b\} &= \{b, ab, a^2b, a^4b\}. \end{aligned}$$

An exhaustive case-by-case analysis gives that these only hold when $n = 5$, $i = 0$, $s = -1$ and $t = 1$, or $n = 6, i = 0, s = -1$ and $t = 2$. □

3.2 A Babai-type lemma

For a group G and an element $g \in G$, let $R(g)$ be the permutation of $G \times \{0,1\}$ defined by

$$(x,i)^{R(g)} = (xg, i) \text{ for every } x \in G \text{ and } i \in \{0,1\}.$$

We set $R(G) = \{R(g) : g \in G\}$. Obviously, $R(G) \leq \mathrm{Aut}(\mathrm{BCay}(G,S))$ for every bi-Cayley graph $\mathrm{BCay}(G,S)$. The group $R(G)$ is semiregular with orbits $G \times \{0\}$ and $G \times \{1\}$. In what follows we will denote by $\mathcal{S}(\mathrm{Aut}(\mathrm{BCay}(G,S)))$ the set of all semiregular subgroups of $\mathrm{Aut}(\mathrm{BCay}(G,S))$ whose orbits are $G \times \{0\}$ and $G \times \{1\}$.

In the following lemma we characterize the BCI-graphs by group theoretical terms in the same way as the CI-objects are characterized in Lemma 2.15. The proof below is from our paper [41]. It should be mentioned that this result was also derived by Arezoomand and Taeri in [2, Theorem C].

Lemma 3.5. *The following are equivalent for every bi-Cayley graph* $\Gamma = \mathrm{BCay}(G, S)$.

(i) $\mathrm{BCay}(G,S)$ *is a BCI-graph.*

(ii) The normalizer $N_{\mathrm{Aut}(\Gamma)}(R(G))$ *is transitive on* $V(\Gamma)$, *and every two subgroups in* $\mathcal{S}(\mathrm{Aut}(\Gamma))$, *isomorphic to* G, *are conjugate in* $\mathrm{Aut}(\Gamma)$.

Proof. In order to simplify notation, we will write below $(G,0)$ for $G \times \{0\}$ and $(G,1)$ for $G \times \{1\}$.

We start with the part $(i) \Rightarrow (ii)$. Let $X \in \mathcal{S}(\mathrm{Aut}(\Gamma))$ such that $X \cong G$. We have to show that X and $R(G)$ are conjugate in $\mathrm{Aut}(\Gamma)$. Let $i \in \{0,1\}$, and set $X^{(G,i)}$ and $R(G)^{(G,i)}$ for the permutation groups of the set (G,i) induced by X and $R(G)$ respectively. The groups $X^{(G,i)}$ and $R(G)^{(G,i)}$ are conjugate in $\mathrm{Sym}((G,i))$, because these are isomorphic and regular on (G,i). Thus X and $R(G)$ are conjugate by a permutation $\phi \in \mathrm{Sym}(G \times \{0,1\})$ such that $(G,0)$ is ϕ-invariant. We write $X = \phi R(G) \phi^{-1}$. Consider the graph Γ^ϕ, the image of Γ under ϕ. Then $R(G) = \phi^{-1} X \phi \leq$

$\mathrm{Aut}(\Gamma^\phi)$. Using this and that $(G,0)$ is ϕ-invariant, we obtain that $\Gamma^\phi = \mathrm{BCay}(G,T)$ for some subset $T \subseteq G$. Then $\Gamma \cong \mathrm{BCay}(G,T)$, and by (i), $T = gS^\alpha$ for some $g \in G$ and $\alpha \in \mathrm{Aut}(G)$. Define the permutation σ of $G \times \{0,1\}$ by

$$(x,i)^\sigma = \begin{cases} (x^\alpha, 0) & \text{if } i = 0 \\ (gx^\alpha, 1) & \text{if } i = 1. \end{cases}$$

Then,

$$(x,i)^{\sigma^{-1}R(h)\sigma} = \begin{cases} ((x^{\alpha^{-1}}h)^\alpha, 0) = (xh^\alpha, 0) = (x,0)^{R(h^\alpha)} \\ ((g^{-1}x)^{\alpha^{-1}}h), 1)^\sigma = (g((g^{-1}x)^{\alpha^{-1}}h)^\alpha, 1) = (x,1)^{R(h^\alpha)}. \end{cases}$$

This shows that $\sigma^{-1}R(h)\sigma = R(h^\alpha)$ if $h \in G$. Thus σ normalizes $R(G)$. The vertex $(x,0)$ of $\mathrm{BCay}(G,S)$ has neighbourhood $(Sx,1)$. This is mapped by σ to the the set $(gS^\alpha x^\alpha, 1) = (Tx^\alpha, 1)$. This proves that σ is an isomorphism from Γ to Γ^ϕ, and in turn it follows that, $\Gamma^\phi = \Gamma^\sigma$, $\phi\sigma^{-1} \in \mathrm{Aut}(\Gamma)$, and thus $\phi = \rho\sigma$ for some $\rho \in \mathrm{Aut}(\Gamma)$. Finally, $X = \phi R(G)\phi^{-1} = \rho\sigma R(G)\sigma^{-1}\rho^{-1} = \rho R(G)\rho^{-1}$, i. e., X and $R(G)$ are conjugate in $\mathrm{Aut}(\Gamma)$.

In order to prove that the normalizer $N_{\mathrm{Aut}(\Gamma)}(R(G))$ is transitive on $V(\Gamma)$, it is sufficient to find some automorphism η which switches $(G,0)$ and $(G,1)$ and normalizes $R(G)$. Observe that $\mathrm{BCay}(G,S) \cong \mathrm{BCay}(G,S^{-1})$, where $S^{-1} = \{s^{-1} : s \in S\}$. Then by (i), $S^{-1} = gS^\alpha$ for some $g \in G$ and $\alpha \in \mathrm{Aut}(G)$. We claim that the permutation of $G \times \{0,1\}$ defined below is an appropriate choice for such an η:

$$(x,i)^\eta = \begin{cases} (x^\alpha, 1) & \text{if } i = 0 \\ (gx^\alpha, 0) & \text{if } i = 1. \end{cases}$$

Clearly, η is a bijection from $G \times \{0,1\}$ to itself. Let $\{(x,0),(sx,1)\}$ be an edge of Γ and suppose that $x^\alpha = y \in G$. $\{(x,0),(sx,1)\}^\eta = \{(x,0)^\eta,(sx,1)^\eta\} = \{(x^\alpha,1),(g(sx)^\alpha,0)\}$. Since $S^{-1} = gS^\alpha$, $gs^\alpha = s' \in S^{-1}$, and $\{(x,0),(sx,1)\}^\eta = \{(y,1),(s'y,0)\}$ is an edge of Γ. In the other hand, suppose that $\{(x,0),(sx,1)\}^\eta = \{(y,0),(s'y,1)\}$ for some x, y, $s \in G$ and $s' \in S$. This implies that $x^\alpha = s'y$ and $gs^\alpha x^\alpha = y$. Then $gs^\alpha = (s')^{-1}$, $s^\alpha \in g^{-1}S^{-1} = S^\alpha$, and so $s \in S$. Therefore, η is an automorphism of Γ. Now, for $R(h) \in R(G)$,

$$(x,0)^{\eta^{-1}R(h)\eta} = ((g^{-1}x)^{\alpha^{-1}}h, 1)^\eta = (g((g^{-1}x)^{\alpha^{-1}}h)^\alpha, 0) = (x,0)^{R(h^\alpha)},$$

while

$$(x,1)^{\eta^{-1}R(h)\eta} = (x^{\alpha^{-1}}h, 0)^\eta = (xh^\alpha, 1) = (x,1)^{R(h^\alpha)}.$$

This proves that η normalizes $R(G)$.

We turn to the part $(ii) \Rightarrow (i)$. Let $\Gamma' = \mathrm{BCay}(G,T)$ such that $\Gamma' \cong \Gamma$. We have to show that $T = gS^\alpha$ for some $g \in G$ and $\alpha \in \mathrm{Aut}(G)$.

We claim the existence of an isomorphism $\phi : \Gamma \to \Gamma'$ for which $\phi : (1_G,0) \mapsto (1_G,0)$ and $(G,0)$ is ϕ-invariant (here ϕ is viewed as a permutation of $G \times \{0,1\}$). We construct ϕ in a few steps. To start with, choose an arbitrary isomorphism $\phi_1 : \Gamma \to \Gamma'$. Since the normalizer $N_{\mathrm{Aut}(\Gamma)}(R(G))$ is transitive on $V(\Gamma)$, there exists

$\rho \in N_{\mathrm{Aut}(\Gamma)}(R(G))$ which maps $(1_G, 0)$ to $(1_G, 0)^{\phi_1^{-1}}$. Let $\phi_2 = \rho\phi_1$. Then ϕ_2 is an isomorphism from Γ to Γ', and also $\phi_2 : (1_G, 0) \mapsto (1_G, 0)$. The connected component of Γ containing the vertex $(1_G, 0)$ is equal to the induced subgraph $\Gamma[(H, 0) \cup (sH, 1)]$, where $s \in S$ and $H \leq G$ is generated by the set $s^{-1}S$. It can be easily checked that

$$\Gamma[(H, 0) \cup (sH, 1)] \cong \mathrm{BCay}(H, s^{-1}S).$$

Similarly, the connected component of Γ' containing the vertex $(1_G, 0)$ is equal to the induced subgraph $\Gamma'[(K, 0) \cup (tK, 1)]$, where $t \in T$ and $K \leq G$ is generated by the set $t^{-1}T$, and

$$\Gamma'[(K, 0) \cup (tK, 1)] \cong \mathrm{BCay}(K, t^{-1}T).$$

Since ϕ_2 fixes $(1_G, 0)$, it induces an isomorphism from $\Gamma[(H, 0) \cup (sH, 1)]$ to $\Gamma[(K, 0) \cup (tK, 1)]$; denote this isomorphism by ϕ_3. It follows from the connectedness of these induced subgraphs that ϕ_3 preserves their bipartition classes, moreover, ϕ_3 maps $(H, 0)$ to $(K, 0)$, since it fixes $(1_G, 0)$. Finally, take $\phi : \Gamma \to \Gamma'$ to be the isomorphism whose restriction to each component of Γ equals ϕ_3. It is clear that $\phi : (1_G, 0) \mapsto (1_G, 0)$ and $(G, 0)$ is ϕ-invariant.

Since $R(G) \leq \mathrm{Aut}(\Gamma')$, $\phi R(G)\phi^{-1} \leq \mathrm{Aut}(\Gamma)$. The orbit of $(1_G, 0)$ under $\phi R(G)\phi^{-1}$ is equal to $(G, 0)^{\phi^{-1}} = (G, 0)$, and hence $\phi R(G)\phi^{-1} \in \mathcal{S}(\mathrm{Aut}(\Gamma))$. By (ii), $\phi R(G)\phi^{-1} = \sigma^{-1}R(G)\sigma$ for some $\sigma \in \mathrm{Aut}(\Gamma)$. Since $N_{\mathrm{Aut}(\Gamma)}(R(G))$ is transitive on $V(\Gamma)$, σ can be chosen so that $\sigma : (1_G, 0) \mapsto (1_G, 0)$. To sum up, we have an isomorphism $(\sigma\phi) : \Gamma \mapsto \Gamma'$ which fixes $(1_G, 0)$ and also normalizes $R(G)$. Thus $(\sigma\phi)$ maps $(G, 1)$ to itself. Consider the permutation group $\langle R(G), \sigma\phi\rangle^{(G,1)}$ of $(G, 1)$ obtained by restricting the group $\langle R(G), \sigma\phi\rangle$ to $(G, 1)$. It follows that this is permutation isomorphic to the holomorph $\mathrm{Hol}(G)$ (see [18, Exercise 2.5.6]). Therefore, there exist $g \in G$ and $\alpha \in \mathrm{Aut}(G)$ such that $(\sigma\phi) : (x, 1) \mapsto (gx^\alpha, 1)$ for all $x \in G$. The isomorphism $\sigma\phi$ fixes $(1_G, 0)$ and it maps the neighbourhood $N_\Gamma((1_G, 0)$ to the neighbourhood $N_{\Gamma'}((1_G, 0)$, i. e., $(T, 1) = (S, 1)^{\sigma\phi} = (gS^\alpha, 1)$, from which $T = gS^\alpha$. This completes the proof of the theorem. □

Let us remark that the condition on the normalizer $N_{\mathrm{Aut}(\Gamma)}(R(G))$ cannot be omitted from Lemma 3.5(ii). To see this we give the following example.

Example 3.6. We consider the bi-Cayley graph $\Gamma = \mathrm{BCay}(G, S)$, where

$$G = \langle a, b \,|\, a^5 = b^4 = 1,\ b^{-1}ab = a^2\rangle \text{ and } S = \{1, a, b\}.$$

The group G is the unique Frobenius group of order 20, and we find by the help of the computer package Magma [11] that Γ is arc-transitive (see Appendix A.2). In fact, Γ is the unique arc-transitive cubic graph on 40 points (see [14]). We also compute that any two subgroups in $\mathcal{S}(\mathrm{Aut}(\Gamma))$, isomorphic to G, are conjugate in $\mathrm{Aut}(\Gamma)$. However, we show below that $S^\alpha \neq gS^{-1}$ for any $g \in G$ and $\alpha \in \mathrm{Aut}(G)$, hence by Lemma 3.3, Γ is not a BCI-graph.

To the contrary assume that $S^\alpha = gS^{-1}$ for some $g \in G$ and $\alpha \in \mathrm{Aut}(G)$. It follows at once that $g \in S$. As no element in $bS^{-1} = \{b, ba^{-1}, 1\}$ is of order 5, $g \neq b$. Since every automorphism of G is inner, α equals to the conjugation by some element $c \in G$. Let $g = 1$. Then $S^\alpha = gS^{-1} = S^{-1}$, hence $a^c = a^\alpha = a^{-1}$ and $b^c = b^\alpha = b^{-1}$.

From the first equality $c \in C_G(a)b^2 = \langle a \rangle b^2$. Thus $c = a^i b^2$ for some $i \in \{0, \ldots, 4\}$. Plugging this in the second equality, we get $b^2 a^{-i} b a^i b^2 = b^{-1}$, hence $a^{3i} b = b^{-1}$, which is impossible. Finally, let $g = a$. Then $S^\alpha = gS^{-1} = aS^{-1}$, hence $a^c = a^\alpha = a$ and $b^c = b^\alpha = ab^{-1}$. The first equality gives that $c = a^i$ for some $i \in \{0, \ldots, 4\}$. Plugging this in the second equality, we get $a^{-i} b a^i = ab^{-1}$, hence $a^{2i} b = ab^{-1}$, which is again impossible. □

3.3 m-BCI- and BCI-groups

The study of m-BCI-groups was initiated in [77]. In this paper the authors considered the 1-BCI- and the 2-BCI-groups and derived some basic properties of BCI-graphs. Clearly, for every group G and any two elements a and $b \in G$, the bi-Cayley graphs $\mathrm{BCay}(G, \{a\})$ and $\mathrm{BCay}(G, \{b\})$ are isomorphic, since the edge set of both graphs consists of a perfect matching. In the other hand, we have that $ga = b$, where $g = ba^{-1}$. Therefore, every group is a 1-BCI-group.

It turns out that the class of finite 2-BCI-groups coincides with the class of finite groups in which any two elements of the same order are either fused or inverse-fused. The formal definition is given below.

Definition 3.7. A group G is called a *FIF-group* if for any two elements a and b of the same order there is an automorphism σ of G such that $a^\sigma = b$ or $a^\sigma = b^{-1}$.

Theorem 3.8. *A finite group G is a 2-BCI-group if and only if G is a FIF-group.*

Proof. Suppose first that G is a 2-BCI-group. Let $a, b \in G$ be of the same order, say m. Consider the graphs $\mathrm{BCay}(G, \{1, a\})$ and $\mathrm{BCay}(G, \{1, b\})$ (here 1 denotes the identity element of G). It is easily seen that both graphs are isomorphic to $|G|/m$ disjoint copies of the the cycle of length $2m$. Now, since G is a 2-BCI-group, there is an automorphism σ of G and an element $g \in G$ such that $g\{1, a\}^\sigma = \{1, b\}$. Thus $ga^\sigma = b$ or $ga^\sigma = 1$. In the first case, we have that $g = 1$ and $a^\sigma = b$. For the second case, $g = b$ and $a^\sigma = b^{-1}$. Therefore, G is a FIF-group.

Now, suppose that G is a FIF-group. Consider the isomorphic graphs $\mathrm{BCay}(G, S)$ and $\mathrm{BCay}(G, T)$ such that $|S| = |T| = 2$. Let us write $S = \{s_1, s_2\}$ and $T = \{t_1, t_2\}$. It is not hard to show that the isomorphism of the graphs implies that the elements $s_1^{-1} s_2$ and $t_1^{-1} t_2$ are of the same order in G. Since G is a FIF-group, $(s_1^{-1} s_2)^\sigma = t_1^{-1} t_2$ or $(s_1^{-1} s_2)^\sigma = t_2^{-1} t_1$ holds for some automorphism σ of G. Put $g = t_1 (s_1^\sigma)^{-1}$ in the first case and $g = t_2 (s_1^\sigma)^{-1}$ in the second case. Then in the first case

$$gS^\sigma = t_1 \{1, s_1^{-1} s_2\}^\sigma = t_1 \{1, t_1^{-1} t_2\} = T,$$

and in the second case

$$gS^\sigma = t_2 \{1, s_1^{-1} s_2\}^\sigma = t_2 \{1, t_2^{-1} t_1\} = T.$$

Therefore, the group G is a 2-BCI-group. □

The FIF-groups play an analogous rule in the theory of BCI-groups as the *F-groups* in the theory of DCI-groups. By an F-group we mean a group in which any

two elements of the same order are fused, i.e., one can be mapped to the other by some group automorphism. In [55], Li and Praeger studied the finite FIF-groups in details. As the main result, they have derived a relatively short list containing all possible finite FIF-groups. Here we do not recall this list in full details, only the description given in [55, Corollary 1.3]. For this result we need to introduce some further definitions.

A finite group is called *homocyclic* if it is direct product of cyclic groups of the same order. Let $k \geq 2$ be an integer and let $\mathcal{G}(k)$ denote the class of non-abelian 2-groups G such that

- $Z(G) = G' = \Phi(G) = \mathbb{Z}_2^k$, and $Z(G) \setminus \{1\}$ consists of all involutions of G;
- G/G' is of order 2^k or 2^{2k}.

Theorem 3.9 (Li and Praeger [55]). *If G is a finite FIF-group then one of the following holds:*

(i) If G is a nonabelian simple group then G is one of the following groups: $\mathrm{PSL}(2,q)$ *where* $q \in \{5,7,8,9\}$, $\mathrm{PSL}(3,4)$, *the Suzuki group* $\mathrm{Sz}(8)$, *and the Mathieu groups* M_{11} *and* M_{23}.

(ii) If G is nilpotent then each Sylow p-subgroup of G is either homocyclic, Q_8, or a member of $\mathcal{G}(k)$ for some $k \geq 2$.

(iii) If G is solvable then $G = A \rtimes B$ with $\gcd(|A|,|B|) = 1$ *where A is a nilpotent FIF-group and every Sylow subgroups is cyclic or Q_8.*

(iv) If G is not solvable then $G = A \times B$ where A and B have coprime orders, A is a solvable FIF-group and B is either one of the simple groups in (i), or $\mathrm{SL}(2,q)$ *for $q \in \{5,7,9\}$, or $(C \times \mathrm{Sz}(8)) \rtimes \mathbb{Z}_{3^s m}$, where $m, s \geq 1$ and C is an abelian group.*

The problem of deciding which groups in the above classes (i)-(iv) are really FIF-groups is still open (see [55, Problem 1.5]).

Now, we turn to m-BCI-groups for $m \geq 3$. The concepts of an m-BCI- and BCI-group are relatively new (2007), and thus there are not so many results have been proved about these groups. Wiedemann and Zieve [76] proved that every cyclic group $\mathbb{Z}_n$ is a 3-BCI-group. The particular case when $n = pq$, p and q are different odd primes, was done by Xu et al. [77], and the case when $n = 2p$, p is a prime, was done by Jin and Liu [34]. Also, Jin and Liu proved that every finite p-group is a $(p-1)$-BCI-group. The Sylow p-subgroups of the 3-BCI-groups were considered in two papers of Jin and Liu [35, 36]. They showed that a Sylow 2-subgroup of such a group is either cyclic, or elementary abelian, or Q_8; and a Sylow p-subgroup for an odd prime p is homocyclic. As one of my PhD projects I have proved that the converse of these statements are also true for nilpotent group; i. e., whenever a group is a direct product of the aforementioned groups, then it is a 3-BCI-group. This result is presented in Chapter 5. As for non-solvable groups, Jin and Liu [35] proved the following theorem:

Theorem 3.10 (Jin and Liu [35]). *The alternating group A_5 is the only finite non-abelian simple 3-BCI-group.*

This theorem was obtained after an analysis of the simple groups listed in Theorem 3.9(i). In their latest paper [37] on BCI-groups, Jin and Liu have determined the BCI-groups of order up to 8. These are the following groups:

$$\mathbb{Z}_n, n \leq 7,\ \mathbb{Z}_2^2,\ \mathbb{Z}_2^3, \text{ and } D_6.$$

In the end of this section we mention two very recent results of Arezoomand and Taeri:

Theorem 3.11 (Arezoomand and Taeri [3]). *Let G be a BCI-group and H be a characteristic subgroup of G. Then G/H is a BCI-group.*

Theorem 3.12 (Arezoomand and Taeri [3]). *Every finite BCI-group is solvable.*

Both properties hold also for CI-groups. The CI-group analogue of Theorem 3.11 was proved by Babai and Frankl [6]; while the CI-group analogue of Theorem 3.12 is due to Li [50]. It is worth to mention that Dobson and Morris [19] proved that every quotient of a CI-group is also a CI-group. The question arises naturally whether this property is also shared by BCI-groups.

3.4 BCI-groups versus CI-groups

In this section we compare the class of BCI-groups with the class of CI-groups.

Example 3.1 shows that $\mathbb{Z}_8$ is not a BCI-group, while it is a CI-group, see Theorem 2.11(ii). At present we do not know any BCI-group which is not a CI-group. Moreover, Arezoomand and Taeri [3] stated the following conjecture:

Conjecture 3.13. *Every BCI-group is a CI-group.*

A possible way to settle the conjecture would be to construct non-BCI-graphs from known non-CI-graphs. In this direction we have the following proposition.

Proposition 3.14. *Suppose that $\Gamma = \mathrm{BCay}(\mathbb{Z}_n, S)$ is a connected bi-Cayley graph such that for some $a \in \mathbb{Z}_n$, $\mathrm{Aut}(\Gamma)_{(0,0)} = \mathrm{Aut}(\Gamma)_{(a,1)}$. Then the following are equivalent.*

(i) $\mathrm{BCay}(\mathbb{Z}_n, S)$ *is a BCI-graph.*

(ii) $\mathrm{Cay}(\mathbb{Z}_n, (S-a)\setminus\{0\})$ *is a CI-graph, where $S - a = \{s - a \mid s \in S\}$.*

Proof. For sake of simplicity we put $A = \mathrm{Aut}(\Gamma)$ and $A^+ = A_{\{\mathbb{Z}_n \times \{0\}\}}$, i. e., the setwise stabilizer of $\mathbb{Z}_n \times \{0\}$ in A. Obviously, $X \leq A^+$ for every group $X \in \mathcal{S}(A)$. Observe that, the permutation d of $\mathbb{Z}_n \rtimes \{0,1\}$, defined by $d : (x,i) \mapsto (-x, 1-i)$ where $i \in \{0,1\}$, is an automorphism of Γ. Moreover, $A = \langle A^+, d\rangle$, and d normalizes $R(\mathbb{Z}_n)$. It follows that the conjugacy class of subgroups of A containing $R(\mathbb{Z}_n)$ is equal to the conjugacy class of subgroups of A^+ containing $R(\mathbb{Z}_n)$. This also shows that the normalizer of $R(\mathbb{Z}_n)$ is transitive on the vertex set. Using these and

Lemma 3.5, we obtain that $\mathrm{BCay}(\mathbb{Z}_n, S)$ is a BCI-graph if and only if every group in $\mathcal{S}(A)$ is conjugate to $R(\mathbb{Z}_n)$ in A^+.

Let $W = \{(0,0),(a,1)\}$ and consider the setwise stabilizer $A_{\{W\}}$. Since $A_{(0,0)} = A_{(a,1)}$, $A_{(0,0)} \leq A_{\{W\}}$. By Theorem 2.5, the orbit of $(0,0)$ under $A_{\{W\}}$ is a block for A. Denote this block by Δ and the induced system of blocks by δ (i. e., $\delta = \{\Delta^g \mid g \in A\}$). Denote by c the generator of $R(\mathbb{Z}_n)$ acting as

$$c : (x,i) \mapsto (x+1,i),\ x \in \mathbb{Z}_n, i \in \{0,1\}.$$

Consider the element $g = dc^a$ from A. We see that g switches $(0,0)$ and $(a,1)$, hence $A_{\{W\}} = A_{(0,0)}\langle g\rangle$. Therefore, $\Delta = (0,0)^{A_{\{W\}}} = (0,0)^{A_{0,0)}\langle g\rangle} = (0,0)^{\langle g\rangle} = W$, and so

$$\delta = \big\{\ \{(x,0),(x+a,1)\} \mid x \in \mathbb{Z}_n\ \big\}.$$

Define the mapping $\varphi : \delta \to \mathbb{Z}_n$ by $\varphi : \{(x,0),(x+a,1)\} \mapsto x$, $x \in \mathbb{Z}_n$. Now, an action of A on $\mathbb{Z}_n$ can be defined by letting $g \in A$ act as

$$x^g = x^{\varphi^{-1} g \varphi},\ x \in \mathbb{Z}_n.$$

For $g \in A$ we write $\bar{g}$ for the image of g under the corresponding permutation representation, and for a subgroup $X \leq A$ we let $\bar{X} = \{\bar{x} \mid x \in X\}$. In this action of A the subgroup $A^+ < A$ is faithful. Also notice that, a subgroup $X \leq A^+$ is in $\mathcal{S}(A)$ if and only if $\bar{X}$ is a regular cyclic subgroup of $\bar{A^+}$. In particular, for the group $R(\mathbb{Z}_n)$, $R(\bar{\mathbb{Z}}_n) = (\mathbb{Z}_n)_{\mathrm{right}}$ ($(\mathbb{Z}_n)_{\mathrm{right}}$ is the group generated by the translation $x \mapsto x+1$, $x \in \mathbb{Z}_n$).

Pick $g \in A^+$ and $(x, x+s-a) \in \mathbb{Z}_n \times \mathbb{Z}_n$, where $s \in S$ such that $s \neq a$. Then g maps the arc $((x,0),(x+s,1))$ to an arc $((y,0),(y+r,1))$ for some $y \in \mathbb{Z}_n$ and $r \in S$. Since δ is a system of blocks for A^+, g maps $(x+s-a,0)$ to $(y+r-a,0)$, and so $\bar{g}$ maps the pair $(x, x+s-a)$ to the pair $(y, y+r-a)$. We have just proved that $\bar{g}$ leaves the set $\big\{\ (x, x+s-a) \mid x \in \mathbb{Z}_n, s \in S\setminus\{a\}\ \big\}$ setwise fixed. As the latter set is the arc set of the Cayley graph $\mathrm{Cay}(\mathbb{Z}_n, (S-a)\setminus\{0\})$, $\bar{A^+} \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_n, (S-a)\setminus\{0\}))$. For an automorphism h of $\mathrm{Cay}(\mathbb{Z}_n, (S-a)\setminus\{0\})$, define the permutation g of $\mathbb{Z}_n \times \{0,1\}$ by

$$g : (x,i) \mapsto \begin{cases} (x^h, 0) & \text{if } i = 0 \\ ((x-a)^h + a, 1) & \text{if } i = 1, \end{cases} \qquad x \in \mathbb{Z}_n,\ i \in \{0,1\}.$$

The reader is invited to check that the above permutation g is an automorphism of Γ. It is clear that $g \in A^+$ and $\bar{g} = h$; we conclude that $\bar{A^+} = \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_n, (S-a)\setminus\{0\}))$.

Now, the proposition follows along the following equivalences:

(i) $\iff$ Every group in $\mathcal{S}(A)$, isomorphic to $\mathbb{Z}_n$, is conjugate to $R(\mathbb{Z}_n)$ in A^+.

$\iff$ Every regular cyclic subgroup of $\bar{A^+}$ is conjugate to $R(\bar{\mathbb{Z}}_n)$ in $\bar{A^+}$.

$\iff$ (ii).

The last equivalence is Lemma 2.15. $\square$

In order to apply Proposition 3.14, one requires the condition $\mathrm{Aut}(\Gamma)_{(0,0)} = \mathrm{Aut}(\Gamma)_{(a,1)}$, which is not easy to check in general. In fact, this condition is equivalent to saying that setwise stabilizer $\mathrm{Aut}(\Gamma)_{\{\mathbb{Z}_n\times\{0\}\}}$ acts equivalently on the right part $\mathbb{Z}_n \times \{0\}$ and the left part $\mathbb{Z}_n \times \{1\}$. Unfortunately, this is not always the case. A well-known example comes from finite geometry.

Example 3.15. Let $\mathrm{PG}(d, q)$ the *projective space* of dimension d over the finite field with q elements. The incidence graph Γ of the space is the bipartite graph whose colour classes are identified by the set of points and the set of hyperplanes, and the edges are defined by the incidences between the points and the hyperplanes. It is well-known that $\mathrm{PG}(d, q)$ admits a cyclic group of automorphisms which acts regularly on both the points and the hyperplanes (called a *Singer subgroup*). This also means that Γ is isomorphic to a bi-Cayley graph over the cyclic group $\mathbb{Z}_n$, where $n = \frac{q^{d+1}-1}{q-1}$. The automorphism group $\mathrm{Aut}(\Gamma) = \mathrm{P\Gamma L}(d+1, q) \rtimes \mathbb{Z}_2$; its colour preserving subgroup is $\mathrm{P\Gamma L}(d + 1, q)$, the full group of automorphisms of $\mathrm{PG}(d, 2)$. The actions of the latter group on the set points and hyperplanes, respectively, are inequivalent. □

Let $\mathrm{BCay}(\mathbb{Z}_n, S)$ be an arbitrary bi-Cayley graph. In the above proof we defined the permutation d of $\mathbb{Z}_n \rtimes \{0, 1\}$ as

$$d((x, i)) = (-x, 1 - i).$$

It is not hard to check that d is an automorphism of $\mathrm{BCay}(\mathbb{Z}_n, S)$, and that the group $\langle R(\mathbb{Z}_n), d\rangle$ is isomorphic to the dihedral group D_{2n}. Therefore, $\mathrm{BCay}(G, S)$ is isomorphic to a Cayley graph over D_{2n}. Moreover, if as a Cayley graph over $\langle R(\mathbb{Z}_n), d\rangle$, the graph $\mathrm{BCay}(G, S)$ is a CI-graph, then it is a BCI-graph. To deduce this implication one only needs to observe that the automorphisms of the dihedral group $\langle R(\mathbb{Z}_n), d\rangle$ act on $\mathbb{Z}_n \times \{0, 1\}$ as follows

$$(x, 0) \mapsto (ax, 0) \text{ and } (x, 1) \mapsto (ax + b, 1),\ x \in \mathbb{Z}_n,$$

where $a \in \mathbb{Z}_n^*$ and $b \in \mathbb{Z}_n$. This argument implies the following proposition.

Proposition 3.16. *If D_{2n} is a CI-group, then $\mathbb{Z}_n$ is a BCI-group.*

We finish our comparison of BCI-groups and CI-groups by an example showing that the converse of the above Proposition 3.16 does not hold. In other words, the problem of classifying dihedral CI-groups is not equivalent to the problem of classifying cyclic BCI-groups.

Example 3.17. Let $\Gamma = \mathrm{BCay}(\mathbb{Z}_{10}, \{0,1,3,4\})$, see Fig. 3.3.

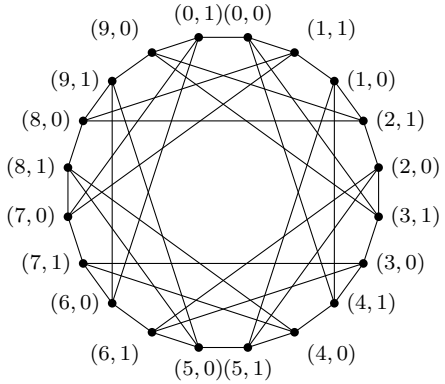

Figure 3.3: The bi-Cayley graph $\mathrm{BCay}(\mathbb{Z}_{10}, \{0,1,3,4\})$.

It follows that Γ is isomorphic to two Cayley graphs over the dihedral group D_{20} see Fig. 3.4, where D_{20} is given by the presentation $\langle a, b \mid a^{10} = b^2 = 1, bab = a^{-1} \rangle$.

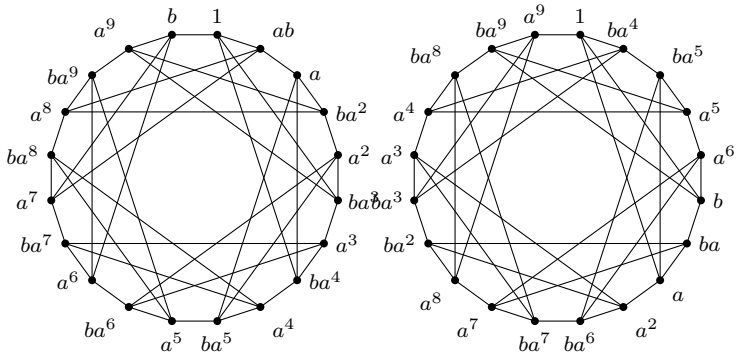

Figure 3.4: The graphs $\mathrm{Cay}(D_{20}, \{b, ba, ba^3, ba^4\})$ and $\mathrm{Cay}(D_{20}, \{a, a^9, b, ba^4\})$.

.

