Eötvös Loránd University

Institute of Mathematics

Ph.D. thesis

Cayley graphs

Gábor Somlai

Doctoral School: Mathematics
Director: Miklós Laczkovich
member of the Hungarian Academy of Sciences

Doctoral Program: Pure Mathematics
Director: András Szűcs
member of the Hungarian Academy of Sciences

Supervisor: Péter Pál Pálfy
member of the Hungarian Academy of Sciences

Department of Algebra and Number Theory
2014 May

CONTENTS

ACKNOWLEDGEMENTS

First of all, I wish to give my sincere thanks to my supervisor, Péter Pál Pálfy, who accepted me as his Ph.D. student. Most probably the turning point in my career was when he started to appreciate my work on the problems he suggested me to solve, so I would like to thank him for encouraging my research and for helping me to grow as a mathematician. It is also important to emphasize that despite his important role in the Hungarian mathematician community, he spent a great amount of time to supervise my research. My papers and the thesis would not have come to a successful completion without his help.

Special thanks are also given to László Pyber. He was the one who suggested me to try to solve problems concerning expander graphs. I am extremely grateful for the trust I received from him. I have also learned from him how to be more conscious in research.

I would like to express my gratitude to Miklós Abért for both his financial support and for the possibility to join his extremely active research group.

0. PREFACE

Two major topics are discussed in this thesis. The central objects we investigate in both of them are the Cayley graphs of finite groups. First, we shortly introduce the definition of Cayley graphs and we collect basic facts about them.

Chapter 1, 2 and 3 are devoted to the investigation of Cayley graphs corresponding to the same group. More precisely, Chapter 1 can be considered as an introduction to the isomorphism problem of Cayley graphs, where we recall the concepts of CI-graphs and CI-groups and related notions (DCI-group, DCI$^{(2)}$-group, etc).

In Chapter 2 we construct non-CI Cayley graphs for elementary abelian p-groups which are the most important candidates for CI-groups. Improving earlier results of Muzychuk [Muz3] and Spiga [Spi1], for every prime $p > 3$ we exhibit a Cayley graph on $\mathbb{Z}_p^{2p+3}$ which is not a CI-graph. This proves that an elementary abelian p-group of rank greater than or equal to $3p$ 0 4 is not a CI-group.

On the positive side, in Chapter 3, for every prime $p > 4$ we prove that $Q \pm \mathbb{Z}_p$ is a DCI-group, where Q denotes the quaternion group of order 9. This gives a new infinite family of non-abelian CI-groups, which are really rare. Using the same method we reprove that $\mathbb{Z}_2^3 \pm \mathbb{Z}_p$ is a CI-group for every prime $p > 4$, which was first obtained by Dobson and Spiga [D,S2]. Our new result completes the description of CI-groups of order $9p$. We also apply our method to prove that for every prime $p > 4$ the group $\mathbb{Z}_q \pm \mathbb{Z}_p^3$ is a DCI-group

if q is also a prime with $q > p^3$. Finally, we prove that if G is p-group which is a DCI$^{(2)}$-group, then $G \pm \mathbb{Z}_q$ is a)q 2+DCI-group if q is a prime with $q >$ \$G\$

In Chapter 4 we solve a problem which was a conjecture of Lubotzky [Lub2] about the Cayley graphs of series of finite simple groups. For every infinite sequence of simple groups of Lie type of growing rank we exhibit connected Cayley graphs of degree at most 21 such that the isoperimetric number of these graphs converges to 1. This proves that these graphs do not form a family of expanders.

CAYLEY GRAPHS

Let G be a group and S a subset of $G \wr \}2\langle$. The directed *Cayley graph* of G with respect to S is the graph $Cay)G, S+$with vertex set G such that x is connected to y if and only if y [xs for some s / S. The set S is called the *connection set* of the Cayley graph $Cay)G, S+$ Clearly, a Cayley graph $Cay)G, S+$is an undirected graph if and only if S [$S^{\ 1}$, where $S^{\ 1}$ [$\}s^{\ 1} \setminus s$ / $S\langle$ and $Cay)G, S+$is connected if and only if S generates G. It is also easy to see that the degree of vertices of the Cayley graph $Cay)G, S+$is equal to the cardinality of S. Hence every Cayley graph is a regular graph.

Every left multiplication via elements of G induces an automorphism of the graph $Cay)G, S+$, so the automorphism group of every Cayley graph on G contains a subgroup, acting regularly on the vertices of the graph, isomorphic to G. Hence every Cayley graph is a vertex-transitive graph. Moreover, a graph is a Cayley graph of the group G if and only if it admits a regular group of automorphism isomorphic to G. Using this observation we can define *Cayley objects* which are relational structures with underlying set G such that the left translation by g: $(x \nvDash gx)$ is an isomorphism of the relational structure for every g / G. A directed Cayley graph $Cay)G, S+$is called a *minimal Cayley graph* if S is a minimal generating set of G and an undirected connected Cayley graph $Cay)G, T+$is called minimal if $T \wr \}t, t^{\ 1}\langle$ does not generate G for any element t / T.

We will mostly restrict our attention to finite groups but we do not require S to be a generating set of the group G.

1. ISOMORPHISM PROBLEM OF CAYLEY GRAPHS

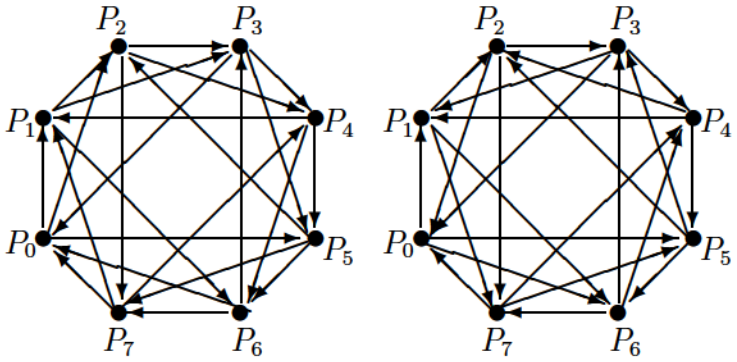
The following seven sections rely on the survey paper of Li [Li1] since it served as a starting points of the author for the research on the isomorphism problem of Cayley graphs. Many of the results we present here were also collected by Li, but we structure them in a different way.

1.1 Origin of the main problem

One of the most important problems in graph theory is the isomorphism problem for graphs. We will only investigate Cayley graphs.

The following problem was proposed by Ádám [Ádá]: For a sequence of integers $1 < k_1 < k_2 < \ldots < k_m < n$ we define the graph $_n)k_1, k_2, \ldots, k_m+$ to be the directed graph with vertices $P_1, P_2, \ldots, P_n$ in which there is an edge from P_i to P_j if $j \quad i \subseteq k_t \ )mod\ n+$for some $2 \geq t \geq m$. Such a graph is called a circulant graph. It is easy to verify that $_n)k_1, k_2, \ldots, k_m+$ is isomorphic to $_n)k_1^{\infty}, k_2^{\infty}, \ldots, k_m^{\infty}+$if there exists an integer $1 < r < n$, what we call a multiplier, relative prime to n such that $k_i^{\infty} \subseteq rk_i \ )mod\ n+$ for $2 \geq i \geq m$. It was conjectured by Ádám that the existence of such a multiplier is also necessary for a pair of circulant graphs $_n)k_1, k_2, \ldots, k_m+$ and $_n)k_1^{\infty}, k_2^{\infty}, \ldots, k_m^{\infty}+$to be isomorphic.

The following example, given by Elspas and Turner see [E,T], shows that Ádám's conjecture does not hold for every pair of circulant graphs:



$_8)2,3,6+$ $_8)2,6,7+$

A reduced residue system *mod* 9 is $2,4,6,8$. It is easy to check that $i\,\}2,3,6\langle\ \{\ \ \}2,6,7\langle$ for $i\ [\ \ 2,4,6,8$. It remains to verify that ϕ is a graph isomorphism, where

$$\phi)P_i+[\ \ P_{3i+2} \quad \text{if } i \text{ is odd}$$
$$\phi)P_i+[\ \ P_{3i} \quad \text{if } i \text{ is even.}$$

The graphs $_1\ [\ \ _{16})2,3,8,:,25,26+$and $_2\ [\ \ _{16})3,4,6,22,24,25+$were also given [E,T]. These graphs can be considered as undirected graphs. An isomorphism from $_1$ to $_2$ is given by

$$\phi^{\infty})P_i+[\ \ P_i \quad \text{if i is even}$$
$$\phi^{\infty})P_i+[\ \ P_{i+4} \quad \text{if i is odd,}$$

where the indices are taken modulo 27. It is straightforward to verify that there is no multiplier r such that $\}r,3r,8r,:r,25r,26r\langle\ [\ \ \}3,4,6,22,24,25\langle$, where the elements are taken modulo 27.

In contrast with the previous results, Turner [Tur] proved that two undirected circulant graphs on prime number of vertices are isomorphic if and only if there exists an isomorphism between the two graphs which is induced by a multiplier. This result was extended [E,T] to directed graphs. Their method is based on the investigation of the eigenvalues of the adjacency ma-

trices of the circulant graphs, which are circulant matrices. The same result was independently proved by Djoković [Dj].

In light of the previous results it seems reasonable to introduce the following definition:

Definition 1. *We denote by* $Adam(n)$ *the set of circulant digraphs of the form* $Cay(\mathbb{Z}_n, S)$*, where* $S \subseteq \mathbb{Z}_n$*, which are isomorphic to some* $Cay(\mathbb{Z}_n, S^\rho)$ *if and only if there exists an* $u \in \mathbb{Z}_n^\pm$ *such that* $S = uS^\rho$.

Alspach and Parsons [A,P] showed that Ádám's conjecture is true for circulant directed graphs on n vertices if $n = pq$, where p and q are distinct primes. They also proved that if n is divisible by p^2, where $p > 4$ is an odd prime or n is divisible by 3^4, then Ádám's conjecture is false. Moreover, they determined which circulant graphs $Cay(\mathbb{Z}_n, S)$ belong to $Adam(p^2)$. It was also proved by Alspach and Parsons [A,P] that a circulant graph $Cay(\mathbb{Z}_n, S)$ is the element of $Adam(n)$ if and only if for every two n-cycles σ and τ in $Aut(\mathbb{Z}_n, S)$ there exists $\alpha \in Aut(\mathbb{Z}_n, S)$ such that $\langle\sigma\rangle^\alpha = \langle\tau\rangle$.

In section 1.5 we present a classification of the circulant graphs. The solution was given using different algebraic methods that we will summarize in the next few sections.

1.2 CI-groups

A natural generalisation of Ádám's problem was given by Babai [Bab1], which is based on the following observation. Two Cayley graphs $Cay(G, S)$ and $Cay(G, T)$ are isomorphic if there exists an automorphism α of the group G which maps S to T. Clearly, α can be considered as a map from $Cay(G, S)$ to $Cay(G, T)$ and induces a graph isomorphism. Such an isomorphism is a called *Cayley isomorphism.*

At this point we introduce the definition that we will use all along Chapter 1.

Definition 2 (CI property). *1. A Cayley graph $Cay)G, S+$is said to be a CI-graph if, for each $T \to G$, the Cayley graphs $Cay)G, S+$and $Cay)G, T+$are isomorphic if and only if there is an automorphism α of G such that S^{α} [T.*

2. A group G is called a DCI-group if every Cayley graph of G is a CI-graph and it is called a CI-group if every undirected Cayley graph of G is a CI-graph.

Definition 3. *Let* $_1$ [$)V_1, E_1+$*and* $_2$ [$)E_2, V_2+$*be directed graphs. We denote by* $_1]$ $_2\hat{}$ *the lexicographic product of* $_2$ *by* $_1$*, where* $V)$ $_1]$ $_2\hat{}+[$ $V_1 \pm V_2$ *and for* v_1, w_1 / V_1 *and* v_2, w_2 / V_2 *the vertex* $)v_1, v_2+$*is connected to* $)v_2, w_2+$*if and only if either* $)v_1, w_1+/$ E_1 *or* v_1 [w_1 *and* $)v_2, w_2+/$ E_2.

Example 4, which was given [Li4] shows that in order to be able to use the CI property we first have to fix the group G.

Example 4. We denote by C_n the directed cycle of length n. Let p be an odd prime.

Let $\mathbb{Z}_p \pm \mathbb{Z}_p$ be generated by g and h. It is easy to see that [$Cay)\mathbb{Z}_p^2, \}h\langle \cap g\rangle h|+$is isomorphic to $C_p]C_p\hat{}$. It was proved by Godsil [God2] that $\mathbb{Z}_p^2$ is a DCI-group so is a CI-graph of the group $\mathbb{Z}_p^2$.

Let a generate $\mathbb{Z}_{p^2}$ and let S [$\}a^p\langle \cap a\rangle a^p|$ and T [$\}a^{2p}\langle \cap a\rangle a^p|$. It is easy to check that $Cay)\mathbb{Z}_{p^2}, S+\not\subset C_p]C_p\hat{} \not\subset Cay)\mathbb{Z}_{p^2}, T+$ We claim that $Cay)G, S+$is not a CI-graph. By contradiction, let us suppose that there exists an α / $Aut)\mathbb{Z}_{p^2}+$with S^{α} [T. Then a^{α} [a^{ip+1} for some i. Since α is an automorphism we have $)a^p+\not\in$ [$)a^{\alpha}+\not\in$ [$)a^{ip+1}+\not\in$ [a^{ip^2+p} [a^p, which is a not an element of T, which is a contradiction.

We conclude that there exists a graph which is a CI-graph of a group but not a CI-graph of another.

Observation 5. *It is important to notice that if* $p \sim 6$, *then* $\mathbb{Z}_{p^2}$ *is a* p*-group which has a directed Cayley graph of valency* $p\,0\ 2$ *which is not a CI-graph. One can also show using the previous construction that* $\mathbb{Z}_{p^2}$ *has an undirected Cayley graph of valency* $3)p\,0\ 2+$*which is not a CI-graph.*

The following lemmas will be formulated for CI-groups but they also hold for DCI-groups as well.

It is easy to prove that every subgroup of a CI-group is also a CI-group. The following lemma was proved in [B,F1].

Lemma 6. *Let* G *be a CI-group and* N *a characteristic subgroup of* G. *Then* G/N *is a CI-group.*

As a strengthening of this result, Dobson [Dob2] recently proved the following.

Lemma 7. *Let* G *be a CI-group. Then the homomorphic images of* G *are also CI-groups.*

We have already noted that the Cayley graph $Cay)G, S+$contains a regular subgroup isomorphic to G. The following lemma, which was proved by Babai [Bab1], is a key observation in the investigation of the isomorphism problem of Cayley graphs. It allows us to use group theoretic tools for the investigation of CI-groups and will be used repeatedly in this thesis.

Lemma 8. $Cay)G, S+$*is a CI-graph if and only if for every pair of regular subgroups* $\mathcal{G}$ *and* $\mathcal{H}$ *of* $Aut)Cay)G, S++$*isomorphic to* G *there is a* $\mu \in Aut)Cay)G, S++$*such that* $\mathcal{G}^{\mu} = \mathcal{H}$.

In order to show the efficiency of the previous lemma we reprove the fact that $\mathbb{Z}_p$ is a CI-group, which was earlier proved in [E,T] and [Tur] using different notation. Let us assume that is a Cayley graph of the cyclic group $\mathbb{Z}_p$. It is easy to see that a Sylow p-subgroup of the symmetric group S_p and

the one of Aut) +is a cyclic group of order p. Therefore the regular subgroups are the Sylow p-subgroups of Aut) +and hence they are conjugate. This proves that $\mathbb{Z}_p$ is a DCI-group. Even though this result seems very simple this could serve as a starting point of the investigation of both the cyclic and the elementary abelian p-groups as well.