Is is easy too see that there is no $\sigma \in \mathrm{Aut}(D_{20})$ such that $\{b, ba, ba^3, ba^4\}^\sigma = \{a, a^9, b, ba^4\}$, and therefore, D_{20} is not a CI-group. On the other hand, we checked by the help of MAGMA that $\mathbb{Z}_{10}$ is a BCI-group. □

Chapter 4

Isomorphic tetravalent cyclic bi-Cayley graphs

By a *cyclic bi-Cayley graph* we simply mean a bi-Cayley graph over a cyclic group. In this chapter we consider the isomorphism problem for cyclic bi-Cayley graphs, i. e., given two such graphs, find effective sufficient and necessary conditions for their isomorphism.

Wiedemann and Zieve [76] proved that $\mathbb{Z}_n$ is a 3-BCI-group, and so the isomorphism can be tested by bi-Cayley isomorphisms if the valency is at most 3. Also, we have seen in Example 3.1 that $\mathbb{Z}_n$ is not a 4-BCI-group, hence bi-Cayley isomorphisms are not enough for tetravalent graphs in general (tetravalent means that the graph is of valency 4). In this chapter we deal with the tetravalent graphs by proving the following theorem:

Theorem 4.1. *Two connected bi-Cayley graphs* $\mathrm{BCay}(\mathbb{Z}_n, S)$ *and* $\mathrm{BCay}(\mathbb{Z}_n, T)$ *with* $|S| = |T| = 4$ *are isomorphic if and only if there exist* $a_1, a_2 \in \mathbb{Z}_n^*$ *and* $b_1, b_2 \in \mathbb{Z}_n$ *such that*

(i) $a_1 S + b_1 = T$; *or*

(ii) $a_1 S + b_1 = \{0, u, v, v+m\}$ *and* $a_2 T + b_2 = \{0, u+m, v, v+m\}$, *where* $n = 2m$, $\mathbb{Z}_n = \langle u, v \rangle$, $2 \mid u$, $2u \mid m$.

It is worth to compare Theorem 4.1 with the solution of the isomorphism problem for cubic circulant digraphs (i. e., Cayley graphs over cyclic groups). It follows that similar conditions can be derived from Muzychuk's general algorithm presented in [64]:

Theorem 4.2. *Two connected Cayley graphs* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *with* $|S| = |T| = 3$ *are isomorphic if and only if there exist* $a_1, a_2 \in \mathbb{Z}_n^*$ *such that*

(i) $a_1 S = T$; *or*

(ii) $a_1 S = \{u, v, v+m\}$ *and* $a_2 T = \{u+m, v, v+m\}$, *where* $n = 2m$, $\mathbb{Z}_n = \langle u, v \rangle$, $2 \mid u$, *and* $2u \mid m$.

However, this phenomenon does not hold in general. The group $\mathbb{Z}_9$ is not a DCI-group, see Theorem 2.11(i), but it was proved to be a BCI-group [2].

4.1 Bicyclic bases

Throughout this chapter we use the following notation. Let

$$V_i = \mathbb{Z}_n \times \{i\},\ i \in \{0,1\},\ \text{and } V = V_0 \cup V_1.$$

Furthermore, let c and d be the permutations of V defined by

$$\begin{aligned} c &: (x,i) \mapsto (x+1,i),\ i \in \{0,1\}, x \in \mathbb{Z}_n \\ d &: (x,i) \mapsto (x,1-i),\ i \in \{0,1\}, x \in \mathbb{Z}_n. \end{aligned}$$

Also, we let $D = \langle c, d\rangle$. As noted before, both c and d will be automorphisms of any bi-Cayley graph $\mathrm{BCay}(\mathbb{Z}_n, S)$, the group $R(\mathbb{Z}_n)$ is generated by c, and the group D acts regularly on V and it is isomorphic to D_{2n}.

We call a permutation group $G \leq \mathrm{Sym}(V)$ *bicyclic* if G is a cyclic group with orbits V_0 and V_1. In this context, the set $\mathcal{S}(\mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, S))$ contains the bicyclic groups contained in $\mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, S))$. Obviously, $R(\mathbb{Z}_n)$ is a bicyclic group, and it will be referred to as the *canonical bicyclic group*.

For a graph $\Gamma = \mathrm{BCay}(\mathbb{Z}_n, S)$, we let $\mathrm{Iso}(\Gamma)$ denote the set of all isomorphisms from Γ to another bi-Cayley graph over $\mathbb{Z}_n$. Formally,

$$\mathrm{Iso}(\Gamma) = \big\{ f \in \mathrm{Sym}(V) \mid \Gamma^f = \mathrm{BCay}(\mathbb{Z}_n, T) \text{ for some } T \subseteq \mathbb{Z}_n \big\}.$$

Furthermore, let $\mathcal{C}_{\mathrm{iso}}(\Gamma)$ denote the *isomorphism class* of cyclic bi-Cayley graphs over $\mathbb{Z}_n$ which contains Γ, i. e., $\mathcal{C}_{\mathrm{iso}}(\Gamma) = \{\Gamma^f \mid f \in \mathrm{Iso}(\Gamma)\}$.

Lemma 4.3. *Let $\Gamma = \mathrm{BCay}(\mathbb{Z}_n, S)$ be a connected bi-Cayley graph and f be a permutation of V. Then $f \in \mathrm{Iso}(\Gamma)$ if and only if $fR(\mathbb{Z}_n)f^{-1}$ is a bicyclic group contained in $\mathrm{Aut}(\Gamma)$.*

Proof. Let $f \in \mathrm{Iso}(\Gamma)$. Then $fR(\mathbb{Z}_n)f^{-1} \leq \mathrm{Aut}(\Gamma)$. Clearly, $fR(\mathbb{Z}_n)f^{-1}$ is a cyclic group. Since the sets V_0 and V_1 are the colour classes of the connected bipartite graph Γ, f preserves these sets, implying that the orbits of $fR(\mathbb{Z}_n)f^{-1}$ are equal to V_0 and V_1. Therefore, $fR(\mathbb{Z}_n)f^{-1}$ is a bicyclic group.

Conversely, suppose that $fR(\mathbb{Z}_n)f^{-1}$ is a bicyclic group which is contained in $\mathrm{Aut}(\Gamma)$. Then $R(\mathbb{Z}_n) = f^{-1}(fR(\mathbb{Z}_n)f^{-1})f \leq \mathrm{Aut}(\Gamma^f)$. Because V_0 and V_1 are the orbits of $fR(\mathbb{Z}_n)f^{-1}$, the graph Γ^f is connected and bipartite whose colour classes are V_0 and V_1. This implies that $\Gamma^f = \mathrm{BCay}(\mathbb{Z}_n, T)$ for some $T \subseteq \mathbb{Z}_n$, and so $f \in \mathrm{Iso}(\Gamma)$. The lemma is proved. □

Lemma 4.3 shows that the normalizer $N_{\mathrm{Sym}(V)}(R(\mathbb{Z}_n)) \subseteq \mathrm{Iso}(\mathrm{BCay}(\mathbb{Z}_n, S))$. It is known that the group $N_{\mathrm{Sym}(V)}(R(\mathbb{Z}_n))$ consists of the following permutations:

$$\varphi_{a,b,c} : (x,i) \mapsto \begin{cases} (ax+b, 0) & \text{if } i = 0 \\ (ax+c, 1) & \text{if } i = 1, \end{cases} \tag{4.1}$$

and

$$\psi_{a,b,c} : (x,i) \mapsto \begin{cases} (ax+b, 1) & \text{if } i = 0 \\ (ax+c, 0) & \text{if } i = 1, \end{cases} \tag{4.2}$$

where $a \in \mathbb{Z}_n^*$ and $b, c \in \mathbb{Z}_n$. Notice that, the equality $T = aS + b$ with some $a \in \mathbb{Z}_n^*$ and $b \in \mathbb{Z}_n$ can be expressed equivalently as the graphs $\mathrm{BCay}(\mathbb{Z}_n, S)$ and $\mathrm{BCay}(\mathbb{Z}_n, T)$ are in the same $N_{\mathrm{Sym}(V)}(R(\mathbb{Z}_n))$-orbit. For a graph $\Gamma = \mathrm{BCay}(\mathbb{Z}_n, S)$, we let

$$\mathcal{C}_{\mathrm{aff}}(\Gamma) = \left\{\Gamma^{\phi} \mid \phi \in N_{\mathrm{Sym}(V)}(R(\mathbb{Z}_n))\right\}.$$

Clearly, the isomorphism class $\mathcal{C}_{\mathrm{iso}}(\Gamma)$ can be decomposed as follows:

$$\mathcal{C}_{\mathrm{iso}}(\Gamma) = \mathcal{C}_{\mathrm{aff}}(\Gamma_1) \dot\cup \cdots \dot\cup \mathcal{C}_{\mathrm{aff}}(\Gamma_k).^1$$

Our goal in this section is to describe the above decomposition with the aid of bicyclic groups contained in $\mathrm{Aut}(\Gamma)$. We first observe that, if Γ is connected, then for any bicyclic group $X < \mathrm{Aut}(\Gamma)$ and for any $g \in \mathrm{Aut}(\Gamma)$, the conjugate group $g^{-1}Xg$ is also bicyclic. We remark that the conclusion does not hold when the graph is disconnected, the group $g^{-1}Xg$ might have orbits different from V_0 and V_1. Thus the set of all bicyclic groups contained in $\mathrm{Aut}(\Gamma)$ is the union of some $\mathrm{Aut}(\Gamma)$-conjugacy classes. We will denote the set of all bicyclic groups contained in $\mathrm{Aut}(\Gamma)$ by $\mathcal{B}(\mathrm{Aut}(\Gamma))$.

Definition 4.4. Let $\Gamma = \mathrm{BCay}(\mathbb{Z}_n, S)$ be a connected bi-Cayley graph. We say that a subset $\Xi \subseteq \mathrm{Iso}(\Gamma)$ is a *bicyclic base* of $\mathrm{Aut}(\Gamma)$ if the subgroups $\xi R(\mathbb{Z}_n)\xi^{-1}, \xi \in \Xi$, form a complete set of representatives of the $\mathrm{Aut}(\Gamma)$-conjugacy classes contained in $\mathcal{B}(\mathrm{Aut}(\Gamma))$.

Theorem 4.5. *Let $\Gamma = \mathrm{BCay}(\mathbb{Z}_n, S)$ be a connected bi-Cayley graph and let Ξ be a bicyclic base of $\mathrm{Aut}(\Gamma)$. Then $\mathcal{C}_{\mathrm{iso}}(\Gamma) = \dot\bigcup_{\xi\in\Xi}\mathcal{C}_{\mathrm{aff}}(\Gamma^{\xi})$.*

Proof. It follows immediately that,

$$\mathcal{C}_{\mathrm{iso}}(\Gamma) \supseteq \bigcup_{\xi\in\Xi} \mathcal{C}_{\mathrm{aff}}(\Gamma^{\xi}). \tag{4.3}$$

We prove that equality holds in (4.3). Pick $\Sigma \in \mathcal{C}_{\mathrm{iso}}(\Gamma)$. Then $\Sigma = \Gamma^f$ for some $f \in \mathrm{Iso}(\Gamma)$. By Lemma 4.3, $fR(\mathbb{Z}_n)f^{-1}$ is a bicyclic group of Γ, hence

$$fR(\mathbb{Z}_n)f^{-1} = g\xi R(\mathbb{Z}_n)(g\xi)^{-1},\ \xi \in \Xi, g \in \mathrm{Aut}(\Gamma).$$

Thus $f^{-1}g\xi = h$, where $h \in N_{\mathrm{Sym}(V)}(R(\mathbb{Z}_n))$. Then

$$\Sigma = \Gamma^f = \Gamma^{g\xi h^{-1}} = \left(\Gamma^{\xi}\right)^{h^{-1}}.$$

This shows that $\Sigma \in \mathcal{C}_{\mathrm{aff}}(\Gamma^{\xi})$, and so

$$\mathcal{C}_{\mathrm{iso}}(\Gamma) \subseteq \bigcup_{\xi\in\Xi} \mathcal{C}_{\mathrm{aff}}(\Gamma^{\xi}).$$

In view of (4.3) the two sides are equal.

[1] Here we mean that $\mathcal{C}_{\mathrm{iso}}(\Gamma) = \mathcal{C}_{\mathrm{aff}}(\Gamma_1) \cup \cdots \cup \mathcal{C}_{\mathrm{aff}}(\Gamma_k)$ and $\mathcal{C}_{\mathrm{aff}}(\Gamma_i) \cap \mathcal{C}_{\mathrm{aff}}(\Gamma_j) = \emptyset$ for every $i, j \in \{1, \ldots, k\}$, $i \neq j$.

Moreover, if $\mathcal{C}_{\mathrm{aff}}(\Gamma^{\xi_1}) \cap \mathcal{C}_{\mathrm{aff}}(\Gamma^{\xi_2}) \neq \emptyset$ for $\xi_1, \xi_2 \in \Xi$, then $\Gamma^{\xi_1} = \Gamma^{\xi_2 h}$ for some $h \in N_{\mathrm{Sym}(V)}(R(\mathbb{Z}_n))$. Hence $\xi_2 h \xi_1^{-1} = g$ for some $g \in \mathrm{Aut}(\Gamma)$, and so

$$\xi_1 R(\mathbb{Z}_n)\xi_1^{-1} = g^{-1}\xi_2 h R(\mathbb{Z}_n) h^{-1}\xi_2^{-1} g = g^{-1}(\xi_2 R(\mathbb{Z}_n)\xi_2^{-1})g.$$

The bicyclic groups $\xi_1 R(\mathbb{Z}_n)\xi_1^{-1}$ and $\xi_2 R(\mathbb{Z}_n)\xi_2^{-1}$ are conjugate in $\mathrm{Aut}(\Gamma)$, hence $\xi_1 = \xi_2$ follows from the definition of the bicyclic base Ξ. We obtain that $\mathcal{C}_{\mathrm{aff}}(\Gamma^{\xi_1}) \cap \mathcal{C}_{\mathrm{aff}}(\Gamma^{\xi_2}) = \emptyset$ whenever $\xi_1, \xi_2 \in \Xi$, $\xi_1 \neq \xi_2$, and so $\mathcal{C}_{\mathrm{iso}}(\Gamma) = \dot{\bigcup}_{\xi \in \Xi} \mathcal{C}_{\mathrm{aff}}(\Gamma^{\xi})$. The theorem is proved. □

4.2 Bi-Cayley graphs BCay($\mathbb{Z}_{2m}, \{0, u, v, v+m\}$)

Theorem 4.1 will follow from the following theorem, which we are going to prove in the next section.

Theorem 4.6. *Two connected bi-Cayley graphs* $\mathrm{BCay}(\mathbb{Z}_n, S)$ *and* $\mathrm{BCay}(\mathbb{Z}_n, T)$ *with* $|S| = |T| = 4$ *are isomorphic if and only if there exist* $a_1, a_2 \in \mathbb{Z}_n^*$ *and* $b_1, b_2 \in \mathbb{Z}_n$ *such that*

(i) $a_1 S + b_1 = T$; *or*

(ii) $a_1 S + b_1 = \{0, u, v, v+m\}$ *and* $a_2 T + b_2 = \{0, u+m, v, v+m\}$, *where* $n = 2m$, $\mathbb{Z}_n = \langle u, v \rangle$, $2 \mid u$, $2u \mid m$ *and* $u/2 \not\equiv v + m/(2u) (\mathrm{mod}\ m/u)$.

Proof of Theorem 4.1. In view of Theorem 4.6, it is sufficient to prove that, if

$$a_1 S + b_1 = \{0, u, v, v+m\} \text{ and } a_2 T + b_2 = \{0, u+m, v, v+m\},$$

where $n = 2m$, $\mathbb{Z}_n = \langle u, v \rangle$, $2 \mid u$, $2u \mid m$ and $u/2 \equiv v + m/(2u) (\mathrm{mod}\ m/u)$, then $\mathrm{BCay}(\mathbb{Z}_n, S) \cong_{\mathrm{aff}} \mathrm{BCay}(\mathbb{Z}_n, T)$.[2] In fact, we are going to show that there exist $a \in \mathbb{Z}_n^*$ and $b \in \mathbb{Z}_n$ such that

$$a \cdot \{0, u, v, v+m\} + b = \{0, u+m, v, v+m\}.$$

Then $(a_2^{-1} a a_1) \cdot S + a_2^{-1}(a b_1 + b - b_2) = T$, and hence indeed $\mathrm{BCay}(\mathbb{Z}_n, S) \cong_{\mathrm{aff}} \mathrm{BCay}(\mathbb{Z}_n, T)$.

Let us consider the following system of congruences:

$$ux \equiv -u + m (\mathrm{mod}\ n) \text{ and } vx \equiv -u + v (\mathrm{mod}\ n). \tag{4.4}$$

By the first congruence, using also that $2u \mid m$, x may be written in the form $x = (n/u)y - 1 + m/u$. Plugging this in the second one, we obtain $(vn/u)y \equiv 2v - u - vm/u (\mathrm{mod}\ n)$, which has an integer solution in y exactly when $\gcd(vn/u, n) \mid (2v - u - vm/u)$. Then $\gcd(vn/u, n) = n/u \gcd(u, v)$, and since $\mathbb{Z}_n = \langle u, v \rangle$, n/u and $\gcd(u, v)$ are coprime. Since $\gcd(u, v)$ is clearly a divisor of $2v - u - vm/u$, a solution in y exists if and only if $n/u \mid (2v - u - vm/u)$, i. e., $u \equiv 2v - vm/u (\mathrm{mod}\ 2m/u)$

[2] We write $\mathrm{BCay}(\mathbb{Z}_n, S) \cong_{\mathrm{aff}} \mathrm{BCay}(\mathbb{Z}_n, T)$ if there is a bi-Cayley isomorphism which maps the first graph to the second, or equivalently, if $T = aS + b$ holds for some $a \in \mathbb{Z}_n^*$ and $b \in \mathbb{Z}_n$.

(recall that $n = 2m$). On the other hand, one of the initial assumptions is $u/2 \equiv v + m/(2u) (\mathrm{mod}\ m/u)$, and so $u \equiv 2v + m/u (\mathrm{mod}\ 2m/u)$. We conclude that (4.4) has an integer solution if $-vm/u \equiv m/u (\mathrm{mod}\ 2m/u)$. Now, the latter congruence holds because of the conditions $2 \mid u$, $2 \mid n$, and $\mathbb{Z}_n = \langle u, v \rangle$.

Let a be a solution of (4.4). It follows from the above argument that $\gcd(a, m/u) = 1$. Notice that, since $2u \mid m$, $2 \nmid a$. Let $d = \gcd(a, u)$. By (4.4), $av \equiv -u + v (\mathrm{mod}\ n)$, implying that $d \mid v$, and so $d = 1$. We see that $\gcd(a, 2m) = 1$, i. e., $a \in \mathbb{Z}_n^*$. Choosing $b = u + m$, we get by (4.4) that $a \cdot 0 + b = u + m$, $au + b = 0$, $av + b = v + m$, and $a(v + m) + b = v$. The theorem is proved. □

In this section we prove Theorem 4.6 for graphs $\mathrm{BCay}(\mathbb{Z}_n, S)$ satisfying certain additional conditions.

Theorem 4.7. *Let $n = 2m$ and $S = \{0, u, v, v + m\}$ such that*

(a) $\mathbb{Z}_n = \langle u, v \rangle$;

(b) $1 < u < m$, $u \mid m$;

(c) The stabilizer $\mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, S))_{(0,0)}$ *leaves the set* $\{(0, 1), (u, 1)\}$ *setwise fixed.*

Then $\mathrm{BCay}(\mathbb{Z}_n, S) \cong \mathrm{BCay}(\mathbb{Z}_n, T)$ *if and only if there exist* $a \in \mathbb{Z}_n^*$ *and* $b \in \mathbb{Z}_n$ *such that*

(i) $aT + b = S$; *or*

(ii) $aT + b = \{0, u + m, v, v + m\}$, *and* $2 \mid u$, $2u \mid m$, $u/2 \not\equiv v + m/(2u) (\mathrm{mod}\ m/u)$.

It follows from Theorem 4.7(b) that $2u \leq m$. We prove first the extremal case when $2u = m$. Notice that, in this case the conditions in Theorem 4.7(ii) that $2 \mid u$, $2u \mid m$ and $u/2 \not\equiv v + m/(2u) (\mathrm{mod}\ m/u)$ can be replaced by one condition: $u \equiv 2 (\mathrm{mod}\ 4)$.

Lemma 4.8. *Let S be the set defined in Theorem 4.7. If $2u = m$, then* $\mathrm{BCay}(\mathbb{Z}_n, S) \cong \mathrm{BCay}(\mathbb{Z}_n, T)$ *if and only if there exist* $a \in \mathbb{Z}_n^*$ *and* $b \in \mathbb{Z}_n$ *such that*

(i) $aT + b = S$; *or*

(ii) $aT + b = \{0, u + m, v, v + m\}$ *and* $u \equiv 2 (\mathrm{mod}\ 4)$.

Proof. Let $d = \gcd(n, v)$. Because of $\langle u, v \rangle = \mathbb{Z}_n$ we have that $\gcd(u, v, n) = 1$, i. e., $\gcd(n/4, v) = 1$, and this gives that $d \in \{1, 2, 4\}$. Note that, if $d \neq 1$, then necessarily $2 \nmid u$. Let us write $v = v_1 d$, where $\gcd(v_1, n) = 1$. Let v_1^{-1} denote the inverse of v_1 in the group $\mathbb{Z}_n^*$. Then the following hold in $\mathbb{Z}_n$ (here we use that $u = n/4$):

$$v_1^{-1} v = d,\ v_1^{-1}(v + m) = d + m \ \text{ and } \ v_1^{-1} u \in \{u, 3u\}.$$

We conclude that S can be mapped by a bi-Cayley isomorphism to one of the sets $S_i(d)$, $i \in \{1, 2\}$ and $d \in \{1, 2, 4\}$, where

$$S_1(d) = \{0, u, d, d + 2u\} \text{ or } S_2(d) = \{0, 3u, d, d + 2u\}.$$

The lemma follows from the following claims:

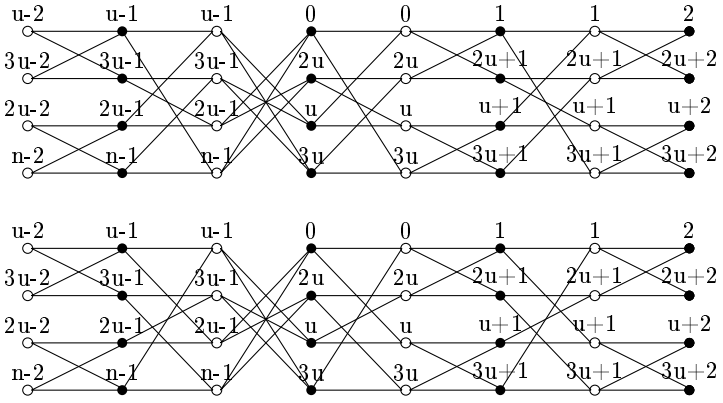

Figure 4.1: Bi-Cayley graphs BCay($\mathbb{Z}_n, S_1(1)$) and BCay($\mathbb{Z}_n, S_2(1)$).

(i) BCay($\mathbb{Z}_n, S_1(1)$) $\cong$ BCay($\mathbb{Z}_n, S_2(1)$).

(ii) BCay($\mathbb{Z}_n, S_1(1)$) $\cong_{\text{aff}}$ BCay($\mathbb{Z}_n, S_1(d)$) for $d \in \{2, 4\}$;

(iii) BCay($\mathbb{Z}_n, S_1(d)$) $\cong_{\text{aff}}$ BCay($\mathbb{Z}_n, S_2(d)$) $\iff$ $d \in \{2, 4\}$ or ($d = 1$ and $u \not\equiv 2 (\text{mod } 4)$);

(i): Define the mapping $f : V \mapsto V$ by

$$f : (x, i) \mapsto \begin{cases} (x, i) & \text{if } x \in \{0, 1, \ldots . u-1\} \cup \{2u, \ldots . 3u-1\}, \\ (x + 2u, i) & \text{otherwise.} \end{cases}$$

We leave for the reader to verify that f is an isomorphism from BCay($\mathbb{Z}_n, S_1(1)$) to BCay($\mathbb{Z}_n, S_2(1)$). Compare the graphs in Figure 4.1. Here the white vertices represent the colour class V_0, while the black ones represent the colour class V_1.

(ii): Since $d \in \{2, 4\}$, u is an odd number. For $d \in \{2, 4\}$ define $r_d \in \mathbb{Z}_n^*$ as follows:

$$r_2 = \begin{cases} 2 + u & \text{if } u \equiv 1 (\text{mod } 4), \\ 2 + 3u & \text{if } u \equiv 3 (\text{mod } 4), \end{cases} \quad r_4 = \begin{cases} 4 + u & \text{if } u \equiv 3 (\text{mod } 4), \\ 4 + 3u & \text{if } u \equiv 1 (\text{mod } 4). \end{cases}$$

It can be directly checked that $r_d S_1(1) + u = S_1(d)$, so BCay($\mathbb{Z}_n, S_1(1)$) $\cong_{\text{aff}}$ BCay($\mathbb{Z}_n, S_1(d)$) for $d \in \{2, 4\}$.

(iii): If u is odd, then $(2u + 1)S_1(d) = S_2(d)$, hence BCay($\mathbb{Z}_n, S_1(d)$) $\cong_{\text{aff}}$ BCay($\mathbb{Z}_n, S_2(d)$). Since u is odd whenever $d \in \{2, 4\}$, we are left with the case that $d = 1$ and u is even. If also $u \equiv 0 (\text{mod } 4)$, then $(u + 1)S_1(1) + 3u = S_2(1)$, and again BCay($\mathbb{Z}_n, S_1(1)$) $\cong_{\text{aff}}$ BCay($\mathbb{Z}_n, S_2(1)$).

Suppose that $d = 1$ and $u \equiv 2 (\text{mod } 4)$. We finish the proof by showing that in this case BCay($\mathbb{Z}_n, S_1(1)$) $\ncong_{\text{aff}}$ BCay($\mathbb{Z}_n, S_2(1)$). Suppose that, there is an affine transformation $\psi : x \mapsto rx + s$, $r \in \mathbb{Z}_n^*$ and $s \in \mathbb{Z}_n$, which maps the set $S_1(1)$ to $S_1(2)$. Then $1^\psi - (1 + 2u)^\psi = 2u$ in $\mathbb{Z}_n$. This implies that $\{1, 1 + 2u\}^\psi = \{1, 1 + 2u\}$ and $\{0, u\}^\psi = \{0, 3u\}$, and hence

$$r + s \in \{1, 1 + 2u\} \text{ and } r\{0, u\} + s = \{0, 3u\}.$$

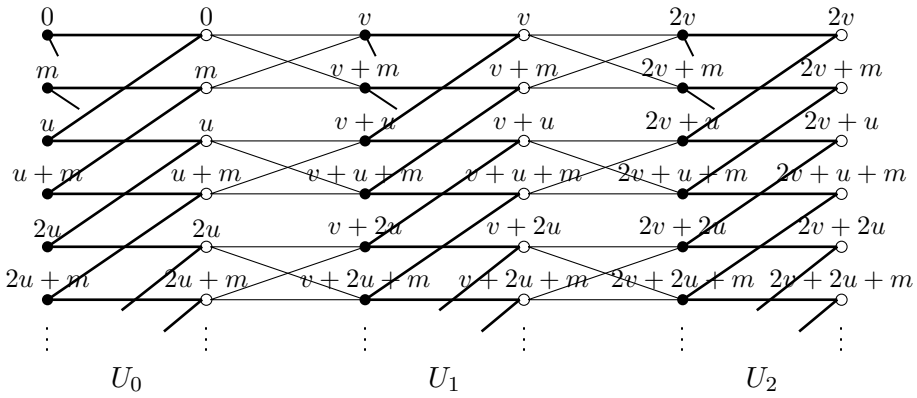

Figure 4.2: The bi-Cayley graph $\mathrm{BCay}(\mathbb{Z}_n, S)$.

A direct analysis shows that the above equations cannot hold if $u \equiv 2 (\mathrm{mod}\ 4)$. Thus $\mathrm{BCay}(\mathbb{Z}_n, S_1(1)) \ncong_{\mathrm{aff}} \mathrm{BCay}(\mathbb{Z}_n, S_2(1))$. This completes the proof of (iii). □

Now, we turn to the case when $2u \neq m$. Recall that the canonical bicyclic group $R(\mathbb{Z}_n)$ is generated by the permutation c defined in the beginning of Section 4.1. For a divisor $\ell \mid n$, $R(\mathbb{Z}_n)^\ell$ will denote the subgroup of $R(\mathbb{Z}_n)$ generated by c^ℓ. It will be convenient to denote by δ_ℓ the partition of V into the orbits of $R(\mathbb{Z}_n)^\ell$, i. e., $\delta_\ell = \mathrm{Orb}(R(\mathbb{Z}_n)^\ell, V)$. Furthermore, we set $\eta_{n,\ell}$ for the homomorphism $\eta_{n,\ell} : \mathbb{Z}_n \to \mathbb{Z}_\ell$ defined by $\eta_{n,\ell}(1) = 1$.

Let $A = \mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, R))$, where R is an arbitrary subset of $\mathbb{Z}_n$. Observe that, if δ_ℓ is, in addition, a system of blocks for A, then we define the action of A on $V(\mathrm{BCay}(\mathbb{Z}_\ell, \eta_{n,\ell}(R)))$ by letting $g \in A$ act as

$$(x,i)^g = (y,j) \iff \big\{(z,i) \mid z \in \eta_{n,\ell}^{-1}(x)\big\}^g = \big\{(z,j) \mid z \in \eta_{n,\ell}^{-1}(y)\big\}. \tag{4.5}$$

We denote by A_{δ_ℓ} the corresponding kernel, and by g^{δ_ℓ} the image of an element $g \in A$. Note that, if X is a bicyclic group in $\mathcal{S}(A)$, then $X^{\delta_\ell} = \{x^{\delta_\ell} : x \in X\}$ is a bicyclic group in $\mathcal{S}(\mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_\ell, \eta_{n,\ell}(R))))$.

Now, let $S = \{0, u, v, v+m\}$ be the subset of $\mathbb{Z}_n$ defined in Theorem 4.7. Let δ be the partition of V defined by

$$\delta = \big\{X \cup X^{\psi_{1,0,0}} \mid X \in \mathrm{Orb}(R(\mathbb{Z}_n)^u, V)\big\}, \tag{4.6}$$

where $\psi_{1,0,0}$ is defined in (4.2). We write $\delta = \{U_0, \ldots, U_{u-1}\}$, where

$$U_i = \big\{(iv + ju, 0), (iv + ju, 1) \mid j \in \{0, 1, \ldots, (n/u) - 1\}\big\}.$$

A part of $\mathrm{BCay}(\mathbb{Z}_n, S)$ is drawn in Figure 4.2 using the partition δ. White and black colours represent again the colour classes V_0 and V_1, respectively. For $i \in \{0, 1, \ldots, u-1\}$ and $k \in \{0, 1\}$, let e_i be the involution of V defined by

$$e_i : (x,k) \mapsto \begin{cases} (x+m, k) & \text{if } (x,k) \in U_i \\ (x,k) & \text{otherwise.} \end{cases}$$

It is clear that each $e_i \in \mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, S))$, and also that $e_i e_j = e_j e_i$ for all $i, j \in \{0, 1, \ldots, u-1\}$. Let $E = \langle e_0, e_1, \ldots, e_{u-1} \rangle$. Thus $E \leq \mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, S))$ and $E \cong \mathbb{Z}_2^u$. For a subset $I \subseteq \{0, 1, \ldots, u-1\}$ let e_I be the element in E defined by $e_I = \prod_{i \in I} e_i$.

The following lemma will be used throughout the chapter.

Lemma 4.9. *Let $\Gamma = \mathrm{BCay}(\mathbb{Z}_n, R)$ be a bi-Cayley graph and suppose that $R_* \subseteq R$ such that the stabilizer $\mathrm{Aut}(\Gamma)_{(0,0)}$ fixes setwise $R_* \times \{1\}$, and let $d = |\langle R_* - R_* \rangle|$, where $R_* - R_* = \{r_1 - r_2 \mid r_1, r_2 \in R_*\}$. Then the partition π of V defined by*

$$\pi = \{X \cup X^{\psi_{1,r,-r}} \mid X \in \mathrm{Orb}(R(\mathbb{Z}_n)^{n/d}, V)\}, \text{ where } r \in R_*,$$

is a system of blocks for $\mathrm{Aut}(\Gamma)$.[3]

Proof. We let $A = \mathrm{Aut}(\Gamma)$. Since $R_* \times \{1\}$ is fixed setwise by $A_{(0,0)}$, we may write

$$R_* = R_1 \cup \cdots \cup R_k,$$

where $R_i \times \{1\}$ is an $A_{(0,0)}$-orbit for every $i \in \{1, 2, \ldots, k\}$. For $i \in \{1, \ldots, k\}$, choose an arc $((0,0), (r_i, 1))$ of Γ, where $r_i \in R_i$. We claim that the A-orbit of this arc is equal to the edge set of the bi-Cayley graph $\mathrm{BCay}(\mathbb{Z}_n, R_i)$.

Let A^+ be the colour preserving subgroup of A (i. e., A^+ is the setwise stabilizer $A_{\{V_0\}}$). Then $A = A^+ \rtimes \langle \psi_{-1,0,0} \rangle$. Also, $A^+ = A_{(0,0)} R(\mathbb{Z}_n)$, as $R(\mathbb{Z}_n)$ is transitive on V_0. Then the A-orbit of the arc $((0,0), (r_i, 1))$ can be obtained as follows

$$\begin{aligned}
((0,0),(r_i,1))^A &= ((0,0),(r_i,1))^{A_{0,0} R(\mathbb{Z}_n) \langle \psi_{-1,0,0} \rangle} = \\
&= \{((0,0),(r_i',1)) \mid r_i' \in R_i\}^{R(\mathbb{Z}_n)\langle \psi_{-1,0,0} \rangle} \\
&= \{((j,0),(j+r_i',1)) \mid r_i' \in R_i, j \in \mathbb{Z}_n\}^{\langle \psi_{-1,0,0} \rangle} \\
&= \{((j,0),(j+r_i',1)) \mid r_i' \in R_i, j \in \mathbb{Z}_n\} \cup \\
&\quad \{((-j,1),(-j-r_i',0)) \mid r_i' \in R_i, j \in \mathbb{Z}_n\}, \\
&= \{(j,0)(j+r_i',1) \mid r_i' \in R_i, j \in \mathbb{Z}_n\}.
\end{aligned}$$

This is clearly equal to the edge set of $\mathrm{BCay}(\mathbb{Z}_n, R_i)$.

Now, we can write $A \leq \mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, R_i))$ for every $i \in \{1, \ldots, k\}$. Since $\mathrm{BCay}(\mathbb{Z}_n, R_*) = \cup_{i=1}^k \mathrm{BCay}(\mathbb{Z}_n, R_i)$, this gives that $A \leq \mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, R_*)$. It is easily seen that the connected component of $\mathrm{BCay}(\mathbb{Z}_n, R_*)$ containing $(0,0)$ is its subgraph induced by the vertex set $X \cup X^{\psi_{1,r,-r}}$, where X is the orbit of $(0,0)$ under $R(\mathbb{Z}_n)^{n/d}$. Clearly, this set is a block for A. The lemma is proved. □

Lemma 4.10. *Let S be the set defined in Theorem 4.7. If $2u \neq m$, then the stabilizer $\mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, S))_{(0,0)}$ is given as follows.*

(i) If $u \not\equiv 2v \pmod{m/u}$, then $\mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, S))_{(0,0)} = E_{(0,0)}$.

(ii) If $u \equiv 2v \pmod{m/u}$, then $\mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, S))_{(0,0)} = E_{(0,0)} \times F$ for a subgroup $F \leq \mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, S))_{(0,0)}$, $|F| = 2$.

[3] Notice that, π does not depend of the choice of the element $r \in R_*$.

PROOF. For short we put $\Gamma = \mathrm{BCay}(\mathbb{Z}_n, S)$ and $A = \mathrm{Aut}(\Gamma)$. Consider the partition δ defined in (4.6). Applying Lemma 4.9 with $R = S$, $R_* = \{0, u\}$ and $r = 0$, we obtain that δ is a system of blocks for A. The quotient graph Γ/δ is a u-cycle if $u > 2$ and a 2-path if $u = 2$. Let $g \in A_{(0,0)}$. Then g fixes the arc (U_0, U_1) of Γ/δ, hence it must fix all sets U_i. Thus $A_{(0,0)} \leq A_\delta$, where A_δ is the kernel of the action of A on δ.

Consider the action of A on U_0. The corresponding kernel is A_{U_0}, the pointwise stabilizer of U_0 in A, and the corresponding image is a subgroup of $\mathrm{Aut}(\Gamma[U_0])$, where $\Gamma[U_0]$ is the subgraph of Γ induced by the set U_0. Using that $2u \neq m$, we show next that $A_{U_0} = E_{(0,0)}$. It is clear that $A_{U_0} \geq E_{(0,0)}$. We are going to prove that $A_{U_0} \leq E_{(0,0)}$ also holds. Let $g \in A_{U_0}$. Then for a suitable element $e \in \langle e_1 \rangle$, the product ge fixes pointwise U_0 and fix the vertex $(v, 1)$ from block U_1 (see Figure 4.2). Thus ge acts on U_1 as the identity or the unique reflection of the cycle $\Gamma[U_1]$ that fixes $(v, 1)$. If this action is not the identity, then ge switches $(v, 0)$ and $(v+n-u, 0)$, and so it must switch $(v+u, 1)$ and $(v+n-u, 1)$. On the other hand, since $(v+u, 1)$ is connected to $(u, 0) \in U_0$, it follows that $(v+u, 1)$ can only be mapped to $(v+u+m, 1)$, and so $(v+n-u, 1) = (v+u+m, 1)$, contradicting that $2u \neq m$. We conclude that ge acts as the identity also on U_1. Continuing in this way, we find that ge' is the identity with a suitable choice of $e' \in E_{(0,0)}$, hence $g = e'$.

The equality $A_{U_0} = E_{(0,0)}$ together with $\mathrm{Aut}(\Gamma[U_0]) \cong D_{4u}$ imply that $|A_{(0,0)} : E_{(0,0)}| \leq 2$. Moreover, $|A_{(0,0)} : E_{(0,0)}| = 2$ holds exactly when $A_{(0,0)}$ contains an involution g for which $g : (0, 1) \leftrightarrow (u, 1)$. In the latter case $A_{(0,0)} = E_{(0,0)} \times \langle g \rangle$ as g centralizes E (to see this, observe that g is in the kernel A_δ, and acts on every block U_i as an element of $D_{2n/u}$, whereas E acts on U_i as the center $Z(D_{2n/u})$.) We settle the lemma by proving the following equivalence :

$$A_{(0,0)} \cong E_{(0,0)} \times \mathbb{Z}_2 \iff u \equiv 2v (\mathrm{mod}\ m/u). \tag{4.7}$$

Suppose first that $A_{(0,0)} = E_{(0,0)} \times \langle g \rangle$, where $g \in A_{(0,0)}$ and $g : (0, 1) \leftrightarrow (u, 1)$. By Theorem 4.7(c), $\{(v, 1), (v + m, 1)\}^{A_{(0,0)}} = \{(v, 1), (v + m, 1)\}$. Applying Lemma 4.9 with $R = S$, $R_* = \{v, v + m\}$ and $r = v$, we obtain that the set $B = \{(0, 0), (m, 0), (v, 1), (v + m, 1)\}$ is a block for A. The induced graph $\Gamma[B]$ is a 4-cycle (see Figure 4.2). Denote by $A_{\{B\}}$ the setwise stabilizer of B in A, and by $A^B_{\{B\}}$ the permutation group of B induced by $A_{\{B\}}$. As $\Gamma[B]$ is a 4-cycle, $A^B_{\{B\}} \leq D_8$. This gives that $\{(0, 0), (m, 0)\}$ is a block for $A^B_{\{B\}}$, and therefore it is also a block for A. We conclude that $\delta_m = \{X \mid X \in \mathrm{Orb}(R(\mathbb{Z}_n)^m, V)\}$ is a system of blocks for A. Consider the action of A on $\mathrm{BCay}(\mathbb{Z}_m, \eta_{n,m}(S))$ defined in (4.5). Then $E \leq A_{\delta_m}$, while $g \notin A_{\delta_m}$. This implies that g^{δ_m} is an automorphism of $\mathrm{BCay}(\mathbb{Z}_m, \eta_{n,m}(S))$ which normalizes its canonical bicyclic group. This means that $g^{\delta_m} = \varphi_{r,s,t}$ for some $r \in \mathbb{Z}_m^*$ and $s, t \in \mathbb{Z}_m$. Using that $g^{\delta_m} : (0, 0) \mapsto (0, 0)$ and $(0, 1) \mapsto (\eta_{n,m}(u), 1)$, we find that $s = 0$ and $t = \eta_{n,m}(u)$, and so

$$A^{\delta_m} = \langle D^{\delta_m}, \varphi_{r,0,\eta_{n,m}(u)} \rangle. \tag{4.8}$$

Also, $g^{\delta_m} : (\eta_{n,m}(u), 1) \mapsto (0, 1)$ and $(\eta_{n,m}(v), 1) \mapsto (\eta_{n,m}(v), 1)$, hence $r\eta_{n,m}(u) = -\eta_{n,m}(u)$ and $r\eta_{n,m}(v) = \eta_{n,m}(v - u)$ hold in $\mathbb{Z}_m$. From these $r \equiv -1 (\mathrm{mod}\ m/u)$

and $rv \equiv v - u \pmod{m/u}$, i. e., $u \equiv 2v \pmod{m/u}$. The implication "$\Rightarrow$" in (4.7) is now proved.

Suppose next that $u \equiv 2v \pmod{m/u}$. Define the permutation g of V by

$$g : (iv + ju, 0) \mapsto \begin{cases} (iv - (i+j)u, 0) & \text{if } i = 0 \\ (iv - (i+j-1)u, 1) & \text{if } i = 1, \end{cases}$$

where $i \in \{0, 1, \ldots, u-1\}$ and $j \in \{0, 1, \ldots, n/u - 1\}$. We complete the proof by verifying that $g \in A_{(0,0)}$. Since $(0,0)^g = (0,0)$ and $g : (0,1) \leftrightarrow (u,1)$, this will imply that $A_{(0,0)} = E_{(0,0)} \times \langle g \rangle$. Thus part "$\Leftarrow$" of (4.7) is also proved.

Choose an arbitrary vertex $w \in V_0$ such that $w = (iv+ju, 0)$, $i \in \{0, 1, \ldots, u-1\}$ and $j \in \{0, 1, \ldots, n/u-1\}$, and suppose for the moment that $i < u-1$. Then w has the following neighbours:

$$(iv + ju, 1), (iv + (j+1)u, 1), ((i+1)v + ju, 1), ((i+1)v + (j + m/u)u, 1),$$

where $v + 1 \in \{0, 1, \ldots, u-1\}$, and $j+1$ and $j + m/u$ are from $\{0, 1, \ldots, n/u - 1\}$. Thus these vertices are mapped by g to

$$(iv-(i+j-1)u, 1), (iv-(i+j)u, 1), ((i+1)v-(i+j)u, 1), ((i+1)v-(i+j+m/u)u, 1).$$

A direct check shows that these are just the neighbours of $w^g = (iv - (i+j)u, 0)$. Let $i = u - 1$. Then the neighbours of w are:

$$(iv + ju, 1), (iv + (j+1)u, 1), ((j+v)u, 1), ((j + v + m/u)u, 1),$$

where $j+v$ and $j+v+m/u$ are from $\{0, ..., n/u-1\}$. Then these vertices are mapped by g to

$$(iv - (i+j-1)u, 1), (iv - (i+j)u, 1), (-(j+v-1)u, 1), (-(j+v+m/u-1)u, 1).$$

The first two are clearly connected with $w^g = (iv-(i+j)u, 0)$; whereas the rest two are connected with w^g if and only if the following equality holds in $\mathbb{Z}_n$:

$$\{iv - (i+j)u + v, iv - (i+j)u + v + m\} = \{-(j+v-1)u, -(j+v+m/u-1)u\}.$$

Using that $v = u-1$, this reduces to $\{-(u-v)u, -(u-v)u+m\} = \{-vu, -vu+m\}$. Finally, observe that this equality holds if $(u-v)u \equiv vu \pmod{m}$, and the latter congruence follows from the initial assumption that $u \equiv 2v \pmod{m/u}$. The lemma is proved. □

Lemma 4.11. *Let S be the set defined in Theorem 4.7, and let us write $A = \mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, S))$. If $2u \neq m$, then for the normalizer $N_A(R(\mathbb{Z}_n))$ of $R(\mathbb{Z}_n)$ in A,*

$$\big|A : N_A(R(\mathbb{Z}_n))\big| = \begin{cases} 2^{u-2} & \text{if } 2 \mid u \text{ and } \big(u \not\equiv 2v \pmod{m/u} \text{ or} \\ & u/2 \equiv v \pmod{m/u}\big) \\ 2^{u-1} & \text{otherwise.} \end{cases} \tag{4.9}$$

PROOF. For short we set $N = N_A(R(\mathbb{Z}_n))$. Recall that $D = \langle c, d\rangle$, see the beginning of Section 4.1. Since $A = DA_{(0,0)}$ and $D \leq N$, $N = D(N \cap A_{(0,0)})$. The two cases of Lemma 4.10 are considered separately.

CASE 1. $u \not\equiv 2v (\mathrm{mod}\ m/u)$.

In this case, from Lemma 4.10, $A_{(0,0)} = E_{(0,0)}$, hence $|A| = 2^u n$. Let $g \in N \cap A_{(0,0)}$. Since $g \in E_{(0,0)}$, it follows quickly that g is the identity element, or $2 \mid u$ and $g = e_1 e_3 \cdots e_{u-1}$. Combining this with $N = D(N \cap A_{(0,0)})$ we find that $|N| = 4n$ if $2 \mid u$, and $|N| = 2n$ if $2 \nmid u$. Formula (4.9) follows.

CASE 2. $u \equiv 2v (\mathrm{mod}\ m/u)$.

From Lemma 4.10, $A_{(0,0)} = E_{(0,0)} \times F$ for a subgroup $F \leq A_{(0,0)}$, $|F| = 2$, hence $|A| = 2^{u+1}n$. It follows from the proof of Lemma 4.10 that, there exists $r \in \mathbb{Z}_m^*$ such that the following hold:

$$r\eta_{n,m}(u) = -\eta_{n,m}(u) \text{ and } r\eta_{n,m}(v) = \eta_{n,m}(v-u).$$

Let $s \in \mathbb{Z}_n^*$ such that $\eta_{n,m}(s) = r$. Then

$$su \in \{-u, -u+m\} \text{ and } sv \in \{v-u, v-u+m\}. \tag{4.10}$$

Suppose that $2 \nmid u$. Then we get as before that $N \cap E_{(0,0)}$ is trivial. Notice also that, $u \equiv 2v + m/u (\mathrm{mod}\ n/u)$, which follows from the assumption that $u \equiv 2v (\mathrm{mod}\ m/u)$ and that $2 \nmid u$. Thus $2 \nmid m$ and $2 \mid (u+m)$, implying that in (4.10) we have $su = -u$. We obtain that $\varphi_{s,u,0} \in N \cap (A_{(0,0)} \setminus E_{(0,0)})$, and so $|N \cap A_{(0,0)}| = 2$.

Suppose next that $2 \mid u$. Then $|N \cap E_{(0,0)}| = 2$. It is easily seen that $|N \cap A_{(0,0)}| = 4$ if and only if there exists $r \in \mathbb{Z}_n^*$ such that $ru = -u$ and $rv = v - u$ hold in $\mathbb{Z}_n$. Consider the following system of linear congruences:

$$xu \equiv u (\mathrm{mod}\ n),\ xv \equiv v - u (\mathrm{mod}\ n). \tag{4.11}$$

From the first congruence we can write x in the form $x = yn/u - 1$. Substitute this into the second congruence. We obtain that $yvn/u \equiv 2v - u (\mathrm{mod}\ n)$. This has a solution if and only if $\gcd(vn/u, n) \mid (2v - u)$. Suppose that $\gcd(v, n) \neq 1$. Using that $\langle u, v\rangle = \mathbb{Z}_n$ and that $2 \mid u$, we obtain that $\gcd(v, m/u) \neq 1$. However, then from the assumption that $u \equiv 2v (\mathrm{mod}\ m/u)$ it follows that also $\gcd(v, u) \neq 1$, which contradicts that $\langle u, v\rangle = \mathbb{Z}_n$. Hence $\gcd(v, n) = 1$, $\gcd(vn/u, n) = n/u$, and so (4.11) has a solution if and only if $u \equiv 2v (\mathrm{mod}\ n/u)$, or equivalently, $u/2 \equiv v (\mathrm{mod}\ m/u)$ (recall that $2 \mid u$ and $u \mid m$). It is not hard to show that any solution to (4.11) is necessarily prime to n, hence is in $\mathbb{Z}_n^*$. The above arguments can be summarized as follows: $|N| = 8n$ if $2 \mid u$ and $u/2 \equiv v (\mathrm{mod}\ m/u)$, and $|N| = 4n$ otherwise. This is consistent with (4.9). The lemma is proved. □

Lemma 4.12. *Let $r \in \mathbb{Z}_n^*$, $r \neq 1$ and $s \in \mathbb{Z}_n$ such that the permutation $\varphi_{r,0,s}$ is of order 2. Then the group $\langle c, d, \varphi_{r,0,s}\rangle$ contains a bicyclic group different from $R(\mathbb{Z}_n)$ if and only if $8 \mid n$, $r = n/2 + 1$, and $s = 0$ or $s = n/2$.*

PROOF. Suppose that $\langle c, d, \varphi_{r,0,s}\rangle$ contains a bicyclic group X such that $X \neq R(\mathbb{Z}_n)$. Then X is generated by a permutation in the form $c^i\varphi_{r,0,s}$. Since $\varphi_{r,0,s}^2$ is the identity

mapping, $r^2 = 1$ in $\mathbb{Z}_n$, and we calculate that $(c^i\varphi_{r,0,s})^2$ sends $(x, 0)$ to $(x+r(r+1)i, 0)$ for every $x \in \mathbb{Z}_n$. That V_0 is an orbit of X is equivalent to the condition that $\gcd(n, r+1) = 2$. Using this and that $r^2 - 1 = (r-1)(r+1) \equiv 0 (\mathrm{mod}\ n)$, we find that $n/2$ divides $r-1$, so $r = 1$ or $r = n/2+1$. Since $r \neq 1$, we have that $r = n/2+1$ and $8 \mid n$. Then $(\varphi_{r,0,s})^2$ sends $(x, 1)$ to $(x + (n/2+2)s, 1)$. Since $(\varphi_{r,0,s})^2$ is the identity mapping, we obtain that $s = 0$ or $s = n/2$.

On the other hand, it can be directly checked that, if $8 \mid n$, $r = n/2+1$ and $s \in \{0, n/2\}$, then the permutation $c\varphi_{r,0,s}$ generates a bicyclic group in $\langle c, d, \varphi_{r,0,s}\rangle$. Obviously, this bicyclic subgroup cannot be $R(\mathbb{Z}_n)$. The lemma is proved. □

Everything is prepared to prove the main result of the section.

Proof of Theorem 4.7. The case that $2u = m$ is settled already in Lemma 4.8, hence let $2u \neq m$. We consider the action of $A = \mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, S))$ on the system of blocks δ_m defined in (4.5). We claim that the corresponding image A^{δ_m} has a unique bicyclic group (which is, of course, $R(\mathbb{Z}_n)^{\delta_m}$).

This is easy to see if $A_{(0,0)} = E_{(0,0)}$, because in this case $A^{\delta_m} = (DA_{(0,0)})^{\delta_m} = D^{\delta_m}$.

Let $A_{(0,0)} \neq E_{(0,0)}$. Then $A_{(0,0)} = E_{(0,0)} \times F$ for some subgroup F, $|F| = 2$. By (4.8), $A^{\delta_m} = \langle D^{\delta_m}, \varphi_{r,0,\eta_{n,m}(u)}\rangle$. Also, $r \equiv -1 (\mathrm{mod}\ m/u)$, hence $r \neq 1$ in $\mathbb{Z}_m$. By Lemma 4.12, A^{δ_m} contains more than one bicyclic group if and only if $8 \mid m$, $r = m/2+1$ and $\eta_{n,m}(u) \in \{0, m/2\}$. In the latter case $u \in \{m, m/2\}$, which is impossible as $u < m/2$. Hence A^{δ_m} contains indeed a unique bicyclic group.

We calculate next the number of bicyclic groups contained in A, and we denote this number by $\mathbb{B}$. In fact, we are going to derive the following formula:

$$\mathbb{B} = \begin{cases} 2^{u-2} & \text{if } 2 \mid u \text{ and } 2 \nmid (m/u) \\ 2^{u-1} & \text{otherwise.} \end{cases} \tag{4.12}$$

Let $g \in G$ such that $\langle g\rangle \leq A$ is a bicyclic group. Since $A = DA_{(0,0)}$, g can be written as $g = xy$ with $x \in D$ and $y \in A_{(0,0)}$. Since $\langle g\rangle$ is a bicyclic group, g fixes the colour classes setwise, implying that $x \in R(\mathbb{Z}_n)$. The image $\langle g\rangle^{\delta_m}$ is also a bicyclic group in A^{δ_m}, hence by the previous paragraph, $\langle g\rangle^{\delta_m} = R(\mathbb{Z}_n)^{\delta_m}$. Now, since $x \in R(\mathbb{Z}_n)$, $y^{\delta_m} \in R(\mathbb{Z}_n)^{\delta_m}$, from which y^{δ_m} is the identity mapping. We conclude that $x = c^i$ for some $i \in \{1, \ldots, n-1\}$ with $\gcd(i, m) = 1$, and $y \in E_{(0,0)}$, and so $y = e_I$ for a subset $I \subseteq \{1, \ldots, u-1\}$.

Obviously, the product $\varphi(n)\mathbb{B}$ calculates the number of elements $g \in G$ such that $\langle g\rangle$ is a bicyclic group in A, where φ denotes Euler's totient function. Therefore, $\varphi(n)\mathbb{B}$ is equal to the number of elements in the form c^ie_I that $i \in \{1, \ldots, n-1\}, \gcd(i, m) = 1$, $I \subseteq \{1, \ldots, u-1\}$, and $\langle c^ie_I\rangle$ is a bicyclic group contained in A.

Let us pick c^ie_I with $i \in \{1, \ldots, n-1\}, \gcd(i, m) = 1$, and $I \subseteq \{1, \ldots, u-1\}$. It is easily seen that $e_Ic^i = c^ie_{I+i}$, where $I + i = \{x + i \mid x \in I\}$, here the addition is taken modulo u. Using this and induction on u, it follows that

$$(c^ie_I)^u = c^{ui}e_Ie_{I+i}\cdots e_{I+(u-1)i}.$$

Since $\gcd(i, m) = 1$ and $u \mid m$, $\gcd(i, u) = 1$, from which

$$e_Ie_{I+i}\cdots e_{I+(u-1)i} = (e_0e_1\cdots e_{u-1})^{|I|} = c^{m|I|}.$$

Thus $(c^i e_I)^u = c^{u(i+\frac{m}{u}|I|)}$. This and $\gcd(i,u) = 1$ show that $\langle c^i e_I \rangle$ is a semiregular group. Therefore, $\langle c^i e_I \rangle$ is a bicyclic group if and only if $c^i e_I$ is of order n, or equivalently,

$$\gcd\left(i + \frac{m}{u}|I|, \frac{2m}{u}\right) = 1. \tag{4.13}$$

Notice that, since $\gcd(i,m) = 1$, the greatest common divisor above is always equal to 1 or 2. Suppose at first that $2 \mid (m/u)$. Then $2 \mid m$ and i is odd. Hence (4.13) always holds. We obtain that the number of elements in A which generate a bicyclic group is $\varphi(n)2^{u-1}$, and so $\mathbb{B} = 2^{u-1}$, as claimed in (4.12). Suppose next that $2 \nmid (m/u)$. Now, if $2 \mid u$, then $2 \mid m$, hence $2 \nmid i$, and so (4.13) holds if and only if $|I|$ is even. We deduce from this that $\mathbb{B} = 2^{u-2}$, as claimed in (4.12). Finally, if $2 \nmid u$, then $2 \nmid m$, and in this case (4.13) holds if and only if $\gcd(i,n) = 1$ and $|I|$ is even, or $\gcd(i,n) = 2$ and $|I|$ is odd. We calculate that $\mathbb{B} = 2^{u-1}$, and this completes the proof of (4.12).

Let Ξ be a bicyclic base of A. By (4.9) and (4.12) we obtain that, $|\Xi| > 1$ if and only if

$$|A : N_A(R(\mathbb{Z}_n))| = 2^{u-2} \text{ and } \mathbb{B} = 2^{u-1}.$$

This happens exactly when

$$\big(2 \mid u \text{ and } (u \not\equiv 2v (\mathrm{mod}\ m/u) \text{ or } u/2 \equiv v (\mathrm{mod}\ m/u))\big) \text{ and } \big(2 \nmid u \text{ or } 2u \mid m\big).$$

After some simplification,

$$|\Xi| > 1 \iff 2 \mid u,\ 2u \mid m \text{ and } u/2 \not\equiv v + m/(2u) (\mathrm{mod}\ m/u).$$

Suppose that $|\Xi| > 1$. Then A contains exactly 2^{n-1} bicyclic groups, 2^{n-2} of which are conjugate to $R(\mathbb{Z}_n)$. These 2^{n-1} subgroups are enumerated as: $\langle ce_I \rangle$, $I \subseteq \{1, \ldots, u-1\}$. For $i \in \{1, \ldots, u-2\}$, $e_i c e_i = c e_{\{i,i+1\}}$. We can conclude that the set of bicyclic groups split into two conjugacy classes:

$$\big\{\langle ce_I \rangle \mid I \subseteq \{1,\ldots,u-1\}, |I| \text{ is even } \big\} \text{ and } \big\{\langle ce_I \rangle \mid I \subseteq \{1,\ldots,u-1\}, |I| \text{ is odd } \big\}.$$

In particular, $|\Xi| = 2$.

Choose ξ from $\mathrm{Sym}(V)$ which satisfies

$$\xi c \xi^{-1} = ce_1 \text{ and } \xi : (0,0) \mapsto (0,0),\ (0,1) \mapsto (0,1).$$

Then Ξ can be chosen as $\Xi = \{id_V, \xi\}$, where id_V is the identity mapping of V. Also, $\{(v,1),(v+m,1)\}^\xi = \{(v,1),(v+m,1)\}$, and since $(ce_1)^{u+m} = c^u$, $(u,1)^\xi = (0,1)^{(ce_1)^{u+m}\xi} = (0,1)^{\xi c^{u+m}} = (u+m,1)$. Thus $\mathrm{BCay}(\mathbb{Z}_n, S)^\xi = \mathrm{BCay}(\mathbb{Z}_n, \{0, u+m, v, v+m\})$. The theorem follows from Theorem 4.5. □

4.3 Proof of Theorem 4.6

Theorem 4.6 follows from Theorem 4.7 and the following theorem.

Theorem 4.13. *Let* $\mathrm{BCay}(\mathbb{Z}_n, S)$ *be a connected bi-Cayley graph such that* $|S| = 4$ *and* $\mathrm{BCay}(\mathbb{Z}_n, S)$ *is not a BCI-graph. Then* $n = 2m$*, and there exist* $a \in \mathbb{Z}_n^*$ *and* $b \in \mathbb{Z}_n$ *such that* $aS + b = \{0, u, v, v + m\}$ *and the conditions Theorem 4.7(a)-(c) hold.*

Before we prove Theorem 4.13 it is necessary to give three preparatory lemmas. For an element $i \in \mathbb{Z}_n$, we denote by $o(i)$ the order of i viewed as an element of the additive group $\mathbb{Z}_n$. Thus we have $o(i) = n/\gcd(n, i)$.

Lemma 4.14. *If* $R = \{i, n - i, j\}$ *is a generating subset of* $\mathbb{Z}_n$ *and* $o(i)$ *is odd, then* $\mathrm{Cay}(\mathbb{Z}_n, R)$ *is a CI-graph.*

Proof. For short we set $A = \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_n, R))$ and denote by A_0 the stabilizer of $0 \in \mathbb{Z}_n$ in A. Clearly, A_0 leaves R setwise fixed. If A_0 acts on R trivially, then $A \cong \mathbb{Z}_n$, and the lemma follows from Lemma 2.15. If A_0 acts on R transitively, then $\mathrm{Cay}(\mathbb{Z}_n, R)$ is edge-transitive. This condition forces that $\mathrm{Cay}(\mathbb{Z}_n, R)$ is a CI-graph (see [53, page 320]).

We are left with the case that R consists of two orbits under A_0. These orbits must be $\{i, n - i\}$ and $\{j\}$. It is clear that A_0 leaves the subgroups $\langle i\rangle$ and $\langle j\rangle$ fixed; moreover, the latter set is fixed pointwise, and since $o(i)$ is odd, $\langle i\rangle$ consists of $(o(i)-1)/2$ orbits under A_0, each of length 2, and one orbit of length 1. We conclude that $\mathbb{Z}_n = \langle i\rangle \times \langle j\rangle$, and also that A is permutation isomorphic to the permutation direct product $\big((\mathbb{Z}_{o(i)})_{\mathrm{right}} \rtimes \langle\pi\rangle\big) \times (\mathbb{Z}_{o(j)})_{\mathrm{right}}$, where for $\ell \in \{o(i), o(j)\}$, $(\mathbb{Z}_\ell)_{\mathrm{right}}$ is generated by the translation $x \mapsto x+1$, and π is the permutation $x \mapsto -x$. We leave for the reader to verify that the above group has a unique regular cyclic subgroup. The lemma follows from Lemma 2.15. □

Lemma 4.15. *Let* $n = 2m$ *and* $R = \{i, n - i, j, j + m\}$ *be a subset of* $\mathbb{Z}_n$ *such that*

(a) R *generates* $\mathbb{Z}_n$*;*

(b) $o(i)$ *is odd;*

(c) the stabilizer $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_n, R))_0$ *leaves the set* $\{i, n - i\}$ *setwise fixed.*

Then $\mathrm{Cay}(\mathbb{Z}_n, R)$ *is a CI-graph.*

Proof. For short we set $A = \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_n, R))$. Let T be a subset of $\mathbb{Z}_n$ such that $\mathrm{Cay}(\mathbb{Z}_n, R) \cong \mathrm{Cay}(\mathbb{Z}_n, T)$ and let f be an isomorphism from $\mathrm{Cay}(\mathbb{Z}_n, R)$ to $\mathrm{Cay}(\mathbb{Z}_n, T)$ such that $f(0) = 0$. Let us consider the subgraphs

$$\Gamma_1 = \mathrm{Cay}(\mathbb{Z}_n, \{i, n - i\}) \text{ and } \Gamma_2 = \mathrm{Cay}(\mathbb{Z}_n, \{j, j + m\}).$$

By condition (c), the group A preserves both of these subgraphs, that is, $A \le \mathrm{Aut}(\Gamma_\ell)$ for $\ell \in \{1, 2\}$. As f is an isomorphism between two Cayley graphs, $f(\mathbb{Z}_n)_{\mathrm{right}} f^{-1} \le A$. Then $f(\mathbb{Z}_n)_{\mathrm{right}} f^{-1} \le A \le \mathrm{Aut}(\Gamma_\ell)$, implying that f maps Γ_ℓ to a Cayley graph $\mathrm{Cay}(\mathbb{Z}_n, T_\ell)$ for both $\ell \in \{1, 2\}$. Clearly, $T = T_1 \cup T_2$. It was proved by Sun [73] (see also [53]) that every Cayley graph over $\mathbb{Z}_n$ of valency 2 is a CI-graph. Using this, it follows from $\mathrm{Cay}(\mathbb{Z}_n, \{i, n-i\}) \cong \mathrm{Cay}(\mathbb{Z}_n, T_1)$ that $T_1 = a\{i, n-i\}$ for some $a \in \mathbb{Z}_n^*$. Letting $t_1 = ai$, we have $T_1 = \{t_1, n - t_1\}$ such that $o(i) = o(t_1)$. In the same way,

$T_2 = a'\{j, j+m\}$ for some $a' \in \mathbb{Z}_n^*$, and letting $t_2 = a'j$, we have $T_2 = \{t_2, t_2+m\}$ with $o(t_2) = o(j)$. Since $f(0) = 0$, f maps $\{i, n-i\}$ to $T_1 = \{t_1, n-t_1\}$ and $\{j, j+m\}$ to $T_2 = \{t_2, t_2+m\}$.

We claim that the partition of $\mathbb{Z}_n$ into the cosets of $\langle m\rangle$ is a system of blocks for $\mathrm{Aut}(\Gamma_2)$, hence also for the group $A \le \mathrm{Aut}(\Gamma_2)$. Let us put $\bar{A} = \mathrm{Aut}(\Gamma_2)$. Then $\bar{A}_0$ leaves the set $T = \{j, j+m\}$ setwise fixed. Thus the setwise stabilizer $\bar{A}_{\{T\}}$ of the set T in $\bar{A}$ can be written as $\bar{A}_{\{T\}} = \bar{A}_{\{T\}} \cap \bar{A} = \bar{A}_{\{T\}} \cap \bar{A}_0(\mathbb{Z}_n)_{\mathrm{right}} = \bar{A}_0(\bar{A}_{\{T\}} \cap (\mathbb{Z}_n)_{\mathrm{right}}) = \bar{A}_0\langle m_{\mathrm{right}}\rangle$. Here m_{right} is the permutation $x \mapsto x+m$, $x \in \mathbb{Z}_n$. Thus $\bar{A}_0\langle m_{\mathrm{right}}\rangle$ is a subgroup of $\bar{A}$ which clearly contains $\bar{A}_0$. By Theorem 2.5, the orbit of 0 under the group $\bar{A}_0\langle m_{\mathrm{right}}\rangle$ is a block for $\bar{A}$. Now, the required statement follows as the latter orbit is equal to $0^{\bar{A}_0\langle m_{\mathrm{right}}\rangle} = 0^{\langle m_{\mathrm{right}}\rangle} = \langle m\rangle$.

Since the partition of $\mathbb{Z}_n$ into the cosets of $\langle m\rangle$ is a system of blocks for A, f induces an isomorphism from $\mathrm{Cay}(\mathbb{Z}_m, \eta_{n,m}(R))$ to $\mathrm{Cay}(\mathbb{Z}_m, \eta_{n,m}(T))$, we denote this isomorphism by $\bar{f}$. Note that, $\bar{f}(0) = 0$ for the identity element $0 \in \mathbb{Z}_m$.

The set $\eta_{n,m}(R)$ satisfies the conditions (a)-(c) of Lemma 4.14, hence it defines a CI-graph. This means that $\bar{f}$ is equal to a permutation $x \mapsto rx$ for some $r \in \mathbb{Z}_m^*$. Let $s \in \mathbb{Z}_n^*$ such that $\eta_{n,m}(s) = r$. Then $\eta_{n,m}(si) = \eta_{n,m}(s)\eta_{n,m}(i) = \eta_{n,m}(t_1)$, and so the following holds in $\mathbb{Z}_n$:

$$si = t_1 \text{ or } si = t_1 + m. \tag{4.14}$$

The order $o(t_1) = o(i)$ is odd by (b), implying that $o(t_1) \neq o(t_1+m)$, and so $si = t_1$ holds in (4.14). We conclude that $sR = T$, so $\mathrm{Cay}(\mathbb{Z}_n, R)$ is a CI-graph. The lemma is proved. □

Lemma 4.16. *Let $n = 2m$ and $S = \{0, u, v, v+m\}$ such that*

(a) S generates $\mathbb{Z}_n$;

(b) $1 < u < n$, $u \mid n$ but $u \nmid m$;

(c) the stabilizer $\mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, S))_{(0,0)}$ leaves the set $\{(0,1),(u,1)\}$ setwise fixed.

Then $\mathrm{BCay}(\mathbb{Z}_n, S)$ is a BCI-graph.