1.3 Different types of isomorphism problems

The results collected in this section are not closely tied to the main topics of this thesis. Still, many of them can serve as an explanation of the difficulty of the original isomorphism problem.

It is easy to see that if for two finite groups G and H we have $\backslash G \backslash [\backslash H \backslash$ then there exists a regular (di)graph of (out-valency 2) valency 2 which is the Cayley graph of both G and H generated by a single element dividing $) \backslash G \backslash , \backslash H \backslash +$. Similar observation holds for a pair of groups having a subgroup of the same size.

It was observed in Example 4 that more complicated Cayley graphs of different abelian groups can be isomorphic.

We present here an interesting observation showing that even a large collection of Cayley graphs of a fixed group does not determine the group itself.

Proposition 9. *Every undirected Cayley graph of* $\mathbb{Z}_2^{n\ 2} \pm \mathbb{Z}_4$ *is isomorphic to a Cayley graph of* $\mathbb{Z}_2^n$.

Proof. Let $[\ Cay) \mathbb{Z}_2^{n\ 2} \pm \mathbb{Z}_4, S +$with $S [\ S\ ^1$. It is enough to show that Aut) +contains a regular subgroup isomorphic to $\mathbb{Z}_2^n$.

Let $a_1, \ldots, a_{n\ 2}, b$ be a generating set of $\mathbb{Z}_2^{n\ 2} \pm \mathbb{Z}_4$, where $o) a_i + [\ 3$ for $2 \geq i \geq n\quad 3$ and $o) b + [\ 5$. Let $\beta = \mathbb{Z}_2^{n\ 2} \pm \mathbb{Z}_4 \not\otimes \mathbb{Z}_2^{n\ 2} \pm \mathbb{Z}_4$ be defined as $\beta) x + [\ ) xb +^1$ and for $g\ /\ \mathbb{Z}_2^{n\ 2} \pm \mathbb{Z}_4$ we denote by α_y the left-

translation by y. We claim that G [$\rangle\alpha_{a_1},\ldots,\alpha_{a_{n-1}},\alpha_{b^2},\beta|$ is a regular group of automorphisms of isomorphic to $\mathbb{Z}_2^p$.

It is easy to see that the group H [$\rangle\alpha_{a_1},\ldots,\alpha_{a_{n-1}},\alpha_{b^2}|$ is isomorphic to $\mathbb{Z}_2^p$ ^{1} and the order of β is 3 since $\mathbb{Z}_2^p$ ^{2} $\pm$ $\mathbb{Z}_4$ is abelian. We also have that $]\alpha_y,\beta\hat{}$)x+[ ))xb+^1y ^1b+^1y [xy^2 [x if o)y+[3 so G is an abelian group generated by elements of order 3. One can also see that G is transitive and hence regular, finishing the proof of Proposition 9. □

Theorem 13 shows that if $n \sim 6$, then $\mathbb{Z}_2^n$ has a Cayley graph which is not isomorphic to any Cayley graph of $\mathbb{Z}_2^n$ ^{2} $\pm$ $\mathbb{Z}_4$.

There are only two non-isomorphic groups of order p^2 and both of them are abelian. It was determined by Joseph |Jos| when a Cayley digraph of one of these groups is isomorphic to a Cayley digraph of the other group.

Theorem 10 (Joseph). *Let* [Cay)G,T+*be a Cayley digraph of a group* G *of order* p^2 *with generating set* T. *Then* *is isomorphic to a Cayley digraph on both* $\mathbb{Z}_p^2$ *and* $\mathbb{Z}_{p^2}$ *if and only if* *is a lexicographic product of two Cayley digraphs of order* p.

This result was generalized by Morris |Mor1|:

Theorem 11 (Morris). *The following are equivalent for a digraph*

1. *is isomorphic to a Cayley graph of both* $\mathbb{Z}_{p^n}$ *and* $\mathbb{Z}_p^n$.
2. *There exists a sequence of Cayley graphs* $_1,\ldots,$ $_n$ *of* $\mathbb{Z}_p$ *such that* *is isomorphic to* $_1$] $_2$]$\ldots$ $_n\hat{}\ldots\hat{}$.

The problem of determining which groups have a Cayley graph isomorphic to the d dimensional cube $_d$ is still unsolved. It was proved by Spiga |Spi3| that there are at least $3^{\frac{d^2}{64}\ \frac{d}{2}\log_2\frac{d}{2}}$ non-isomorphic regular subgroup in Aut) $+_d$. This result is interesting since the number of p-groups of order n [p^α is bounded above by $n^{)\frac{2}{27}+o(1)+\alpha^2}$, see |Hig| and |Sim|.

We have seen that the automorphism group of several classes of graphs contains many (non-isomorphic) regular subgroups. This gives that a Cayley graph does not necessarily determine the underlying group.

Definition 12. *1. A Cayley graph $Cay(G, S)$ is called a directed graphical regular representation, which we will abbreviate by DRR of the group G if $Aut(G) = G$.*

2. An undirected Cayley graph which is a DRR will be called a graphical regular representation (GRR).

By Lemma 8, every Cayley graph $Cay(G, S)$ which is a DRR is a CI-graph of the group G.

The investigation of GRR's started earlier than the one of DRR's but we give Babai's [Bab3] characterisation of groups having DRR first.

Theorem 13 (Babai [Bab3])**.** *There are only five finite groups ($\mathbb{Z}_2^2$, $\mathbb{Z}_2^3$, $\mathbb{Z}_2^4$, $\mathbb{Z}_3^2$, Q) which do not admit a DRR.*

The connection set of a minimal Cayley graph of an elementary abelian p-group G is a basis, when we consider G as a vector space over $\mathbb{Z}_p$. It is easy to see that these Cayley graphs are CI-graphs, therefore $\mathbb{Z}_2^2$, $\mathbb{Z}_2^3$, $\mathbb{Z}_2^4$, $\mathbb{Z}_3^2$, Q have a CI-graph. Moreover, one can also verify that Q is a DCI-group. As a consequence of the previous theorem we get the following.

Theorem 14. *Every finite group G has non-tivial CI-graph.*

Babai also proved in [Bab4] assuming the Axiom of Choice that every infinite group has a DRR. The same proof yields that all but a finite number of finite groups have a DRR.

The description of groups having a GRR is more complicated. We say that a finite group G is a member of *Class I* if and only if G has a GRR. We also say that a finite group G is a member of *Class II* if and only if G

has the property that any subset $S \subseteq S^{-1}$ which generates G is fixed by a non-trivial automorphism of G. This property holds for S if and only it holds for $G \setminus S \setminus \{e\}$ so we can simply drop the assumption on S to be a generating set. It is fairly easy to see, and it was observed by Watkins [Wat1], that Class I and Class II are disjoint. It was also conjectured in [Wat1] that every finite group belongs to either Class I or Class II.

Definition 15. *A finite group G is called a generalized dicyclic group if it is generated by a finite abelian group A and an element x of order 5 such that $x^{-1}ax = a^{-1}$ for all $a \in A$ and $x^2 \notin A$.*

Theorem 16 (Watkins [Wat1])**.** *Let G be a finite group. The following two assertions are equivalent:*

1. *There exists a non-identity automorphism ϕ of G such that $\phi(g) = g$ or $\phi(g) = g^{-1}$ for all $g \in G$.*

2. *G is either abelian of exponent greater than 3 or the following conditions hold for G:*
   G is generated by $a_1, \ldots, a_k, b$ where

   (a) $b^{-1}a_i b = a_i^{l}$ *for* $2 \geq i \geq k$,

   (b) *the group generated by $a_1, \ldots, a_k$ is abelian and $a_i^2 = 2$ for some* $2 \geq i \geq k$

   (c) a_1 *is of even order* $3m$

   (d) $b^2 = a_1^m$.

Clearly, the groups characterised in the previous theorem are members of Class II. It was conjectured by Watkins [Wat2] that only finitely many members of Class II are neither abelian nor generalized dicyclic groups. This conjecture was proved by Babai [Bab2].

It was also showed in [Wat1] that the dihedral groups D_6, D_8 and D_{10} are in Class II. Ten more elements of Class II was collected by different authors, see [Imr], [N,W1], [N,W2], [Wat3], [Wat2].

Finally, Hetzel [Het] showed that with the exception of the previously mentioned 13 groups, the abelian groups of exponent greater than 3 and the generalized dicyclic groups, every finite solvable group belongs to Class I. Godsil proved the following theorem, finishing the description of finite groups having GRR.

Theorem 17 (Godsil [God1]). *Every finite non-solvable group lies in Class I.*

The existence of Cayley graphs of the group G with automorphism group equaling G was completed by the previous theorem. Babai and Godsil [B,G] proved that almost every Cayley graph of a non-abelian nilpotent group of odd order G has automorphism group isomorphic to G. More recently Dobson [Dob3] proved that if G_n is a sequence of abelian p-groups of growing order, then the probability that a directed Cayley graph of G_n is a DRR tends to zero. In Chapter 2 we construct Cayley graphs of elementary abelian p-groups having large automorphism group.

Let $i = G \infty G$ be defined as $i)g+[\ g^{-1}$. We have already seen that undirected Cayley graphs $Cay)A, S+$of abelian groups of exponent greater than 3 contains a subgroup isomorphic to $A \rtimes \rangle i|$. For an abelian group A of exponent greater than 3 let $Small)A+$denote the set of undirected Cayley graphs such that $Aut) +[\ A \rtimes \rangle i|$. Dobson [Dob3] proved that if G_p is a sequence of p-groups, then

$$\lim_{p' \in} \frac{\backslash Small)G_p+\backslash}{\backslash Cay)G_p+\backslash}[\ 2,$$

where $Cay)G_p+$denotes the set of all undirected Cayley graphs of G_p. As a strengthening of this result Dobson, Spiga and Verret [D,S,V] proved that if

A_n is a sequence of abelian groups of growing order, then $\frac{\backslash Small(A_n)\backslash}{\backslash Cay(A_n)\backslash}$ tends to 2. It was also proved in [D,S,V] that if A_n is an abelian group of order n, then the proportion of subsets S of A such that $Cay)A_n, S+$is a DRR goes to 2 as $n \infty$ $\in$. Finally, Morris, Spiga and Verret investigated the second exceptional infinite class of finite groups, the generalised dicyclic groups which do not admit GRR. They proved that if R is a generalised dicyclic group of order n, which is not isomorphic to $Q \pm \mathbb{Z}_2^l$, then $\frac{\backslash Small(R)\backslash}{\backslash Cay(R)\backslash}$ tends to 2 as $n \infty \in$.

1.4 Generalizations of the CI property

There are several types of generalizations of the CI property based on the previous lemma of Babai. In order to formulate one of these we need one more definition.

Definition 18 (3-closure)**.** *Let $G \geq Sym)^- +$be a permutation group.*

$$G^{(2)} [\quad \Big\} \pi \ / \ Sym)^- + \Big(\exists a, b \ / \ ^- \ \emptyset g_{a,b} \ / \ G \ with \quad \pi)a+[\quad g_{a,b})a+ and \quad \pi)b+[\quad g_{a,b})b+ \quad \Big\langle .$$

We say that $G^{(2)}$ is the 3-closure of the permutation group G and G is 3-closed if $G [\quad G^{(2)}$.

The following lemma is well-known and follows directly from the definition of $G^{(2)}$.

Lemma 19. *Let be a graph. If $G \geq Aut) \ +$, then $G^{(2)} \geq Aut) \ +$*

It is easy to see that $G^{(2)}$ is 3-closed for every permutation group G. There are several equivalent non-constructive versions of this definition. Let $G \geq Sym)^- +$be a permutation group. Clearly, G induces an action on $^- {}^2$. Then $G^{(2)}$ is the largest subgroup of $Sym)^- +$leaving the orbits of G on $^- {}^2$ invariant. The elements of $^- {}^2$ can be considered as directed edges of the

complete graph. Now we color the edges contained in the same orbit with the same color but edges in different orbits with different color. It is easy to verify that $G^{(2)}$ is the automorphism group of this colored graph. Moreover, the 3-closed permutation groups are those which can be obtained in such a way.

Now we can introduce the following definition:

Definition 20. *1. We say that a Cayley graph $Cay(G, S)$ is a $CI^{(2)}$-graph if and only if for every regular subgroup H of $Aut(Cay(G, S))$ isomorphic to G there is a $\sigma \in \langle H, A \rangle^{(2)}$ such that $H^\sigma = A$.*

2. A group G is called a $DCI^{(2)}$-group if for every $S \subset G$ the Cayley graph $Cay(G, S)$ is a $CI^{(2)}$-graph.

It is clear that that every (D)CI$^{(2)}$-group is a (D)CI-group. However it is also important to mention that there is no known example of a (D)CI-group that is not (D)CI$^{(2)}$.

Another important generalization of the CI property was introduced by Babai [Bab1].

Definition 21. *Let G be a finite group. We say that G is a CI-group with respect to every relational structure if for every pair of isomorphic Cayley objects $\mathcal{E}_1$ and $\mathcal{E}_2$ there exists $\alpha \in Aut(G)$ which induces an isomorphism between $\mathcal{E}_1$ and $\mathcal{E}_2$.*

Lemma 8 was originally proved for arbitrary relational structures. Hence we define pronormal groups.

Definition 22. *Let H be a group and G be a subgroup of H. We say that G is a pronormal subgroup of H if for every $h \in H$ we have that G and G^h are conjugate in $\langle G, G^h \rangle$.*

Using this definition and the fact that every permutation group can be obtained as the automorphism group of a relational structure, Lemma 8 asserts that G is a CI-group with respect to every relational structure if and only if G is a pronormal subgroup of $Sym)G+$

Pálfy [Pál2] proved that if G is a finite CI-group with respect to every relational structure, then either G is a cyclic group with $)n, \phi)n++[\ 2$, where ϕ denotes the Euler's totient function, or $\backslash G\backslash[\ 5$. It was also proved in [Pál2] that a cyclic group $\mathbb{Z}_n$ is a CI-group with respect to every relational structure if $n\ [\ \bigcup_{i=1}^{k} p_i$, where $p_1 < p_2 < \ldots < p_k$ are prime numbers, $\bigcup_{i=1}^{l\ 1} p_i < p_l$ for every $3 \geq k \geq l$ and $)n, \phi)n++[\ 2$. As an extension of this result, Pálfy [Pál1] proved the following:

Theorem 23. *G is CI-group for every relational structure if and only if G is a cyclic group of order n, where $)n, \phi)n++[\ 2$. If G is not a CI-group for some relational structure, then there exists a quaternary relational structure such that its automorphism group contains two nonconjugate regular subgroups isomorphic to G.*

1.5 Solution for cyclic groups

Pálfy's general results on CI-groups gave us new families of cyclic CI-groups. It was also proved in [Pál1] that Ádám's conjecture on undirected graphs fails for cyclic groups $\mathbb{Z}_n$ if $n\ [\ 9a$ and $n\ [\ :b$, where $a > 2$ and $b > 3$.

Now we return to the original question posed by Ádám and collect the results on cyclic groups. The following table contains the positive results on cyclic DCI-groups $\mathbb{Z}_n$, where p and q are different primes.

n	Author
p	Elspas, Turner [E,T], Turner [Tur], Djoković [Dj]
$3p$ and $4q$ $(q > 4)$	Babai [Bab1]
$5p$ $(p > 3)$	Godsil [God2]
pq	Alspach, Parsons [A,P], Godsil [God2] and Klin, Pöschel [K,P4]
$)n, \phi)n{+}{+}[\ \ 2$	Pálfy [Pál2]
n is square-free	Muzychuk [Muz1]
$3n$, where n is square-free	Muzychuk [Muz2]

The following table collects the most important steps proving that Ádám's conjecture fails for some n.

n	Author
9 for directed, 27 for undirected graphs	Elspas, Turner [E,T]
$9 \setminus n$ directed graphs	Egorov and Markov [E,M]
$n\ [\ \ k^2$, where $k\ \{\ \ 2, 3, 4, 7$	Babai, Frankl [B,F2]
undirected $27 \setminus n$, $38 \setminus n$, $p^2 \setminus n$ with $p\ \{\ \ 3, 4$ directed graphs $9 \setminus n$, $: \setminus n$	Alspach, Parsons [A,P]

The classification of cyclic CI-groups was finally obtained by Muzychuk [Muz1, Muz2].