Proof. Let δ be the partition of V defined in (4.6). Applying Lemma 4.9 with $R = S$, $R_* = \{0, u\}$ and $r = 0$, we obtain that δ is a system of blocks for $A = \mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, S))$. Thus the stabilizer $A_{(0,0)}$ leaves the set V_0 setwise fixed, and we may consider the action of $A_{(0,0)}$ on V_0. The subgraph of $\mathrm{BCay}(\mathbb{Z}_n, S)$ induced by the set V_0 is a cycle of length $2n/u$, thus $A_{(0,0)}$ fixes also the vertex on this cycle antipodal to $(0,0)$. We find that this antipodal vertex is $(u/2+m, 1)$. Therefore, $A_{(0,0)} = A_{(m+u/2,1)}$. By Proposition 3.14, $\mathrm{BCay}(\mathbb{Z}_n, S)$ is a BCI-graph if and only if $\mathrm{Cay}(\mathbb{Z}_n, S - u/2 + m)$ is a CI-graph. The latter set is

$$S - u/2 + m = \big\{\, u/2+m, -u/2+m, v-u/2, v-u/2+m \,\big\}.$$

Since $u \nmid m$, u is even and the order $|u/2+m|$ is odd. Thus we can apply Lemma 4.15 to the set $S - u/2 + m$ (choose $i = u/2+m$ and $j = v - u/2$). This gives us that $S - u/2 + m$ defines a CI-graph. This completes the proof of the lemma. □

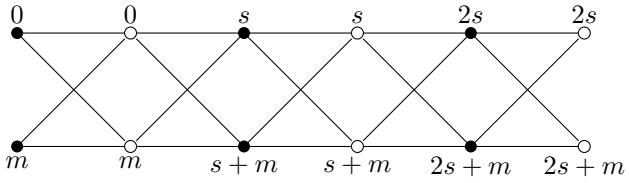

Figure 4.3: The lexicographical product $C_n[K_2^c]$.

Proof of Theorem 4.6. Let S be the subset of $\mathbb{Z}_n$ given in Theorem 4.6. We deal first with the case when the canonical bicyclic group $R(\mathbb{Z}_n)$ is normal in $A = \mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, S))$.

Case 1. $R(\mathbb{Z}_n) \trianglelefteq A$.

By Theorem 4.5, there is a bicyclic group X of A such that $X \neq R(\mathbb{Z}_n)$. Since $R(\mathbb{Z}_n) \trianglelefteq A$, X is generated by a permutation in the form $c^i\varphi_{r,0,s}$, $r \in \mathbb{Z}_n^*$, $s \in \mathbb{Z}_n$, and the order of $\varphi_{r,0,s}$ is at least 2. The permutation $\varphi_{r,0,s}$ acts on both V_0 and V_1 as an affine transformation. This fact together with the connectedness of $\mathrm{BCay}(\mathbb{Z}_n, S)$ imply that, $\varphi_{r,0,s}$ acts faithfully on $S \times \{1\}$. Thus the order of $\varphi_{r,0,s}$ is at most 4. Let o denote this order.

Suppose that $o = 4$. We may assume without loss of generality that $S \times \{1\}$ can be obtained as $S \times \{1\} = \{(0,1)^{\varphi_{r,0,s}^j} \mid j \in \{0,1,2,3\}\}$, and so $S = \{0, s, (r+1)s, (r^2+r+1)s\}$ and $(r^3+r^2+r+1)s = 0$. Since $\mathrm{BCay}(\mathbb{Z}_n, S)$ is connected, $\gcd(s,n) = 1$, and $(r+1)(r^2+1) = 0$. We find that $(c^i\varphi_{r,0,s})^4$ sends $(x,0)$ to $(x + r(r+1)(r^2+1)i), 0) = (x,0)$. Since $X = \langle c^i\varphi_{r,0,s}\rangle$ is a bicyclic group, $n = 4$, and so $\mathrm{BCay}(\mathbb{Z}_n, S) \cong K_{4,4}$. This, however, contradicts that $R(\mathbb{Z}_n) \trianglelefteq A$.

Now, suppose that $o = 3$. If $A_{(0,0)}$ is transitive on $S \times \{1\}$, then it must be regular, see [44, Theorem 4.3]. This implies that $S \times \{1\}$ splits into two orbits under $A_{(0,0)}$ with length 1 and 3, respectively. Let $s \in S$ such that $\{(s,1)\}$ is an orbit under $A_{(0,0)}$. Then $A_{(0,0)} = A_{(s,1)}$, and by Proposition 3.14, $S - s$ does not define a CI-graph. However, in this case the graph $\mathrm{Cay}(\mathbb{Z}_n, S - s)$ is edge-transitive, and thus it is a CI-graph (see [53, page 320]), which is a contradiction.

Finally, suppose that $o = 2$. If $r = 1$, then $2 \mid n$ and $s = m$, where $n = 2m$. This implies that $S \times \{1\}$ is a union of two orbits of $R(\mathbb{Z}_n)^m$, we may write $S = \{0, m, s, s+m\}$. The graph $\mathrm{BCay}(\mathbb{Z}_n, S)$ is then isomorphic to the lexicographical product $C_n[K_2^c]$ of an n-cycle C_n with the graph K_2^c, see Figure 4.3. It is easily seen that then $A_{(0,0)}$ is not faithful on the set $S \times \{1\}$, which is a contradiction.

Let $r \neq 1$. By Lemma 4.12, $8 \mid n$, $r = m+1$ and $s \in \{0, m\}$, where $n = 2m$. We consider only the case when $s = 0$ (the case when $s = m$ can be treated in the same manner). Then V_1 splits into the following orbits under $\varphi_{r,0,s}$:

$$\{(2i,1)\},\ \{(2i+1,1),(2i+1+m,1)\},\ \text{where } i \in \{0,1,\ldots,m-1\}.$$

Since $\mathrm{BCay}(\mathbb{Z}_n, S)$ is connected and cannot be the union $R(\mathbb{Z}_n)^m$-orbits (see above), $S \times \{1\}$ contains one orbit under $\varphi_{r,0,s}$ of length 2, and two orbits of length 1. Let S_1 denote the orbit of length 2 and let $S_2 = S \setminus S_1$. Then we may write $S_1 = \{s, s+m\}$, and $S_2 = \{s', s''\}$, where both s' and s'' are even. Let $u = \gcd(s' - s'', n)$. Then u is

a divisor of n and also $2 \mid u$. There exist $a \in \mathbb{Z}_n^*$ such that $a(s' - s'') \equiv u (\mathrm{mod}\, n)$. Choosing $b = -as''$ (all arithmetic is done in $\mathbb{Z}_n$), we find that $aS_2 + b = \{u, 0\}$. Now, letting $v = as + b$, we get $aS_1 + b = \{v, v + m\}$. We finish the proof of this case by showing that the set $R = aS + b = \{0, u, v, v + m\}$ satisfies the conditions Theorem 4.6(a)-(c).

(a): As $\mathrm{BCay}(\mathbb{Z}_n, S)$ is connected, $\mathrm{BCay}(\mathbb{Z}_n, R)$ is also connected. This implies that $\{u, v\}$ is a generating set of $\mathbb{Z}_n$.

(c): Since $R(\mathbb{Z}_n) \trianglelefteq A$, $R(\mathbb{Z}_n) \trianglelefteq \mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, R))$. To the contrary assume that the stabilizer $\mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, R))_{(0,0)}$ does not leave $\{(0, 1), (u, 1)\}$ setwise fixed. Thus there exists some $g \in A_{(0,0)}$ and thus the image of $(v, 1)$ under g is in $\{(0, 1), (u, 1)\}$. Letting $(w_1, 1) = (v, 1)^g$ and $(w_2, 1) = ((v + m), 1)^g$, we find that $w_1 - w_2 = m$, and from this that $u = m$. However, then $\mathrm{BCay}(\mathbb{Z}_n, R) \cong C_n[K_2^c]$, which we have already excluded above. Thus $\mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, R))_{(0,0)}$ fixes setwise $\{(0, 1), (u, 1)\}$.

(b): We have already showed (see previous paragraph) that $u \neq m$ and $1 < u$. Since S does not define a BCI-graph, neither does R. This also implies that $u \mid m$ by Lemma 4.12, and we conclude that $1 < u < m$ and $u \mid m$, as required.

Case 2. $R(\mathbb{Z}_n) \not\trianglelefteq A$.

Let $A_{(0,0)}$ act transitively on $S \times \{1\}$. This gives that $\mathrm{BCay}(\mathbb{Z}_n, S)$ is edge-transitive. Since $R(\mathbb{Z}_n) \not\trianglelefteq A$, $D \not\trianglelefteq A$, in other words, $\mathrm{BCay}(\mathbb{Z}_n, S)$ is non-normal as a Cayley graph over the dihedral group D, where $D = \langle c, d \rangle$. We apply [45, Theorem 1.2], and obtain that $\mathrm{BCay}(\mathbb{Z}_n, S)$ is either isomorphic to $K_n[K_2^c]$, or to one of 5 graphs of orders $10, 14, 26, 28$ and 30, respectively. Suppose that the former case holds. Then $n = 2m$, and we obtain quickly that S consists of two $R(\mathbb{Z}_n)^m$-orbits. Then S can be mapped by an affine transformation to a set $\{0, m, v, v + m\}$, where $\langle m, v \rangle \cong \mathbb{Z}_n$. Then v or $v + m$ is a generating element of $\mathbb{Z}_n$, and so S can actually be mapped by an affine transformation to $\{0, m, 1, 1 + m\}$. Now, the same holds for any set T with $\mathrm{BCay}(\mathbb{Z}_n, T) \cong \mathrm{BCay}(\mathbb{Z}_n, S) \cong K_n[K_2^c]$, contradicting that $\mathrm{BCay}(\mathbb{Z}_n, S)$ is not a BCI-graph. In the latter case, a direct computation by the computer package Magma [11] shows that none of these graphs is possible (in fact, in each case the corresponding subset S defines a BCI-graph).

The set $S \times \{1\}$ cannot split into two orbits under $A_{(0,0)}$ having size 1 and 3, respectively (see the argument above). Thus we are left with the case that $S = S_1 \cup S_2$, $|S_1| = |S_2|$, and $A_{(0,0)}$ leaves both sets S_1 and S_2 setwise fixed. For $i \in \{1, 2\}$, let $n_i = |\langle S_i - S_i \rangle|$, $n_1 \leq n_2$, where $S_i - S_i = \{a - b \mid a, b \in S_i\}$.

We claim that $n_1 = 2$. To the contrary assume that $n_1 > 2$. We prove first that $R(\mathbb{Z}_n)^{n/n_1} \trianglelefteq A$. Apply Lemma 4.9 with $R = S$, $R_* = S_1$ and $r = s_1 \in S_1$. We obtain that the partition

$$\delta = \left\{ X \cup X^{\psi_{1,s_1,-s_1}} \mid X \in \mathrm{Orb}(R(\mathbb{Z}_n)^{n/n_1}, V) \right\},$$

is a system of blocks for A. Let us consider the action of $A_{(\delta)}$ (the kernel of A acting on δ) on the block of δ which contains $(0, 0)$. Denote this block by Δ, and by Δ' the block which contains $(s, 1)$ for some $s \in S_2$. Notice that, the subgraph of $\mathrm{BCay}(\mathbb{Z}_n, S)$ induced by any block of δ is a cycle of length $2n_1$, and when deleting

these cycles, the rest splits into pairwise disjoint cycles of length $2n_2$. Let Σ denote the unique $(2n_2)$-cycle through $(s,1)$. Now, suppose that $g \in A_{(\delta)}$ which fixes Δ pointwise. If $V(\Sigma) \cap \Delta = \{(0,0)\}$, then g must fix the edge $(0,0)(s,1)$, and so fixes also $(s,1)$. If $V(\Sigma) \cap \Delta \neq \{(0,0)\}$, then $|V(\Sigma) \cap \Delta| = n_2 > 2$. This implies that g fixes every vertex on Σ, in particular, also $(s,1)$. The block Δ' has at least n_1 vertices having a neighbour in Δ, hence by the previous argument we find that all are fixed by g. Since $n_1 > 2$, Δ' is fixed pointwise by g. It follows, using the connectedness of $\mathrm{BCay}(\mathbb{Z}_n, S)$, that g is the identity mapping, hence that $A_{(\delta)}$ is faithful on Δ. Thus $R(\mathbb{Z}_n)^{n/n_1}$ is a characteristic subgroup of $A_{(\delta)}$, and since $A_{(\delta)} \trianglelefteq A$, $R(\mathbb{Z}_n)^{n/n_1} \trianglelefteq A$.

Let A^+ be the subgroup of A that fixes setwise the colour classes V_0 and V_1. We consider $N = A^+ \cap Z_A(R(\mathbb{Z}_n)^{n/n_1})$. Then $R(\mathbb{Z}_n) \leq N$ and $N \trianglelefteq A$. Pick $g \in N_{(0,0)}$ such that g acts non-trivially on $S \times \{1\}$. Since N centralizes $R(\mathbb{Z}_n)^{n/n_1}$, g fixes pointwise the orbit of $(0,0)$ under $R(\mathbb{Z}_n)^{n/n_1}$, and hence also Δ. Then g^2 fixes $S \times \{1\}$ pointwise, and so also Δ'. We conclude that g^2 is the identity mapping, and thus that either $N = R(\mathbb{Z}_n)$, or $N = R(\mathbb{Z}_n) \rtimes \langle g \rangle$. The case $N = R(\mathbb{Z}_n)$ is impossible because $R(\mathbb{Z}_n) \not\trianglelefteq A$. Let $N = R(\mathbb{Z}_n) \rtimes \langle g \rangle$. Then $(S_i \times \{1\})^g = S_i \times \{1\}$ (for both $i \in \{1,2\}$), hence S_i is a union of $\langle g \rangle$-orbits. As g normalizes $R(\mathbb{Z}_n)$ and fixes $(0,0)$, $g = \varphi_{r,0,s}$. Recall that the order of g is equal to 2. If $r \neq 1$, then by Lemma 4.12, either $R(\mathbb{Z}_n)$ is the unique cyclic subgroup of N, or $8 \mid n$, $r = n/2 + 1$ and $s = 0$ or $s = n/2$. In the former case $R(\mathbb{Z}_n)$ is characteristic in N, and since $N \trianglelefteq A$, $R(\mathbb{Z}_n) \trianglelefteq A$, a contradiction. Therefore, we are left with the case that $r = 1$ (and so $s = n/2$), or $8 \mid n$, $r = n/2 + 1$ and $s = 0$ or $s = n/2$. Then every $\langle g \rangle$-orbit is of length 1 or 2, and if it is of length 2, then is in the form $\{(j,0),(j+m,0)\}$ or $\{(j,1),(j+m,1)\}$ as we have proved in Case 1. Since $n_i > 2$, we see that $S_i \times \{1\}$ must be fixed pointwise by g for both $i \in \{1,2\}$. This, however, contradicts that g was assumed to act non-trivially on $S \times \{1\}$; and so $n_1 = 2$.

This means that $2 \mid n$, say $n = 2m$, and the group generated by the set $S_1 - S_1 = \{x - y : x, y \in S_1\}$ is equal to $\{0, m\}$. Then we can write $S_1 = \{s, s+m\}$. It can be proved as before that there exist $a \in \mathbb{Z}_n^*$ and $b \in \mathbb{Z}_n$ such that $aS_2 + b = \{0, u\}$ for some divisor u of n. Then, letting $v = as + b$, we get $aS_1 + b = \{v, v+m\}$. We finish the proof of this case by showing that the set $R = aS + b = \{0, u, v, v+m\}$ satisfies the conditions Theorem 4.6(a)-(c).

(a): As $\mathrm{BCay}(\mathbb{Z}_n, S)$ is connected, $\mathrm{BCay}(\mathbb{Z}_n, R)$ is also connected. This implies that $\{u, v\}$ is a generating set of $\mathbb{Z}_n$.

(c): Since S_1 and S_2 are left fixed setwise by A, $\mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, R))_{(0,0)}$ leaves the set $\{(0,1),(u,1)\}$ setwise fixed.

(b): If $u = 1$, then $\mathrm{Aut}(\mathrm{BCay}(\mathbb{Z}_n, \{0,u\})) \leq D_{4n}$. But then $R(\mathbb{Z}_n) \trianglelefteq A$, which is a contradiction. We conclude that $1 < u$, and by Lemma 4.16, $u \mid m$ also holds, i. e., $1 < u < m$ and $u \mid m$, as required. □

Chapter 5

Nilpotent 3-BCI-groups

Let G be a 3-BCI-group, i. e., every bi-Cayley graph over G valency at most 3 has the BCI-property. Jin and Liu [35] proved a Sylow 2-subgroup of G is $\mathbb{Z}_{2^r}$, or $\mathbb{Z}_2^4$ or Q_8; and they also proved in [36] that a Sylow p-subgroup for an odd prime is homocyclic, i. e., a direct product of cyclic groups of the same order. Therefore, if G is nilpotent, then it is necessarily a direct product of the groups described above. In this chapter we prove that the converse implication also holds.

Theorem 5.1. *Every finite group $G = U \times V$ is a 3-BCI-group, if U is an abelian group of odd order whose Sylow p-subgroups are homocyclic, and V is trivial or one of the following groups: $\mathbb{Z}_{2^r}$, $\mathbb{Z}_2^r$ and Q_8.*

Throughout this chapter $\mathcal{C}$ will denote the set of all groups $G = U \times V$, where U is an abelian group of odd order whose Sylow p-subgroups are homocyclic, and V is either trivial or one of the groups $\mathbb{Z}_{2^r}$, $\mathbb{Z}_2^r$ and Q_8. Furthermore, $\mathcal{C}_{\mathrm{sub}}$ will denote set of all groups that have an overgroup in $\mathcal{C}$.

5.1 Preparatory lemmas

Our first lemma generalizes Lemma 3.14.

Lemma 5.2. *Let $\Gamma = \mathrm{BCay}(G, S)$ such that there exists an involution $\tau \in \mathrm{Aut}(\Gamma)$ which normalizes $R(G)$ and $(1_G, 0)^\tau = (1_G, 1)$. Suppose, in addition, that $\mathrm{Aut}(\Gamma)_{(1_G,0)} = \mathrm{Aut}(\Gamma)_{(1_G,1)}$. Then $\mathrm{BCay}(G, S)$ is a BCI-graph whenever $\mathrm{Cay}(G, S)$ is a CI-graph.*

Proof. Set $A = \mathrm{Aut}(\Gamma)$ and $A^+ = A_{\{G\times\{0\})\}}$, and let us suppose that $\mathrm{Cay}(G, S)$ is a CI-graph. Recall that, by $\mathcal{S}(A)$ we denote the set of all semiregular groups in A with orbits $G \times \{0\}$ and $G \times \{1\}$. Let $X \in \mathcal{S}(A)$ such that $X \cong G$. Obviously, $X, R(G) \leq A^+$. The normalizer $N_A(R(G)) \geq \langle R(G), \tau\rangle$, hence it is transitive on $V(\Gamma)$. Thus, by Lemma 3.5, we are done if we show that X and $R(G)$ are conjugate in A^+.

In order to prove this we define a faithful action of A^+ on G as follows. Let $\Delta = \{(1_G, 0), (1_G, 1)\}$ and consider the setwise stabilizer $A_{\{\Delta\}}$. Since $A_{(1_G,0)} = A_{(1_G,1)}$, $A_{(1_G,0)} \leq A_{\{\Delta\}}$. By Theorem 2.5, the orbit of $(1_G, 0)$ under $A_{\{\Delta\}}$ is a block for A. Since τ switches $(1_G, 0)$ and $(1_G, 1)$, this orbit is equal to Δ, and the system of blocks

induced by Δ is $\delta = \{\Delta^{R(x)} \mid x \in G\} = \big\{\{(x,0),(x,1)\} \mid x \in G\big\}$. Now, define the action of A^+ on G by letting $x^\sigma = x'$, where $x \in G$ and $\sigma \in A^+$, if σ maps the block $\{(x,0),(x,1)\}$ to the block $\{(x',0),(x',1)\}$. We will write $\bar{\sigma}$ for the image of σ under the corresponding permutation representation, and let $\bar{B} = \{\bar{\sigma} : \sigma \in B\}$ for a subgroup $B \leq A^+$. It is easily seen that this action is faithful. Therefore, X and $R(G)$ are conjugate in A^+ exactly when $\bar{X}$ and $R(\bar{G})$ are conjugate in $\bar{A^+}$. Also, $R(\bar{G}) = G_{\mathrm{right}}$, and $\bar{X}$ is regular on G. We finish the proof by showing that $\bar{A^+} = \mathrm{Aut}(\mathrm{Cay}(G,S))$. Then the conjugacy of $\bar{X}$ and $R(\bar{G})$ follows by Lemma 2.15 and the assumption that $\mathrm{Cay}(G,S)$ is a CI-graph.

Pick an automorphism $\sigma \in A^+$ and an arc (x,sx) of $\mathrm{Cay}(G,S)$. Then the edge $\{(x,0),\,(sx,1)\}$ of Γ is mapped by σ to an edge $\{(x',0),(s'x',1)\}$ for some $x' \in G$ and $s' \in S$. Hence $\bar{\sigma} : x \mapsto x'$ and $sx \mapsto s'x'$, i.e., it maps the arc (x,sx) to the arc $(x',s'x')$. We have just proved that $\bar{\sigma} \in \mathrm{Aut}(\mathrm{Cay}(G,S))$, and hence $\bar{A^+} \leq \mathrm{Aut}(\mathrm{Cay}(G,S))$. In order to establish the relation "$\geq$", for an arbitrary automorphism $\rho \in \mathrm{Aut}(\mathrm{Cay}(G,S))$, define the permutation π of $G \times \{0,1\}$ by $(x,i)^\pi = (x^\rho, i)$ for all $x \in G$ and $i \in \{0,1\}$. Repeating the previous argument we obtain that $\pi \in A$. It is clear that $\pi \in A^+$ and $\bar{\pi} = \rho$. Thus $\bar{A^+} \geq \mathrm{Aut}(\mathrm{Cay}(G,S))$, and so $\bar{A^+} = \mathrm{Aut}(\mathrm{Cay}(G,S))$. The lemma is proved. □

Lemma 5.3. *Let Γ be a cubic bipartite graph with bipartition classes Δ_i, $i = 1,2$, and $X \leq \mathrm{Aut}(\Gamma)$ be a semiregular subgroup whose orbits are Δ_i, $i = 1, 2$, and $X \in \mathcal{C}_{\mathrm{sub}}$. Then $\mathrm{Aut}(\Gamma)$ has an element τ_X which satisfies:*

(i) every subgroup of X is normal in $\langle X, \tau_X\rangle$;

(ii) $\langle X, \tau_X\rangle$ is regular on $V(\Gamma)$.

Proof. It is straightforward to show that $\Gamma \cong \mathrm{BCay}(X,S)$ for some subset $S \subseteq X$ with $1_X \in S$ and $|S| = 3$. Moreover, there is an isomorphism from Γ to $\mathrm{BCay}(X,S)$ which induces a permutation isomorphism from X to $R(X)$. Therefore, it is sufficient to find $\tau \in \mathrm{Aut}(\mathrm{BCay}(X,S))$ for which every subgroup of $R(X)$ is normal in $\langle R(X), \tau\rangle$; and $\langle R(X), \tau\rangle$ is regular on $V(\mathrm{BCay}(X,S))$.

Since $X \in \mathcal{C}_{\mathrm{sub}}$, $X = U \times V$, where U is an abelian group of odd order, and V is trivial or one of $\mathbb{Z}_{2^r}$, $\mathbb{Z}_2^r$ and Q_8. We prove below the existence of an automorphism $\iota \in \mathrm{Aut}(X)$, which maps the set S to its inverse S^{-1}. Let π_U and π_V denote the projections $U \times V \to U$ and $U \times V \to V$ respectively. It is sufficient to find an automorphism $\iota_1 \in \mathrm{Aut}(U)$ which maps $\pi_U(S)$ to $\pi_U(S)^{-1}$, and an automorphism $\iota_2 \in \mathrm{Aut}(V)$ which maps $\pi_V(S)$ to $\pi_V(S)^{-1}$. Since U is abelian, we are done by choosing ι_1 to be the automorphism $x \mapsto x^{-1}$. If V is abelian, then let $\iota_2 : x \mapsto x^{-1}$. Otherwise, $V \cong Q_8$, and since $|\pi_V(S) \setminus \{1_V\}| \leq 2$, it follows that $\pi_V(S)$ is conjugate to $\pi_V(S)^{-1}$ in V. This ensures that ι_2 can be chosen to be some inner automorphism. Now, define ι by setting its restriction $\iota|_U$ to U as $\iota|_U = \iota_1$, and its restriction $\iota|_V$ to V as $\iota|_V = \iota_2$. Define the permutation τ of $X \times \{0,1\}$ by

$$(x,i)^\tau = \begin{cases} (x^\iota, 1) & \text{if } i = 0, \\ (x^\iota, 0) & \text{if } i = 1. \end{cases}$$

The vertex $(x,0)$ of $\mathrm{BCay}(X,S)$ has neighbourhood $(Sx,1)$. This is mapped by τ to the set $(S^{-1}x^\iota,0)$, which is equal to the neighbourhood of $(x^\iota,1)$. We have proved that $\tau \in \mathrm{Aut}(\mathrm{BCay}(X,S))$.

It follows from its construction that τ is an involution. Fix an arbitrary subgroup $Y \leq X$, and pick $y \in Y$. We may write $y = y_U y_V$ for some $y_U \in U$ and $y_V \in V$. Then $\langle y_U, y_V\rangle \leq Y$, since y_U and y_V commute and $\gcd(|U|,|V|) = 1$. Also, $(y_U)^{\iota_1} = y_U^{-1}$ and $(y_V)^{\iota_2} \in \langle y_V\rangle$, implying that $y^\iota = (y_U)^{\iota_1}(y_V)^{\iota_2} \in \langle y_U, u_V\rangle \leq Y$. We conclude that ι maps Y to itself. Thus $\tau^{-1}R(y)\tau = \tau R(y)\tau = R(y^\iota)$ is in $R(Y)$, and τ normalizes $R(Y)$. Since $X \in \mathcal{C}_{\mathrm{sub}}$, $R(Y)$ is also normal in $R(X)$, and part (i) follows.

For part (ii), observe that $|\langle R(X),\tau\rangle| = 2|X| = |V(\mathrm{BCay}(X,S))|$. Clearly, $\langle R(X),\tau\rangle$ is transitive on $V(\mathrm{BCay}(X,S))$, so it is regular. □

In the next lemma we recall some properties of normal quotients of cubic bi-Cayley graphs. The proof of the lemma is rather straightforward, and thus it is omitted. For instance, it can be deduced from [58, Theorem 9]).

Lemma 5.4. *Let $\Gamma = \mathrm{BCay}(G,S)$ be a connected arc-transitive graph, G be any finite group, $|S| = 3$, and let $N < R(G)$ be a subgroup which is normal in $\mathrm{Aut}(\Gamma)$. Then the following hold for the normal quotient Γ_N:*

(i) Γ_N is a connected cubic arc-transitive graph. Moreover, if Γ is $(\mathrm{Aut}(\Gamma),s)$-transitive, then Γ_N is $(\mathrm{Aut}(\Gamma)/N,s)$-arc-transitive.[1]

(ii) Γ_N is isomorphic to the bi-Cayley graph $\mathrm{BCay}(G/M,\pi_{G/M}(S))$, where $M < G$ is the subgroup that $N = \{R(x) \mid x \in M\}$, and $\pi_{G/M}$ is the natural projection from G to G/M (clearly, $M \trianglelefteq G$ as $R(M) = N \trianglelefteq R(G)$).

(iii) N is equal to the kernel of $\mathrm{Aut}(\Gamma)$ acting on the set of N-orbits.

5.2 The proof of Theorem 5.1

The proof of Theorem 5.1 in the case of arc-transitive graphs will be based on three lemmas about cubic connected arc-transitive bi-Cayley graphs to be proved below. In these lemmas we we keep the following notation:

(∗) $\Gamma = \mathrm{BCay}(G,S)$ is a connected arc-transitive graph, where $G \in \mathcal{C}_{\mathrm{sub}}$ and $|S| = 3$.

Recall that, $\mathcal{S}(\mathrm{Aut}(\Gamma))$ is the set of all semiregular subgroups of $\mathrm{Aut}(\Gamma)$ whose orbits are $G\times\{0\}$ and $G\times\{1\}$.

Lemma 5.5. *With notation (∗), let δ be a system of blocks for $\mathrm{Aut}(\Gamma)$ induced by a block properly contained in $G\times\{0\}$, and X be in $\mathcal{S}(\mathrm{Aut}(\Gamma))$ such that $X \in \mathcal{C}_{\mathrm{sub}}$. Then the kernel $\mathrm{Aut}(\Gamma)_\delta < X$. Moreover, if δ is non-trivial, then $\mathrm{Aut}(\Gamma)_\delta$ is also non-trivial.*

[1] The group $\mathrm{Aut}(\Gamma)$ acts on the set of N-orbits which is, by definition, coincides with the vertex set $V(\Gamma_N)$. By part (iii) of the lemma, the image of the action is isomorphic to $\mathrm{Aut}(\Gamma)/N$. In what follows, by some abuse of notation, this image will also be denoted by $\mathrm{Aut}(\Gamma)/N$, and in this context we shall write $\mathrm{Aut}(\Gamma)/N \leq \mathrm{Aut}(\Gamma_N)$.

PROOF. Set $A = \mathrm{Aut}(\Gamma)$. Let $Y = X \cap A_{\{\Delta\}}$, where $\Delta \in \delta$ with $\Delta \subset G \times \{0\}$. Then Δ is equal to an orbit of Y, and $|Y| = |\Delta|$ because $\Delta \subset G \times \{0\}$ and X is regular on $G \times \{0\}$. Formally, $\Delta = \mathrm{Orb}(Y, v)$ for some vertex $v \in \Delta$.

Let $\tau_X \in A$ be the automorphism defined in Lemma 5.3, and set $L = \langle X, \tau_X \rangle$. The group L is regular on $V(\Gamma)$, and $Y \trianglelefteq L$. These yield

$$\delta = \{\Delta^l \mid l \in L\} = \{\mathrm{Orb}(Y, v)^l \mid l \in L\} = \{\mathrm{Orb}(Y, v^l) \mid l \in L\}.$$

From this $Y \leq A_\delta$. This shows that, if $|Y| = |\Delta| \neq 1$, then A_δ is non-trivial. Since δ has more than 2 blocks, and Γ is a connected and cubic graph, it is known that A_δ is semiregular. These imply that $A_\delta = Y < X$. □

Corollary 5.6. *With notation* $(*)$*, let* $N < R(G)$ *be normal in* $\mathrm{Aut}(\Gamma)$*, and* X *be in* $\mathcal{S}(\mathrm{Aut}(\Gamma))$ *such that* $X \in \mathcal{C}_{\mathrm{sub}}$*. Then* $N < X$*.*

PROOF. Let δ be the system of blocks for $\mathrm{Aut}(\Gamma)$ consisting of the N-orbits, see Theorem 2.6. Then $A_\delta = N$ because of Lemma 5.4(iii). The corollary follows directly from Lemma 5.5. □

We denote by Q_3 the graph of the cube and by $\mathcal{H}$ the Heawood graph. The latter is graph is the incidence graph of the Fano plane, it is the unique arc-transitive cubic graph on 14 points [14]. Recall that, the *core* of a subgroup $H \leq K$ in the group K is the largest normal subgroup of K contained in H.

Lemma 5.7. *With notation* $(*)$*, suppose that* $R(G)$ *is not normal in* $\mathrm{Aut}(\Gamma)$*, and let* N *be the core of* $R(G)$ *in* $\mathrm{Aut}(\Gamma)$*. Then* $(R(G)/N, \Gamma_N)$ *is isomorphic to one of the pairs* $(\mathbb{Z}_3, K_{3,3})$*,* $(\mathbb{Z}_4, Q_3)$ *and* $(\mathbb{Z}_7, \mathcal{H})$*.*

PROOF. Set $A = \mathrm{Aut}(\Gamma)$. Consider the normal quotient Γ_N, and suppose that $M \leq R(G)$ such that $N \leq M$ and $M/N \trianglelefteq \mathrm{Aut}(\Gamma_N)$ (here $M/N \leq A/N \leq \mathrm{Aut}(\Gamma_N)$, see Footnote 1 in the previous page). This in turn implies that, $M/N \trianglelefteq A/N$, $M \trianglelefteq A$, and $M = N$. We conclude that, Γ_N is a bi-Cayley graph of $R(G)/N$, $R(G)/N$ is in $\mathcal{C}_{\mathrm{sub}}$, and $R(G)/N$ has trivial core in $\mathrm{Aut}(\Gamma_N)$. This shows that it is sufficient to prove Lemma 5.7 in the particular case when N is trivial. For the rest of the proof we assume that the core N is trivial, and we write $N = 1$.

By Theorem 2.7, Γ is k-regular for some $k \leq 5$. Set $A^+ = A_{\{G \times \{0\}\}}$. It follows from the connectedness of Γ that $A = \langle A^+, \tau_{R(G)} \rangle$, where $\tau_{R(G)} \in A$ is the automorphism defined in Lemma 5.3. Let M be the core of $R(G)$ in A^+. Then $M \trianglelefteq A$, since M is normalized by $\tau_{R(G)}$, see Lemma 5.3(i), and $A = \langle A^+, \tau_{R(G)} \rangle$. Thus $M \leq N = 1$, hence M is also trivial.

Let us consider A^+ acting on the set $[A^+ : R(G)]$ of right $R(G)$-cosets in A^+. This action is faithful because M is trivial. The corresponding degree is equal to $|A^+ : R(G)|$, which is $3 \cdot 2^{k-1}$ because Γ is k-regular. Since $R(G)$ acts as a point stabilizer in this action, we have an embedding of G into $S_{3 \cdot 2^{k-1}-1}$. We will write below that $G \leq S_{3 \cdot 2^{k-1}-1}$.