Theorem 24. *1. The cyclic group $\mathbb{Z}_n$ is a CI-group if and only if $n\ [\ \ k$ or $3k$, where k is square-free or $n\ [\ \ 9, : , 29$.*

2. The cyclic group $\mathbb{Z}_n$ is a DCI-group if and only if $n\ [\ \ k$ or $3k$, where k is square-free.

Even though Ádám's conjecture is far from to be true it was a starting point of another type of investigation. Several authors, including Klin and

Pšchel [K,P1], [K,P2], [K,P3], [K,P4] worked out a method to determine which pair of circulant graphs are isomorphic using the theory of Schur rings. The final result [Muz4] was also given by Muzychuk. The description of the isomorphism classes uses only elementary tools but we omit to describe them here since it is complicated. The main ideas are to view generating sets as the union of subsets of special form and using this partition to define types of generating sets. Then one can investigate different types of generating sets separately for the same group $\mathbb{Z}_n$. Finally, it is enough to extend the class of functions, the set of multipliers, for isomorphism testing to generalized multipliers, what they also call a solving set. This approach was first worked out by Alspach and Parsons [A,P] when they gave a method to determine which pair of Cayley graphs $Cay)\mathbb{Z}_{p^2}, S+$and $Cay)\mathbb{Z}_{p^2}, T+$are isomorphic. Similarly, the isomorphism problem of Cayley objects was investigated by Huffman [Huf1] and [Huf2] for the cyclic group $\mathbb{Z}_{pq}$ where p and q are distinct primes with $)pq, \phi)pq++[$ 2 and $\mathbb{Z}_{p^2}$, respectively. It is important to note that Muzychuk's result [Muz4] shows that the number of elements in each isomorphism class of the Cayley graphs of a $\mathbb{Z}_n$ is at most $\phi)n+$and the same result holds for the Cayley objects investigated in [Huf1] and [Huf2].

1.6 Refinements of Ádám's conjecture and the CI property

It is easy to see that a Cayley graph generated by a single element of finite order n is just the disjoint union of n-cycles. Therefore elements of the same order in a CI-group G have to be conjugate in $Aut)G+$ This simple observation has serious consequences on the structure of CI- and DCI-groups.

We define the m-CI and the m-DCI property.

Definition 25. *A group G is called an m-CI-group if every undirected Cayley graph $Cay)G, S+$is a CI-graph if $\backslash S\backslash \geq m$ and G is called an m-DCI-group if the same holds for directed graphs as well.*

It seems there are only a few finite groups which are CI-groups. The previous definition gives the possibility to refine statements on the isomorphism problem of Cayley graphs. A finite group G which can be expressed as the direct sum of cyclic p-groups of the same order is called a homocyclic group.

Fang and Xu [F,X] proved the following theorem.

Theorem 26. *Let G be a finite abelian group.*

1. *G is a 2-CI-group if and only if the Sylow 3-subgroup of G is homocyclic.*
2. *G is a 5-CI-group if and only if for every prime p the Sylow p-subgroup of G is homocyclic and the Sylow 3-subgroup is cyclic or elementary abelian.*

As a consequence of the previous theorem we get that the cyclic group $\mathbb{Z}_n$ is a 5-CI-group for every $n \not\in \mathbb{N}$ which was conjectured by Boesch and Tindell, see [B,T]. Similar and more general result was proved for connected Cayley graphs by Delorme, Favaron and Mahéo [D,F,M]:

Theorem 27. *Let G_1 and G_2 be two abelian groups which are isomorphic to neither $\mathbb{Z}_{4n}$ nor $\mathbb{Z}_{2n} \pm \mathbb{Z}_2$.*

1. *If $Cay(G_1, S_1) \not\cong Cay(G_2, S_2)$, where $Cay(G_1, S_1)$ is connected and $|S_1| \leq 5$, $|S_2| \leq 5$, then G_1 and G_2 are isomorphic and $Cay(G_1, S_1)$ is a CI-graph.*
2. *Any, not necessarily connected, circulant graph of degree 5 is a CI-graph.*

It was proved by Babai and Frankl [B,F2] that if G is a non-solvable CI-group, then G is isomorphic to the direct product $U \pm V$, where $(|U|, |V|) = 2$ and U is the direct product of some elementary abelian p-groups and V is isomorphic to one of the following four groups: $PSL(3, 6)$, $SL(3, 6)$, $PSL(3, 24)$,

$SL)3,24+$ Li and Praeger [L,P] proved that a non-abelian finite simple 3-CI-groups can only be A_5 or $L_2)9+$and they also proved that $L_2)9+$is not a 4-CI-group. They conjectured that A_5 is a 5-CI group which was proved in [X,X,S,B] and it was also proved in [X,X] that A_5 is a 6-DCI-group. Finally, Li [Li3] proved that A_5 is not a 3:-CI-group. As a consequence of these results we get the following:

Theorem 28 (Li)**.** *Every CI-group is solvable*

Xu [Xu] conjectured that every minimal Cayley graph is a CI-graph. This is a natural conjecture since it seems likely that an isomorphism between such Cayley graphs induces a group isomorphism as well, but this conjecture also turned out to be false, see [Li2]. The following characterisation of finite abelian groups for which all minimal Cayley graphs are CI-graphs was first obtained by Meng and Xu [M,X].

Theorem 29. *Every minimal Cayley graph of a finite abelian group G is a CI-graph if and only if G is a 3-group or the Sylow 3-subgroup of G does not have a direct summand isomorphic to $\mathbb{Z}_2 \pm \mathbb{Z}_{2^k}$ with $k \sim 3$.*

Another remarkable class of CI-graphs was determined by Li [Li2] by proving the following:

Theorem 30. *Let G be a nilpotent group of odd order and A the automorphism group of a Cayley graph [$Cay)G,S+$of G. We denote by A_1 the stabilizer of the identity element.*

1. *If)\G\, \A1\+[2, then is CI-graph.*
2. *If G is abelian and)\G\, \A1\+[p, where p is a prime, then either is a CI-graph or S contains a coset of some subgroup of G.*

It is not hard and in fact it was derived from Theorem 30 in [Li2] that if p is the smallest prime divisor of \G\ then every connected Cayley graph

of valency less than p is a CI-graph. This is a generalization of Babai's result [Bab1] who proved the same for connected Cayley graphs of p-groups. Observation 5 shows that these statements are almost tight. However, Li [Li2] constructed minimal Cayley graphs of abelian groups which are not CI-graphs and in the same paper he proved that if G is an abelian group of odd order, then every minimal Cayley graph of G is a CI-graph.

Li also asked whether there exists a non-CI-graph of an abelian group G for which the connection set does not contain a coset of a subgroup of G. This problem has remained unsolved. We note that in Chapter 2 we construct non-CI-graphs for elementary abelian groups $\mathbb{Z}_p^n$, and the connection sets in each case is the union of cosets, which can be considered as affine subspaces of $\mathbb{Z}_p^n$ as well.

A similar refinement of Ádám's conjecture is due to Toida. It was conjectured in [Toi] that if S is a subset of $\mathbb{Z}_n^{\pm}$, then $Cay)\mathbb{Z}_n, S+$is a CI-graph. Toida's conjecture was finally proved by Klin, Muzychuk an Pöschel [K,M,P]. This can also be obtained, and in fact was obtained, as a special case of an isomorphism criterion for circulant graphs given by Klin and Muzychuk, which led to the complete classification of isomorphism classes of circulant graphs.

1.7 Candidates of CI-groups

Since every subgroup of a CI-group is also a CI-group it is natural to start the investigation with p-groups. Babai and Frankl [B,F1] proved the following theorem, which is a serious restriction on the structure of CI-groups.

Theorem 31. *The Sylow p-subgroup of a finite CI-group can only be elementary abelian p-group, $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_9$, $\mathbb{Z}_{27}$ or the quaternion group of order* 9.

It is clear from the description of the cyclic groups, given in Theorem 24, that $\mathbb{Z}_{27}$ is not a CI-group and $\mathbb{Z}_9$ is not a DCI-group.

The semidirect product of G by H will be denoted by $G \rtimes H$ and we denote by g˜s$)G+$the exponent of the group G, which is the least common multiple of the integers appearing as the order of an element of G.

Definition 32. *Let A be and abelian group of odd order, with the additional condition that for every prime p the Sylow p-subgroup of A is an elementary abelian p-group. Further, let n / $\{3,4,5,9\langle$ with $)\backslash A\backslash, n+[$ 2. We denote by $E)A,g+,$ the semidirect product $A \rtimes \rangle g|$, where $o)g+[$ n and the following holds. If $o)g+$is even, then g inverts the elements of A, if $o)g+[$ 4, then a^g [a^l, where l is an integer with $l^3 \subseteq 2$ $)mod$ g˜s$)A++$and $)l)l$ $2+,$g˜s$)A++[$ 2.*

The following list of candidates of CI-groups was given by Li, Lu and Pálfy |L,L,P| in 2007.

Theorem 33 (Candidates of CI-groups)**.** *Every finite CI-group G is a member of the following two set of groups.*

1. *G [$U \pm V$ such that the following conditions hold: $)\backslash U\backslash, \backslash V\backslash+[$ 2 and all Sylow subgroups of G are elementary abelian or isomorphic to $\mathbb{Z}_4$ or Q. The direct summand U is abelian and V is isomorphic to one of the following groups: 2, Q, A_4, $E)A,n+,$ where n / $\{3,4,5\langle$ or $Q \pm E)A,4+$ or $E)A,n+\pm E)A^{\infty},4+,$ where n [3 or 5 and $)\backslash A\backslash, 7+[$ $)\backslash A^{\infty}, 7+[$ 2.*

2. *G is one of the groups: $\mathbb{Z}_8$, $\mathbb{Z}_9$, $\mathbb{Z}_{18}$, the dihedral group D_{18}, $\mathbb{Z}_9 \rtimes \mathbb{Z}_4$ with centre of order 3, $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_9$ with centre of order 4, $E)A,9+,$ or $\mathbb{Z}_2^d \pm \mathbb{Z}_9$.*

A more precise statement was also formulated by Li, Lu and Pálfy.

Theorem 34. *Let G be a finite CI-group*

1. *If G does not contain elements of order 9 or :, then G [$H_1 \pm H_2 \pm H_3$, where the orders of H_1, H_2, and H_3 are pairwise coprime, where*

(a) H_1 *is an abelian group, and each Sylow subgroup of* H_1 *is elementary abelian or* Z_4,

(b) H_2 *is one of the groups* $E)A, 3+$, $E)A, 5+$, Q, *or* 2,

(c) H_3 *is one of the groups* $E)A, 4+$, A_4, *or* 2.

2. *If* G *contains elements of order* 9, *then* G [$E)A, 9+$*or* $\mathbb{Z}_8$

3. *If* G *contains elements of order* :, *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* $\mathbb{Z}_9 \pm \mathbb{Z}_2^n$ *with* $n \geq 6$.

It is a difficult problem to determine which groups listed in the previous two theorems are indeed CI-groups. Finite CI-groups are rare. We provide a short list of the known examples of CI-groups, which were known by Li, Lu and Pálfy.

1. $\mathbb{Z}_n$, where either n \ $5k$ and k is odd square-free, or n / }9, :, 29⟨ (Muzychuk [Muz1, Muz2]).

2. $\mathbb{Z}_2^4$ (Conder and Li [C,L]), $\mathbb{Z}_p^4$ for $p > 3$, (Hirasaka and Muzychuk [H,M]).

3. D_{2p} (Babai [Bab1]) (finishing the description of groups of order $3p$), Frobenius groups F_{3p} of order $4p$, (Babai and Frankl, The paper including the proof has never appeared).

4. $\mathbb{Z}_2^2 \pm \mathbb{Z}_3$, $\mathbb{Z}_2^5$ (Conder and Li [C,L]), Q, $\mathbb{Z}_3 \rtimes \mathbb{Z}_8$ (Royle [Roy]).

5. A_4 (see [Li1]), $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$, $\mathbb{Z}_9 \rtimes \mathbb{Z}_2$, $\mathbb{Z}_9 \rtimes \mathbb{Z}_4$, $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_9$ (Conder and Li [C,L]).

6. G [$\rangle a, z$ \ a^p [$2, z^r$ [$2, z$ ^1az [a ^{1}|, where r [5 or 9 (Li, Lu, Pálfy [L,L,P]).

7. Frobenius groups of order $4p$, where $p \subseteq 2$ $)mod$ 4+(Li, Lu, Pálfy [L,L,P]), (finishing the description of groups of order $3p$).

The previous list, Theorem 33 and Theorem 34 is the starting point of the work presented in the rest of Chapter 1.

Finally, we conclude that Theorem 31, Theorem 33 and Theorem 34 show that the two main questions in this area are the following:

Question. *(I) Which elementary abelian p-groups are CI-groups? The investigation of the elementary abelian p-groups was initiated by Babai and Frankl [B,F1].*

(II) Determine whether the direct product of two CI-groups of coprime order is a CI-group. It was conjectured by Kovács and Muzychuk [K,M], that the direct product of CI-groups of coprime order is a CI-group.

In order to give answer for the first question, in Chapter 2 we develop a new method to prove that for every prime $p \sim 4$ the elementary abelian p-group of rank $3p\,0\ 4$ is not a CI-group, improving the result of Muzychuk [Muz3] and Spiga [Spi1]. Chapter 3 is devoted to give new examples of CI-groups which are the direct product of CI-groups, providing positive answer for the second question in many particular cases.

Further known results about CI-groups, which are more closely related to the theorems proved in this thesis, will be presented in Chapter 2 and Chapter 3.

2. ELEMENTARY ABELIAN P-GROUPS OF RANK $3P\ 0\ 4$ ARE NOT CI-GROUPS

For our discussion the following two previously mentioned results are relevant. We have already mentioned that if G is a (D)CI-group, then every subgroup of G is a (D)CI-group. Theorem 31 shows that the Sylow subgroups of a CI-group can only be $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_9$, $\mathbb{Z}_{27}$, the quaternion group of order 9 or an elementary abelian p-group. Also, they asked whether every elementary abelian p-group is CI-group.

Hirasaka and Muzychuk proved |H,M| that $\mathbb{Z}_p^4$ is a CI-group for every prime $p > 3$ and this result was also proved by Morris |Mor2|. This result was recently reproved by Morris |Mor3| using elementary tools. On the other hand, Muzychuk |Muz3| proved that an elementary abelian p-group of rank $3p \quad 20 \quad {}^{2p}_{p}{}^{1}[$ is not a CI-group and more recently as a strengthening of this result Spiga |Spi1| showed that if $n \sim 5p \quad 3$, then $\mathbb{Z}_p^n$ is not a CI-group.

The problem of determining whether or not an elementary abelian group $\mathbb{Z}_p^n$ is a CI-group is solved if $p\ [\ \ 3$ as the CI property holds for $\mathbb{Z}_2^5$, see |C,L|, and a non-CI-graph for $\mathbb{Z}_2^6$ was constructed by Nowitz |Now|.

Finally, for $p\ [\ \ 4$ we have more precise results. Spiga |Spi4| proved that $\mathbb{Z}_3^5$ is a DCI-group but $\mathbb{Z}_3^8$ is not a DCI-group.