It is well-known that $A_{(1_G,0)}$ is determined uniquely by k, namely, $A_{(1_G,0)} \cong \mathbb{Z}_3$, or S_3, or D_{12}, or S_4, or $S_4 \times \mathbb{Z}_2$ correspondingly to $k = 1, 2, 3, 4$ or 5. We go through each case.

Case 1. $k = 1$.

This case can be excluded at once by observing that we have $G \leq S_2$ by the above discussion, which contradicts the obvious bound $|G| \geq 3$.

Case 2. $k = 2$.

In this case $G \leq S_5$. Using also that $G \in \mathcal{C}_{\mathrm{sub}}$, we see that G is abelian, hence $|G| \leq 6$, $|V(\Gamma)| \leq 12$. We obtain by [14, Table] that $\Gamma \cong Q_3$, and $G \cong \mathbb{Z}_4$.

Case 3. $k = 3$.

Then $A^+ = R(G)A_{(1_G,0)} = R(G)D_{12}$, a product of a nilpotent and a dihedral subgroup. By Theorem 2.2, A^+ is solvable. Assume for the moment that A^+ is imprimitive on $G \times \{0\}$. This implies that A is also imprimitive on $V(\Gamma)$ and it has a non-trivial block system δ which has a block properly contained in $G \times \{0\}$. Lemma 5.5 gives that $A_\delta < R(G)$, and A_δ is non-trivial. This, however, contradicts that the core $N = 1$. Thus A^+ is primitive on $G \times \{0\}$. Using that A^+ is also solvable, we find that G is a p-group. We see that G is either abelian or it is Q_8. In the latter case $|V(\Gamma)| = 16$, and Γ is isomorphic to the Moebius-Kantor graph, which is, however, 2-regular, see [14, Table]. Therefore, G is an abelian p-group. Let $S = \{s_1, s_2, s_3\}$. Since G is abelian, in Γ we find the closed walk:

$$\big((1_G,0),(s_1,1),(s_2^{-1}s_1,0),(s_3s_2^{-1}s_1,1) = (s_1s_2^{-1}s_3,1),(s_2^{-1}s_3,0),(s_3,1)\big).$$

Thus the girth of Γ is equal to 4 or 6 (3 and 5 are impossible as the graph is bipartite).

It was proved in [15, Theorem 2.3] that the Pappus graph on 18 points and the Desargues graph on 20 points are the only 3-regular cubic graphs of girth 6. For the latter graph $|G| = 10$, contradicting that G is a p-group. We can exclude the former graph by the help of Magma, namely, we computed that the Pappus graph has no abelian semiregular automorphism group of order 9 which has trivial core in the full automorphism group.

Thus Γ is of girth 4. It is well-known that there are only three cubic connected arc-transitive graphs of girth 4 (e. g., see [47, page 163]): K_4, $K_{3,3}$ and Q_3. We get at once that $\Gamma \cong K_{3,3}$ and $G \cong \mathbb{Z}_3$.

Case 4. $k = 4$.

It is sufficient to show that G is abelian. Then by the above reasoning Γ is of girth 6, and as the Heawood graph is the only cubic 4-regular graph of girth 6 (see [15, Theorem 2.3]), we get at once that $\Gamma \cong \mathcal{H}$ and $G \cong \mathbb{Z}_7$.

Assume, towards a contradiction, that G is non-abelian. Thus $G = U \times V$, where U is an abelian group of odd order, and $V \cong Q_8$. We have already shown above that A^+ is primitive on $G \times \{0\}$. In other words, Γ is a 4-transitive bi-primitive cubic graph. Two possibilities can be deduced from the list of 4-transitive bi-primitive graphs given in [52, Theorem 1.4]:

- Γ is the *standard double cover* of a connected vertex-primitive cubic 4-regular graph, in which case $A = A^+ \times \langle \eta \rangle$ for an involution η; or
- Γ isomorphic to the *sextet graph* $S(p)$ [9], where $p \equiv \pm 7 (\mathrm{mod}\ 16)$, in which case $A \cong \mathrm{PGL}(2, \mathrm{p})$, and $A^+ \cong \mathrm{PSL}(2, p)$.

The second possibility cannot occur, because then $A^+ \cong \mathrm{PSL}(2,p)$, whose Sylow 2-subgroup is a dihedral group (cf. [33, Satz 8.10]), which contradicts that $R(V) \leq R(G) \leq A^+$, and $V \cong Q_8$.

It remains to exclude the first possibility. We may assume, by replacing S with xS for a suitable $x \in G$ if necessary, that η switches $(1_G, 0)$ and $(1_G, 1)$. Since η commutes with $R(G)$, we find $(x,1)^\eta = (1_G,1)^{R(x)\eta} = (1_G,1)^{\eta R(x)} = (1_G,0)^{R(x)} = (x,0)$ for every $x \in G$. Let $s \in S$. Then $(1_G,0) \sim (s,1)$, hence $(1_G,1) = (1_G,0)^\eta \sim (s,1)^\eta = (s,0)$, which shows that $s \in S^{-1}$, and thus $S = S^{-1}$. Thus there exists $s \in S$ of order $o(s) \leq 2$. Put $T = s^{-1}S = sS$. Then $1_G \in T$, and since Γ is connected, $G = \langle T \rangle$. Notice that $s \in Z(G)$. This implies that $T^{-1} = S^{-1}s = sS = T$, and thus $\pi_V(T)$ satisfies $1_V \in \pi_V(T)$ and $\pi_V(T) = \pi_V(T)^{-1}$. Since $V \cong Q_8$, this implies that $\langle \pi_V(T) \rangle \neq V$, a contradiction to $G = \langle T \rangle$. This completes the proof of this case.

Case 5. $k = 5$.

In this case Γ is a 5-transitive bi-primitive cubic graph. It was proved in [52, Corollary 1.5] that Γ is isomorphic to either the $\mathrm{P\Gamma L}(2,9)$-graph on 30 points (also known as Tutte's 8-Cage), or the standards double cover of the $\mathrm{PSL}(3,3).\mathbb{Z}_2$-graph on 468 points. These graphs are of girth 8 and 12 respectively (see [14, Table]). Also, in both cases $8 \nmid |G|$, hence G is abelian, which, however, implies that Γ cannot be of girth larger than 6. This proves that this case does not occur. □

For a group A and a prime p dividing $|A|$, we let A_p denote a Sylow p-subgroup of A.

Lemma 5.8. *With notation* $(*)$*, let* $X \in \mathcal{S}(\mathrm{Aut}(\Gamma))$ *such that* $X \in \mathcal{C}_{\mathrm{sub}}$ *and* $X_2 \cong G_2$*. Then* X *and* $R(G)$ *are conjugate in* $\mathrm{Aut}(\Gamma)$*.*

Remark 5.9. We remark that, the assumption $X_2 \cong G_2$ cannot be deleted. The Möbius-Kantor graph is a bi-Cayley graph of the group Q_8, which has a semiregular cyclic group of automorphisms of order 8 which preserves the bipartition classes.

Proof. Set $A = \mathrm{Aut}(\Gamma)$. The proof is split into two parts according to whether $R(G)$ is normal in A.

Case 1. $R(G)$ is not normal in A.

Let N be the core of $R(G)$ in A. By Corollary 5.6, $N < X \cap R(G)$. Therefore, it is sufficient to show that

$$X/N \text{ and } R(G)/N \text{ are conjugate in } A/N. \tag{5.1}$$

Recall that, the group $A/N \leq \mathrm{Aut}(\Gamma_N)$, where Γ_N is the normal quotient of Γ induced by N (see Lemma 5.4). Both groups X/N and $R(G)/N$ are semiregular whose orbits are the bipartition classes of Γ_N. Also notice that, $R(G)/N$ cannot be normal in A/N, otherwise $R(G)$ will be normal in A.

According to Lemma 5.7, $(R(G)/N, \Gamma_N) \cong (\mathbb{Z}_3, K_{3,3})$, or $(\mathbb{Z}_4, Q_3)$, or $(\mathbb{Z}_7, \mathcal{H})$. Thus (5.1) follows immediately from Sylow Theorems when $(R(G)/N, \Gamma_N) \cong (\mathbb{Z}_7, \mathcal{H})$.

Let $(R(G)/N, \Gamma_N) \cong (\mathbb{Z}_3, K_{3,3})$. Since $R(G)/N$ is not normal in A/N, and Γ_N is $(A/N, 1)$-arc-transitive, we compute by Magma that either $A/N = \mathrm{Aut}(\Gamma_N)$, or it is a subgroup of $\mathrm{Aut}(\Gamma_N)$ of index 2. In both cases A/N has one conjugacy class

of semiregular subgroups whose orbits are the bipartition classes of Γ_N. Thus (5.1) holds.

Let $(R(G)/N, \Gamma_N) \cong (\mathbb{Z}_4, Q_3)$. Since $X_2 \cong G_2$, $X/N \cong R(G)/N \cong \mathbb{Z}_4$. Using this and that Γ_N is $(A/N, 1)$-arc-transitive, we compute by MAGMA that $A/N = \mathrm{Aut}(\Gamma_N)$, and that $\mathrm{Aut}(\Gamma_N)$ has one conjugacy class of semiregular cyclic subgroups whose orbits are the bipartition classes of Γ_N. Thus (5.1) holds also in this case.

CASE 2. $R(G)$ is normal in A.

We have to show that $X = R(G)$. Notice that, X contains every proper subgroup $K < R(G)$ which is characteristic in $R(G)$. Indeed, since $R(G) \trianglelefteq A$, we have that $K \trianglelefteq A$, and hence $K < X$ follows from Corollary 5.6. This property will be used often below.

In particular, $R(G)_p \leq R(G)$ is characteristic for every prime p dividing $|R(G)|$. If G is not a p-group, then $R(G)_p < R(G)$, and by the above observation $R(G)_p < X$. This gives that $X = R(G)$ if G is not a p-group. Let G be a p-group. If $p > 3$, then both $R(G)$ and X are Sylow p-subgroups of A, and the statement follows from Sylow Theorems. Notice that, since Γ is connected, G is generated by the set $s^{-1}S$ for some $s \in S$, hence it is generated by two elements.

Let $p = 2$. Assume for the moment that G is cyclic. Then $R(G)$ has a characteristic subgroup K such that $R(G)/K \cong \mathbb{Z}_4$. Then $K \trianglelefteq A$, $\Gamma_K \cong Q_3$. Moreover, Γ_K is a bi-Cayley graph of $R(G)/K$, and $R(G)/K$ is normal in $A/K \leq \mathrm{Aut}(\Gamma_K)$. A simple computation, using MAGMA, shows that this situation does not occur. Let G be a non-cyclic 2-group in $\mathcal{C}_{\mathrm{sub}}$. Also using the fact that G is generated by two elements, we conclude that either $G \cong \mathbb{Z}_2^2$ and $\Gamma \cong Q_3$, or $G \cong Q_8$ and Γ is the Möbius-Kantor graph. Now, $X = X_2 \cong G_2 = G$. The equality $X = R(G)$ can be verified by the help of MAGMA in either case.

Let $p = 3$. Observe first that $|G| > 3$. For otherwise, $\Gamma \cong K_{3,3}$, but no semiregular automorphism group of order 3 is normal in $\mathrm{Aut}(K_{3,3})$. Since G is generated by two elements, we may write $G \cong \mathbb{Z}_{3^e} \times \mathbb{Z}_{3^f}$, where $e \geq 1$ and $0 \leq f \leq e$. If $e = 1$, then $f = 1$, $G \cong \mathbb{Z}_3^2$, and Γ is the Pappus graph. However, this graph has no automorphism group which is isomorphic to $\mathbb{Z}_3^2$ and also normal in the full automorphism group. Therefore, $e \geq 2$. Define $K = \{R(x) \mid x \in G \text{ and } o(x) \leq 3^{e-2}\}$. Then K is a characteristic subgroup of $R(G)$. Thus $K \triangleleft A$, and Γ_K is a Bi-Cayley graph of $R(G)/K$.

Let $f \leq e - 2$. Then $R(G)/K \cong \mathbb{Z}_9$, and Γ_K is the Pappus graph. This graph, however, does not have a cyclic semiregular automorphism group of order 9. We conclude that $f \in \{e - 1, e\}$.

Let $f = e - 1$. Then $R(G)/K \cong \mathbb{Z}_9 \times \mathbb{Z}_3$. It follows that Γ_K is the unique cubic arc-transitive graph on 54 points (see [14, Table]). We have checked by MAGMA that this graph has a unique semiregular abelian automorphism group whose orbits are the bipartition classes. Therefore, $X/K = R(G)/K$. This together with $K < X \cap R(G)$ yield that $X = R(G)$.

Finally, let $f = e$. Then $R(G)/K \cong \mathbb{Z}_9 \times \mathbb{Z}_9$. It follows that Γ_K is the unique cubic arc-transitive graph on 162 points (see [14, Table]). A direct computation, using MAGMA, gives that $X/K = R(G)/K$, which together with $K < X \cap R(G)$ yield that $X = R(G)$. □

Recall that, a group H is *homogeneous* if every isomorphism between two subgroups of H can be extended to an automorphism of H. A finite group G is called an *m-DCI-group* if every Cayley graph over G of valency at most m is a CI-graph. The following result is [51, Proposition 3.2]:

Proposition 5.10. *Every 2-DCI-group is homogeneous.*

Since every group in $\mathcal{C}$ is a 2-DCI-group (see [51, Theorem 1.3]), we have the corollary that every group in $\mathcal{C}$ is homogeneous.

Everything is prepared to prove Theorem 5.1.

Proof of Theorem 5.1. Let $G \in \mathcal{C}$ and $\Gamma = \mathrm{BCay}(G, S)$ such that $|S| \leq 3$. We have to show that Γ is a BCI-graph. This holds trivially when $|S| = 1$, and follows from the homogeneity of G when $|S| = 2$. Let $|S| = 3$.

Case 1. Γ is arc-transitive.

Let $\mathrm{BCay}(G, S) \cong \mathrm{BCay}(G, T)$ for some subset $T \subseteq G$. We may assume without loss of generality that $1_G \in S \cap T$. Let $H = \langle S \rangle$ and $K = \langle T \rangle$. Then $H, K \in \mathcal{C}_{\mathrm{sub}}$, both bi-Cayley graphs $\mathrm{BCay}(H, S)$ and $\mathrm{BCay}(K, T)$ are connected, and $\mathrm{BCay}(H, S) \cong \mathrm{BCay}(K, T)$. We claim that $\mathrm{BCay}(H, S)$ is a BCI-graph. In view of Lemma 3.5, this holds if the normalizer of $R(H)$ in $\mathrm{Aut}(\mathrm{BCay}(H, S))$ is transitive on the vertex-set $V(\mathrm{BCay}(H, S))$, and for every $X \in \mathcal{S}(\mathrm{Aut}(\mathrm{BCay}(H, S)))$, isomorphic to H, X and $R(H)$ are conjugate in $\mathrm{Aut}(\mathrm{BCay}(H, S))$. Now, the first part follows from Lemma 5.3, while the second part follows from Lemma 5.8.

Let ϕ be an isomorphism from $\mathrm{BCay}(K, T)$ to $\mathrm{BCay}(H, S)$, and consider the group $X = \phi^{-1} R(K) \phi \leq \mathrm{Sym}(H)$. Since ϕ maps the bipartition classes of $\mathrm{BCay}(K, T)$ to the bipartition classes of $\mathrm{BCay}(H, S)$, we have $X \in \mathcal{S}(\mathrm{Aut}(\mathrm{BCay}(H, S)))$. Also, $X_2 \cong R(H)_2$, because $X \cong K$, $|H| = |K|$ and H and K are both contained in the group G from $\mathcal{C}$. Thus Lemma 5.8 is applicable, as a result, X and $R(H)$ are conjugate in $\mathrm{Aut}(\mathrm{BCay}(H, S))$. In particular, $H \cong K$. Since G is homogeneous, there exists $\alpha_1 \in \mathrm{Aut}(G)$ such that $K^{\alpha_1} = H$. This α_1 induces an isomorphism from $\mathrm{BCay}(K, T)$ to $\mathrm{BCay}(H, T^{\alpha_1})$. Therefore, $\mathrm{BCay}(H, S) \cong \mathrm{BCay}(H, T^{\alpha_1})$, and since $\mathrm{BCay}(H, S)$ is a BCI-graph, $T^{\alpha_1} = gS^{\alpha_2}$ for some $g \in H$ and $\alpha_2 \in \mathrm{Aut}(H)$. By the homogeneity of G, α_2 extends to an automorphism of G, implying that $\mathrm{BCay}(G, S)$ is a BCI-graph.

Case 2. Γ is not arc-transitive

Since Γ is vertex-transitive (see Lemma 5.3), but not arc-transitive, we have $A_{(1_G,0)} = A_{(s,1)}$ for some $s \in S$. We show below that $\mathrm{BCay}(G, s^{-1}S)$ is a BCI-graph, this obviously yields that the same holds for $\mathrm{BCay}(G, S)$. Define the permutation ϕ of $G \times \{0, 1\}$ by $(x, i)^\phi = (x, 0)$ if $i = 0$, and $(x, i)^\phi = (s^{-1}x, 1)$ if $i = 1$. The vertex $(x, 0)$ of $\mathrm{BCay}(G, S)$ has neighbourhood $(Sx, 1)$. This is mapped by ϕ to the set $(s^{-1}Sx, 1)$. This shows that ϕ is an isomorphism from Γ to $\Gamma' = \mathrm{BCay}(G, s^{-1}S)$. Then $\mathrm{Aut}(\Gamma')_{(1_G,0)} = \phi^{-1} A_{(1_G,0)} \phi = \phi^{-1} A_{(s,1)} \phi = \mathrm{Aut}(\Gamma')_{(1_G,1)}$. Let $\tau_{R(G)}$ be the automorphism of Γ' defined in Lemma 5.3. It follows that $\tau_{R(G)}$ is an involution (see the proof of Lemma 5.3), which normalizes $R(G)$ and maps $(1_G, 0)$ to $(1_G, 1)$. Now, we can apply Lemma 5.2 to Γ', as a result, it is sufficient to show that $\mathrm{Cay}(G, s^{-1}S \setminus$

$\{1_G\}$) is a CI-graph. This follows because $|s^{-1}S \setminus \{1_G\}| = 2$ and that G is a 2-DCI-group (see [51, Theorem 1.3]). This completes the proof of the theorem. □

Chapter 6

Connected arc-transitive cubic bi-Cayley graphs

In this chapter we turn to the class of connected arc-transitive cubic bi-Cayley graphs $\mathrm{BCay}(G, R, L, S)$. As a first result, we give a classification of these graphs in the case when G is an abelian group. For sake of simplicity we call such a graph also an *abelian bi-Cayley graph*. We start with a definition.

Definition 6.1. We say that a bi-Cayley graph $\mathrm{BCay}(G, R, L, S)$ is of *type* s if $|R| = |L| = s$.

Clearly, if $\mathrm{BCay}(G, R, L, S)$ is cubic, then it is of s-type for $s \in \{0, 1, 2\}$. The classification in the cases of 0- and 2-type graphs follows from results in [15, 24, 46, 47]. The 0-type graphs are listed in Table 6.1.

no.	G	S	k-reg.	other name
1.	$\mathbb{Z}_{rm} \times \mathbb{Z}_m = \langle a, b \,\vert\, a^{rm} = b^{rm} = 1, b^m = a^{m(u+1)} \rangle$, $r = 3^s p_1^{e_1} \cdots p_t^{e_t}$, $r > 3$ and $r \geq 11$ if $m = 1$, $s \in \{0, 1\}$, every $p_i \equiv 1 (\mathrm{mod}\ 3)$, and $u^2 + u + 1 \equiv 0 (\mathrm{mod}\ r)$	$\{1, a, b\}$	1	–
2.	$\mathbb{Z}_8 = \langle a \rangle$	$\{1, a^2, a^3\}$	2	Möbius-Kantor graph
3.	$\mathbb{Z}_m^2 = \langle a, b \rangle$, $m > 1, m \neq 3$	$\{1, a, b\}$	2	–
4.	$\mathbb{Z}_{3m} \times \mathbb{Z}_m = \langle a, b \,\vert\, a^{3m} = b^{3m} = 1, a^m = b^m \rangle$, $m > 1$	$\{1, a, b\}$	2	–
5.	$\mathbb{Z}_3 = \langle a \rangle$	$\{1, a, a^{-1}\}$	3	$K_{3,3}$
6.	$\mathbb{Z}_3^2 = \langle a, b \rangle$	$\{1, a, b\}$	3	Pappus graph
7.	$\mathbb{Z}_7 = \langle a \rangle$	$\{1, a, a^3\}$	4	Heawood graph

Table 6.1: Connected arc-transitive cubic abelian 0-type bi-Cayley graphs.

In deriving Table 6.1, the key observation is that each 0-type graph is of girth 4 or 6, which we have already deduced in the proof of Lemma 5.7. Let Γ be a connected arc-transitive cubic bi-Cayley graph over an abelian group G. If the girth of Γ is 4, then the it is isomorphic to $K_{3,3}$ or Q_3. The graph $K_{3,3}$ is isomorphic to the bi-Cayley graph given in row no. 5 of Table 6.1, and Q_3 is isomorphic to the

bi-Cayley graph given in row no. 3 of Table 6.1 with $m = 2$. Assume that Γ is of girth 6. Then by Theorem 2.8, Γ is k-regular for some $k \leq 4$. We consider each case of the theorem separately.

CASE 1. $k = 1$.

In this case $\mathrm{Aut}(\Gamma)$ contains a regular normal subgroup K isomorphic to $\mathrm{Dih}(L)$, where $L \cong \mathbb{Z}_{rm} \times \mathbb{Z}_m$, $r = 3^s p_1^{e_1} \cdots p_t^{e_t}$, $r > 3$ and $r \geq 11$ if $m = 1$, $s \in \{0, 1\}$, and every $p_i \equiv 1 (\mathrm{mod}\, 3)$. Consequently, the subgroup $G \leq K$ that $G \cong L$ is semiregular and has two orbits on $V(\Gamma)$. Notice that, the group L is characteristic in $\mathrm{Dih}(L)$. Thus G is characteristic in K, and since $K \trianglelefteq \mathrm{Aut}(\Gamma)$ we conclude that $G \trianglelefteq \mathrm{Aut}(\Gamma)$. Using this and that Γ is arc-transitive, we find that Γ is bipartite, and the bipartition classes are equal to the orbits of G. Therefore, $\Gamma \cong \mathrm{BCay}(G, S)$ for a subset S of G. We may assume without loss of generality that $1 \in S$, here 1 denotes the identity element of G. Since Γ is arc-transitive and G is normal in $\mathrm{Aut}(\Gamma)$, there exist $\sigma \in \mathrm{Aut}(G)$ and $h \in G$ with the property that S is equal to the orbit of 1 under the mapping $\varphi : x \mapsto x^\sigma h$, $x \in G$. Thus we may write $S = \{1, a, b\}$ such that $1^\varphi = a$, $a^\varphi = b$ and $b^\varphi = 1$. It follows from this that $h = a$, $a^\sigma = a^{-1}b$ and $b^\sigma = a^{-1}$. This shows that both elements a and b are of the same order. On the other hand Γ is connected, hence $\langle a, b\rangle = G \cong \mathbb{Z}_{rm} \times \mathbb{Z}_m$, and thus a and b are of order rm, and $\langle a^m\rangle = \langle b^m\rangle$. Then we can write $\langle a^m\rangle^\sigma = \langle b^m\rangle^\sigma = \langle (b^\sigma)^m\rangle = \langle a^m\rangle$, and thus $(a^m)^\sigma = (a^m)^u$ for some integer u, $\gcd(u, r) = 1$. From this $(a^m)^u = (a^m)^\sigma = a^{-m}b^m$, hence $b^m = a^{m(u+1)}$. Also, $(a^m)^{u^2} = (a^m)^{\sigma^2} = (a^{-m}b^m)^\sigma = (a^m)^{-u-1}$, and this gives that $u^2+u+1 \equiv 0 (\mathrm{mod}\, r)$. To sum up, $\mathrm{BCay}(G, \{1, a, b\})$ is one the graphs described in row no. 1 of Table 6.1. In fact, any graph in that row is arc-transitive, the proof of this claim we leave for the reader.

CASE 2. $k = 2$. In this case $\Gamma \cong GP(8, 3)$, or $\mathrm{Aut}(\Gamma)$ contains a regular normal subgroup isomorphic to $\mathrm{Dih}(L)$, where $L \cong \mathbb{Z}_{rm} \times \mathbb{Z}_m$, $r \in \{1, 3\}$, $m > 1$, and if $r = 1$, then $m \neq 3$. We have checked by MAGMA that $GP(8, 3)$ admits a bi-Cayley representation given in row no. 2 of Table 6.1. Otherwise, copying the same argument as in CASE 1, we derive that $\Gamma \cong \mathrm{BCay}(G, S)$, where $S = \{1, a, b\}$, and either $G = \langle a, b\rangle \cong \mathbb{Z}_m \times \mathbb{Z}_m$, $m > 1$ and $m \neq 3$, or $G = \langle a, b \,|\, a^{3m} = b^{3m} = 1, a^m = b^m\rangle \cong \mathbb{Z}_{3m} \times \mathbb{Z}_m$, $m > 1$. Therefore, $\mathrm{BCay}(G, \{1, a, b\})$ is one of the graphs described in row no. 3 of Table 6.1 in the former case, while it is one of the graphs described in row no. 4 of Table 6.1 in the latter case. In fact, any graph in these rows is arc-transitive, the proof is again left for the reader.

CASE 3. $k = 3$. In this case $\Gamma \cong F18$ (the Pappus graph) or $GP(10, 3)$ (the Desargues graph). The Pappus graph admits a bi-Cayley representation given in row no. 6 of Table 6.1, and we have checked by MAGMA that the Desargues graph cannot be represented as a 0-type abelian bi-Cayley graph.

CASE 4. $k = 4$. In this case $\Gamma \cong F14$ (the Heawood graph), which admits a bi-Cayley representation given in row no. 7 of Table 6.1.

The 2-type connected arc-transitive cubic abelian bi-Cayley graphs are listed in Table 6.2.

Table 6.2 follows directly from the classification of connected arc-transitive abelian bi-Cayley graphs $\mathrm{BCay}(G, R, L, S)$ with $|S| = 1$ given in [46, Theorem 1.1].

G	R	L	S	k-trans	other name
$\langle a,b\rangle = \mathbb{Z}_2^2$	$\{a,b\}$	$\{a,b\}$	$\{1\}$	2	$GP(4,1)$
$\langle a\rangle \times \langle b\rangle = \mathbb{Z}_2 \times \mathbb{Z}_{10}$	$\{ab^3, ab^{-3}\}$	$\{b, b^{-1}\}$	$\{1\}$	2	–
$\langle a\rangle = \mathbb{Z}_n$	$\{a\}$	$\{a^k\}$	$\{1\}$	2	$GP(n,k)$, $(n,k) =$ $(4,1)$, $(8,3)$, $(10,2)$, $(12,5)$, $(24,5)$
$\langle a\rangle = \mathbb{Z}_n$	$\{a\}$	$\{a^k\}$	$\{1\}$	3	$GP(n,k)$, $(n,k) =$ $(5,2)$, $(10,3)$

Table 6.2: Connected arc-transitive cubic abelian 2-type bi-Cayley graphs.

In Section 6.1 we complete the classification by proving the following theorem:

Theorem 6.2. *There are exactly four connected arc-transitive cubic* 1*-type abelian bi-Cayley graphs:* K_4*,* Q_3*,* $GP(8,3)$ *and* $GP(12,5)$*.*

In Section 6.2 we turn to the BCI-property of cubic bi-Cayley graphs $\mathrm{BCay}(G,S)$ where G is a finite abelian group. We have seen in the previous chapter that G is a 3-BCI-group if and only if $G = U \times V$, where U is an abelian group of odd order whose Sylow subgroups are homocyclic and V is trivial, $\mathbb{Z}_{2^r}$ or $\mathbb{Z}_2^r$ (see Theorem 5.1 and the preceding paragraph). Consequently, the class of abelian 3-BCI groups is quite restricted. As our second main result in this chapter, we prove that the situation changes completely when one considers only connected arc-transitive graphs.

Theorem 6.3. *Let* G *be a finite abelian group. Then every connected arc-transitive cubic bi-Cayley graph* $\mathrm{BCay}(G,S)$ *is a BCI-graph.*

6.1 Proof of Theorem 6.2

Till the end of the section we keep the following notation:

$$\Gamma = \mathrm{BCay}(G, \{r\}, \{s\}, \{1,t\})$$

is a cubic symmetric graph, $G = \langle r,s,t\rangle$ is an abelian group and, r and s are involutions.

The *core* of a subgroup A in a group B is the largest normal subgroup of B contained in A. In order to derive Theorem 6.2, we analyse the core of $R(G)$ in $\mathrm{Aut}(\Gamma)$.

Lemma 6.4. *If* $R(G)$ *has trivial core in* $\mathrm{Aut}(\Gamma)$*, then one of the following holds:*

(i) $G \cong \mathbb{Z}_2$*,* $s = r = t$*, and* $\Gamma \cong K_4$*.*

(ii) $G \cong \mathbb{Z}_2^2$*,* $s \neq r$*,* $t = sr$ *and* $\Gamma \cong Q_3$*.*

Proof. If Γ is of girth 4, then it is isomorphic to K_4, or $K_{3,3}$, or Q_3. In the first case we get at once (i), and it is not hard to see that $K_{3,3}$ is impossible. Furthermore, we compute by Magma that Q_3 is possible, $G \cong \mathbb{Z}_2^2$, and r, s, t must be as given in (ii).

For the rest of the proof we assume that the girth of Γ is larger than 4. Then $r \neq s$, for otherwise, we find the 4-circuit $((1,0),(1,1),(r,1),(r,0))$. Then either $\langle r,s\rangle \cap \langle t\rangle$ is trivial, and

$$G = \langle r,s\rangle \times \langle t\rangle \cong \mathbb{Z}_2^2 \times \mathbb{Z}_n; \tag{6.1}$$

or t is of even order, say $2n$, $t^n \in \langle r,s\rangle$, and

$$G = \langle r,s,t\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2n}. \tag{6.2}$$

Note that, we have $|G| = 4n$.

By Tutte's Theorem (Theorem 2.7), Γ is k-regular for some $k \leq 5$. The order $|\operatorname{Aut}(\Gamma)| = |V(\Gamma)| \cdot 3 \cdot 2^{k-1} = |G| \cdot 3 \cdot 2^k$, and thus $|\operatorname{Aut}(\Gamma) : R(G)| = 3 \cdot 2^k$. Consider the action of $\operatorname{Aut}(\Gamma)$ on the set of its right $R(G)$-cosets. Since $R(G)$ has trivial core in $\operatorname{Aut}(\Gamma)$, this action is faithful. Using this and that $R(G)$ acts as a point stabilizer, we have an embedding of $R(G)$ into $S_{3\cdot 2^k-1}$. We shall write below $G \leq S_{3\cdot 2^k-1}$. It was proved in [12, Theorem 1] that, if $n = 3m+2$ and $A \leq S_n$ is an abelian subgroup, then

$$|A| \leq 2 \cdot 3^m, \tag{6.3}$$

and equality holds if and only if $A \cong \mathbb{Z}_2 \times \mathbb{Z}_3^m$.

Case 1. $k = 1$. In this case $\mathbb{Z}_2^2 \leq G \leq S_5$. This implies that $|G| = 4$, $\Gamma \cong Q_3$ (see [14, Table]), which contradicts that the girth is larger than 4.

Case 2. $k = 2$. In this case $G \leq S_{11}$. Since $|G| = 4n$, we obtain by (6.3) that $n \leq 13$. We compute by Magma that, if G is given as in (6.1) and $n \leq 13$, then Γ is not edge-transitive. Furthermore, if G is given as in (6.2) and $n \leq 13$, then Γ is edge-transitive only if $n = 2$ or $n = 3$. Consequently, $\Gamma \cong GP(8,3)$ or $GP(12,5)$ (see [14, Table]). However, we have checked by Magma that in both cases the possible semiregular subgroups have a non-trivial core in the full automorphism group, and thus this case is excluded.

Case 3. $k \geq 3$. We may assume that $n > 13$, see the previous paragraph. We find in Γ the 8-cycle $(\,(1,0),(r,0),(r,1),(rs,1),(rs,0),(s,0),(s,1),(1,1))$. Thus there must be an 8-cycle, say C, starting with the 3-arc $((1,0),(t,1),(t,0),(t^2,1))$, let this be written in the form:

$$C = \big(\,(1,0),(t,1),(t,0),(t^2,1),(\delta t^2,x),(\gamma\delta t^2,x'),(\beta\gamma\delta t^2,x''),(\alpha\beta\gamma\delta t^2,x''')\,\big),$$

where $x,x',x'',x'''' \in \{0,1\}$ and $\alpha,\beta,\gamma,\delta \in \{1,r,s,t,t^{-1}\}$. Put $\eta = \alpha\beta\gamma\delta t^2$. Observe that, $\eta = t^i r^j s^k$ for some integers $i,j,k \geq 0$. Moreover, $i \leq 4$ and $i = 0$ if and only if

$$C = (\,(1,0),(t,1),(t,0),(t^2,1),(t^2s,1),(ts,0),(ts,1),(s,0)\,),$$

and so $\eta = s$. On the other hand, since $1_0 \sim \eta_{x'''}$ and $\eta_{x'''} \neq t_1$, $\eta \in \{1,r\}$, and we conclude that $i > 0$ (recall that $r \neq s$). Now, $1 = \eta^2 = t^{2i}r^{2j}s^{2k} = t^{2i}$, which implies that the order of t is at most 8, and hence $n \leq 8$ (see (6.1) and (6.2)), which contradicts that $n > 13$. This completes the proof of the lemma. □

Lemma 6.5. *Let $R(N)$ be the core of $R(G)$ in* $\mathrm{Aut}(\Gamma)$. *Then one of the following holds:*

(i) $G = N \times \langle r \rangle$, *and* $Nr = Ns = Nt$.

(ii) $G = N \times \langle r, s \rangle$, $r \neq s$, *and* $Nt = Nrs$.