Further improving the upper bounds in |Muz3| and |Spi1|, we prove the following.

Theorem 35 (|Som|)**.** *For every prime $p > 3$, the group $\mathbb{Z}_p^{2p+3}$ has a Cayley graph of valency $)3p\ 0\ 4{+}p^{p+1}$ which is not a CI-graph. Consequently, an*

elementary abelian p-group of rank greater than or is equal to $3p0\ 4$ *is not a DCI-group.*

We can formulate a similar theorem for undirected Cayley graphs.

Theorem 36. *For every prime* $p > 4$*, the group* $\mathbb{Z}_p^{2p+3}$ *has an undirected Cayley graph which is not a CI-graph.*

The proof of Theorem 35 is elementary and uses only the definition of the CI property. We will construct two isomorphic Cayley graphs in Section 2.1. The connection sets in both graphs are the union of affine subspaces in $\mathbb{Z}_p^{2p+3}$ and the isomorphism between the Cayley graphs is given in terms of multivariate polynomials. Finally, the proof in Section 2.4 that our Cayley graphs are not CI-graphs uses only elementary tools from linear algebra. Section 2.5 is devoted to prove Theorem 36. In addition, in Section 2.6 we will indicate how the previous results of Muzychuk and Spiga can be easily obtained applying our technique.

2.1 The construction

Let $U \subsetneq \mathbb{Z}_p^{p+1}$ and $V \subsetneq \mathbb{Z}_p^{p+2}$, then the groups U and V can be regarded as vector spaces over the field $\mathbb{Z}_p$ with bases $\}e_1, e_2, \ldots, e_{p+1}\langle$ and $\}f_0, f_1, \ldots, f_{p+1}\langle$, respectively. We endow V with the natural bilinear form:

$$\Big\langle \bigcup_{j=0}^{p+1} \alpha_j f_j, \bigcup_{j=0}^{p+1} \beta_j f_j \Big(\Big[\bigcup_{j=0}^{p+1} \alpha_j \beta_j.$$

Let us define the following affine subspaces of $G = U \oplus V$:

$$A_i = \{e_i\} + V = \langle v, f_0, f_i \rangle = \{1\}, \qquad i = 2, \ldots, p-2+$$

$$B_i = \bigcup_{j \neq i} \{e_j\} + V = \langle v, f_i, \bigcup_{j=0}^{p+1} f_j \rangle = \{1\}, \qquad i = 2, \ldots, p-2+$$

$$C_0 = \bigcup_{i=1}^{p+1} \{e_i\} + V = \langle v, \bigcup_{j=0}^{p+1} f_j \rangle = \{1\},$$

$$C_1 = \bigcup_{i=1}^{p+1} \{e_i\} + V = \langle v, \bigcup_{j=0}^{p+1} f_j \rangle = \{2\}.$$

Now

$$S = \bigcup_{i=1}^{p+1} A_i \cup B_i \cup C_0 \quad \text{and} \quad T = \bigcup_{i=1}^{p+1} A_i \cup B_i \cup C_1 \tag{2.1}$$

will be the connection sets of two Cayley graphs defined on $G = U \oplus V$. Note that the sets S and T are the union of affine subspaces of G. Namely, S and T are the union of $3p-4$ affine subspaces of dimension $p-2$. Therefore $|S| = |T| = 3p-4 = p^{p+1}$ as promised.

We are going to show in Section 2.3 that $Cay(G, S) \cong Cay(G, T)$, but we will also prove in Section 2.4 that there is no automorphism of G mapping S to T. Taken together, these two facts establish Theorem 35.

2.2 Preliminary facts

In this section we introduce some notation concerning polynomials and we establish certain equations over the field $\mathbb{Z}_p$. These equations will be used in the proof of the isomorphism between the two Cayley graphs $Cay(G, S)$ and $Cay(G, T)$.

For a sequence of integers $\underline{n} = (n_1, \ldots, n_{p+1})$ we denote $x_1^{n_1} \cdots x_{p+1}^{n_{p+1}}$ by $x^{\underline{n}}$ and let $k(x^{\underline{n}}) = |\{i : n_i > 1\}|$ denote the number of variables occuring in

$x^{\underline{n}}$. Let $\mathcal{O}$ be the set of monomials of degree p involving at least two variables and for each i [$2, \ldots, p0\ 2$ we cut it into two subsets $\mathcal{O}$ [$\mathcal{O}\ {}^{0}_{i} \cap \mathcal{O}\ {}^{+}_{i}$, where $\mathcal{O}\ {}^{0}_{i}$ [$\}\, x^{\underline{n}} \setminus n_i$ [$1\,\langle$ and $\mathcal{O}\ {}^{+}_{i}$ [$\}\, x^{\underline{n}} \setminus n_i > 1\,\langle$. For a monomial $x^{\underline{n}}$ / $\mathcal{O}$ we define the number $c_{\underline{n}}$ [$\frac{(p\ \ 1)!}{n_1! \times\!\!\times n_{p+1}!}$. An obvious consequence of the Multinomial Theorem is that $\frac{p!}{n_1! \times\!\!\times n_{p+1}!}$ is an integer. If $x^{\underline{n}}$ / $\mathcal{O}$, then $k)x^{\underline{n}}+\!\sim 3$ so p does not divide the denominator of $c_{\underline{n}}$ and hence $c_{\underline{n}}$ is an integer as well. Finally, for $\underline{\alpha}$ / $\mathbb{Z}_p^k$ and $f)\underline{x}+/\ \mathbb{Z}_p]x_1, \ldots, x_k\hat{}$ we denote

$$\Lambda_{\underline{\alpha}} f)\underline{x}+[\ \ f)\underline{x}\ 0\ \ \underline{\alpha}+\ \ f)\underline{x}+$$

.

Lemma 37. *Let* s [$\prod_{i=1}^{p+1} x_i$ *and* s_i [$s\ \ \ x_i$ [$\prod_{j \not\equiv i} x_j$.

The following two equations hold over $\mathbb{Z}]x_1, \ldots, x_k\hat{}$.

1.
$$s^p\ [\ \bigcup_{j=1}^{p+1} x_j{}^p\ 0\ \bigcup_{\underline{x^n}/\mathcal{O}} pc_{\underline{n}} x^{\underline{n}}.$$

2.
$$s_i^p\ [\ \bigcup_{j \not\equiv i} x_j{}^p\ 0\ \bigcup_{\underline{x^n}/\mathcal{O}\ {}^{0}_{i}} pc_{\underline{n}} x^{\underline{n}}.$$

Proof. These identities are obvious. □

Define the following polynomials in $\mathbb{Z}_p]x_1, \ldots, x_{p+1}\hat{}$:

$$r_i\ [\ \bigcup_{x^{\underline{n}}/\mathcal{O}\ {}^{0}_{i}})2\ \ \ k)x^{\underline{n}} + c_{\underline{n}} x^{\underline{n}}\ 0\ \bigcup_{x^{\underline{n}}/\mathcal{O}\ {}^{+}_{i}})3\ \ \ k)x^{\underline{n}} + c_{\underline{n}} x^{\underline{n}} \tag{2.2}$$

for i [$2, \ldots, p\ 0\ 2$ and

$$r_0\ [\ \bigcup_{x^{\underline{n}}/\mathcal{O}})k)x^{\underline{n}} +\ \ 3 + c_{\underline{n}} x^{\underline{n}}. \tag{2.3}$$

Lemma 38.

$$\bigcup_{j=0}^{p+1} r_j \; [\quad \frac{ps^p \quad \prod_{j=1}^{p+1} s_j^p}{p}. \tag{2.4}$$

The polynomial $\frac{ps^p \ \sum_{j=1}^{p+1} s_j^p}{p}$ *is defined in* $\mathbb{Z}_p]x_1, \ldots, x_{p+1}\hat{}$, *while* (2.4) *holds over* $\mathbb{Z}_p$.

Proof.

$$\bigcup_{j=0}^{p+1} r_j \; [\quad \bigcup_{x^{\underline{n}}/\mathcal{O}}))p\,0\;\; 2 \quad k)x^{\underline{n}} + +)2 \quad k)x^{\underline{n}} + +0\;\;)k)x^{\underline{n}} + \quad 2 +)3 \quad k)x^{\underline{n}} + + + c_{\underline{n}}x^{\underline{n}}$$

$$[\quad)2 \quad p + \bigcup_{x^{\underline{n}}/\mathcal{O}})k)x^{\underline{n}} + \quad 2 + e_{\underline{n}}x^{\underline{n}} \; [\quad \bigcup_{x^{\underline{n}}/\mathcal{O}})k)x^{\underline{n}} + \quad 2 + e_{\underline{n}}x^{\underline{n}} \tag{2.5}$$

and Lemma 37 gives

$$\frac{ps^p \quad \prod_{j=1}^{p+1} s_j^p}{p} \; [\quad \bigcup_{x^{\underline{n}}/\mathcal{O}})k)x^{\underline{n}} + \quad 2 + e_{\underline{n}}x^{\underline{n}}$$

as well. □

2.3 Isomorphism

Proposition 39. $Cay)G, S + \subsetneq Cay)G, T +$

Proof. Let $\phi = \mathbb{Z}_p^{2p+3} \infty \mathbb{Z}_p^{2p+3}$ be defined by

$$\phi\,)x_1, \ldots, x_{p+1}, y_0, y_1, \ldots, y_{p+1} + [$$

$$[\quad x_1, \ldots, x_{p+1}, y_0\,0\;\; r_0)x_1, \ldots, x_{p+1} + , \ldots, y_{p+1}\,0\;\; r_{p+1})x_1, \ldots, x_{p+1} + [$$

where $r_i \;/\; \mathbb{Z}_p]x_1, \ldots, x_{p+1}\hat{}$ are defined by equations (2.2) and (2.3) .

We claim that ϕ is an isomorphism from $Cay)G, S +$ to $Cay)G, T +$ Note that ϕ acts by translation on $u\,0\;\; V$ for every $u \;/\; U$ so ϕ is bijective. It remains to show that for $a, b \;/\; G$ if $b \quad a \;/\; S$, then $\phi)b + \quad \phi)a + / T$.

Since G is the direct sum of U and V, an element of G can be written as $)\underline{x},\underline{y}+$ where $\underline{x} \ / \ U$ and $\underline{y} \ / \ V$. For the element $)\underline{x},\underline{y}+$we will also use the notation $)x_1,\ldots,x_{p+1},y_0,y_1,\ldots,y_{p+1}+$

Assume first that $b \quad a \ / \ A_i$ for some $2 \geq i \geq p\,0\ \ 2$ and write $a \,[\ \ )\underline{x},\underline{y}+$ with $\underline{x} \ / \ U$ and $\underline{y} \ / \ V$. Then we may set $b \,[\ \ a\,0\ \ )e_i\,0\ \ v+$ where $v \ / \ V$ such that $\rangle v, f_0\,0\ \ f_i| \ [\ \ 1$. Clearly ϕ does not affect the first $p\,0\ \ 2$ coordinates hence we need to show $\phi)b+ \quad \phi)a+/ \ A_i$. Now we have

$$\phi)b+ \quad \phi)a+[\quad b \quad a[\,[\quad \phi)b+ \quad b[\quad \phi)a+ \quad a[\,[$$
$$[\ \ )1,\ldots,1,\Lambda_{e_i}r_0)\underline{x}+,\Lambda_{e_i}r_1)\underline{x}+,\ldots,\Lambda_{e_i}r_{p+1})\underline{x}++.$$

Thus we have to check that $\rangle)\Lambda_{e_i}r_0)\underline{x}+,\Lambda_{e_i}r_1)\underline{x}+,\ldots,\Lambda_{e_i}r_{p+1})\underline{x}++,f_0\,0\ \ f_i| \ [\ 1$. Now

$$\rangle)\Lambda_{e_i}r_0)\underline{x}+,\Lambda_{e_i}r_1)\underline{x}+,\ldots,\Lambda_{e_i}r_{p+1})\underline{x}++,f_0\,0\ \ f_i| \ [\ \ \Lambda_{e_i}r_0)\underline{x}+0\ \ \Lambda_{e_i}r_i)\underline{x}+$$
$$[\ \ \Lambda_{e_i})r_0)\underline{x}+0\ \ r_i)\underline{x}++[\ \ 1,$$

since $r_0\,0\ \ r_i$ does not involve x_i.

By the same argument if $b \quad a \ / \ C_0$, then using Lemma 38 we get

$$\Lambda_{\sum_{j=1}^{p+1}e_j}\Big)\bigcup_{j=0}^{p+1}r_j\Big[\ [\ \ \frac{p)s\,0\ \ p\,0\ \ 2+^{p} \quad \prod_{j=1}^{p+1})s_j\,0\ \ p+^{p}}{p} \quad \frac{ps^p \quad \prod_{j=1}^{p+1}s_j^p}{p}$$
$$[\ \ )s\,0\ \ 2+^{p} \quad s^p \ [\ \ 2.$$

These equations hold over $\mathbb{Z}_p$ since $)t0\ p+^{p} \subseteq t^p\ \ )\mathrm{o}\ \mathrm{pe}\ \ p^2+$ Hence if $b \quad a \ / \ C_0$, then $\phi)b+ \quad \phi)a+/ \ C_1$.

Finally, if $b \quad a \ / \ B_i$ we need a little more computation. Equation (2.5) shows that

$$\bigcup_{j=0}^{p+1}r_j \ [\ \ \bigcup_{x^{\underline{n}}/\mathcal{O}}\ )k)x^{\underline{n}}+ \quad 2+e_{\underline{n}}x^{\underline{n}}.$$

Hence

$$r_i\,0\bigcup_{j=0}^{p+1} r_j\,[\quad \bigcup_{x^{\underline{n}}/\mathcal{O}\ {}_i^{0}})2\quad k)x^{\underline{n}}+\!\!+e_{\underline{n}}x^{\underline{n}}\,0\quad \bigcup_{x^{\underline{n}}/\mathcal{O}\ {}_i^{+}})3\quad k)x^{\underline{n}}+\!\!+e_{\underline{n}}x^{\underline{n}}$$

$$0\bigcup_{x^{\underline{n}}/\mathcal{O}})k)x^{\underline{n}}+\quad 2+\!\!e_{\underline{n}}x^{\underline{n}}\,[\quad \bigcup_{x^{\underline{n}}/\mathcal{O}\ {}_i^{+}} c_{\underline{n}}x^{\underline{n}},$$

which is, by Lemma 37, is equal to

$$\frac{s^p\quad x_i^p\quad s_i^p}{p}.$$

Therefore

$$\Lambda_{\sum_{j\neq i}e_j}\Big)r_i\,0\bigcup_{j=0}^{p+1} r_j\Bigg[\quad[\quad\frac{)s\,0\;\;p\text{-}\!\!\not\;\;x_i^p\quad)s_i\,0\;\;p\text{-}\!\!\not\;}{p}\quad\frac{s^p\quad x_i^p\quad s_i^p}{p}\,[\quad 1,$$

using again the fact that $)t\,0\;\;p\text{-}\!\!\not\;\subseteq t^p\;\;)$o pe p^2+ Hence if $b\quad a\;/\;B_i$, then $\phi)b+\quad\phi)a+/\;B_i$ and this finishes the proof of the fact that ϕ is indeed a graph isomorphism. □

2.4 Checking the CI property

Now in order to show that $Cay)G,S+$is not a CI-graph we have to show that there is no $\sigma\;/\;Aut)G+[\quad GL)U\sum V+$satisfying $\sigma)S+[\quad T$.

Proposition 40. *There is no linear transformation $\sigma\;/\;GL)U\sum V+$such that $\sigma)S+[\quad T$.*

Proof. Assume by way of contradiction that $\sigma\;/\;GL)U\sum V+$with $\sigma)S+[\quad T$. Let M denote the matrix of the linear transformation σ with respect to the the basis $\}e_1,\ldots,e_{p+1},f_0,f_1,\ldots,f_{p+1}\langle$ and write $M\,[\,\rceil\begin{matrix}M_{1,1}&M_{1,2}\\M_{2,1}&M_{2,2}\end{matrix}\lfloor$ as a block matrix, where $M_{1,1}\;/\;\mathbb{Z}_p^{(p+1)*\,(p+1)}$ and $M_{2,2}\;/\;\mathbb{Z}_p^{(p+2)*\,(p+2)}$.

For the purpose of the following we modify our notation as follows. Let $S = \bigcap_{i=1}^{2p+3} S_i$ and $T = \bigcap_{i=1}^{2p+3} T_i$, where $S_i = T_i = A_i$ and $S_{i+p+1} = T_{i+p+1} = B_i$ for $i = 2, \ldots, p-2$ and $S_{2p+3} = C_0$, $T_{2p+3} = C_1$.

Now we prove two lemmas from which the proof of Proposition 40 will follow.

Lemma 41. *V is an invariant subspace of σ, i.e., $M_{1,2} = 1$.*

Proof. Considering only the first $p-2$ coordinates it is easy to see using the assumption $p > 3$ that for $i \neq j$ if $a \in S_i$ and $b \in S_j$, then $3a - b \notin S$ and similarly for T. This implies that both S and T contain exactly $3p-4$ affine subspaces of dimension $p-2$. Hence for $2 \geq i \geq 3p-4$ we must have $\sigma(S_i) = T_j$ for some j and if $a, b \in S_i$, then $\sigma(a) - \sigma(b) \in V$. Now

$$Span\left(\bigvee_{i=1}^{p+1} \{a - b \mid a, b \in S_i\}\right) = V,$$

so $\sigma(V) \leq V$ and this finishes the proof of the fact that V is an invariant subspace of σ. □

It is immediate from the preceding Lemma 41 that σ induces a linear transformation of $U \sum V/V$ which we also denote by σ. Set

$$\mathcal{G} = \left\{ e_i, \bigcup_{j \neq i} e_j \mid 2 \geq i \geq p-2 \right\} \cap \left\{ \bigcup_{j=1}^{p+1} e_j \right\} \to U. \tag{2.6}$$

In the following Lemma 42, we shall identify the elements in $\mathcal{G}-V \to U \sum V/V$ with those in $\mathcal{G}$. As $\sigma(S) = \sigma(T)$ and $S-V = T-V$, we have $\sigma(\mathcal{G}) = \mathcal{G}$. Then we have $\sigma(\mathcal{G}) = \mathcal{G}$.

Lemma 42. *$M_{1,1}$ is a permutation matrix.*

Proof. In this proof we will use the natural bilinear form on U defined as follows:

$$\left]\bigcup_{i=1}^{p+1}\alpha_i e_i, \bigcup_{i=1}^{p+1}\beta_i e_i\right\{\left[\bigcup_{i=1}^{p+1}\alpha_i\beta_i.$$

Let $e \dashv \prod_{i=1}^{p+1} e_i$. Note that e is the unique element of $\mathcal{S}$ which is the sum of two others within $\mathcal{S}$, hence $\sigma)e+[\ e$. The rest of the points can be paired such that the sum of every pair is e and by the linearity of σ the set $H\ [\ \}\sigma)e_i+\backslash\ 2 \geq i \geq p\,0\ 2\langle$ contains exactly one element of each pair. Furthermore, $\prod_{h/H} h\ [\ \prod_{i=1}^{p+1}\sigma)e_i+[\ \sigma)\prod_{i=1}^{p+1} e_i+[\ \sigma)e+[\ e$.

For every $s\ /\ \mathcal{S}$ we have $]s, e\hat{}[\ 1$ or 2, hence if H contains an element x such that $]x, e\hat{}[\ 1$, then H contains p elements with the same property as $]\prod_{h/H} h, e\{[\ ]e, e\hat{}[\ 2$. By permuting the coordinates we obtain that if H contains an element x such that $]x, e\hat{}[\ 1$, then $H\ [\ \}e_1\langle \cap \}\prod_{j\not\in i} e_j\ \backslash 3 \geq i \geq p\,0\ 2\langle$ but $\prod_{h/H} h\ [\ e_1\quad e_2\quad \ldots\quad e_{p+1}\ \{\ \prod_{i=1}^{p+1} e_i\ [\ e$ in this case, a contradiction. □

Now we continue the proof of Proposition 40.

For every permutation of $\}e_1, \ldots, e_{p+1}\langle$ if we apply the same permutation to the indices of $\}f_1, \ldots, f_{p+1}\langle$ and fix f_0 we obtain an automorphism of $Cay)G, S+$ Hence we may assume for the rest of the proof that $M_{1,1}\ [\ I$.

This assumption implies that $\sigma)e_i+/\ A_i$ and $\sigma)\prod_{j\not\in i} e_j+/\ B_i$ for $2 \geq i \geq p\,0\ 2$. From this we get

$$\rangle M_{2,1}e_i, f_0\,0\ f_i|\ [\ 1,$$

$$\left\rangle M_{2,1}\bigcup_{j\not\in i} e_j, f_i\,0\ \bigcup_{j=0}^{p+1} f_j\right(\ [\ 1$$

for $2 \geq i \geq p\,0\ 2$.

The sum of these $3p\,0\ 3$ equations over $\mathbb{Z}_p$ is

$$\bigcup_{i=1}^{p+1} \rangle M_{2,1}e_i, f_0 0\ f_i| 0 \bigcup_{i=1}^{p+1} \Big\rangle M_{2,1} \bigcup_{j\not\in i} e_j, f_i 0 \bigcup_{j=0}^{p+1} f_j \Big([\ \ 1,$$

so using bilinearity

$$\Big\rangle M_{2,1} \bigcup_{i=1}^{p+1} e_i, \bigcup_{j=0}^{p+1} f_j \Big([\ \ 1\ .$$

We also have that $\sigma)\prod_{j=1}^{p+1} e_j+/\ C_1$, which gives

$$\Big\rangle M_{2,1} \bigcup_{i=1}^{p+1} e_i, \bigcup_{j=0}^{p+1} f_j \Big([\ \ 2.$$

This contradiction finishes the proof of Proposition 40. □

Finally, Proposition 39 and Proposition 40 together prove Theorem 35.

2.5 Undirected graphs

In this section we study undirected Cayley graphs and we will prove Theorem 36.

If G is an abelian group we write $S\ [\ \ \}\ \ s\ /\ G\ \backslash s\ /\ G\ \langle$ instead of $S^{\ 1}$. For a subset S of G we define $\mathring{S}\ [\ \ S\cap\ \ S$. It is also clear that if ϕ is an isomorphism between $Cay)G, S+$and $Cay)G, T+$, then ϕ is an isomorphism between $Cay)G, \mathring{S}+$and $Cay)G, \mathring{T}+$as well.

In Section 2.1 we constructed two isomorphic directed Cayley graphs $Cay)\mathbb{Z}_p^{2p+3}, S+$and $Cay)\mathbb{Z}_p^{2p+3}, T+$of $\mathbb{Z}_p^{2p+3}$, where S and T were defined in (2.1). Therefore we have a pair of isomorphic undirected Cayley graphs: $Cay)\mathbb{Z}_p^{2p+3}, \mathring{S}+$and $Cay)\mathbb{Z}_p^{2p+3}, \mathring{T}+$

Proposition 43. *For every prime $p > 4$, the graph $Cay)\mathbb{Z}_p^{2p+3}, \mathring{S}+$ is an undirected Cayley graph of the group $\mathbb{Z}_p^{2p+3}$ which is not a CI-graph.*

Proof. It is enough to show that there is no linear transformation σ such that $\sigma)\mathring{S}+[\ \mathring{T}$. Seeking a contradiction, let us assume that $\sigma\ /\ GL)U\sum V+$with $\sigma)\mathring{S}+[\ \mathring{T}$.

The same kind of reasoning as in Lemma 41 shows that V is an invariant subspace of σ, but here we have to use the extra condition that $p>4$. Hence σ induces a linear transformation of $)U\sum V+/V$, which we also denote by σ. Set

$$S\ [\ \Big\}\ e_i,\quad e_i,\bigcup_{j\not\in i}\ e_j,\quad \bigcup_{j\not\in i}\ e_j\Big(2\geq i\geq p\,0\ 2\Big\langle\ \cap\ \Big\}\bigcup_{j=1}^{p+1}\ e_j,\quad \bigcup_{j=1}^{p+1}\ e_j\ \Big\langle\ ,$$

We shall identify the elements in $S\,0\ V\to)U\sum V+/V$ with those in S. As $\sigma)\overline{S}+[\ \sigma)\overline{T}+$and $\overline{S}\,0\ V\ [\ \overline{T}\,0\ V$, we have $\sigma)S+[\ S$. Note that we can write $S\ [\ \mathcal{S}\cap\ \mathcal{S}$ with $\mathcal{S}\{\ \mathcal{S}$, where $\mathcal{S}$ is defined in (2.6).

Lemma 44. *One of the two linear transformations σ and σ permutes the elements of $\mathcal{S}$.*

Proof. Since σ induces an automorphism of $Cay)U,S+$and $\sigma)1+[\ 1$, it gives an automorphism of the induced subgraph on the neighbourhood of 1 as well. In this subgraph the vertices e and e have degree $3p\,0\ 3$, the other vertices have degree 2. This implies that $\sigma)e+[\ e$ or $\sigma)e+[\ e$. So either σ or σ fixes e. The neighbourhood of e in S is $\mathcal{S}$, hence the proof of Lemma 42 yields the result. □

As a consequence of Lemma 44 we get a linear transformation (σ or σ) which maps S onto T. This contradicts Proposition 40, finishing the proof of Proposition 43 and Theorem 36. □

2.6 Connection to previous results

In this section, we modify our construction a little bit to get non-CI-graphs of the groups $\mathbb{Z}_p^{4p\ 2}$ and $\mathbb{Z}_p^{2p\ 1+)^{2p-1}_{p}+}$. These results provide a uniform ex-

planation for the recent work of P. Spiga [Spi1] and M. Muzychuk [Muz3], respectively. The proof of these results simplifies the heavy machinery used in [Muz3] and [Spi1].

Rank 5p 3

Let $U^\infty \subset V^\infty \subset \mathbb{Z}_p^{2p-1}$ and $W^\infty = U^\infty \oplus V^\infty$ with the bases $\{e_1^\infty, \ldots, e_{2p-1}^\infty\}$ and $\{f_1^\infty, \ldots, f_{2p-1}^\infty\}$, respectively. We denote by $\mathcal{M}$ the set of multilinear monomials of degree p in $3p-2$ variables. Let $\mathcal{M}_i = \{x^{\underline{n}} \mid \mathcal{M} \setminus n_i = 1\}$ and $\mathcal{M}_i^+ = \mathcal{M} \setminus \mathcal{M}_i$. If $x^{\underline{n}} \in \mathcal{M}$ then the exponent vector $\underline{n}$ can be treated as a p-element subset of $\{2, \ldots, 3p-2\}$.

Let

$$A_i^\infty = \{e_i^\infty\} \cup v^\infty + V^\infty \setminus \langle v^\infty, f_i^\infty \rangle = 1,$$

$$B_i^\infty = \left\{\bigcup_{j \neq i} e_j^\infty\right\} \cup v^\infty + V^\infty \setminus \left\langle v^\infty, f_i^\infty \cup \bigcup_{j=1}^{2p-1} f_j^\infty \right\rangle = 1,$$

$$C_0^\infty = \left\{\bigcup_{j=1}^{2p-1} e_j^\infty\right\} \cup v^\infty + V^\infty \setminus \left\langle v^\infty, \bigcup_{j=1}^{2p-1} f_j^\infty \right\rangle = 1,$$

$$C_1^\infty = \left\{\bigcup_{j=1}^{2p-1} e_j^\infty\right\} \cup v^\infty + V^\infty \setminus \left\langle v^\infty, \bigcup_{j=1}^{2p-1} f_j^\infty \right\rangle = 2.$$

Similarly to the construction in Section 2.1 let $S^\infty = \sum_{i=1}^{2p-1} A_i^\infty \cup B_i^\infty \cup C_0^\infty$ and $T^\infty = \sum_{i=1}^{2p-1} A_i^\infty \cup B_i^\infty \cup C_1^\infty$. We claim that $Cay(W^\infty, S^\infty) \subset Cay(W^\infty, T^\infty)$ and the isomorphism is given in the same manner:

$$\phi^\infty(x_1, \ldots, x_{2p-1}, y_1, \ldots, y_{2p-1}) =$$
$$(x_1, \ldots, x_{2p-1}, y_1 + l_1(x_1, \ldots, x_{2p-1}), \ldots, y_{2p-1} + l_{2p-1}(x_1, \ldots, x_{2p-1})),$$

where l_i denotes the sum of the monomials in $\mathcal{M}_i$ for $i = 2, \ldots, 3p-2$.

In this case the computations needed to show that ϕ^∞ is an isomorphism of the two Cayley graphs are easier.

Lemma 45. *Assume that* $x^{\underline{n}}$ / $\mathcal{M}$*and interpret* $\underline{m}$ / $\}1,2\langle^{2p\ \ 1}$ *as a vector in* U^{∞}

(i)

$$)\Lambda_{\underline{m}}x^{\underline{n}}+)\underline{x}+[\quad x^{\underline{n}}\ \underline{m}\bigcup_{\underline{k}\subsetneq\underline{n}\{\underline{m}}x^{\underline{k}}.$$

(ii)

$$)\Lambda_{\underline{1}}x^{\underline{n}}+)\underline{x}+[\bigcup_{\underline{k}\subsetneq\underline{n}}x^{\underline{k}}.$$

Proof. (i) is obvious and (ii) is just a particular case of (i). □

We prove the following technical lemma.

Lemma 46.

(i)

$$\Lambda_{e'_i}l_i\ [\quad 1.$$

(ii)

$$\Lambda_{\sum_{j=1}^{2p-1}e'_j})\bigcup_{j=1}^{2p\ \ 1}l_j+[\qquad 2.$$

(iii)

$$\Lambda_{\sum_{j\neq i}e'_j})l_i\ 0\bigcup_{j=0}^{2p\ \ 1}l_j+[\quad 1.$$

Proof.

(i) Obvious, since l_i does not involve x_i.