Proof. By Lemma 5.4(iii), the quotient graph $\Gamma_{R(N)}$ can be written in the form

$$\Gamma_{R(N)} = \mathrm{BCay}(G/N, \{Nr\}, \{Ns\}, \{N, Nt\}).$$

We claim that $R(G/N)$ has trivial core in $\mathrm{Aut}(\Gamma_{R(N)})$. This and Lemma 6.4 will yield (i) and (ii).

Let ρ be the permutation representation of $\mathrm{Aut}(\Gamma)$ derived from its action on the set of $R(N)$-orbits. By Lemma 5.4(ii), the kernel $\ker \rho = R(N)$, $\rho(R(G)) = R(G/N)$, and any subgroup of $R(G/N)$ is in the form $\rho(R(K))$ for some $N \leq K \leq G$. Assume that $\rho(R(K)) \trianglelefteq \mathrm{Aut}(\Gamma_{R(N)})$. Then $\rho(R(K)) \trianglelefteq \rho(\mathrm{Aut}(\Gamma))$, and hence $R(K) \trianglelefteq \mathrm{Aut}(\Gamma)$. Thus $R(K) = R(N)$, because $R(N)$ is the core. We find that $\rho(R(K))$ is trivial, and the claim is proved. □

In the next lemma we deal with case (i) of Lemma 6.5.

Lemma 6.6. *Let $R(N)$ be the core of $R(G)$ in* $\mathrm{Aut}(\Gamma)$, *and suppose that $N \neq 1$ and case (i) of Lemma 6.5 holds. Then one of the following holds:*

(i) $G \cong \mathbb{Z}_2^2$, $r = s \neq t$, *and* $\Gamma \cong Q_3$.

(ii) $G = \langle r \rangle \times \langle t \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_4$, *and* $\Gamma \cong \mathrm{BCay}(G, \{r\}, \{rt^2\}, \{1, t\}) \cong GP(8, 3)$.

Proof. In this case $G = N \times \langle r \rangle$, and $Nr = Ns = Nt$. Thus $s = n_1 r$, and $t = n_2 r$ for some $n_1, n_2 \in N$. Furthermore, n_1 is an involution, and since $G = \langle r, s, t \rangle$, $N = \langle n_1, n_2 \rangle$.

Assume for the moment that N is not a 2-group, and let p be an odd prime divisor of $|N|$. Then $M = \langle n_1, n_2^p \rangle$ is the unique subgroup in N of index p, hence it is characteristic in N. Using also that $R(N) \trianglelefteq \mathrm{Aut}(\Gamma)$, this gives that $R(M) \trianglelefteq \mathrm{Aut}(\Gamma)$. The quotient graph $\Gamma_{R(M)}$ is a cubic symmetric graph on $4p$ points admitting a 1-type bi-Cayley representation over G/M. It was proved in [23, Theorem 6.2] that $\Gamma_{R(M)}$ is isomorphic to one of the graphs: $GP(10, 3)$, $GP(10, 5)$, and the Coxeter graph $F28$. We compute by Magma that none of the these graphs has a 1-type bi-Cayley representation.We conclude that N is a 2-group.

Notice that, $N \cong \mathbb{Z}_{2^m}$ or $\mathbb{Z}_2 \times \mathbb{Z}_{2^{m-1}}$. If $|N| \geq 8$, then N has a characteristic subgroup M such that $|N : M| = 8$. Using also that $R(N) \trianglelefteq \mathrm{Aut}(\Gamma)$, we find in turn that, $R(M) \trianglelefteq \mathrm{Aut}(\Gamma)$, and $\Gamma_{R(M)}$ is a cubic symmetric graph on 32 points which admits a 1-type bi-Cayley representation over G/M. Thus Γ is isomorphic to the Dyck graph $F32$ (see [14, Table]), which can be excluded by the help of Magma. Therefore, $|N| \in \{2, 4\}$, and these yield easily cases (i) and (ii) respectively. □

In the next lemma we deal with case (ii) of Lemma 6.5.

Lemma 6.7. *Let $R(N)$ be the core of $R(G)$ in* $\mathrm{Aut}(\Gamma)$, *and suppose that $N \neq 1$ and case (ii) of Lemma 6.6 holds. Then $G = \langle r \rangle \times \langle t \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_6$, and $\Gamma \cong \mathrm{BCay}(G, \{r\}, \{rt^3\}, \{1, t\}) \cong GP(12, 5)$.*

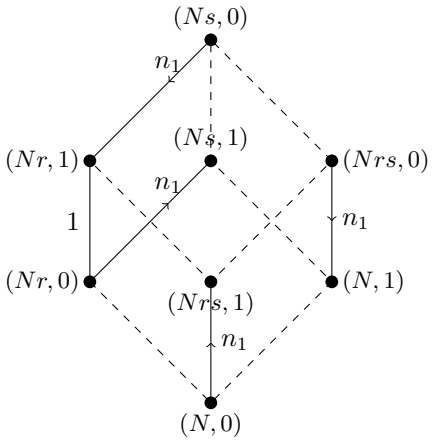

Figure 6.1: Voltage assignment ζ of $\Gamma_{R(N)}$.

Proof. In this case $G = N \times \langle r, s\rangle$, $r \neq s$, and $Nt = Nrs$. Thus $t = n_1 rs$ for some $n_1 \in N$. Since $G = \langle r, s, t\rangle$, $N = \langle n_1\rangle$. Now, by Lemma 5.4(iii) we may write

$$\Gamma_{R(N)} = \mathrm{BCay}(G/N, \{Nr\}, \{Ns\}, \{N, Nrs\}) \cong Q_3.$$

We proceed by defining an N-voltage assignment of the quotient graph $\Gamma_{R(N)}$. For this purpose we have depicted $\Gamma_{R(N)}$ in Fig. 6.1, where we have also fixed the spanning tree T specified by the dashed edges. Now, let $\zeta : A(\Gamma_{R(N)}) \to N$ be the T-reduced N-voltage assignment with its voltages being given in Fig. 6.1. To simplify notation we set $\widehat{\Gamma} = \Gamma_{R(N)} \times_\zeta N$. Recall that $\widehat{N}$ is a subgroup of $\mathrm{Aut}(\widehat{\Gamma})$ (see Subsection 2.2.3). Next, we prove the following properties:

$$\Gamma \cong \widehat{\Gamma}, \text{ and } \widehat{N} \trianglelefteq \mathrm{Aut}(\widehat{\Gamma}). \tag{6.4}$$

Define the mapping $f : V(\widehat{\Gamma}) \to V(\Gamma)$ by

$$f\colon ((Nx,0),n) \mapsto (nx,0) \text{ and } ((Nx,1),n) \mapsto (nx,1),\ x \in \{1,r,s,rs\},\ n \in N.$$

Notice that, f is well-defined because $\{1, r, s, rs\}$ is a complete set of coset representatives of N in G. We prove below that f is an isomorphism from $\widehat{\Gamma}$ to Γ. Let $\widehat{v}_1$ and $\widehat{v}_2$ be two adjacent vertices of $\widehat{\Gamma}$. This means that $\widehat{v}_1 = ((Nx,i),n)$ and $\widehat{v}_2 = ((Ny,j),\zeta(a)n)$, where $a = ((Nx,i),(Ny,j))$ is an arc of $\Gamma_{R(N)}$. Then$f(\widehat{v}_1) = (xn,i)$ and $f(\widehat{v}_2) = (y\zeta(a)n,j)$.

Let $i = j = 0$. Then it can be seen in Fig. 6.1 that $y = rx$ and $\zeta(a) = 1$. Thus in Γ we find $f(\widehat{v}_1) = (nx,0) \sim (rnx,0) = (y\zeta(a)n,0) = f(\widehat{v}_2)$. Let $i = j = 1$. Then $y = sx$, $\zeta(a) = 1$, and so $f(\widehat{v}_1) = (nx,1) \sim (snx,1) = (y\zeta(a)n,1) = f(\widehat{v}_2)$. Finally, let $i = 0$ and $j = 1$. Then $y = x$ or $y = rsx$. In the former case $\zeta(a) = 1$, and $f(\widehat{v}_1) = (nx,0) \sim (nx,1) = (y\zeta(a)n,1) = f(\widehat{v}_2)$. In the latter case $\zeta(a) = n_1$, and

$$f(\widehat{v}_1) = (nx,0) \sim (tnx,1) = (n_1 rsnx,1) = (y\zeta(a)n,1) = f(\widehat{v}_2).$$

By these we have proved that f is indeed an isomorphism.

For the second part of (6.4), compute that $fR(m)f^{-1}$ maps $((Nx,i),n)$ to $((Nx,i),nm)$ for every $m \in N$. Thus $fR(m)f^{-1} = \hat{m}$, and so $fR(N)f^{-1} = \widehat{N}$. Since $R(N) \trianglelefteq \mathrm{Aut}(\Gamma)$, $\widehat{N} = fR(N)f^{-1} \trianglelefteq f\,\mathrm{Aut}(\Gamma)f^{-1} = \mathrm{Aut}(\widehat{\Gamma})$, as claimed.

Now, (6.4) holds, implying that $\mathrm{Aut}(\widehat{\Gamma})$ projects to an edge-transitive subgroup of $\mathrm{Aut}(\Gamma_{R(N)})$. We obtain from this that the automorphism $\alpha \in \mathrm{Aut}(\Gamma_{R(N)})$ lifts, where

$$\alpha = (\,(Nr,0),(Nrs,1),(N,1))(\,(Nr,1),(Nrs,0),(Ns,1)\,).$$

Apply Theorem 2.10 to $\widehat{\Gamma}$ with $\sigma = \alpha$ and the following directed base circuits relative to T:

$$\vec{C} = ((Ns,0),(Nrs,0),(N,1),(Ns,1)) \text{ and } \vec{C}' = ((N,0),(Nr,0),(Ns,1),(N,1)).$$

Let σ_* be the automorphism of N given in Theorem 2.10. Since $\zeta(\vec{C}) = \zeta(\vec{C}') = n_1$, $\zeta(\vec{C}^{\,\alpha}) = \sigma_*(n_1) = \zeta(\vec{C}'^{\,\alpha})$, which gives $n_1^{-2} = n_1$. Thus $|N| = 3$, and this yields easily the statement of the lemma. □

Proof of Theorem 6.2. The theorem follows directly from Lemmas 6.4 - 6.7.

6.2 Proof of Theorem 6.3

Till the end of the section we keep the following notation:

$$\Gamma = \mathrm{BCay}(G, \{1, a, b\})$$

is a cubic arc-transitive graph, where $G = \langle a, b\rangle$ is an abelian group.

Recall that, $\mathcal{S}(\mathrm{Aut}(\Gamma))$ denotes the set of all semiregular subgroups of $\mathrm{Aut}(\Gamma)$ whose orbits are $G\times\{0\}$ and $G\times\{1\}$. The next lemma is a special case of Lemma 5.3.

Lemma 6.8. *For every abelian group $X \in \mathcal{S}(\mathrm{Aut}(\Gamma))$, there exists an involution $\tau_X \in \mathrm{Aut}(\Gamma)$ which satisfies the following properties:*

(i) Every subgroup $Y \leq X$ is normalized by τ_X.

(ii) The group $\langle X, \tau_X\rangle$ is regular on $V(\Gamma)$.

Lemma 6.9. *Let $N \leq \mathrm{Aut}(\Gamma)$ be a normal subgroup such that there exists an N-orbit properly contained in $G \times \{0\}$, and let X be an abelian group from $\mathcal{S}(\mathrm{Aut}(\Gamma))$. Then $N < X$.*

Proof. We copy the argument in the proof of Corollary 5.6. Let Δ be an N-orbit such that $\Delta \subset G \times \{0\}$, and let us consider $Y = X \cap \mathrm{Aut}(\Gamma)_{\{\Delta\}}$. Since Δ is a block contained in an X-orbit, we obtain that Δ is an Y-orbit. We write $\Delta = \mathrm{Orb}(Y, v)$. Moreover, as X is semiregular, Y is regular on Δ, and by this and Lemma 5.4(ii) we have

$$|Y| = |\Delta| = |N|. \tag{6.5}$$

Let $\tau_X \in \mathrm{Aut}(\Gamma)$ be the automorphism defined in Lemma 6.8, and set $L = \langle X, \tau_X \rangle$. According to Lemma 6.8 the group L is transitive on $V(\Gamma)$, and also $Y \trianglelefteq L$. Denote by δ the system of blocks induced by Δ. Then we may write

$$\delta = \{\Delta^l \mid l \in L\} = \{\mathrm{Orb}(Y, v)^l \mid l \in L\} = \{\mathrm{Orb}(Y, v^l) \mid l \in L\}.$$

From this $Y \leq \mathrm{Aut}(\Gamma)_\delta$, where $\mathrm{Aut}(\Gamma)_\delta$ is the kernel of $\mathrm{Aut}(\Gamma)$ acting on δ. Since $\mathrm{Aut}(\Gamma)_\delta = N$ (see Lemma 5.4(ii)), we have that $Y \leq N$. This and (6.5) imply that $N = Y < X$. □

For a group G and a prime p dividing $|G|$, we let G_p denote a Sylow p-subgroup of G.

Proof of Theorem 6.3. We have to show that Γ is a BCI-graph. Let $X \in \mathcal{S}(\mathrm{Aut}(\Gamma))$ such that $X \cong G$. By Lemma 3.5 and Lemma 6.8, it is sufficient to show the following

$$X \text{ and } R(G) \text{ are conjugate in } \mathrm{Aut}(\Gamma). \tag{6.6}$$

Recall that the girth of Γ is 4 or 6, and if it is 4, then Γ is isomorphic to $K_{3,3}$ or Q_3. It is easy to see that (6.6) holds when $\Gamma \cong K_{3,3}$, and we have checked by the help of Magma that it also holds when $\Gamma \cong Q_3$. Thus assume that Γ is of girth 6. By Theorem 2.8, Γ is k-regular for some $k \leq 4$.

Case 1. $k = 1$. In this case $\mathrm{Aut}(\Gamma)$ contains a regular normal subgroup K isomorphic to $\mathrm{Dih}(L)$, where $L \cong \mathbb{Z}_{rm} \times \mathbb{Z}_m$, $r = 3^s p_1^{e_1} \cdots p_t^{e_t}, r > 3$ and $r \geq 11$ if $m = 1$, $s \in \{0, 1\}$, and every $p_i \equiv 1 (\mathrm{mod}\ 3)$. We have proved in the second paragraph following Table 6.1 that $\mathrm{Aut}(\Gamma)$ contains a semiregular normal subgroup N such that $N \cong L$, and the orbits of N are $G \times \{0\}$ and $G \times \{1\}$. Notice that, X contains every proper characteristic subgroup K of N. Indeed, since $N \trianglelefteq \mathrm{Aut}(\Gamma)$, $K \trianglelefteq \mathrm{Aut}(\Gamma)$, and Lemma 6.9 can be applied for N, implying that $K < X$. In particular, if N is not a p-group, then $N_p < X$ for every prime p dividing $|N|$, and thus $N = X$. Since this holds for every $X \in \mathcal{S}(\mathrm{Aut}(\Gamma))$ with $X \cong G$, it holds also for $X = R(G)$, and we get $R(G) = N = X$. In this case (6.6) holds trivially. Let N be a p-group for a prime p. Then it follows from the fact that $N \cong L$ that $p > 3$, and thus both $R(G)$ and X are Sylow p-subgroups of $\mathrm{Aut}(\Gamma)$. In this case (6.6) follows from Sylow's Theorem.

Case 2. $k = 2$. In this case $\Gamma \cong GP(8, 3)$, or $\mathrm{Aut}(\Gamma)$ contains a regular normal subgroup isomorphic to $\mathrm{Dih}(L)$, where $L \cong \mathbb{Z}_{rm} \times \mathbb{Z}_m$, $r \in \{1, 3\}$, $m > 1$, and if $r = 1$, then $m \neq 3$. If $\Gamma \cong GP(8, 3)$, then we have checked by Magma that $G \cong \mathbb{Z}_8$ and (6.6) holds. Assume that $\Gamma \ncong GP(8, 3)$. We have proved in the third paragraph following Table 6.1 that $\mathrm{Aut}(\Gamma)$ contains a semiregular normal subgroup N such that $N \cong L$, and the orbits of N are $G \times \{0\}$ and $G \times \{1\}$. Now, repeating the argument in Case 1 above, we obtain that $N = X = R(G)$ if N is not a p-group. Let N be a p-group for a prime p. If $p > 3$, then both $R(G)$ and X are Sylow p-subgroups of $\mathrm{Aut}(\Gamma)$, and (6.6) follows from Sylow's Theorem. We are left with the case that $p \in \{2, 3\}$.

Let $p = 2$. Since $N \cong L$, we find that $N \cong \mathbb{Z}_{2^e} \times \mathbb{Z}_{2^e}$, $e \geq 1$. Define $K = \{x \in N \mid o(x) \leq 2^{e-1}\}$. Then K is characteristic in N and thus $K \trianglelefteq \mathrm{Aut}(\Gamma)$. By Lemma 6.9, $K \leq X \cap R(G)$. By Lemma 5.4(iii), the quotient graph Γ_K is a 0-type

Bi-Cayley graph over the group $N/K \cong \mathbb{Z}_2^2$. Then $\Gamma_K \cong Q_3$ and both N/K and $R(G)/K$ are semiregular on $V(\Gamma_K)$ having orbits the two bipartition classes of Γ_K. Since $X \cong R(G)$, $X/K \cong R(G)/K$. A direct computation, using MAGMA, gives that there are two possibilities: $X/K \cong R(G)/K \cong \mathbb{Z}_2^2$ or $\mathbb{Z}_4$. Furthermore, In the former case $X/K = R(G)/K$, which together with $K < X \cap R(G)$ yield that $X = R(G)$, and (6.6) holds trivially. Suppose that the latter case holds and consider $\mathrm{Aut}(\Gamma)$ acting on the set of K-orbits. The kernel of this action is equal to K, see Lemma 5.4.(ii), and thus the image $\mathrm{Aut}(\Gamma)/K$ is a subgroup of $\mathrm{Aut}(\Gamma_K)$ which is transitive on the set of 2-arcs of Γ_K. However, Γ_K is 2-regular (it is, in fact, isomorphic to Q_3), and we obtain that $\mathrm{Aut}(\Gamma)/K = \mathrm{Aut}(\Gamma_K)$. We compute by MAGMA that X/K and $R(G)/K$ are conjugate in $\mathrm{Aut}(\Gamma_K) = \mathrm{Aut}(\Gamma)/K$, and so (6.6) follows from this and the fact that $K < X \cap R(G)$.

Let $p = 3$. Observe first that $|N| > 3$. For otherwise, $\Gamma \cong K_{3,3}$, contradicting that the girth is 6. Since $N \cong L$, we find that $N \cong \mathbb{Z}_{3^{e+\varepsilon}} \times \mathbb{Z}_{3^e}$, $e \geq 1$, $\varepsilon \in \{0, 1\}$, and if $\varepsilon = 0$, then $e \geq 2$. Let $\varepsilon = 0$. Define $K = \{x \in N : o(x) \leq 3^{e-2}\}$. Then K is characteristic in N and thus $K \trianglelefteq \mathrm{Aut}(\Gamma)$. By Lemma 6.9, $K \leq X \cap R(G)$. By Lemma 5.4(iii), the quotient graph Γ_K is a 0-type Bi-Cayley graph of the group $N/K \cong \mathbb{Z}_9^2$. It follows that Γ_K is the unique cubic symmetric graph on 162 points of girth 6 (see [14, Table]). A direct computation, using MAGMA, gives that $X/K = R(G)/K = N/K$, which together with $K < X \cap R(G)$ yield that $X = R(G)$, and (6.6) holds trivially. Let $\varepsilon = 1$. Define $K = \{x \in N \mid o(x) \leq 3^{e-1}\}$. Then K is characteristic in N and thus $K \trianglelefteq \mathrm{Aut}(\Gamma)$. By Lemma 6.9, $K \leq X \cap R(G)$. By Lemma 5.4(iii), the quotient graph Γ_K is a 0-type Bi-Cayley graph of the group $N/K \cong \mathbb{Z}_9 \times \mathbb{Z}_3$. It follows that Γ_K is the unique cubic symmetric graph on 54 points (see [14, Table]). A direct computation, using MAGMA, gives that $X/K = R(G)/K = N/K$, which together with $K < X \cap R(G)$ yield that $X = R(G)$, and (6.6) holds also in this case.

CASE 3. $k = 3$. In this case $\Gamma \cong F18$ (the Pappus graph) or $GP(10, 3)$ (the Desargues graph). We have checked by MAGMA that in the former case $G \cong \mathbb{Z}_3^2$ and (6.6) holds, and the latter case cannot occur.

CASE 4. $k = 4$. In this case $\Gamma \cong F14$ (the Heawood graph), and (6.6) follows at once because X and $R(G)$ are Sylow 7-subgroups of $\mathrm{Aut}(\Gamma)$. □

Chapter 7

CI-property of cyclic balanced configurations

An *incidence geometry* $(P, \mathcal{B})$ consists of a set of v *points* $P = \{p_1, ..., p_v\}$ and a collection of b *lines* (or blocks) $\mathcal{B} = \{B_1, ..., B_b\}$ such that $B_i \subseteq P$ for every $i \in \{1, ..., b\}$, and $|B_i \cap B_j| \leq 1$ for every $i, j \in \{1, ..., b\}$ and $i \neq j$. The incidence geometry $(P, \mathcal{B})$ is called a *configuration* of type (v_r, b_k) (*combinatorial configuration* in the sense of [29]) if

- $|\{B_j \in \mathcal{B} : p_i \in B_j\}| = r$ for every $i \in \{1, .., v\}$; and
- $|B_j| = k$ for every $j \in \{1, .., b\}$ with $k \geq 3$.

A configuration with $v = b$ (and therefore $r = k$) is called *balanced,* or a k-*configuration*, and its *type* is simply denoted by (v_k).

A configuration $(P, \mathcal{B})$ is called *decomposable* if it is the disjoint union of two configurations $(P_r, \mathcal{B}_r), r = 1, 2$, i. e., $P = P_1 \cup P_2$, $P_1 \cap P_2 = \emptyset$, and $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$. Indecomposable configurations are also called *connected*. An *isomorphism* between two incidence geometries $(P_r, \mathcal{B}_r), r = 1, 2$, is a bijective mapping $\sigma : P_1 \to P_2$ which maps $\mathcal{B}_1$ onto $\mathcal{B}_2$. Here a line $B \in \mathcal{B}_1$ with $B = \{p_1, ..., p_k\}$ is mapped onto $B^\sigma = \{p_1^\sigma, ..., p_k^\sigma\}$. If $(P_1, \mathcal{B}_1) = (P_2, \mathcal{B}_2)$, then σ is called an *automorphism*, and the group of all automorphisms will be denoted by $\mathrm{Aut}(P, \mathcal{B})$.

Let $(P, \mathcal{B})$ be an incidence geometry with v points. We say that $(P, \mathcal{B})$ is *cyclic* if it has an automorphism which permutes its points in a full cycle. From now on we identify the point set P with the cyclic group $\mathbb{Z}_v$ and also assume that $(\mathbb{Z}_v)_{\mathrm{right}} \leq \mathrm{Aut}(P, \mathcal{B})$. Thus $(\mathbb{Z}_v, \mathcal{B})$ can be regarded as a Cayley object of $\mathbb{Z}_n$ where $\mathcal{B}$ defines the k-ary relation consisting of all k-tuples $(x_1, \ldots, x_k)$ for which $\{x_1, \ldots, x_k\}$ is a line in $\mathcal{B}$. Thus two cyclic configurations are isomorphic if and only if they are isomorphic as Cayley objects. In this chapter we study the CI-property of cyclic configurations. It follows at once from Pálfy's Theorem 2.16 that the CI-property is guaranteed provided that the number of points is $v = 4$ or it satisfies $(v, \varphi(v)) = 1$, where φ is Euler's totient function. Another special when the configuration is a projective plane was considered by Jungnickel.

Theorem 7.1 (Jungnickel [39]). *Every projective plane with a regular abelian automorphism group has the CI-property*

Projective planes are examples of balanced configurations. As for an example of a cyclic configuration which does not have the CI-property, we refer to [68]; in this paper Phelps gave an example of cyclic 2-$(v, 3, 1)$ design which does not have the CI-property. It is worth to note that the latter configuration is not balanced. In this thesis we restrict our attention exclusively to the balanced case.

In Section 7.1, we make the simple observation that the incidence graph of a cyclic balanced configuration is a bi-Cayley graph over $\mathbb{Z}_v$; moreover, the configuration has the CI-property if and only if the incidence graph is a BCI-graph. In fact, this idea occurred in several papers [10, 30, 66, 67], see also the monograph [69]. Some easy corollaries of this equivalence will be also derived, namely, we give a short proof for the fact that all cyclic balanced 3- and 4-configurations have the CI-property.

In Section 7.2, we give more examples of cyclic balanced configurations having the CI-property. The main result will be the following theorem:

Theorem 7.2. *Every cyclic balanced configuration with v-points has the CI-property if $v = pq$ or $v = p^n$, where p, q are primes.*

Finally, in Section 7.3, we turn to the enumeration problem for configurations. This problem, both for geometrical and combinatorial configurations, attracted considerable attention, see the monograph [29, Chapters 2-3]. Betten et al. [8] produced the list of all configurations of type (v_3). Here we are going to derive a close formula for the number of connected cyclic configurations of type (v_3).

Theorem 7.3. *Let $v > 4$ be an integer with prime factorization $v = p_1^{n_1} \cdots p_k^{n_k}$. Then the number of connected cyclic configurations of type (v_3) is given by the following formula:*

$$\begin{array}{ll} \frac{v}{6} \prod_{i=1}^{k} \left(1 + \frac{1}{p_i}\right) + \alpha 2^k - 2 & \text{if } v \text{ is odd}, \\ \frac{v}{6} \prod_{i=1}^{k} \left(1 + \frac{1}{p_i}\right) + \beta 2^k - 3 & \text{if } v \text{ is even}, \end{array} \tag{7.1}$$

where α is defined for v odd by

$$\alpha = \begin{cases} 5/6 & \text{if every } p_i \equiv 1 (\mathrm{mod}\ 3), \\ 2/3 & \text{if } p_1^{n_1} = 3 \text{ and if } i > 1, \text{ then } p_i \equiv 1 (\mathrm{mod}\ 3), \\ 1/2 & \text{otherwise}, \end{cases}$$

and β is defined for v even by

$$\beta = \begin{cases} 1/4 & \text{if } \ v \equiv 2 (\mathrm{mod}\ 8) \text{ or } v \equiv 6 (\mathrm{mod}\ 8), \\ 1/2 & \text{if } \ v \equiv 4 (\mathrm{mod}\ 8), \\ 1 & \text{if } \ v \equiv 0 (\mathrm{mod}\ 8). \end{cases}$$

7.1 Balanced configurations and bi-Cayley graphs

Let $\mathcal{C} = (P, \mathcal{B})$ be an arbitrary configuration. The *incidence graph* $\Gamma(\mathcal{C})$ of $\mathcal{C}$ is the bipartite graph whose colour classes are identified with the point set P and the line set $\mathcal{B}$, and the vertex associated with a point $p \in P$ is adjacent to the vertex associated with a line $B \in \mathcal{B}$ if and only if $p \in B$.

Example 7.4. We depicted in Fig. 7.1 the *Fano plane* $\mathcal{F}$, the unique projective plane of order 2, and its incidence graph. The point set of $\mathcal{F}$ is the set $\{1, 2, \ldots, 7\}$, and it has 7 lines each having 3 points. These lines correspond to the 3 sides, the 3 altitudes, and the inner circle of the triangle.

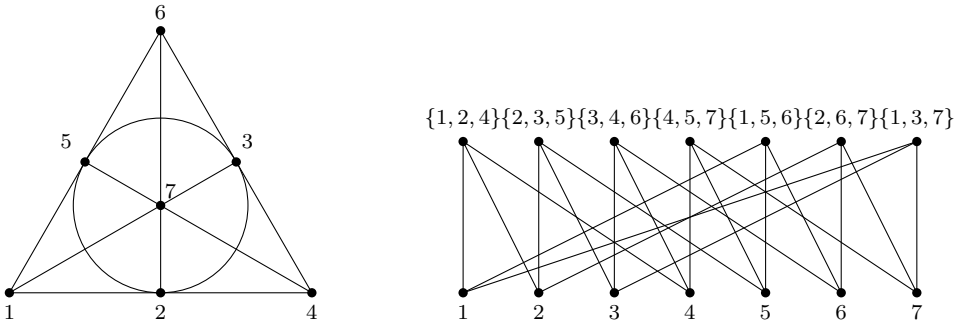

Figure 7.1: The Fano plane $\mathcal{F}$ and its incidence graph $\Gamma(\mathcal{F})$.

It can be checked directly that the cycle $\pi = (1\,2\,3\,4\,5\,6\,7)$ is an automorphism of $\mathcal{F}$ which permutes the lines in a 7-cycle. Thus the group $G := \langle \pi \rangle$ induces an automorphism group of the graph $\Gamma(\mathcal{F})$ such that G is semiregular on the vertex set, and its orbits coincide with the point set and the line set. By definition, $\Gamma(\mathcal{F})$ is a bi-Cayley graph of G. A possible bi-Cayley representation of $\Gamma(\mathcal{F})$ is shown in Fig. 7.2.

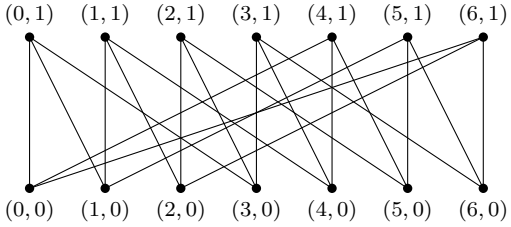

Figure 7.2: A bi-Cayley representation $\mathrm{BCay}(\mathbb{Z}_7, \{0, 4, 6\})$ of the graph $\Gamma(\mathcal{F})$.

□

In the following lemma we generalize the above example.

Lemma 7.5. *Let $\mathcal{C} = (\mathbb{Z}_v, \mathcal{B})$ be a balanced configuration such that $(\mathbb{Z}_v)_{\mathrm{right}} \leq \mathrm{Aut}(\mathcal{C})$. Then the following hold.*

(i) There exists a subset S of $\mathbb{Z}_v$ such that $\mathcal{B}$ consists of the sets in the form $S+i$, $i \in \mathbb{Z}_v$.

(ii) The incidence graph $\Gamma(\mathcal{C})$ is isomorphic to $\mathrm{BCay}(\mathbb{Z}_v, S)$.

PROOF. For sake of simplicity we put $G = (\mathbb{Z}_v)_{\mathrm{right}}$. Choose a line $B \in \mathcal{B}$ such that $0 \in B$, where 0 is the zero element of $\mathbb{Z}_v$. Assume for the moment that B satisfies the following property:

$$B^g = B \text{ or } B^g \cap B = \emptyset \text{ for every } g \in G. \tag{7.2}$$

In other words, B is a block for G. Since G is regular on $\mathbb{Z}_v$, B is an orbit of a subgroup of G of size k, where k is the size of the lines. Since G is a cyclic group, the set B is uniquely determined. Choose next a line $B' \in \mathcal{B}$ for which $0 \in B'$ and $B' \neq B$. Then (7.2) does not hold for B', i. e., there exists $g \in G$ such that B' and B'^g have a nonempty intersection. Since B and B' are two lines they intersect at a unique point, let $i \in \mathbb{Z}_v$ be this point.

Consider the action of G on the set $\mathcal{B}$. The stabilizer $G_{B'}$ of the line B' in this action is defined as $G_{B'} = \{g \in G \mid B'^g = B'\}$. Then $G_{B'^g} = g^{-1}G_{B'}g$, $|G_{B'^g}| = |G_{B'}|$, and so $G_{B'^g} = G_{B'}$ as G is a cyclic group. Clearly, every element in $G_{B'} \cap G_{B'^g}$ fixes the point i. Since G is regular on the points, we get $G_{B'} = G_{B'} \cap G_{B'^g} = 1$. By Theorem 2.3, the orbit of B' under G is of length $|G| = |P| = |\mathcal{B}|$. Letting $S = B'$, the part (i) of the lemma follows.

In order to prove part (ii), we associate the point set $\mathbb{Z}_v$ with $\mathbb{Z}_v \times \{1\}$ by associating the point $i \in \mathbb{Z}_v$ with $(i, 1)$; and the line set $\mathcal{B}$ with $\mathbb{Z}_v \times \{0\}$ by associating the line $S + i \in \mathcal{B}$ with $(i, 0)$. It follows from part (i) that the bi-Cayley graph $\mathrm{BCay}(\mathbb{Z}_v, S)$ is isomorphic to the incidence graph $\Gamma(\mathcal{C})$. □

We shall refer to the set S in Lemma 7.5 as a *base line* of $\mathcal{C}$, and use the symbol $\mathrm{Con}(\mathbb{Z}_v, S)$ for $\mathcal{C}$. Base lines are characterized in the next lemma.

Lemma 7.6 (Hladnik et al. [30]). *The following (i)-(ii) are equivalent for every subset S of $\mathbb{Z}_v$.*

(i) S is a base line of a cyclic configuration of type (v_k).

(ii) $|S| = k$ and $|S - S| = k^2 - k + 1$, where $S - S = \{s_1 - s_2 : s_1, s_2 \in S\}$.

Suppose that S is a base line such that $0 \in S$ (clearly, every configuration admits base lines with this property). The set S generates a subgroup of $\mathbb{Z}_v$, say of order d, and denote it by $\mathbb{Z}_d$. Then $\mathrm{Con}(\mathbb{Z}_d, S)$ is a connected configuration. Also, $\mathrm{Con}(\mathbb{Z}_v, S)$ decomposes to the union of v/d copies of $\mathrm{Con}(\mathbb{Z}_d, S)$:

$$\mathrm{Con}(\mathbb{Z}_v, S) \cong \mathrm{Con}(\mathbb{Z}_d, S) \cup \cdots \cup \mathrm{Con}(\mathbb{Z}_d, S). \tag{7.3}$$

Note that, if S is an arbitrary base line (0 is not necessarily in S), then it holds:

$$\mathrm{Con}(\mathbb{Z}_v, S) \text{ is connected} \iff \langle S - S \rangle = \mathbb{Z}_v. \tag{7.4}$$

The following necessary condition, which follows from Lemma 7.6(ii), for a set to be a base line will be used frequently through the chapter.