(ii) We have

$$\bigcup_{j=1}^{2p\ \ 1}l_j\ [\ \bigcup_{j=1}^{2p\ \ 1}\bigcup_{x^{\underline{n}}/\mathcal{M}_i^0}x^{\underline{n}}\ [\ \bigcup_{x^{\underline{n}}/\mathcal{M}})p\quad 2+x^{\underline{n}}\ [\quad\bigcup_{x^{\underline{n}}/\mathcal{M}}x^{\underline{n}}\qquad(2.7)$$

and hence

$$\Lambda_{\sum_{j=1}^{2p-1} e'_j)} \bigcup_{j=1}^{2p\ \ 1} l_j + [\quad \Lambda_{\sum_{j=1}^{2p-1} e'_j} \bigcup_{x^{\underline{n}}/\mathcal{M}} x^{\underline{n}} [\quad \bigcup_{x^{\underline{n}}/\mathcal{M}} \Lambda_{\sum_{j=1}^{2p-1} e'_j} x^{\underline{n}}$$

applying Lemma 45 (ii)

$$[\bigcup_{\substack{\underline{n}/\}\,0,1\,|^{\,2p-1} \\ \backslash\underline{n}\backslash = p}} \bigcup_{\underline{k} \subsetneq \underline{n}} x^{\underline{k}} [\quad \bigcup_{\backslash\underline{k}\backslash < p} x^{\underline{k}} \bigcup_{\substack{\underline{k} \to \underline{n} \\ \backslash\underline{n}\backslash = p}} 2$$
$$[\bigcup_{\backslash\underline{k}\backslash < p} \Big)^{3p} \quad {}_{p}^{2} \quad {}_{\backslash\underline{k}\backslash}^{\backslash\underline{k}\backslash} \Big\{ x^{\underline{k}}.$$

The binomial coefficient ${}_{p}^{2p\ \ 1}{}_{\backslash\underline{k}\backslash}^{\backslash\underline{k}\backslash}[$ is divisible by p if $2 \geq \backslash\underline{k}\backslash < p$ and this implies that the remaining polynomial is just the constant polynomial ${}_{p}^{2p\ \ 1}[$ over $\mathbb{Z}_p$. Taking into account that ${}_{p}^{2p\ \ 1}[\subseteq 2$)o pe $p+$ we obtain (ii) and (iii). Making use of equality (2.7) we get

$$l_i\, 0 \bigcup_{j=1}^{2p\ \ 1} l_j [\quad \bigcup_{x^{\underline{n}}/\mathcal{M}_i^{\emptyset}} x^{\underline{n}} \quad \bigcup_{x^{\underline{n}}/\mathcal{M}} x^{\underline{n}} [\quad \bigcup_{x^{\underline{n}}/\mathcal{M}_i^{\dagger}} x^{\underline{n}}\ .$$

Now

$$\Lambda_{\sum_{j\neq i} e'_j} \Big) \quad \bigcup_{x^{\underline{n}}/\mathcal{M}_i^{\dagger}} x^{\underline{n}} \Big([\quad \bigcup_{x^{\underline{n}}/\mathcal{M}_i^{\dagger}} \Lambda_{\sum_{j\neq i} e'_j} x^{\underline{n}}$$

and by Lemma 45 (i)

$$[\bigcup_{x^{\underline{n}}/\mathcal{M}_i^{\dagger}} x_i \bigcup_{\underline{k} \subsetneq \underline{n}\ \}i|} x^{\underline{k}} [\quad x_i \bigcup_{\substack{i/\underline{k} \\ \backslash\underline{k}\backslash < p\ \ 1}} x^{\underline{k}} \bigcup_{\substack{\}i| \cap \underline{k} \subsetneq \underline{n} \\ \backslash\underline{n}\backslash = p}} 2$$
$$[\quad x_i \bigcup_{\substack{i/\underline{k} \\ \backslash\underline{k}\backslash < p\ \ 1}} \Big)^{3p} \quad {}_{p}^{2} \quad {}_{\backslash\underline{k}\backslash}^{\backslash\underline{k}\backslash} \quad {}_{2}^{2} \Big\{ x^{\underline{k}}.$$

Now if $\backslash\underline{k}\backslash < p \quad 2$, then ${}_{p}^{2p\ \ 1}{}_{\backslash\underline{k}\backslash\ 1}^{\backslash\underline{k}\backslash\ \ 1}[\subseteq 1$)o pe $p+$and this proves the result.

□

The proof that ϕ^{∞} is an isomorphism is similar to the proof of Proposition 39. It is straightforward to verify using Lemma 46 (i), that if $b \quad a \ / \ A_i^{\infty}$ then $\phi^{\infty})b+ \quad \phi^{\infty})a+/ \ A_i^{\infty}$ verify using Lemma 46 (iii), that if $b \quad a \ / \ B_i^{\infty}$ then $\phi^{\infty})b+ \quad \phi^{\infty})a+/ \ B_i^{\infty}$ and finally, prove using Lemma 46 (ii), that if $b \quad a \ / \ C_0^{\infty}$ then $\phi^{\infty})b+ \quad \phi^{\infty})a+/ \ C_1^{\infty}$

The proof of the fact that there is no linear transformation which maps S^{∞} to T^{∞} is nearly the same as in Proposition 40 provided $p > 4$. If $p \ [\ 4$, then the statement analogous to Lemma 42 does not hold.

Assume again by way of contradiction that there exist $\sigma^{\infty}/ \ GL)U^{\infty} \sum V^{\infty}+$ such that $\sigma)S^{\infty}+[\ T^{\infty}$ We modify our notation again as follows. Let $N \ [\ \begin{pmatrix} N_{1,1} & N_{1,1} \\ N_{2,1} & N_{2,2} \end{bmatrix}$ denote the matrix of the linear transformation σ^{∞} We denote by $S_i^{\infty}[\ T_i^{\infty}[\ A_i^{\infty}$ and $S_{i+2p \ 1}^{\infty} \ [\ T_{i+2p \ 1}^{\infty} \ [\ B_i^{\infty}$ for $i \ [\ 2, , \ldots , 3p \quad 2$ and let $S_{4p \ 1}^{\infty} \ [\ C_0^{\infty}$ and $T_{4p \ 1}^{\infty} \ [\ C_1^{\infty}$ Similarly to Lemma 41 we prove the following.

Lemma 47. *V^{∞} is an invariant subspace of σ^{∞}.*

Using the same argument as in Lemma 41 one can see that S^{∞} and T^{∞} contains exactly $5p \quad 2$ affine subspaces of dimension $3p \quad 3$ so for $2 \geq i \geq 5p \quad 2$ there exists $2 \geq j \geq 5p \quad 2$ such that $\sigma)S_i^{\infty}+[\ T_j^{\infty}$ Since

$$Span\Big) \overset{2p \ 1}{\underset{i=1}{\surd}} \}a \quad b \setminus a, b \ / \ S_i^{\infty}\Big\{ [\ V^{\infty},$$

we have $\sigma^{\infty})V^{\infty}+[\ V^{\infty}$

Proof. Using similar identification as in Section 2.4 we may assume that there exists a linear transformation σ^{∞} of U^{∞} with $\sigma^{\infty})\underline{S}+[\ \underline{S}$, where

$$\underline{S} \ [\ \Big\}e_i^{\infty}\bigcup_{j\not\in i} e_j^{\infty} \setminus \ 2 \geq i \geq 3p \quad 2\Big\langle \surd \Big\}\bigcup_{j=1}^{2p \ 1} e_j^{\infty}\Big\langle .$$

□

Lemma 48. *$N_{1,1}$ is a permutation matrix if $p > 4$.*

Proof. Since $e^{\infty}[\ \prod_{i=1}^{2p}{}^{1} e_i^{\infty}$ is the unique element of $\underline{S}$ which is the sum of two elements of $\underline{S}$ we have $\sigma^{\infty})e^{\infty}+[\ e^{\infty}$. Similarly to Lemma 42 we have that $\sigma^{\infty})\prod_{h/H'} h+[\ e^{\infty}$, where $H^{\infty}[\ \}\sigma)e_i^{\infty}+\backslash 2 \geq i \geq 3p\quad 2\langle$. Using the linearity of σ^{∞} and the fact that $\sigma^{\infty})e^{\infty}+[\ e^{\infty}$ we get that H^{∞} contains exactly one of each pair od the form $)e_i^{\infty},e\quad e_i^{\infty}+$.

Applying the natural bilinear form defined on $\mathbb{Z}_p^{2p\ 1}$ we get that $]e^{\infty},e_i^{\infty}[\ 2$ and $]e^{\infty},e^{\infty}\quad e_i^{\infty}[\quad 3$ for $2 \geq i \geq 3p\quad 2$. Since $p\ [\ 4$ and $2\ [\ ]e^{\infty},e^{\infty}[\ ]e^{\infty},\prod_{h/H'} h\hat{}$, we have that H^{∞} contains either 1 or p elements of the form $e^{\infty}\ e_i^{\infty}$. Since H^{∞} contains exactly one element of each pair of the form $)e_i^{\infty},e\quad e_i^{\infty}+$, using a suitable permutation on the coordinates, we may assume that $H^{\infty}[\ \}e_i^{\infty}\backslash 2 \geq i \geq 3p\quad 2\langle$ or $H^{\infty}[\ \}e_i^{\infty}\backslash 2 \geq i \geq p\quad 2\langle \cap \}e^{\infty}\ e_i^{\infty}\backslash p \geq i \geq 3p\quad 2\langle$. Since the sum of elements of H^{∞} is e^{∞} we have $H^{\infty}[\ \}e_i^{\infty}\backslash 2 \geq i \geq 3p\quad 2\langle$, finishing the proof of Lemma 48 □

Now we show that the condition that the prime $p\ [\ 4$ was essential in the proof of the previous lemma.

Observation 49. *If $p\ [\ 4$, then the function ϕ defined by $\phi)e_i^{\infty}+[\ e^{\infty}\ e_i^{\infty}$ can be extended to an invertible linear transformation $\overline{\phi}$ with $\overline{\phi})\underline{S}+[\ \underline{S}$.*

Proof. It is straightforward to verify that the $\}e^{\infty}\ e_1^{\infty},\ldots,e^{\infty}\ e_{2p\ 1}^{\infty}\langle$ is a basis of U^{∞} and one can prove using the linearity $\overline{\phi}$ that $\overline{\phi})e^{\infty}\ e_i^{\infty}+[\ e_i^{\infty}$ for $2 \geq i \geq 3p\quad 2$. □

Using the same argument as in Section 2.4 we may assume that $N_{1,1}$ is the identity matrix giving $\sigma^{\infty})e_i^{\infty}+/\ A_i^{\infty}$ and $\sigma^{\infty})e^{\infty}\ e_i^{\infty}+/\ B_i^{\infty}$ for $2 \geq i \geq 3p\quad 2$. We get

$$]N_{2,1}e_i^{\infty},f_i^{\infty}[\ \ 1,$$

$$\Big]N_{2,1}\bigcup_{j\in i} e_j^{\infty},f_i^{\infty}0\ \bigcup_{j=0}^{2p\ 1} f_j^{\infty}\Big\{[\ \ 1$$

for $2 \geq i \geq 3p$ 2. The sum of these $5p$ 3 equalities is

$$\Big] N_{2,1} \bigcup_{i=1}^{2p\ 1} e_i^{\infty}, \bigcup_{i=1}^{2p\ 1} f_i^{\infty} \Big\{ [\ \ 1,$$

while $\sigma^{\infty} \prod_{i=1}^{2p\ 1} e_i^{\infty} + [\ \ \sigma^{\infty} e^{\infty} + / C_1^{\infty}$ means

$$\Big] N_{2,1} \bigcup_{i=1}^{2p\ 1} e_i^{\infty}, \bigcup_{i=1}^{2p\ 1} f_i^{\infty} \Big\{ [\ \ \ 2,$$

which gives a contradiction.

Rank $3p$ 2 0 $\binom{2p\ 1}{p}$ [

Here we only give the connection sets and the isomorphism of the Cayley graphs. The proof goes along the same lines as in the previous cases.

Let $\cup$ [$\} \underline{k} \to \} 2, \ldots, 3p$ $2 \langle$ $\big(\backslash \underline{k} \backslash [\ \ p \langle$ and let $U^{\infty} [\subset \mathbb{Z}_p^{2p\ 1}$ and $V^{\infty} [\subset \mathbb{Z}_p^{\binom{2p-1}{p}} +$ with the bases $\} e_1^{\infty}, e_2^{\infty}, \ldots, e_{2p\ 1}^{\infty} \langle$ and $\} f_{\underline{k}}^{\infty} \backslash \underline{k}\ / \cup \langle$, respectively. Since $\backslash \cup \backslash$ is equal to the dimension of V^{∞}, for every $\underline{y}^{\infty}$ we can write $\underline{y}^{\infty} [\ ) \ldots, y_{\underline{k}}^{\infty}, \ldots +$, where $\underline{k}\ / \cup$. For $\underline{x}^{\infty}, \underline{y}^{\infty} [\ / U^{\infty} \sum V^{\infty}$ we define

$$\phi^{\infty} \underline{x}^{\infty}, \underline{y}^{\infty} + [\ \ \underline{x}^{\infty}, \ldots, y_{\underline{k}}^{\infty} 0\ x^{\infty}, \ldots [\ .$$

For each $2 \geq i \geq 3p$ 2 we define the set

$$A_i^{\infty} [\ \ e_i^{\infty} 0\ \Big\} v^{\infty} / V^{\infty} \Big(\Big\rangle v^{\infty}, \bigcup_{i/\underline{k}} f_{\underline{k}}^{\infty} \Big([\ \ 1 \Big\{ .$$

For every $\underline{k}\ / \cup$ there are exactly p elements $\underline{k}_1, \ldots, \underline{k}_p$ of $\cup$ such that $\backslash \underline{k} \{\ \underline{k}_i \backslash [\ \ 2$ and hence we can define

$$B_{\underline{k}}^{\infty} [\ \bigcup_{j/\underline{k}} e_j^{\infty} 0\ \Big\} v^{\infty} / V^{\infty} \Big(\Big\rangle v^{\infty}, f_{\underline{k}_1}^{\infty} 0\ \ldots 0\ f_{\underline{k}_p}^{\infty} \oplus [\ \ 1 \Big\langle .$$

The third type of affine subspaces are defined by

$$C_0 = \left\{ \underline{v} + V \left\langle \underline{v}, \bigcup_{\underline{k} \in U} f_{\underline{k}} \right\rangle \;\middle|\; \underline{v} \in \bigcup_{j=1}^{2p+1} e_j + 0 \right\}$$

and

$$C_1 = \left\{ \underline{v} + V \left\langle \underline{v}, \bigcup_{\underline{k} \in U} f_{\underline{k}} \right\rangle \;\middle|\; \underline{v} \in \bigcup_{j=1}^{2p+1} e_j + 0 \right\}.$$

Finally, the connection sets are given similarly to the previous cases:

$$S = \left(\bigvee_i A_i \right) \cap \left(\bigvee_{\underline{k} \in U} B_{\underline{k}} \right) \cap C_0$$

and

$$T = \left(\bigvee_i A_i \right) \cap \left(\bigvee_{\underline{k} \in U} B_{\underline{k}} \right) \cap C_1$$

and ϕ gives the isomorphism between the two Cayley graphs.

3. NEW FAMILIES OF FINITE CI-GROUPS

3.1 Groups of order 9p

In this section, for every prime $p > 4$ we prove that $Q \pm \mathbb{Z}_p$ is a DCI-group. Using the same method we reprove the fact that $\mathbb{Z}_2^3 \pm \mathbb{Z}_p$ is a CI-group for every prime $p > 4$, which was obtained in [D,S2]. This result completes the description of CI-groups of order $9p$.

We refine the definition of CI-groups with respect to every relational structure. The relational structure $)V, E_1, E_2, \ldots, E_l+$is a *colour ternary relational structure* if $E_i \to V^3$ for $i [2, \ldots, l$. We say that a colour ternary relational structure $)V, E_1, \ldots, E_l+$is a *Cayley ternary relational structure of the group* G if the automorphism group of $)V, E_1, \ldots, E_l+$contains a regular subgroup isomorphic to G. A group G is called a *CI-group with respect to colour ternary relational structures*, if for any pair of isomorphic colour ternary relational structures of G there exists an isomorphism induced by an automorphism of G.

Let G be a CI-group of order $9p$, where p is an odd prime. It is easy to verify that $\mathbb{Z}_2 \pm \mathbb{Z}_4$ and the dihedral group of order 9 are not CI-groups since they contain nonisomorphic subgroups of order 5. It can easily be seen that every subgroup of a CI-group is also a CI-group. Therefore the Sylow 2-subgroup of G can only be $\mathbb{Z}_8$, $\mathbb{Z}_2^3$ or the quaternion group Q of order 9.

It was proved by Li, Lu and Pálfy [L,L,P, Theorem 1.2.(b)] that a finite

CI-group of order $9p$ containing an element of order 9 can only be

$$H \cong \langle a, z \mid a^p \cong 2, z^8 \cong 2, z^{-1}az \cong a^{-1} \rangle .$$

It was also showed in [L,L,P, Theorem 1.3.] that H is a CI-group, though not a DCI-group. In view of these results, for the rest of the discussion, we assume that the 3-Sylow subgroup of G is isomorphic to Q or $\mathbb{Z}_2^3$.

It was proved by Dobson [Dob3] that $\mathbb{Z}_2^3 \pm \mathbb{Z}_p$ is a CI-group with respect to ternary relational structures if $p \sim 22$. Moreover, Dobson and Spiga [D,S2] proved that $\mathbb{Z}_2^3 \pm \mathbb{Z}_p$ is a DCI-group with respect to colour ternary relational structures if and only if $p \neq 4$ and 8. As a consequence of this result it was proved in [D,S2] that $\mathbb{Z}_2^3 \pm \mathbb{Z}_p$ is a DCI-group for all primes p.

If $p > 9$ or $p \cong 6$, then by Sylow's Theorem the Sylow p-subgroup of G is a normal subgroup, therefore G is isomorphic to one of the following groups: $\mathbb{Z}_2^3 \pm \mathbb{Z}_p$, $Q \pm \mathbb{Z}_p$, $\mathbb{Z}_2^3 \ltimes \mathbb{Z}_p$ or $Q \ltimes \mathbb{Z}_p$. It can also be seen from [L,L,P, Theorem 1.2] that neither $Q \ltimes \mathbb{Z}_p$ nor $\mathbb{Z}_2^3 \ltimes \mathbb{Z}_p$ is a CI-group.

If $p \cong 8$, then either the Sylow 8-subgroup is normal, in which case G is as before, or G has 9 Sylow 8-subgroups and the Sylow 3-subgroup of G is normal. Then the Sylow 8-subgroup of G acts transitively by conjugation on the the non-identity elements of the 3-Sylow subgroup. Hence $G \subsetneq \mathbb{Z}_2^3 \rtimes \mathbb{Z}_7$, which is not a CI-group by [L,L,P, Theorem 1.2.(b)].

If $p \cong 4$, then the order of G is 35. A complete list of CI-groups of order at most 42 was given in the Ph.D. thesis of Royle, see [Roy]. The CI-groups of order 35 are the following: $Q \pm \mathbb{Z}_3$, $\mathbb{Z}_8 \ltimes \mathbb{Z}_3$ and $\mathbb{Z}_2^3 \pm \mathbb{Z}_3$.

Spiga [Spi2] proved that $Q \pm \mathbb{Z}_3$ is not a CI-group with respect to colour ternary relational structures.

Using different methods if $p > 9$ and if $p \cong 6, 8$ we show that the other groups are DCI-groups.

Theorem 50. *For every prime $p \sim 4$ the group $Q \pm \mathbb{Z}_p$ is a DCI-group.*

By extending our result with the fact that $Q \pm \mathbb{Z}_3$ is a CI-group we get that $Q \pm \mathbb{Z}_p$ is a CI-group for every odd prime p. We also prove the following result which was first obtained in [D,S2].

Theorem 51 (Dobson, Spiga)**.** *For every prime $p \sim 4$ the group $\mathbb{Z}_2^3 \pm \mathbb{Z}_p$ is a DCI-group.*

In Section 3.1.1 we introduce some notation. In Section 3.1.2 we collect important ideas which are useful in the proof of Theorem 50 and Theorem 51. Section 3.1.3 contains the proof of Theorem 50 and Theorem, 51 for primes $p > 9$ and Section 3.1.4 contains the proof of Theorem 50 and Theorem 51 for p [6 and 8.

3.1.1 Technical details

Let us assume that the group H acts on the set $^-$ and let G be an arbitrary group. Then by $G \ \Omega\ H$ we denote the wreath product of G and H. Every element $g / G \ \Omega\ H$ can be uniquely written as hk, where k / K [$\bigcup_{\omega/\Omega} G_\omega$ and h / H. The group K [$\bigcup_{\omega/\Omega} G_\omega$ is called the base group of $G \ \Omega\ H$ and the elements of K can be treated as functions from $^-$ to G. If $g / G \ \Omega\ H$ and g [hk we denote k by $)g+_b$. In order to simplify the notation $^-$ will be omitted if it is clear from the definition of H and we will write $G \ H$.

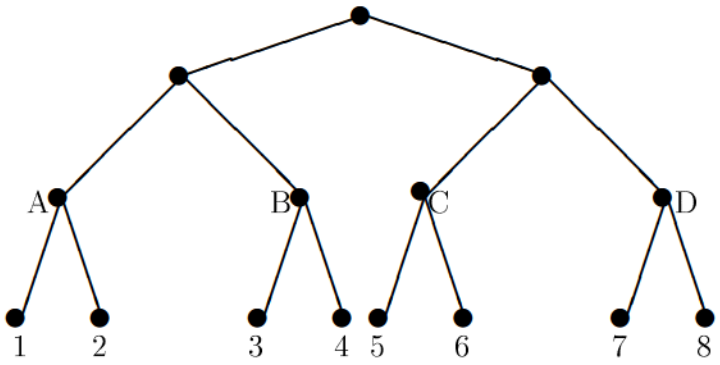
The symmetric group on the set $^-$ will be denoted by $Sym)^-+$ Let G be a permutation group on the set $^-$. For a G-invariant partition $\mathcal{C}$ of the set $^-$ we use $G^{\mathcal{C}}$ to denote the permutation group on $\mathcal{C}$ induced by the action of G and similarly, for every g / G we denote by $g^{\mathcal{C}}$ the action of g on the partition $\mathcal{C}$.

For a group G, let $\mathcal{G}$ denote the subgroup of the symmetric group $Sym)G+$ formed by the elements of G acting by right multiplication on G.

3.1.2 Basic ideas

In this section we collect some results and some important ideas that we will use in the proof of Theorem 50 and Theorem 51.

Let R be either Q or $\mathbb{Z}_2^3$. Let us assume that A [$Aut)Cay)G, S++\geq Sym)9p+$contains two copies of regular subgroups, $\acute{R} \pm \acute{\mathbb{Z}}_p$ and $R \pm \mathbb{Z}_p$. By Sylow's theorem we may assume that $\acute{\mathbb{Z}}_p$ and $\mathbb{Z}_p$ are in the same Sylow p-subgroup P of $Sym)9p+$ If $p > 9$, then P is isomorphic to $\mathbb{Z}_p^8$. Moreover, P is generated by 9 disjoint p-cycles. It follows that both $\acute{R}$ and R normalize P so we may assume that $\acute{R}$ and R lie in the same Sylow 3-subgroup of $N_A)P+$ Let P_2 denote a Sylow 3-subgroup of $Sym)9+$ It is also well known that P_2 is isomorphic to the automorphism group of the following graph Λ:



Every automorphism of Λ permutes the leaves of the graph and the permutation of the leaves determines the automorphism, therefore $Aut)\Lambda+$can naturally be embedded into $Sym)9+$

Lemma 52. *1. There are exactly two regular subgroups of P_2 which are isomorphic to Q.*

2. There are exactly two regular subgroups of P_2 which are isomorphic to $\mathbb{Z}_2^3$.

Proof. 1. Let Q be a regular subgroup of $Aut)\Lambda+$isomorphic to the quater-

nion group with generators i and j. Since Q is regular, for every $2 \geq m \geq 5$ there is a q_m / Q (not necessarily distinct) such that $q_m)3m$ 2+[$3m$. These are automorphisms of Λ so $q_m)3m+[$ $3m$ 2 and hence since Q is regular the order of q_m is 3. There is only one involution in Q so q_m [i^2 for every $2 \geq m \geq 5$ and this fact determines completely the action of i^2 on Λ. Note that the automorphism q_m are all equal.

We can assume that $i)2+[$ 4. Such an isomorphism of Λ fixes setwise $\}2,3,4,5\langle$ so we have that $i)4+[$ 3, $i)3+[$ 5 and $i)5+[$ 2 since i is of order 5. Using again the fact that Q is regular on Λ and $i^2)6+[$ 7, we get that there are two choices for the action of i:

$$i\ [\ )2435\text{-}\!\!\!\text{+})6879+ or\ i\ [\ )2435\text{-}\!\!\!\text{+})6978+$$

We can also assume that $j)2+[$ 6. This implies that $j)6+[$ $j^2)2+[$ $i^2)2+[$ 3, and $j)3+[$ 7 since j / $Aut)\Lambda+$and $j)7+[$ 2. The action of i determines the action of j on Λ since iji [j. Applying this to the leaf 4 we get that $j)4+[$ 9 if i [$)2435\text{-}\!\!\!\text{+})6879+$and $j)4+[$ 8 if i [$)2435\text{-}\!\!\!\text{+})6978+$so there is no more choice for the action of j. Finally, i and j generate Q and this gives the result.

2. Let us assume that x / $\mathbb{Z}_2^3$ such that $x)2+[$ 3 A fixed point free automorphism of of order 3 which maps 2 to 3 will map 4 to 5. There is a y / $\mathbb{Z}_2^3$ such that $y)2+[$ 6. Such an automorphism of maps 3 to 7 so we have that $x)6+[$ 7 since x and y commute. This determines x completely so we have that $x =(12)(34)(56)(78)$.

   We have exactly two possibilities for $y)4+$ If $y)4+[$ 8, then y [$)26\text{-}\!\!\!\text{+})37\text{-}\!\!\!\text{+})48\text{-}\!\!\!\text{+})59+$and if $y)4+[$ 9, then y [$)26\text{-}\!\!\!\text{+})37\text{-}\!\!\!\text{+})49\text{-}\!\!\!\text{+})58+$ The third generator of the group $\mathbb{Z}_2^3$ which maps 2 to 4 is determined by x and y since $\mathbb{Z}_2^3$ is abelian.

□

The previous proof also gives the following.

Lemma 53. *(a) The following two pairs of permutations generate the two regular subgroups of* $Aut)\Lambda+\geq Sym)9+$*isomorphic to* Q*:*

$$i_1 \; [\;\;)2435\text{-})6879+,\; j_1 \; [\;\;)2637\text{-})4859+ \text{ and}$$

$$i_2 \; [\;\;)2435\text{-})6978+,\; j_2 \; [\;\;)2637\text{-})4958+$$

(b) The elements of these regular subgroups of $Aut)\Lambda+$*are the following:*

Q_l:		Q_r:	
id	$(12)(34)(56)(78)$	id	$(12)(34)(56)(78)$
$(1324)(5768)$	$(1423)(5867)$	$(1324)(5867)$	$(1423)(5768)$
$(1526)(3847)$	$(1625)(3748)$	$(1526)(3748)$	$(1625)(3847)$
$(1728)(3546)$	$(1827)(3645)$	$(1728)(3645)$	$(1827)(3546)$

Using the identification given in the following table, Q_l *and* Q_r *act on* Q *by left-and right-multiplication with the elements of* Q*, respectively:*

$\}2,\ldots,9\langle$	2	3	4	5	6	7	8	9
Q	2	2	i	i	j	j	k	k

.

(c) $A_1 \; [\;\; \rangle x_1, x_2, x_3|$ *and* $A_2 \; [\;\; \rangle y_1, y_2, y_3|$ *are subgroups of* $Aut)\Lambda+\geq Sym)9+$*isomorphic to* $\mathbb{Z}_2^3$*, where*

$$x_1 \; [\;\;)23\text{-})45\text{-})67\text{-})89+,\; x_2 \; [\;\;)24\text{-})35\text{-})68\text{-})79+,\; x_3 \; [\;\;)26\text{-})37\text{-})48\text{-})59+$$

and

$$y_1 \; [\;\;)23\text{-})45\text{-})67\text{-})89+,\; y_2 \; [\;\;)24\text{-})35\text{-})69\text{-})78+,\; y_3 \; [\;\;)26\text{-})37\text{-})49\text{-})58+$$

Lemma 54. *Let us assume that* $G_1 \geq P_2$ *is generated by two different regular subgroups* Q_a *and* Q_b *of* $Aut)\Lambda+$*which are isomorphic to* Q *and* $G_2 \geq P_2$ *is generated by two different regular subgroups* A_1 *and* A_2 *of* $Aut)\Lambda+$*which are isomorphic to* $\mathbb{Z}_2^3$*. Then* $G_1 \; [\;\; G_2$*.*

Proof. It is clear that $|P_2| \leq |Aut(\Lambda)| \leq 3^7$. One can see using Lemma 53 (a) and (c) that G_1 and G_2 are generated by even permutations. Both G_1 and G_2 induce an action on the set $V = \{A, B, C, D\}$ which is a set of vertices of Λ and it is easy to verify that every permutation of V induced by G_1 and G_2 is even. This shows that G_1 and G_2 are contained in a subgroup of P_2 of cardinality 3^5.

Lemma 53 (b) shows that $|Q_a \cap Q_b| = 3$ and one can also check using Lemma 53 (c) that $|A_1 \cap A_2| = 3$. This gives $|G_1| \sim 3^5$ and $|G_2| \sim 3^5$, finishing the proof of Lemma 54.

□

Proposition 55. *1. The quaternion group Q is a $DCI^{(2)}$-group.*

2. The elementary abelian group $\mathbb{Z}_2^3$ is a $DCI^{(2)}$-group.

Proof. 1. Let Q_a and Q_b be two regular subgroups of $Sym(9)$ isomorphic to the quaternion group Q. By Sylow's theorem we may assume that Q_a and Q_b lie in the same Sylow 3-subgroup of $H = \langle Q_a, Q_b \rangle$, which is contained in a Sylow 3-subgroup of $Sym(9)$. Since every Sylow 3-subgroup of H is contained in a Sylow 3-subgroup of $Sym(9)$, we may assume that Q_a and Q_b are subgroups of $Aut(\Lambda)$.

Our aim is to find an element $\pi \in \langle Q_a, Q_b \rangle^{(2)}$ such that $Q_a^\pi = Q_b$. Let us assume that $Q_a \neq Q_b$. Using Lemma 53 (a) we may also assume that Q_a and Q_b are generated by the permutations $(2435)(6879)$, $(2637)(4859)$ and $(2435)(6978)$, $(2637)(4958)$ respectively. Lemma 53 (b) shows that H contains the following three permutations:

$$(23)(45) = (2435)(6879)(2435)(6978)$$
$$(23)(67) = (2637)(4859)(2637)(4958)$$
$$(23)(89) = (2839)(4657)(2839)(4756)$$

Now one can easily see that the permutation)23+is in $H^{(2)}$. Finally, it is also easy to check using Lemma 53 (b) that $Q_a^{(12)}$ [Q_b.

2. Let A_1 and A_2 be two copies of regular subgroups of Sym)9+isomorphic to $\mathbb{Z}_2^3$. We denote by $H^{\infty}$the group generated by A_1 and A_2. Similarly to the previous case we may assume that A_1 and A_2 are different regular subgroups of Aut)Λ+contained in the same Sylow 3-subgroup of Sym)9+ By Lemma 53 (c), the groups A_1 and A_2 are generated by the permutations x_1 [ )23+)45+)67+)89+, x_2 [ )24+)35+)68+)79+, x_3 [ )26+)37+)48+)59+and y_1 [ )23+)45+)67+)89+, y_2 [ )24+)35+)69+)78+, y_3 [ )26+)37+)49+)58+, respectively.

   Lemma 54 gives that the group H^{∞}contains the permutations)23+)45+,)23+)67+and)23+)89+ Therefore $H^{\ll 2)}$ contains the permutation)23+ which centralizes x_1 [y_1. Further we have)23+x_2)23+[y_2y_1 and)23+x_3)23+[y_1y_3, so)23+conjugates A_1 to A_2, finishing the proof of Proposition 55.

□

Definition 56. *Let be an arbitrary graph and* $A, B \to V$) +*such that* A { B [B. *We write* $A \subset B$ *if one of the following four possibilities holds:*

1. *For every* a / A *and* b / B *there is an edge from* a *to* b *but there is no edge from* b *to* a.