Corollary 7.7. *If a subset S of $\mathbb{Z}_v$ is a base line of a cyclic configuration, then S contains no H-coset for every nontrivial subgroup $H \leq \mathbb{Z}_v$.*

For positive integers v and k denote by $B(v,k)$ the set of all base lines of $\mathbb{Z}_v$ of size k, and by $B_{\rm con}(v,k)$ the set of those which define connected configurations. More formally,

$$\begin{aligned} B(v,k) &= \big\{X \subseteq \mathbb{Z}_v : \ |X| = k \text{ and } |X - X| = k^2 - k + 1\big\}, \\ B_{\rm con}(v,k) &= \big\{X \in B(v,k) : \langle X - X\rangle = \mathbb{Z}_v\big\}. \end{aligned}$$

Notice that, if $X \in B(v,k)$, $a \in \mathbb{Z}_v^*$ and $b \in \mathbb{Z}_v$, then the set $aX+b$ is also in $B(v,k)$. Hence the mapping $X \mapsto aX+b$ defines an action of the group $AGL(1,v)$ on $B(v,k)$. Clearly, the subset $B_{\rm con}(v,k)$ of $B(v,k)$ is invariant with respect to this action.

Next, we review the definition of a circulant matrix. Let A be an v-by-v matrix. The matrix A is a *permutation matrix* if it is a $(0,1)$-matrix, and every row and column contains exactly one 1's. Furthermore, $A = (a_{i,j})$ is a *circulant matrix* if $a_{i+1,j+1} = a_{i,j}$ holds for every $i,j \in \{0,1,...,v-1\}$, where the additions in subscripts are modulo v. Here we label rows and columns by elements of $\mathbb{Z}_v$. We let $\mathbb{Z}_v = \{0,1,...,v-1\}$, the leftmost column is labelled 0, the next is 1 and so on. If $A = (a_{i,j})$ is an v-by-v $(0,1)$ circulant matrix, then denote by S_A the subset of $\mathbb{Z}_v$ defined by

$$S_A = \{i \in \mathbb{Z}_v : a_{0,i} = 1\}.$$

The cardinality $|S_A|$ is also called the *weight* of A. Also, A^T denotes the transpose of the matrix A.

Let $S \in B(v,k)$, and let A be the circulant $(0,1)$-matrix defined by $S_A = S$. It follows immediately from the definitions that, A is a *line-point incidence matrix* of the cyclic configuration $\mathrm{Con}(\mathbb{Z}_v, S)$ (see [29]).

Lemma 7.8. *For $r = 1,2$, let $S_r \in B(v,k)$, and let A_r be the $(0,1)$ circulant matrix defined by $S_{A_r} = S_r$.*

(i) The following are equivalent:

- *(i1)* $\mathrm{Con}(\mathbb{Z}_v, S_1) \cong \mathrm{Con}(\mathbb{Z}_v, S_2)$
- *(i2)* $A_1 = PA_2Q$ *for some v-by-v permutation matrices P and Q.*
- *(i3)* $\mathrm{BCay}(\mathbb{Z}_v, S_1) \cong \mathrm{BCay}(\mathbb{Z}_v, S_2)$.

(ii) The configuration $\mathrm{Con}(\mathbb{Z}_v, S)$ *has the CI-property if and only if* $\mathrm{BCay}(\mathbb{Z}_v, S)$ *is a BCI-graph.*

Proof. Let P and Q arbitrary v-by-v permutation matrices. Associate the permutation π of $\mathbb{Z}_v$ with P and the permutation σ of $\mathbb{Z}_v$ with Q as follows:

$$i^\pi = j \iff^{def} P_{i,j} = 1 \text{ and } i^\sigma = j \iff^{def} Q_{j,i} = 1 \text{ for evey } i,j \in \mathbb{Z}_v.$$

Then

$$(PA_2Q)_{i,j} = \sum_{k,l=0}^{v-1} P_{i,k}(A_2)_{k,l}Q_{l,j} = (A_2)_{i^\pi, j^\sigma}.$$

Now, $A_1 = PA_2Q$ can be interpreted as the permutation σ maps the line $S_1 + i$ to the line $S_2 + i^\pi$. Equivalently, σ induces an isomorphism from $\mathrm{Con}(\mathbb{Z}_v, S_1)$ to $\mathrm{Con}(\mathbb{Z}_v, S_2)$. The equivalence $(i1) \Leftrightarrow (i2)$ follows.

We finish the proof of (i) by showing the equivalence $(i1) \Leftrightarrow (i3)$. It is easy seen that $(i1) \Rightarrow (i3)$ holds. For $(i1) \Leftarrow (i3)$, suppose that the graph $\mathrm{BCay}(\mathbb{Z}_v, S_1) \cong \mathrm{BCay}(\mathbb{Z}_v, S_2)$. We have shown in the proof of Lemma 3.5 that there exists an isomorphism ϕ from the first graph to the second one which, as a permutation of $\mathbb{Z}_v \times \{0, 1\}$, fixes setwise $\mathbb{Z}_v \times \{0\}$ (and thus $\mathbb{Z}_v \times \{1\}$ as well). By Lemma 7.5(ii), there also exists an isomorphism σ from the incidence graph of $\mathrm{Con}(\mathbb{Z}_v, S_1)$ to the incidence graph of $\mathrm{Con}(\mathbb{Z}_v, S_2)$ such that σ preserves the colour classes defined by the two point sets. This gives immediately that σ induces an isomorphism between the two configurations, and so $(i1) \Leftarrow (i3)$ holds too.

By definition, the configuration $\mathrm{Con}(\mathbb{Z}_v, S)$ has the CI-property if whenever $\mathrm{Con}(\mathbb{Z}_v, S) \cong \mathrm{Con}(\mathbb{Z}_v, T)$ for some $T \in B(v, |S|)$, there is some $a \in \mathbb{Z}_v^*$ such that

$$a \cdot \{S + i \mid i \in \mathbb{Z}_v\} = \{T + i \mid i \in \mathbb{Z}_v\}.$$

Clearly, this is equivalent to the condition that $T = aS + b$ for some $b \in \mathbb{Z}_v$. On the other hand, $\mathrm{BCay}(\mathbb{Z}_v, S)$ is a BCI-graph if whenever $\mathrm{BCay}(\mathbb{Z}_v, S) \cong \mathrm{BCay}(\mathbb{Z}_v, R)$ for some subset R, then there is some $c \in \mathbb{Z}_v^*$ and $d \in \mathbb{Z}_v$ such that $R = cS + d$. Because of these and part (i) we are done if show the following: if $\mathrm{BCay}(\mathbb{Z}_v, S) \cong \mathrm{BCay}(\mathbb{Z}_v, R)$ for some subset R, then $R \in B(v, |S|)$. This follows by the observation that $R \in B(v, |S|)$ if and only if the graph $\mathrm{BCay}(\mathbb{Z}_v, R)$ has girth larger than 4. This completes the proof of part (ii). □

Lemma 7.8(i2) brings us to the following result of Wiedemann and Zieve:

Theorem 7.9 (Wiedemann and Zieve [76])**.** *The following (i)-(iv) are equivalent for every two v-by-v $(0, 1)$ circulant matrices A_1 and A_2 of weight at most 3.*

(i) There is $a \in \mathbb{Z}_v^*$ and $b \in \mathbb{Z}_v$ such that $S_{A_1} = aS_{A_2} + b$.

(ii) There are v-by-v permutation matrices P, Q such that $A_1 = PA_2Q$.

(iii) There is an v-by-v permutation matrix P such that $A_1A_1^T = PA_2A_2^TP^{-1}$.

(iv) The complex matrices $A_1A_1^T$ and $A_2A_2^T$ are similar.

The above theorem and Lemma 7.8 give us the following corollary:

Corollary 7.10. *Every cyclic 3-configuration has the CI-property.*

Our description of isomorphic tetravalent circulant bi-Cayley graphs in Theorem 4.1 allows us to extend the above statement to 4-configurations. We finish the section with this statement.

Proposition 7.11. *Every cyclic 4-configuration has the CI-property.*

PROOF. We prove the proposition for connected configurations. The general case follows then by using the decomposition in (7.3) and induction on the number of points.

Let $\mathrm{Con}(\mathbb{Z}_v, S)$ be a connected 4-configuration. Then $\langle S - S\rangle = \mathbb{Z}_v$, see (7.4), and hence $\mathrm{BCay}(\mathbb{Z}_v, S)$ is a connected graph. By Lemma 7.8, it is sufficient to show that $\mathrm{BCay}(\mathbb{Z}_v, S)$ is a BCI-graph. For this purpose we apply Theorem 4.1. This implies that, if $\mathrm{BCay}(\mathbb{Z}_v, S)$ is not a BCI-graph, then there exist $a \in \mathbb{Z}_v^*$ and $b \in \mathbb{Z}_v$ such that

$$aS + b = \{0, u, v, v + m\},$$

where $v = 2m$, $\mathbb{Z}_v = \langle u, v\rangle$, $2 \mid u$ and $2u \mid m$. However, in this case S contains a coset of the nontrivial subgroup $\langle m\rangle \leq \mathbb{Z}_v$. This is impossible by Corollary 7.7, hence $\mathrm{BCay}(\mathbb{Z}_v, S)$ is indeed a BCI-graph. □

7.2 Proof of Theorem 7.2

Recall that, $\mathrm{Obj}(\mathbb{Z}_v)$ denotes the set of all cyclic objects of the group $\mathbb{Z}_v$, and given a class $\mathcal{K}$ of cyclic objects in $\mathrm{Obj}(\mathbb{Z}_v)$, a solving set for $\mathcal{K}$ is a set Δ of permutations of $\mathbb{Z}_v$ satisfying the following property:

$$(\forall X \in \mathcal{K})\ (\forall Y \in \mathrm{Obj}(\mathbb{Z}_v)\ (X \cong Y \iff X^\sigma = Y \text{ for some } \sigma \in \Delta).$$

In this context Lemma 2.15 implies the following equivalence:

Lemma 7.12. *The following are equivalent for every object $X \in \mathrm{Obj}(\mathbb{Z}_v)$.*

(i) $\mathbb{Z}_v^*$ is a solving set for X.

(ii) Every two regular cyclic subgroup of $\mathrm{Aut}(X)$ are conjugate in $\mathrm{Aut}(X)$.

PROOF OF THEOREM 7.2. Obviously, the theorem can be rephrased as follows: $\mathbb{Z}_v^*$ is a solving set for the class of cyclic configurations on v points if $v = pq$ or $v = p^n$, where p and q are primes.

THE CASE $v = pq$: We prove the above statement for connected configurations. The general case follows then by using the decomposition in (7.3) and the fact that the statement is true for configurations with a prime number of points, so let $\mathcal{C} = \mathrm{Con}(\mathbb{Z}_{pq}, S)$ be a connected cyclic configuration.

Towards a contradiction assume that $\mathbb{Z}_{pq}^*$ is not a solving set for $\mathcal{C}$. Because of Theorem 2.16 we may also assume that q divides $p - 1$. In the rest of the proof we follow the notations set in page 14 and 15: τ_0, a, b, α and $\nu_0, \nu_1, ..., \nu_{q-1}$. Let $P = \{0, q, ..., (p-1)q\}$, i.e., the subgroup of $\mathbb{Z}_{pq}$ of order p. Replace S with a suitable line $S + i$ if necessary to ensure that $S \cap P \neq \emptyset$. Also, $S \not\subseteq P$ by the connectedness of X, i.e., there exists $t \in \{1, ..., q - 1\}$ such that

$$S \cap P \neq \emptyset \text{ and } S \cap (P + t) \neq \emptyset. \tag{7.5}$$

Suppose for the moment that $\tau_0 \in \mathrm{Aut}(\mathcal{C})$. Using that τ_0 fixes every point outside P, (7.5) and that $|S| \geq 3$, we conclude $|S^{\tau_0^k} \cap S| \geq 2$ for some $k \in \{1, ..., q - 1\}$.

Hence $S^{\tau_0^k} = S$. As P is an orbit of τ_0^k, $P \subseteq S$, which contradicts Corollary 7.7. Thus $\tau_0 \notin \mathrm{Aut}(\mathcal{C})$.

Therefore, Theorems 2.17 and 2.18, together with the assumption that $\mathbb{Z}_{pq}^*$ is not a solving set, imply that $\mathcal{C}$ admits a solving set Δ defined in (2.3). Consider the permutation $\sigma = \prod_{l=0}^{q-1} \tau_l^{b^{(l+1)k}}$, $k \in \{0, 1, ..., q-1\}$. If $k = 0$, then $\sigma = \tau^q$ which is clearly in $\mathrm{Aut}(\mathcal{C})$. The corresponding permutations in Δ are $\mu_a^i \, \nu_0 \, \mu_j^{-1} = \mu_a^i \, \mu_{a^\alpha} \, \mu_j^{-1}$. Since $\Delta \not\subseteq \mathbb{Z}_v^*$, there must exist $k > 0$ for which $\sigma = \prod_{l=0}^{q-1} \tau_l^{b^{(l+1)k}}$ belongs to $\mathrm{Aut}(\mathcal{C})$. Notice that,

$$\forall i, j \in \{0, 1, ..., q-1\} : \; i \neq j \implies b^{ik} \not\equiv b^{jk} (\mathrm{mod}\, p). \tag{7.6}$$

For otherwise, $b^{(i-j)k} \equiv 1 (\mathrm{mod}\, p)$. Since $\mathrm{ord}_{\mathrm{m}}(a) = p - 1$, $a \equiv 1 (\mathrm{mod}\, q)$ and $b = a^{(p-1)/q}$, we find from $a^{(p-1)(i-j)k/q} = b^{(i-j)k} \equiv 1 (\mathrm{mod}\, p)$ that $p - 1$ divides $(p-1)(i-j)k/q$, and so q divides $(i-j)k$, a contradiction.

Consider the product $\sigma' = \sigma \tau^{-b^k}$. Now, σ' fixes each point in P, but because of (7.6) it permutes the points of $P + t$ in a p-cycle. Unless $|S \cap (P + x)| \leq 1$ for every $x \in \{0, 1, ..., q-1\}$, we may also assume that $|S \cap P| \geq 2$. However, if $|S \cap P| \geq 2$, then σ' fixes S, implying that $(P + t) \subseteq S$, which is impossible.

We are left with the case that $|S \cap (P + x)| \leq 1$ for every $x \in \{0, 1, ..., q-1\}$. Note that, then the same holds for all lines $S + i$. It is obvious that $|S| \leq q$. Let $\{s\} = S \cap P$. As $\mathcal{C}$ is balanced, there are exactly $|S|$ lines through s. Now, each of the lines $S, S^{\sigma'}, ..., S^{\sigma'^{p-1}}$ contains s, while they intersect $P + t$ at distinct points. These imply in turn that, they are pairwise distinct, hence $|S| \geq p$, and so $p \leq |S| \leq q$, a contradiction. This completes the proof of case $v = pq$.

We turn next to the case $v = p^n$. Now, we cannot relay on a list of solving sets covering all cyclic objects as such list is available only when $v = p^2$ (see [32]). The argument below will be a combination of Lemma 7.12 with Sylow's theorems.

The case $v = p^n$: Again, it is sufficient to consider connected configurations, the general case follows then by using the decomposition in (7.3) and induction on n. Let $\mathcal{C} = \mathrm{Con}(\mathbb{Z}_{p^n}, S)$ be a connected cyclic configuration, $G = \mathrm{Aut}(\mathcal{C})$ and C be the group generated by $\tau : x \mapsto x + 1$. Let G_p be a Sylow p-subgroup of G such that $C \leq G_p$. By Lemma 7.12 and Sylow's theorems it is sufficient to prove that $G_p = C$.

Towards a contradiction assume that $C < G_p$. Then the normalizer $N_{G_p}(C) > C$. Let us put $N = N_{G_p}(C)$ and let N_0 be the stabilizer of 0 in N. Then N_0 is non-trivial, and we may choose σ from N_0 of order p. Since σ normalizes the regular subgroup C and fixes 0, $\sigma = \mu_a$ for some $a \in \mathbb{Z}_{p^n}^*$ (see [18, Exercise 2.5.6]). Then $\mathrm{ord}_{\mathrm{m}}(a) = p$. Using the well-known structure of $\mathbb{Z}_{p^n}^*$ (cf. [38, Theorem 6.7 and Exercise 6.12]) we deduce that $n \geq 2$, and either

$$a = a' p^{n-1} + 1 \text{ for some } a' \in \{1, \ldots, p-1\},$$

or $n \geq 3$, $p = 2$ and $a \in \{2^n - 1, 2^{n-1} - 1\}$.

Assume for the moment that the latter case holds. Let $Q = \langle C, \sigma \rangle$. It is a routine exercise to show that C is the only cyclic subgroup of Q of order 2^n. This implies that the normalizer $N_{G_2}(Q) \leq N_{G_2}(C) = N$. Let H be an arbitrary regular

cyclic subgroup of G. If $Q = G_2$, then, by Sylow's theorems, $H^g < Q$ for some $g \in G$, and so $H^g = C$, and we are done by Lemma 7.12. Thus we may assume that $Q < G_2$. Then $Q < N_{G_2}(Q) \leq N$. Choose an element $\sigma' \in N_0$ such that $\sigma' \neq \sigma$. It is well-known that $5^{2^{n-3}} \equiv 2^{n-1} + 1 (\mathrm{mod}\, 2^n)$ (see [38, Lemma 6.9]), and that $\mathbb{Z}_{2^n}^* = \langle 5 \rangle \times \langle -1 \rangle \cong \mathbb{Z}_{2^{n-2}} \times \mathbb{Z}_2$ (see [38, Theorem 6.10]). These imply that $\mu_{2^{n-1}+1} \in \langle \sigma, \sigma' \rangle$, and so $\mu_{2^{n-1}+1} \in N_0$. Therefore, we may assume that $\mu_a \in \mathrm{Aut}(\mathcal{C})$ where $a = a'p^{n-1} + 1$ for some $a' \in \{1, \ldots, p-1\}$.

Now, μ_a maps S to a line of $\mathcal{C}$, hence we may write $aS + b = S$ for some $b \in \mathbb{Z}_{p^n}$. Equivalently, S is a union of orbits of the affine transformation $\varphi : x \mapsto ax + b$. Then φ^p is equal to the translation $x \mapsto x + (1 + a + \cdots + a^{p-1})b$. By Corollary 7.7, S contains no non-trivial cosets. Form this and that S is a union orbits of φ^p, we find that $(1 + a + \cdots + a^{p-1})b \equiv 0 (\mathrm{mod}\, p^n)$. This quickly implies that p^{n-1} divides b, hence we may write $b = b'p^{n-1}$ for some $b' \in \{0, 1, ..., p-1\}$. Also,

$$\varphi : x \mapsto ax + b = x + (a'x + b')p^{n-1}.$$

From this we easily find the orbits of φ. For $x \in \mathbb{Z}_v$, let O be the orbit which contains x. Then

$$O = \begin{cases} \{x\} & \text{if } a'x + b' \equiv 0 (\mathrm{mod}\, p), \\ P + x & \text{otherwise,} \end{cases}$$

where $P = \{0, p^{n-1}, ..., (p-1)p^{n-1}\}$, i.e., the subgroup of $\mathbb{Z}_{p^n}$ of order p. Since X is connected, $\langle S - S \rangle = \mathbb{Z}_{p^n}$. This implies that $a's + b' \not\equiv 0 (\mathrm{mod}\, p)$ for some $s \in S$. But then the coset $(P + s) \subseteq S$, contradicting Corollary 7.7. This completes the proof of the theorem. □

7.3 Proof of Theorem 7.3

From now on we denote by $\#C(v_3)$ the total number cyclic balanced configurations of type (v_3). Corollary 7.10 implies that the number $\#C(v_3)$ is equal to the number of orbits of $AGL(1, v)$ acting on $B_{\mathrm{con}}(v, 3)$.

Lemma 7.13. *Let v and k be integers such that $k \geq 3$ and $v \geq k^2 - k + 1$, and denote by $\mathcal{N}$ the number of orbits of $AGL(1, v)$ acting on $B_{\mathrm{con}}(v, k)$. Then*

$$\mathcal{N} = \frac{1}{k\phi(v)} \sum_{l \in \mathbb{Z}_v^*} N(v, k, l),$$

where $N(v, k, l) = \big\{X \in B_{\mathrm{con}}(v, k) : 0 \in X \text{ and } lX = X - x \text{ for some } x \in X\big\}$.

Proof. For short we put $B_0 = \{X \in B_{\mathrm{con}}(v, k) : 0 \in X\}$, and for $X \in B_0$ with $X = \{x_1, x_2, ..., x_k\}$, define the set

$$\widehat{X} = \{X - x_1, X - x_2, ..., X - x_k\}.$$

It is easily seen that for every set $Y = X - x_i$ it holds $\widehat{Y} = \widehat{X}$. It follows from this that the sets $\widehat{X}$, $X \in B_0$, form a partition of B_0. This partition will be denoted by π. Notice also that $|\widehat{X}| = k$ holds for every class $\widehat{X} \in \pi$ because $|X - X| = k^2 - k + 1$

(see (2) in Lemma 7.6). Let us consider the action of $\mathbb{Z}_v^*$ on B_0 defined by $X^l = l\,X = \{lx : x \in X\}$ for every $l \in \mathbb{Z}_v^*$ and $X \in B_0$. The partition π is preserved by $\mathbb{Z}_v^*$ in this action, denote by $\mathrm{Orb}(\mathbb{Z}_v^*, \pi)$ the set of the corresponding orbits. For $X \in B_0$, denote by $O(X)$ the orbit of X under $AGL(1, v)$, and by $O(\widehat{X})$ the orbit of $\widehat{X}$ under $\mathbb{Z}_v^*$.

We claim that the mapping $f : O(\widehat{X}) \mapsto O(X)$ establishes a bijection from $\mathrm{Orb}(\mathbb{Z}_v^*, \pi)$ to the set of orbits of $AGL_1(v)$ acting on $B_{\mathrm{con}}(v, k)$ (notice that, the mapping f is well-defined). It is clear that f is surjective. To settle that it is also injective choose $X, Y \in B_{\mathrm{con}}(v, k)$ such that $O(X) = O(Y)$. We may assume without loss of generality that $0 \in X \cap Y$. By definition, $Y = aX + b$ for some $a \in \mathbb{Z}_v^*$ and $b \in \mathbb{Z}_v$. Since $0 \in Y$, $b = -ax$ for some $x \in X$. Thus $a'Y = X - x$, where $aa' \equiv 1 (\mathrm{mod}\, v)$, implying that $O(\widehat{X}) = O(\widehat{Y})$, and so f is also injective, hence bijective. We obtain that the required number $\mathcal{N} = |\,\mathrm{Orb}(\mathbb{Z}_v^*, \pi)|$. Then the Lemma 2.4 applied to $\mathrm{Orb}(\mathbb{Z}_v^*, \pi)$ yields the formula:

$$\mathcal{N} = \frac{1}{\phi(v)} \sum_{l \in \mathbb{Z}_v^*} \big|\{\widehat{X} \in \pi : \widehat{X}l = \widehat{X}\}\big|.$$

In order to finish the proof one only needs to observe that $\widehat{X}l = \widehat{X}$ happens exactly when $lX = X - x$ for some $x \in X$; and if this is so, then every set $Y \in \widehat{X}$ satisfies $lY = Y - y$ for some $y \in Y$.This gives us

$$|\{\widehat{X} \in \pi : \widehat{X}l = \widehat{X}\}| = \frac{N(v, k, l)}{k}.$$

The lemma is proved. □

By Corollary 7.10 and Lemma 7.13, we find that,

$$\#C(v_3) = \frac{1}{3\phi(v)} \sum_{l \in \mathbb{Z}_v^*} N(v, 3, l). \tag{7.7}$$

We compute next the parameters $N(v, 3, l)$ in (7.7).

Define first the function $\Phi : \mathbb{N} \to \mathbb{N}$ by $\Phi(1) = 1$, and for $v > 1$ let

$$\Phi(v) = v\Big(1 + \frac{1}{p_1}\Big) \cdots \Big(1 + \frac{1}{p_k}\Big),$$

where v has prime factorization $v = p_1^{n_1} \cdots p_k^{n_k}$. Obviously, Φ is a multiplicative function, i.e., $\Phi(v_1 v_2) = \Phi(v_1)\Phi(v_2)$ whenever $\gcd(v_1, v_2) = 1$.

Lemma 7.14. *If $v > 4$, then*

$$N(v, 3, 1) = \begin{cases} \frac{1}{2}\phi(v)(\Phi(v) - 6) & \text{if } v \text{ is odd,} \\ \frac{1}{2}\phi(v)(\Phi(v) - 6) - 3\phi(v/2) & \text{if } v \text{ is even.} \end{cases}$$

Proof.Define the sets:

$$\begin{aligned} S(v) &= \{(x, y) \in \mathbb{Z}_v \times \mathbb{Z}_v : \langle x, y\rangle = \mathbb{Z}_v\}, \\ S^*(v) &= \{(x, y) \in S(v) : |\{0, x, y, -x, -y, x - y, y - x\}| < 7\}. \end{aligned}$$

We leave for the reader to verify that the function $v \mapsto |S(v)|$ is multiplicative. Let $v = p^n$, p is a prime. Then two elements x, y generate $\mathbb{Z}_v$ if and only if one of them is a generator. By this we calculate that $|S(v)| = 2\phi(v)v - \phi(v)^2 = \phi(v)(2v - \phi(v)) = \phi(v)\,\Phi(v)$. We find, using that all functions ϕ, Φ and $v \mapsto |S(v)|$ are multiplicative, that $|S(v)| = \phi(v)\,\Phi(v)$ for every number v.

Now, for every $x, y \in \mathbb{Z}_v$, $\{0, x, y\} \in B_{\rm con}(v, 3)$ if and only if $(x, y) \in S(v) \setminus S^*(v)$. Therefore,

$$N(v, 3, 1) = \frac{|S(v)| - |S^*(v)|}{2} = \frac{1}{2}\big(\,\phi(v)\Phi(v) - |S^*(v)|\,\big). \tag{7.8}$$

It remains to calculate $|S^*(v)|$. Let v be odd. Then $S^*(v)$ can be expressed as

$$S^*(v) = \{(0,x), (x,0), (x,x), (x,-x), (x,2x), (2x,x) : x \in \mathbb{Z}_v^*\}.$$

Since $v > 4$, there is no coincidence between the above pairs, and so $|S^*(v)| = 6\phi(v)$. The formula for $N(v, 3, 1)$ follows by this and (7.8).

Let v be even, say $v = 2u$. In this case

$$\begin{aligned} S^*(v) \;\; = \;\; & \{(0,x), (x,0), (x,x), (x,-x), (x,2x), (2x,x) : x \in \mathbb{Z}_v^*\} \cup \\ & \{(u,x), (x,u), (x,x+u) : x \in \mathbb{Z}_v \text{ and } \langle x, u\rangle = \mathbb{Z}_v\}. \end{aligned}$$

Again, since $v > 4$, there is no coincidence between the above pairs. A quick computation gives that $|S^*(v)| = 6\phi(v) + 6\phi(u)$. The formula for $N(v, 3, 1)$ follows by this and (7.8). The lemma is proved. □

For $l \in \mathbb{Z}_v^*$, denote by $\mathrm{ord_m}(l)$ the order of l as an element of $\mathbb{Z}_v^*$. Furthermore, $O(l)$ denotes the set of orbits of $\mathbb{Z}_v$ under l, i.e.,

$$O(l) = \big\{\ \{x, lx, ..., l^{m-1}x\} : x \in \mathbb{Z}_v\ \big\} \text{ where } m = \mathrm{ord_m}(l).$$

Lemma 7.15. *Let $l \in \mathbb{Z}_v^*$, $l \neq 1$.*

(i) If $\mathrm{ord_m}(l) > 3$, then $N(v, 3, l) = 0$.

(ii) If $\mathrm{ord_m}(l) = 2$, then

$$N(v,3,l) = \begin{cases} 0 & \text{if } l+1 \equiv 0 (\mathrm{mod}\ v),\ \text{or } v \equiv 0 (\mathrm{mod}\ 4) \text{ and } l \equiv 1 (\mathrm{mod}\ v/2), \\ \frac{3\phi(v)}{2} & \text{otherwise.} \end{cases}$$

(iii) If $\mathrm{ord_m}(l) = 3$, then

$$N(v,3,l) = \begin{cases} 0 & \text{if } l^2 + l + 1 \not\equiv 0 (\mathrm{mod}\ v), \\ \phi(v) & \text{otherwise.} \end{cases}$$

Proof. Put again $B_0 = \{X \in B_{\rm con}(v, 3) : 0 \in X\}$, and let $X \in B_0$ such that $X = \{0, x, y\}$ and

$$lX = X \text{ or } lX = X - x. \tag{7.9}$$

We consider step-by-step all cases (i)-(iii).

(i): Assume by contradiction that (7.9) holds for some $l \in \mathbb{Z}_v^*$ with $\mathrm{ord}_{\mathrm{m}}(l) > 3$. If $Xl = X$, then $l^2x = x$ and $l^2y = y$. This together with $\langle x, y\rangle = \mathbb{Z}_v$ imply that $l^2 \equiv 1 (\mathrm{mod}\, v)$, a contradiction to $\mathrm{ord}_{\mathrm{m}}(l) > 2$. Let $Xl = X - x$, and so $\{lx, ly\} = \{-x, y - x\}$. Now, if $lx = -x$ and $ly = y - x$, then $l^2x = x$ and $l^2y = y$ which is impossible. If $lx = y - x$ and $ly = -x$, then $l^3x = x$ and $l^3y = y$, implying that $l^3 \equiv 1 (\mathrm{mod}\, v)$, which is in contradiction with $\mathrm{ord}_{\mathrm{m}}(l) > 3$.

(ii): Assume that (7.9) holds with $\mathrm{ord}_{\mathrm{m}}(l) = 2$. If $lX = X$, then $lx = y$ and $ly = x$ and so we find X as $X = \{0, x, lx\}$, $x \in \mathbb{Z}_v^*$. Let $lX = X - x$. Then it follows that $lx = -x$ and $ly = y - x$ (otherwise $l^3 \equiv 1 (\mathrm{mod}\, v)$, a contradiction to $\mathrm{ord}_{\mathrm{m}}(l) = 2$), and so $X = \{0, y, -ly + y\}$ where $y \in \mathbb{Z}_v^*$. Since $X \in B_0$, the elements 0, 1, -1, l, $-l$, $l - 1$ and $1 - l$ must be pairwise distinct. We conclude from these that, $N(v, 3, l) = 0$ if $l + 1 = 0 (\mathrm{mod}\, v)$ or $l \equiv 1 (\mathrm{mod}\, v/2)$, and otherwise $N(v, 3, l)$ is the size of the following set:

$$\big\{\{0, x, lx\} : x \in \mathbb{Z}_v^*\big\} \cup \big\{\{0, x, -lx + x\} : x \in \mathbb{Z}_v^*\big\}.$$

We observe in turn that, the two sets above are disjoint, the first has size $\phi(v)/2$, while the second has cardinality $\phi(v)$. Then (ii) follows.

(iii): Assume that (7.9) holds with $\mathrm{ord}_{\mathrm{m}}(l) = 3$. Then $X = lX - x$, $lx = y - x$ and $ly = -x$ (otherwise $l^2 \equiv 1 (\mathrm{mod}\, v)$, see above). Thus $X = \{0, x, x + lx\}$, $x \in \mathbb{Z}_v^*$ and $l^2 + l \equiv -1 (\mathrm{mod}\, v)$. We conclude that, $N(v, 3, l) = 0$ if $l^2 + l + 1 \not\equiv 0 (\mathrm{mod}\, v)$, and otherwise $N(v, 3, l) = \big|\big\{\{0, x, lx + x\} : x \in \mathbb{Z}_v^*\big\}\big| = \phi(v)$. Thus (iii) follows, and this completes the proof of the lemma. □

Proof of Theorem 7.2. By Lemmas 7.13 and 7.14, the sum in (7.7) reduces to

$$\#C(v_3) = \begin{cases} \frac{1}{6}\Phi(v) - 1 + \frac{1}{2}\gamma_1 + \frac{1}{3}\gamma_2 & \text{if } v \text{ is odd,} \\ \frac{1}{6}\Phi(v) - \frac{\phi(v/2)}{\phi(v)} - 1 + \frac{1}{2}\gamma_1 + \frac{1}{3}\gamma_2 & \text{if } v \text{ is even,} \end{cases} \tag{7.10}$$

where γ_1 and γ_2 are defined by

$$\begin{aligned} \gamma_1 &= |\{l \in \mathbb{Z}_v^* : \mathrm{ord}_{\mathrm{m}}(l) = 2,\ l + 1 \not\equiv 0 (\mathrm{mod}\, v) \text{ and } l \not\equiv 1 (\mathrm{mod}\, v/2) \text{ if} \\ &\qquad v \equiv 0 (\mathrm{mod}\, 4)\}|, \\ \gamma_2 &= |\{l \in \mathbb{Z}_v^* : \mathrm{ord}_{\mathrm{m}}(l) = 3 \text{ and } l^2 + l + 1 \equiv 0 (\mathrm{mod}\, v)\}|. \end{aligned}$$

In calculating γ_1 and γ_2 below we shall use the fact $\mathbb{Z}_v^*$ can be written as $\mathbb{Z}_v^* = \mathbb{Z}_{p_1^{n_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{n_k}}^*$, and every $l \in \mathbb{Z}_v^*$ can be expressed as

$$l = (l_1, ..., l_k), \text{ where } l_i \in \mathbb{Z}_{p_i^{n_i}}^* \text{ for every } i \in \{1, ..., k\}. \tag{7.11}$$

Note that, we may assume that $l_i \equiv l (\mathrm{mod}\, p_i^{n_i})$ for every $i \in \{1, ..., k\}$.

Case 1. v is odd.

Since v is odd, there are exactly $2^k - 1$ elements $l \in \mathbb{Z}_v^*$ such that $\mathrm{ord}_{\mathrm{m}}(l) = 2$, and all but one contributes to γ_1 (namely, $l = v - 1$ is excluded in the definition of

γ_1). Thus $\gamma_1 = 2^k - 2$. The value of γ_2 depends solely on the residue of v modulo 9 and the reside of prime factors p_i modulo 3. Let $l \in \mathbb{Z}_v^*$ such that $\mathrm{ord_m}(l) = 3$ and write $l = (l_1, ..., l_k)$ as described in (7.11). Thus l_i is of order 1 or 3 in $\mathbb{Z}^*_{p_i^{n_i}}$.

Case 1.1. $p_i \equiv 1 (\mathrm{mod}\ 3)$ for every $i \in \{1, ..., k\}$.

If l_i is of order 1 in $\mathbb{Z}^*_{p_i^{n_i}}$, then $l \equiv l_i \equiv 1 (\mathrm{mod}\ p_i^{n_i})$, from which $l^2 + l + 1 \equiv 3 (\mathrm{mod}\ p_i^{n_i})$, hence $l^2 + l + 1 \not\equiv 0 (\mathrm{mod}\ v)$, so l cannot contribute to γ_2. If l_i is of order 3 in $\mathbb{Z}^*_{p_i^{n_i}}$, then $l^2 + l + 1 \equiv l_i^2 + l_i + 1 \equiv 0 (\mathrm{mod}\ p_i^{n_i})$ for every $i \in \{1, ..., k\}$, hence $l^2 + l + 1 \equiv 0 (\mathrm{mod}\ v)$. Since there are exactly two elements in $\mathbb{Z}_{p_i^{n_i}}$ of order 3, $\gamma_2 = 2^k$. Substitute this and $\gamma_1 = 2^k - 2$ in (7.10). We obtain that $\#C(v_3) = \frac{1}{6}\Phi(v) + \frac{5}{6}2^k - 2$.

Case 1.2. $v \equiv 3 (\mathrm{mod}\ 9)$ and $p_i \equiv 0/1 (\mathrm{mod}\ 3)$ for every $i \in \{1, ..., k\}$.

We may write $p_1^{n_1} = 3$. We obtain, by the same argument as in the previous case, that l contributes to γ_2 if and only if l_1 is of order 1 in $\mathbb{Z}_{p_1^{n_1}}$, and l_i is of order 3 in $\mathbb{Z}^*_{p_i^{n_i}}$ if $i \geq 2$. Thus $\gamma_2 = 2^{k-1}$, which together with $\gamma_1 = 2^k - 2$ yield in (7.10) that $\#C(v_3) = \frac{1}{6}\Phi(v) + \frac{2}{3}2^k - 2$.

Case 1.3. $v \equiv 0 (\mathrm{mod}\ 9)$ or $p_i \equiv 2 (\mathrm{mod}\ 3)$ for some $i \in \{1, ..., k\}$.

We show that in this case $l^2 + l + 1 \not\equiv 0 (\mathrm{mod}\ v)$ independently of the choice l. Thus $\gamma_2 = 0$, and so $\#C(v_3) = \frac{1}{6}\Phi(v) + \frac{1}{2}2^k - 2$.

Suppose first that $v \equiv 0 (\mathrm{mod}\ 9)$. We may write $p_1 = 3$, now $n_1 \geq 2$. Since $\mathrm{ord_m}(l) = 3$, $l_1 \equiv 1 (\mathrm{mod}\ 3^{n_1 - 1})$. We claim that $l_1^2 + l_1 + 1 \equiv 3 (\mathrm{mod}\ 3^{n_1})$. Indeed, $l_1 \equiv 3^{n_1 - 1}k + 1 (\mathrm{mod}\ 3^{n_1})$ for some $k \in \{0, 1, 2\}$. Hence

$$l_1^2 + l_1 + 1 \equiv (k + 2k)3^{n_1 - 1} + 3 \equiv 3 (\mathrm{mod}\ 3^{n_1}).$$

Therefore, $l^2 + l + 1 \equiv l_1^2 + l_1 + 1 \equiv 3 (\mathrm{mod}\ 3^{n_1})$, and since $n_1 \geq 2$, $l^2 + l + 1 \not\equiv 0 (\mathrm{mod}\ 3_1^{n_1})$, and so $l^2 + l + 1 \not\equiv 0 (\mathrm{mod}\ v)$.

Suppose next that $p_i \equiv 2 (\mathrm{mod}\ 3)$ for some $i \in \{1, ..., k\}$. Then l_i must be of order 1 in $\mathbb{Z}_{p_i^{n_i}}$, and hence $l^2 + l + 1 \equiv l_i^2 + l_i + 1 \equiv 3 (\mathrm{mod}\ p_i^{n_i})$, and so $l^2 + l + 1 \not\equiv 0 (\mathrm{mod}\ v)$.

Case 2. v is even.

Since v is even, l is odd, and thus $l^2 + l + 1 \not\equiv 0 (\mathrm{mod}\ v)$. We obtain that $\gamma_2 = 0$. The value of γ_1 depends on the residue of n modulo 8. The number of elements of order 2 in $\mathbb{Z}_v^*$ is $2^{k-1} - 1$ if $v \equiv 2/6 (\mathrm{mod}\ 8)$, $2^k - 1$ if $v \equiv 4 (\mathrm{mod}\ 8)$, and $2^{k+1} - 1$ if $v \equiv 0 (\mathrm{mod}\ 8)$ (see [38, Exercise 6.12]). Thus

$$\gamma_1 = \begin{cases} 2^{k-1} - 2 & \text{if} \quad v \equiv 2/6 (\mathrm{mod}\ 8), \\ 2^k - 3 & \text{if} \quad v \equiv 4 (\mathrm{mod}\ 8), \\ 2^{k+1} - 3 & \text{if} \quad v \equiv 0 (\mathrm{mod}\ 8). \end{cases} \tag{7.12}$$

Obviously, $\phi(v/2)/\phi(v) = 1$ if $v \equiv 2 (\mathrm{mod}\ 4)$ and it is $1/2$ if $v \equiv 0 (\mathrm{mod}\ 4)$. Substituting this, (7.12) and $\gamma_2 = 0$ in (7.10) yields formula (7.1). The theorem is proved. □

Chapter 8

Conclusions

A number of research problems in algebraic graph theory were solved and are presented in this work. In particular, the isomorphism problem of tetravalent cyclic bi-Cayley graphs was solved, the classification of nilpotent 3-BCI-groups and of connected arc-transitive cubic abelian BCI-graphs were obtained; the CI-problems of balanced cyclic configurations on p^n and pq points, where p and q are primes, were solved, and the enumeration of balanced cyclic configurations of type (v_3) was obtained.

These results represent a contribution to open research problems previously posted in the literature, such as the classification of m-BCI-groups, the CI-problem of combinatorial objects and the enumeration problem for configurations.

The general tools used in this research work range from group theory, algebraic methods in graph theory and purely combinatorial techniques. Computer-implemented algebraic tools, such as MAGMA, were used for particular cases, examples and testing results.

In addition to the results presented in this thesis, this work discusses directions of future research work, such as the relation between the BCI-problem for bi-Cayley graphs and the CI-problem for Cayley graphs, the CI-problem for cyclic configurations or other combinatorial objects, and the study of the automorphism groups of balanced cyclic configurations.

Appendix A

MAGMA calculations

This Appendix contains two calculations we did in the PhD Thesis using the computer package MAGMA.

A.1 BCI-graphs of $\mathbb{Z}_n$

The following procedure checks the BCI-property of all possible cyclic bi-Cayley graphs with connection set $\{0, u, v, w\}$ of $\mathbb{Z}_n$ for a fixed n. As an output, it prints all bi-Cayley graphs BCay($\mathbb{Z}_n$, $\{0, u, v, w\}$), and for each it tells if it is a BCI-graph or not. Notice that, this procedure can be easily modified to check larger valencies.

```
procedure checkBCI(n)

   Cs:={ {0,u,v,w} : u in {1..(n-1)}, v in {1..(n-1)}, w in {1..n-1}|
   (u ne v) and (u ne w) and (v ne w)};

   for S in Cs do

      l:=2*n -1;
      V:={0..l};
      Vp:={1..n-1};
      c:=0;
      E:={ {a,((a+x) mod n) + n} : a in Vp , x in S};
      X:= Graph< V | E >;
      A:= AutomorphismGroup(X);
      L:= Subgroups(A: IsCyclic:=true, OrderEqual:=n);

      for i in {1..#L} do
         if (Orbit(L[i]`subgroup,1) eq {1..n}) and
            (Orbit(L[i]`subgroup,(n+1))
            eq {n+1..2*n}) then
            c:=c+1;
         end if;
      end for;
```

```
      if c eq 1 then
         "BCay(", n, B, ")", "is BCI";
      else
         "BCay(", n, B, ")", "is non-BCI";
      end if;

   end for;
end procedure;
```

A.2 Example 3.6

In the Example 3.6, we considered the bi-Cayley graph $\Gamma = \mathrm{BCay}(G, \{1, a, b\})$, where $G = \langle a, b \mid a^5 = b^4,\ b^{-1}ab = a^2 \rangle$. In the program below we computed that, there is only one conjugacy classes of subgroups of $\mathrm{Aut}(\Gamma)$ isomorphic to G and with orbits equal to the bipartition classes.

```
   a:=Sym(5)!id;
   b:=Sym(5)!(1,2,3,4,5);
   c:=Sym(5)!(1,2,4,3);
   G:=PermutationGroup<20|(1,2,3,4,5),(1,2,4,3)>;

   V:=SetToSequence({x: x in G});
   S:={a,b,c};
   E:={{i,j+20}: i,j in {1..20} | V[j]*Inverse(V[i]) in S};
   X:=Graph<40|E>;
   A:=AutomorphismGroup(X);
   L:=Subgroups(A:OrderEqual := 20);

   for i in {1..#L} do
      if (Orbit(L[i]`subgroup,1) eq {1..20}) and
      (Orbit(L[i]`subgroup,2) eq {21..40}) then
         i;
      end if;
   end for;
>4
   H:=L[4]`subgroup;
   IsIsomorphic(H,G);
>true
```

Bibliography

[1] A. Ádám. 'research problems 2–10'. *J. Combin. Theory*, 2:393, 1967.

[2] M. Arezoomand and B. Taeri. Finite BCI-groups are solvable. To appear in *Int. J. Group Theory*.

[3] M. Arezoomand and B. Taeri. Isomorphisms of finite semi-Cayley graphs. To appear in *Acta Math. Sin. (Engl. Ser.)*.

[4] M. Arezoomand and B. Taeri. Normality of 2-Cayley digraphs. *Discrete Math.*, 338(3):41–47, 2015.

[5] L. Babai. Isomorphism problem for a class of point-symmetric structures. *Acta Math. Acad. Sci. Hungar.*, 29:329–336, 1977.

[6] L. Babai and P. Frankl. Isomorphisms of Cayley graphs. I. In *Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. I*, volume 18 of *Colloq. Math. Soc. János Bolyai*, pages 35–52. North-Holland, Amsterdam-New York, 1978.

[7] S. Bays. Sur les systèmes cycliques des triples de steiner différents pour n premier (ou puissance du nombre premier) de la forme $6n + 1$. *I. Comment. Math. Helv.*, 2:294–305, 1930.

[8] A. Betten, G. Brinkmann, and T. Pisanski. Counting symmetric configurations v_3. *Discrete Appl. Math.*, 99:331–338, 2000.

[9] N. Biggs and M. Hoare. The sextet construction for cubic graphs. *Combinatorica*, 8:153–165, 1983.

[10] M. Boben, T. Pisanski, and A. Žitnik. I-graphs and the corresponding configurations. *J. Combin. Designs*, 13:406–424, 2005.

[11] W. Bosma, J. Cannon, and C. Playoust. The MAGMA Algebra System I: The User Language. *J. Symbolic Comput.*, 24:235–265, 1997.

[12] J. M. Burns and B. Goldsmith. Maximal order abelian subgroups of symmetric groups. *Bull. London Math. Soc.*, 21:70–72, 1989.

[13] M. D. E. Conder. `https://www.math.auckland.ac.nz/~conder/symmcubic10000list.txt`. August 2012.

[14] M. D. E. Conder and P. Dobcsányi. Trivalent symmetric graphs on up to 768 vertices. *J. Combin. Math. & Combin. Comp.*, 40:41–63, 2002.

[15] M. D. E. Conder and R. Nedela. Symmetric cubic graphs of small girth. *J. Combin. Theory Ser. B*, 97:757–768, 2007.

[16] H. S. M. Coxeter. Self-dual configurations and regular graphs. *Bul. Amer. Math. Soc.*, 56:413–435, 1950.

[17] M. J. de Resmini and D. Jungnickel. Strongly regular semi-Cayley graphs. *J. Algebraic Combin.*, 1:171–195, 1992.

[18] J. D. Dixon and B. Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[19] E. Dobson and J. Morris. Quotients of CI-groups are CI-groups. *Graphs and Combin.*, 7:1–4, 2013.

[20] E. Dobson, J. Morris, and P. Spiga. A comment on: "Further restrictions on the structure of finite DCI-groups". arXiv:1402.4373v1 [math.CO] (2014).

[21] S. F. Du and D. Marušič. An infinite family of biprimitive semysimmetric graphs. *J. Graph Theory*, 32:217–228, 1999.

[22] B. Elspas and J. Turner. Graphs with circulants adjacency matrices. *J. Combin. Theory*, 9:297–307, 1970.

[23] Y. Q. Feng and J. H. Kwak. Cubic symmetric graphs of order a small number time a prime or a prime square. *J. Combin. Theory Ser. B*, 97:627–646, 2007.

[24] Y. Q. Feng and R. Nedela. Symmetric cubic graphs of girth at most 7,. *Acta Univ. M. Belii Math.*, 13:33–55, 2006.

[25] Y. Q. Feng and J. X. Zhou. Cubic bi-Cayley graphs over abelian groups. *Europ. J. Combin.*, 36:679–693, 2014.

[26] R. Foster. *The Foster census*. Charles Babbage Research Centre, Winnipeg, MB, 1988. Foster's census of connected symmetric trivalent graphs, with a foreword by H. S. M. Coxeter, with a biographical preface by Seymour Schuster, with an introduction by I. Z. Bouwer, W. W. Chernoff, B. Monson and Z. Star, edited and with a note by Bouwer.

[27] C. Godsil and G. Royle. *Algebraic graph theory*, volume 207 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2001.

[28] J. L. Gross and T. W. Tucker. *Topological graph theory*. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons Inc., New York, 1987.

[29] B. Grünbaum. *Configurations of points and lines*, volume 103 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2009.

[30] M. Hladnik, D. Marušič, and T. Pisanski. Cyclic Haar graphs. *Discrete Math.*, 244:137–152, 2002.

[31] W. C. Huffman. The equivalence of two cyclic objects on pq elements. *Discrete Math.*, 154:103–127, 1996.

[32] W. C. Huffman, V. Job, and V. Pless. Multipliers and generalized multipliers of cyclic objects and cyclic codes. *J. Combin. Theory Ser. A*, 62:183–215, 1993).

[33] B. Huppert. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, 1967.

[34] W. Jin and W. Liu. Two results on BCI-subset of finite groups. *Ars Combin.*, 93:169–173, 2009.

[35] W. Jin and W. Liu. A classification of nonabelian simple 3-BCI-groups. *European J. Combin.*, 31:1257–1264, 2010.

[36] W. Jin and W. Liu. On sylow subgroups of BCI-groups. *Util. Math.*, 86:313–320, 2011.

[37] W. Jin and W. Liu. On isomorphisms of small order bi-Cayley graphs. *Util. Math.*, 92:317–327, 2013.

[38] G. A. Jones and J. M. Jones. *Elementary number theory.* Springer Undergraduate Mathematics Series. Springer-Verlag London Ltd., London, 1998.

[39] D. Jungnickel. The isomorphism problem for Abelian projective planes. *Applicable Algebra in Eng., Comm. and Comp.*, 19:195–200, 2008.

[40] H. Koike and I. Kovács. Arc-transitive cubic abelian bi-cayley graphs and BCI-graphs. to appear in FILOMAT.

[41] H. Koike and I. Kovács. A classification of nilpotent 3-BCI groups. submitted.

[42] H. Koike and I. Kovács. Isomorphic tetravalent circulant Haar graphs. *Ars Math. Contemporanea*, 7(2):215–235, 2014.

[43] H. Koike, I. Kovács, and T. Pisanski. The number of cyclic configurations of type (v_3) and the isomorphism problem. *J. Combin. Des.*, 22(5):216–229, 2014.

[44] I. Kovács, B. Kuzman, A. Malnič, and S. Wilson. Characterization of edge-transitive 4-valent bicirculants. *J. Graph Theory*, 69(4):441–463, 2012.

[45] I. Kovács, B. Kuzman, and A. Malnič. On non-normal arc transitive 4-valent dihedrants. *Acta Math. Sinica (Engl. ser.)*, 26(8):1485–1498, 2010.

[46] I. Kovács, A. Malnič, D. Marušič, and Š. Miklavič. One-mathcing bi-Cayley graph over Abelian groups. *Europ. J. Combin*, 30:602–616, 2009.

[47] K. Kutnar and D. Marušič. A complete classification of cubic symmetric graphs of girth 6. *J. Combin. Theory Ser. B*, 99:162–184, 2009.

[48] P. Lambossy. Sur une manière de différentcier les fonctions cycliques de 'une forme donnée. *I. Comment. Math. Helv.*, 3:69–102, 1931.

[49] K. H. Leung and S. L. Ma. Partial difference triples. *J. Algebraic Combin.*, 2:397–409, 1993.

[50] C. H. Li. Finite CI-groups are soluble. *Bull. London Math. Soc.*, 31(4):419–423, 1999.

[51] C. H. Li. Isomorphism of finite Cayley digraphs of bounded valency, II. *J. Combin. Theory. Ser. A*, 87:333–346, 1999.

[52] C. H. Li. The finite vertex-primitive and vertex-biprimitive s-transitive graphs for $s \geq 4$. *Trans. Amer. Math. Soc.*, 353:3511–3529, 2001.

[53] C. H. Li. On isomorphisms of finite Cayley graphs - a survey. *Discrete Math.*, 256:301–334, 2002.

[54] C. H. Li, Z. P. Lu, and P. Pálfy. Further restrictions on the structure of finite CI-groups. *J. Algebraic Combin.*, 26(2):161–181, 2007.

[55] C. H. Li and C. E. Praeger. Finite groups in which any two elements of the same order are either fused or inverse fused. *Comm. Algebra*, 25(10):3081–3118, 1997.

[56] C. H. Li and C. E. Praeger. On the isomorphism problem for finite Cayley graphs of bounded valency. *European J. Combin.*, 20(4):279–292, 1999.

[57] C. H. Li, C. E. Praeger, and M. Y. Xu. Isomorphisms of finite Cayley digraphs of bounded valency. *J. Combin. Theory. Ser. B*, 73:164–183, 1998.

[58] P. Lorimer. Vertex-transitive graphs: symmetric graphs of prime valency. *J. Graph Theory*, 8:55–68, 1984.

[59] A. Malnič. Group actions, coverings and lifts of automorphisms. *Discrete Math.*, 182:203–218, 1998.

[60] A. Malnič, D. Marušič, and P. Šparl. On strongly regular bicirculants. *Europ. J. Combin.*, 28:891–900, 2007.

[61] M. Muzychuk. Ádám's conjecture is true in the square-free case. *J. Combin Theory Ser. A*, 72:118–134, 1995.

[62] M. Muzychuk. Corrigendum: On Ádám's conjecture for circulant graphs. *Discrete Math.*, 176:285–298, 1997.

[63] M. Muzychuk. On the isomorphism problem for cyclic combinatorial objects. *Discrete Math.*, 197, 198:589–606, 1999.

[64] M. Muzychuk. A solution of the isomorphism problem for circulant graphs. *London Math. Soc.*, 88(3):1–41, 2004.

[65] P. Pálfy. Isomorphism problem for relational structures with a cyclic automorphism. *Eur. J. Combin.*, 8:35–43, 1987.

[66] M. Petkovšek and T. Pisanski. Counting disconnected structures: chemical trees, fullerenes, I-graphs, and others. *Croat. Chem. Acta.*, 78:563–567, 2005.

[67] M. Petkovšek and H. Zakrajšek. Enumeration of I-graphs: Burnside does it again. *Ars Math. Contemp.*, 2:241–262, 2009.

[68] K. T. Phelps. Isomorphism problems for cyclic block designs. *Ann. Discrete Math.*, 34:385–392, 1987.

[69] T. Pisanski and B. Servatius. *Configurations from a graphical viewpoint.* Birkhäuser Advanced Texts: Basler Lehrbücher. Birkhäuser/Springer, New York, 2013.

[70] D. J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1996.

[71] G. Sabidussi. On a class of fixed-point-free graphs. *Proc. Amer. Math. Soc.*, 9:800–804, 1958.

[72] W. R. Scott. *Group Theory.* Dover Publications Inc., New York, 1987.

[73] L. Sun. Isomorphisms of circulants with degree 2. *J. Beijing Ins. Technol.*, 9:42–46, 1984.

[74] W. T. Tutte. A family of cubical graphs. *Proc. Cambr. Philosoph. Soc.*, 43:459–474, 1947.

[75] M. E. Warkins. A theorem on Tait colorings with application to generalized petersen graphs. *J. Combin. Theory*, 6:152–164, 1969.

[76] D. Wiedemann and M. E. Zieve. Equivalence of sparse circulants: the bipartite Ádám problem. arXiv:0706.1567v1 [math. CO] (2007).

[77] S. J. Xu, W. Jin, Q. Shi, and J. J. Li. The BCI-property of the Bi-Cayley graphs. *J. Guangxi Norm. Univ.: Nat. Sci. Edition*, 26:33–36, 2008.

List of Figures

Povzetek v slovenskem jeziku

V doktorski disertaciji obravnavamo problem izomorfnosti bi-Cayleyjevih grafov in z njim povezano vprašanje klasifikacije končnih BCI-grup. Obravnavani so naslednji konkretni problemi oz. vprašanja:

(i) Poiskati učinkovite potrebne in zadostne pogoje za izomorfnost dveh cikličnih bi-Cayleyjevih grafov.

(ii) Katere grupe so 3-BCI-grupe?

(iii) Kateri kubični bi-Cayleyjevi grafi so BCI-grafi?

(iv) Katere ciklične uravnotežene konfiguracije imajo CI-lastnost?

(v) Analitično oštevilčenje uravnoteženih cikličnih konfiguracij.

V doktorski disertaciji je Problem (i) rešen za tetravalentne grafe, Problem (ii) pa za nilpotentne grupe. Prispevek k rešitvi Problema (iii) je dokaz, da je vsak povezan kubičen ločno-tranzitiven bi-Cayleyjev graf BCI-graf. Kar se tiče Problema (iv), je v doktorski disertaciji dokazano, da ima CI-lastnost vsaka ciklična uravnotežena konfiguracija, katere število točk je bodisi enako produktu dveh različnih praštevil ali pa je enako potenci nekega praštevila. Za Problem (v) je izpeljana formula za število povezanih cikličnih konfiguracij tipa (v_3).

BCI-grafi in BCI-grupe

Na podlagi koncepta CI-grafov, m-CI-grup in CI-grup so leta 2008 Xu in ostali [77] predstavili koncept BCI-grafov, m-BCI-grup in BCI-grup. Bi-Cayleyjev graf $\mathrm{BCay}(G, S)$ je *BCI-graf*, če iz $\mathrm{BCay}(G, S) \cong \mathrm{BCay}(G, T)$ za neko podmnožico T grupe G sledi, da je $T = gS^\sigma$ za nek element $g \in G$ in nek avtomorfizem $\sigma \in \mathrm{Aut}(G)$. Grupa G je *m-BCI-grupa*, če je vsak bi-Cayleyjev graf grupe G, ki je stopnje največ m, BCI-graf. Grupa G je *BCI-grupa*, če je vsak bi-Cayleyjev graf grupe G BCI-graf. Teorija BCI-grafov in BCI-grup je precej manj razvita kot teorija CI-grafov in CI-grup. Nekatere osnovne lastnosti BCI-grafov in BCI-grup sta obravnavala Jin in Liu v seriji člankov [34, 35, 36, 37], ne dolgo nazaj pa tudi Arezoomand in Taeri v člankih [3, 2]. V naslednji lemi karakteriziramo BCI-grafe s stališča teorije grup na podoben način, kot je Babai [5] karakteriziral CI-objekte. V tej lemi z $R(G)$ označimo grupo vseh permutacij $R(g)$, $g \in G$, kjer je permutacija $R(g)$ definirana kot $R(g) : (x, i) \mapsto (xg, i)$ za vsak $x \in G$ in $i \in \{0, 1\}$.

Lema 1. *Za vsak bi-Cayleyjev graf* $\Gamma = \mathrm{BCay}(G, S)$ *sta naslednji izjavi ekvivalentni.*

(i) $\mathrm{BCay}(G, S)$ *je BCI-graf.*

(ii) Normalizator $N_{\mathrm{Aut}(\Gamma)}(R(G))$ *je tranzitiven na množici* $V(\Gamma)$ *in je vsaka semiregularna podgrupa grupe avtomorfizmov* $\mathrm{Aut}(\Gamma)$ *z orbitama* $G \times \{0\}$ *in* $G \times \{1\}$*, ki je izomorfna grupi* G*, v grupi* $\mathrm{Aut}(\Gamma)$ *konjugirana podgrupi* $R(G)$*.*

Bolj podrobno obravnavamo povezavo med BCI-grupami in CI-grupami. Med drugim dokažemo naslednjo trditev:

Trditev 1. *Naj bo* $\Gamma = \mathrm{BCay}(G, S)$ *tak graf, da obstaja involucija* $\tau \in \mathrm{Aut}(\Gamma)$*, ki normalizira grupo* $R(G)$*, in da velja enakost* $(1_G, 0)^\tau = (1_G, 1)$*. Predpostavimo še, da je* $\mathrm{Aut}(\Gamma)_{(1_G,0)} = \mathrm{Aut}(\Gamma)_{(1_G,1)}$*. Potem je* $\mathrm{BCay}(G, S)$ *BCI-graph, če je* $\mathrm{Cay}(G, S)$ *CI-graf.*

V bistvu je naša primarna motivacija za obravnavanje BCI-grafov in BCI-grup ta, da nam lahko poznavanje teh objektov prinese nov vpogled v že znan in obravnavan problem klasifikacije CI-grup.

Izomorfni tetravalentni ciklični bi-Cayleyjevi grafi

Problem izomorfnosti grafov, ki jih imenujemo cirkulanti, je bil obdelan s strani mnogih raziskovalcev, popolno rešitev tega problema pa je podal Muzychuk [64]. V doktorski disertacije je obravnavan enak problem za razred *cikličnih bi-Cayleyjevih grafov* (to so bi-Cayleyjevi grafi cikličnih grup). Kolikor je znano, je edini rezultat v smeri rešitve tega problema rezultat Wiedemanna in Zieveja [76], ki sta dokazala, da je vsak cikličen bi-Cayleyjev graf stopnje največ 3 BCI-graf. Poleg tega sta podala primere ne-BCI-grafov stopnje 4, zato tetravalentni bi-Cayleyjevi grafi predstavljajo prvi naslednji netrivialen primer, ki ga je smiselno obravnavati. V doktorski disertaciji je dokazan naslednji izrek:

Izrek 1. *Povezana bi-Cayleyjeva grafa* $\mathrm{BCay}(\mathbb{Z}_n, S)$ *in* $\mathrm{BCay}(\mathbb{Z}_n, T)$*, kjer je* $|S| = |T| = 4$*, sta izomorfna natanko tedaj, ko obstajajo taki elementi* $a_1, a_2 \in \mathbb{Z}_n^*$ *in* $b_1, b_2 \in \mathbb{Z}_n$*, da velja*

(i) $a_1 S + b_1 = T$*; ali*

(ii) $a_1 S + b_1 = \{0, u, v, v + m\}$ *in* $a_2 T + b_2 = \{0, u + m, v, v + m\}$*, kjer je* $n = 2m$*,* $\mathbb{Z}_n = \langle u, v \rangle$*,* $2 \mid u$*,* $2u \mid m$*.*

Zanimivo je, da pogoji za aritmetiko v zgornjem izreku popolnoma sovpadajo s pogoji v rezultatu za kubične cirkulante, ki jih lahko dobimo iz splošnega algoritma, ki ga je podal Muzychuk [64].

Nilpotentne 3-BCI-grupe

V doktorski disertaciji so oravnavani BCI-grafi in 3-BCI-grupe. Trivialno je videti, da je vsaka grupa 1-BCI-grupa, medtem ko so 2-BCI-grupe v smislu teorije

grup opisane v [77]. Klasifikacija 3-BCI-grup je še vedno odprt problem, nekatere delne rezultate, pa lahko najdemo v [34, 35, 36]. V teoriji CI-grup je tovrsten problem obdelan v [53, Problem 9.6]. V doktorski disertaciji je dokazan naslednji izrek, ki predstavja delno rešitev klasifikacije nilpotentnih 3-BCI-grup:

Izrek 2. *Vsaka končna grupa $U \times V$, kjer je U grupa lihega reda tako da so vse p-Sylowke od grupe U homociklične (to je direktni produkt cikličnih grup istega reda), grupa V pa je trivialna, ali pa je ena izmed grup $\mathbb{Z}_{2^r}$, $\mathbb{Z}_2^r$ ali grupa kvaternionov Q_8, je 3-BCI-grupa.*

Povezani ločno-tranzitivni kubični bi-Cayleyjevi grafi so BCI-grafi

V doktorski disertaciji so podani še nekateri novi primeri kubičnih BCI-grafov.

Izrek 3. *Naj bo G končna abelska grupa. Potem je vsak povezan ločno-tranzitiven kubičen bi-Cayleyjev graf* $\mathrm{BCay}(G, S)$ *BCI-graf.*

Poleg tega je v doktorski disertaciji podan popoln opis grafov iz Izreka 3, ki so zanimivi iz različnih razlogov. Ta rezultat je naprimer primerljiv z nedavno klasifikacijo točkovno-tranzitivnih kubičnih bi-Cayleyjevih grafov abelskih grup, ki sta jo naredila Feng in Zhou [25]. Grafi iz Izreka 3 so zanimivi tudi zaradi klasifikacije povezanih ločno-tranzitivnih grafov ožine 6, ki sta jo naredila Kutnar in Marušič [47]. Izkaže se, da ima vsak od grafov iz njunega rezultata semiregularno abelsko grupo avtomorfizmov z dvema orbitama.

CI-lastnost cikličnih uravnoteženih konfiguracij

V tem delu raziskovanja je pozornost usmerjena h konfiguracijam. *Ciklična konfiguracija* $(P, \mathcal{B})$ je sestavljena iz množice točk P in množice premic $\mathcal{B}$, katere elementi so določene podmnožice množice P, poleg tega pa predpostavljamo, da ciklična grupa avtomorfizmov G deluje regularno na množici P. V tem primeru lahko na kanoničen način identificiramo množico P z grupo G in lahko zato na $(P, \mathcal{B})$ gledamo kot na *Cayleyjev-objekt* grupe G. Če je poleg tega konfiguracija $(G, \mathcal{B})$ tudi *uravnotežena* (to pomeni, da je $|G| = |\mathcal{B}|$), potem je pripadajoči incidenčni graf konfiguracije $(G, \mathcal{B})$ bi-Cayleyjev graf grupe G in ima konfiguracija $(G, \mathcal{B})$ CI-lastnost natanko tedaj, ko je pripadajoči bi-Cayleyjev graf BCI-graf. Z upoštevanjem vseh teh dejstev, je v dokotrski disertaciji dokazan naslednji izrek:

Izrek 4. *Vsaka ciklična uravnotežena konfiguracija z v-točkami ima CI-lastnost, če je $v = pq$ ali $v = p^n$, kjer sta p in q različni praštevili.*

Poleg tega je v doktorski disertaciji podana zaprta formula za izračun števila neizomorfnih povezanih cikličnih konfiguracij tipa (v_3) (to so uravnotežene konfiguracije na v točkah, v katerih ima vsaka premica 3 točke):

Izrek 5. *Naj bo $v > 4$ celo število s praštevilsko faktorizacijo $v = p_1^{n_1} \cdots p_k^{n_k}$. Potem lahko število povezanih cikličnih konfiguracij tipa (v_3) izračunamo po naslednji formuli:*

$$\begin{aligned} &\tfrac{v}{6}\prod_{i=1}^{k}\left(1+\tfrac{1}{p_i}\right)+\alpha 2^k-2 \quad && \text{če je } v \text{ lih},\\ &\tfrac{v}{6}\prod_{i=1}^{k}\left(1+\tfrac{1}{p_i}\right)+\beta 2^k-3 \quad && \text{če je } v \text{ sod}, \end{aligned}$$

kjer je število α *definirano za lihe* v *z*

$$\alpha=\begin{cases} 5/6 & \text{če je vsak } p_i\equiv 1(mod\ 3),\\ 2/3 & \text{če je } p_1^{n_1}=3 \text{ in če je } i>1, \text{ potem je } p_i\equiv 1(mod\ 3),\\ 1/2 & \text{sicer}, \end{cases}$$

in je število β *definirano za sode* v *z*

$$\beta=\begin{cases} 1/4 & \text{če je } \ v\equiv 2(mod\ 8) \text{ ali } v\equiv 6(mod\ 8),\\ 1/2 & \text{če je } \ v\equiv 4(mod\ 8),\\ 1 & \text{če je } \ v\equiv 0(mod\ 8). \end{cases}$$

Naj omemimo še, da so rezultati disertacije objavlejni v naslednjih znanstvenih člankih:

- H. Koike, I.Kovács, Isomorphic tetravalent circulant Haar graphs, *Ars Math. Contemporanea* **7** (2014), 215–235.
- H. Koike, I. Kovács, T. Pisanski, The number of cyclic configurations of type (v_3) and the isomorphism problem, *J. Combin. Designs* **22** (2014), 216–229.
- H. Koike, I. Kovács, Arc-transitive cubic abelian bi-Cayley graphs and BCI-graphs, *Filomat*, v tisku.
- H. Koike, I. Kovács, A classification of nilpotent 3-BCI groups, poslano v objavo.

Declaration

I declare that this thesis does not contain any material previously published or written by another person except where due reference is made in the text.

Sergio Hiroki Koike Quintanar