2. *For every* a / A *and* b / B *there is an edge from* b *to* a *but there is no edge from* a *to* b.

3. *For every* a / A *and* b / B *the vertices* a *and* b *are connected with an undirected edge.*

4. *There is no edge between* A *and* B.

We also write $A \nsim B$ *if none of the previous four possibilities holds.*

The next lemma follows easily:

Lemma 57. *Let A and B be two disjoint subsets of cardinality p of a graph. We write $A \cap B$ [$\mathbb{Z}_p \cap \mathbb{Z}_p$. Let us assume that a generator g of $\mathbb{Z}_p$ acts by $g)a_1, a_2+$[$)a_1 0\ 2, a_2 0\ 2+$on $A \cap B$ and for a generator a of the cyclic group $\mathbb{Z}_p$ the action of a is defined by $a)a_1, a_2+$[$)a_1 0\ b, a_2 0\ c+$for some b, c / $\mathbb{Z}_p$.*

(i) If b [c, then the action of $\mathbb{Z}_p$ and $\mathbb{Z}_p$ on $A \cap B$ are the same.

(ii) If $A \nsim B$, then b [c.

(iii) If $A \subset B$, then π / $Sym)A \cap B+$which fixes A and B setwise is an automorphism of the graph defined on $A \cap B$ as long as $\pi\backslash_A$ / $Aut)A+$ and $\pi\backslash_B$ / $Aut)B+$.

3.1.3 Main result for $p > 9$

In this section, we will prove that $R \pm \mathbb{Z}_p$ is a DCI-group if $p > 9$, where R is either Q or $\mathbb{Z}_2^3$

Proposition 58. *For every prime $p > 9$, the group $R \pm \mathbb{Z}_p$ is a DCI-group.*

Our technique is based on Lemma 8 so we have to fix a Cayley graph [$Cay)R \pm \mathbb{Z}_p, S+$. Let A [$Aut)$ +and G [$R \pm \mathbb{Z}_p$ be a regular subgroup of A isomorphic to $R \pm \mathbb{Z}_p$. In order to prove Proposition 58 we have to find an α / A such that G^α [G [$R \pm \mathbb{Z}_p$. We will achieve this in three steps.

Step 1

Since $p > 9$, the Sylow p-subgroup of $Sym)9p+$is generated by 9 disjoint p-cycles. We may assume $\mathbb{Z}_p$ and $\mathbb{Z}_p$ lie in the same Sylow p-subgroup P of $Sym)9p+$. Then both R and R are subgroups of $N_{Sym(8p)})P+\{$ A so we may assume that R and R lie in the same Sylow 3-subgroup of $N_{Sym(8p)})P+\{$ A which is contained in a Sylow 3-subgroup of A.

Clearly, the Sylow p-subgroup P gives a partition $\mathcal{C} = \{B_1, B_2, \ldots, B_8\}$ of the vertices of , where $|B_i| = p$ for every $i = 2, \ldots, 9$ and $\mathcal{C}$ is P-invariant. It is easy to see that $\mathcal{C}$ is invariant under the action of R and L and hence $\langle \mathcal{C}, G \rangle \geq Sym(p) \wr Sym(9)$. Moreover, both G and $\mathcal{C}$ are regular. so L and R induce regular action on $\mathcal{C}$ which we denote by R_1 and R_2, respectively. The assumption that L and R lie in the same Sylow 3-subgroup of A implies that R_1 and R_2 are in the same Sylow 3-subgroup of $Sym(9)$.

Step 2

Let us assume that $R_1 \neq R_2$. We intend to find an element $\alpha \in A = N(P)$ such that $L^\alpha(\mathcal{C}) = R_2$.

We define a graph $_0$ on $\mathcal{C}$ such that B_m is adjacent to B_n if and only if $B_m \nsim B_n$. This is an undirected graph with vertex set $\mathcal{C}$ and both R_1 and R_2 are regular subgroups of $Aut(_0)$. It follows that $_0$ is a Cayley graph of R.

Observation 59. *Since $R_1 \leq Aut(_0)$ acts transitively on $\mathcal{C}$ we have that the order of each connected component of $_0$ divides 9.*

We can also define a coloured graph $_1$ on $\mathcal{C}$ by colouring the edges of the complete directed graph on 9 vertices. The vertex B_m is adjacent to the vertex B_n with the same coloured edge as $B_{m'}$ is adjacent to $B_{n'}$ in $_1$ if and only if there exists a graph isomorphism ϕ from the induced subgraph of on $B_m \cap B_n$ to the induced subgraph of on $B_{m'} \cap B_{n'}$ such that $\phi(B_m) = B_{m'}$ and $\phi(B_n) = B_{n'}$. The graph $_1$ is a coloured Cayley graph of R. Moreover, both R_1 and R_2 act regularly on $_1$. Using the fact that R has property $DCI^{(2)}$, it is clear that there exists an $\alpha^\infty \in \langle R_1, R_2 \rangle^{(2)} \leq Aut(_1)$ such that $R_2^{\alpha'} = R_1$. We would like to lift α^∞ to an automorphism α of such that $\alpha^{\mathcal{L}} = \alpha^\infty$.

1. Let us assume first that $_0$ is a connected graph.

Lemma 60. *(a)* $R \pm \mathbb{Z}_p \geq \mathbb{Z}_p \ \ Sym)9+$.

(b) If $R \pm \mathbb{Z}_p \geq \mathbb{Z}_p \ \ Sym)9+$, *then for every* $r \ / \ R$ *we have* $)r+ \ [\ \ id.$

Proof. (a) We first prove that $\mathbb{Z}_p \ [\ \mathbb{Z}_p$. Let x and y generate $\mathbb{Z}_p$ and $\mathbb{Z}_p$, respectively. Since x and y lie in the same Sylow p-subgroup and $\backslash B_1 \backslash \ [\ \ p$, we can assume that $x \backslash_{B_1} \ [\ \ y \backslash_{B_1}$. Using Lemma 57 (ii) we get that $x \backslash_{B_m} \ [\ \ y \backslash_{B_m}$ if there exists a path in $\ _0$ from B_1 to B_m. This shows that $x \ [\ \ y$ since $\ _0$ is connected. Moreover, $R \pm \mathbb{Z}_p \geq \mathbb{Z}_p \ \ Sym)9+$since the elements of $\mathbb{Z}_p$ and the elements of R commute.

(b) Let $A^{\infty} \ [\ \ A\{ \ )\mathbb{Z}_p \ \ Sym)9+($. We have already assumed that R and R lie in the same Sylow 3-subgroup of A^{∞}. Let r be an arbitrary element of R. For every $)a, u+ / \ R \pm \mathbb{Z}_p$ we have $r)a, u+ \ [\ \ )b, u0 \ t+$ for some $b \ / \ R$ and $t \ / \ \mathbb{Z}_p$, where t only depends on r and a since $r \geq \mathbb{Z}_p \ \ Sym)9+$. The permutation group G is transitive, hence there exist $n_1, n_2 \ / \ R$ such that $n_1)2, u+ \ [\ \ )a, u+$and $n_2)b, u \ 0 \ \ t+ \ [\ \ )2, u \ 0 \ \ t+$. The order of $n_2 r n_1$ is a power of 3 since n_2, r, n_1 lie in a Sylow 3-subgroup. Therefore $t \ [\ \ 1$ and hence $)r+ \ [\ \ id.$

□

Lemma 60 says that if $\ _0$ is connected, then $\rangle R, R| \geq \mathbb{Z}_p \ \ Sym)9+$and $)r+ \ [\ \ id$ for every $r \ / \ \rangle R, R|$. Therefore we can define $\alpha \ [\ \ \alpha \% d_{\mathcal{L}}$ to be an element of the wreath product $\mathbb{Z}_p \ \ Sym)9+$and clearly $\alpha \% d_{\mathcal{L}}$ is an element of A with $\alpha^{\mathcal{L}} \ [\ \ \alpha^{\infty}$.

2. Let us assume that $\ _0$ is the empty graph.

   Then Lemma 57(iii) shows that every permutation in $\rangle R_1, R_2|^{(2)}$ lifts to an automorphism of $\ .$

3. Let us assume that $\ _0$ is neither connected nor the empty graph.

Observation 61. *If* $R_1 \{ R_2$, *then* $\rangle R, R| \geq A$ *contains* β_1, β_2, β_3 *such that*

$$\beta_1^{\mathcal{L}} [ )B_1B_2 \dashv B_3B_4 +, \beta_2^{\mathcal{L}} [ )B_1B_2 \dashv B_5B_6 +, \beta_3^{\mathcal{L}} [ )B_1B_2 \dashv B_7B_8 +$$

Proof. Recall from Lemma 54 that $\rangle R, R|$ is the same group whether R is Q or $\mathbb{Z}_2^3$. By Lemma 53 the elements β_1, β_2, β_3 can be generated as products of an element of R and of R, as in the proof of Proposition 55, for the case $R [Q$.

□

Lemma 62. *We claim that* $B_{2k\ 1}$ *and* B_{2k} *are in the same connected component of* $_0$ *for* $k [2, 3, 4, 5$.

Proof. Since $_0$ is a Cayley graph and R_1 is transitive on the pairs of the form $)B_{2k\ 1}, B_{2k}+$it is enough to prove that B_1 and B_2 are in the same connected component of $_0$. If $B_1 \nsim B_2$, then B_1 is adjacent to B_2 in $_0$, so we can assume that $B_1 \subset B_2$. Since $_0$ is not the empty graph B_1 is adjacent to B_l for some $l > 3$, so $B_1 \nsim B_l$. By Observation 61 there exists β / A such that $\beta)B_1+[B_2$ and $\beta)B_l+[B_l$. This shows that $B_2 \nsim B_l$ and hence there is a path from B_1 to B_2 in $_0$. □

$_0$ is not connected, so the order of the connected components of cannot be bigger than 5. Since B_1 and B_2 are in the same connected component of $_0$ there exists a partition $H_1 \cap H_2 [\mathcal{C}$ such that $\backslash H_1 \backslash [\backslash H_2 \backslash [5$, $B_1, B_2 / H_1$ and no vertex in H_1 is adjacent to any vertex of H_2 in $_0$.

Lemma 63. *There exists* α / A *such that* $\alpha^{\mathcal{L}} [\alpha^{\infty}$.

Proof. Let us assume first that $H_1 = \{B_1, B_2, B_3, B_4\}$. Then we define α_1 to be equal to β_2 on H_1 and the identity on H_2, where β_2 is defined in Observation 61. Using Lemma 57 (ii) we get that α_1 is in $\langle R, R_1 \rangle^{(2)}$.

If $H_1 = \{B_1, B_2, B_5, B_6\}$ or $H_1 = \{B_1, B_2, B_7, B_8\}$, then we define α_2 by $\alpha_2|_{H_1} = \beta_1$ and $\alpha_2|_{H_2} = id$, where β_1 is defined in Observation 61. Lemma 57(ii) shows again that $\alpha_2 \in A$.

It is easy to see that $\alpha_1^{\mathcal{L}} = \alpha_2^{\mathcal{L}} = (B_1 B_2)^+$. Therefore A contains an element α such that $R_1^{\alpha^{\mathcal{B}}} = R_2$.

□

We conclude that we can assume that $R_1 = R_2$.

Step 3

Let us now assume that $R_1 = R_2$. We intend to find $\gamma \in A$ such that $R^\gamma = R$.

Let π and σ denote the generators of $\mathbb{Z}_p$ and $\mathbb{Z}_p$, respectively. We may assume that $\pi|_{B_1} = \sigma|_{B_1}$.

Lemma 64. *There exists $\gamma \in A$ such that $\sigma^\gamma = \pi$.*

Proof. Let us assume first that Γ_0 is connected. It is clear by Lemma 57 (ii) that $\sigma = \pi$. So, we may take $\gamma = 2$.

Let us assume that Γ_0 is not connected. In this case there are at least two connected components which we denote by $\mathcal{C}_1, \ldots, \mathcal{C}_n$. We may assume that $B_1 \in \mathcal{C}_1$. The permutations π and σ are elements of the base group of $\mathbb{Z}_p \wr Sym(9)^+$ and hence they can be considered as functions on $\mathcal{C}$. We may assume that $\pi(r, u)^+ = (r, u0)^+$ for every $(r, u)^+ \in R \pm \mathbb{Z}_p$. By Lemma 57 (ii), the function σ is constant on each equivalence class.

For every $2 \geq m \geq n$ there exists $r_m \in R$ such that $(r_m)\mathcal{C}_1^+ = \mathcal{C}_m$ and for every $r_m \in R$ there exists $\pi_m \in R$ such that $r_m^{\mathcal{L}} = \pi_m^{\mathcal{L}}$. Let γ be defined as

follows:

$$\gamma|_{\mathcal{C}_1} = id$$
$$\gamma|_{\mathcal{C}_m} = \rho_m \sigma_m^{-1} \text{ for } 3 \geq m \geq n.$$

Let $(b, v) \in B_e$ with $B_e \in \mathcal{C}_1$ and we denote $\rho_m^{-1}(b, v)$ by (a, u). Since ρ is constant on $\mathcal{C}_m$ we have $\rho^s(b, v) = (b, v + c_m s)$ for some c_m which only depends on $\mathcal{C}_m$. Thus $\rho_m(a, u + s) = (b, v + c_m s)$ since ρ and ρ_m commute and $\rho|_{B_e} = \sigma|_{B_e}$. Therefore we have

$$\gamma(b, w) = \rho_m(a, w) = \rho_m(a, u + w - u) = (b, v + c_m w - u)$$

for every $(b, w) \in B_e$. It is easy to verify that $\gamma^{-1}(b, w) = (b, \frac{w - v + uc_m}{c_m})$ for every $w \in \mathbb{Z}_p$ which gives

$$\gamma^{-1}\rho\gamma(b, w) = \gamma^{-1}\rho(b, wc_m + v - uc_m) = \gamma^{-1}(b, wc_m + v - uc_m + c_m) = (b, w + 2).$$

It follows that $\gamma^{-1}\rho\gamma = \sigma$.

It remains to show that $\gamma \in A$. Let y and z be two vertices of $R \times \mathbb{Z}_p$.

We denote by B_y and B_z the elements of $\mathcal{C}$ containing y and z, respectively. If B_y and B_z are in the same connected component of Γ_0, then either γ is defined on B_y and B_z by $\rho_m \sigma_m^{-1}$ which is the element of the group $\langle G, G' \rangle \leq A$ or $\gamma(y) = y$ and $\gamma(z) = z$.

If B_y and B_z are not in the same connected component, then $B_y \subset B_z$. The definition of γ shows that $\gamma^{\mathcal{L}} = id$. Using Lemma 57 (iii) we get that $\gamma|_{B_y \cap B_z}$ is an automorphism of the induced subgraph of Γ on the set $B_y \cap B_z$, which proves that $\gamma \in A$, finishing the proof of Lemma 64.

□

Using Lemma 64 we may assume that $\rho = \sigma$. Since ρ and ρ' commute we have $(R \times \mathbb{Z}_p \geq \mathbb{Z}_p \wr Sym(3))$. Now we can apply Lemma 60 which gives $(\rho')^6 = id$ for every $\rho' \in R$. This proves that $R = R_1$ since $R_1 = R_2$. Therefore $G = G'$, finishing the proof of Proposition 58. □

It is straightforward to check that the proof of Proposition 58 uses $p > 9$ only in the first step of the argument. We can formulate this fact in Proposition 65.

Proposition 65. *Let be a Cayley graph of* G [$Q \pm \mathbb{Z}_p$ *or* G [$\mathbb{Z}_2^3 \pm \mathbb{Z}_p$, *where* p *is an odd prime and let* G [$Q \pm \mathbb{Z}_p$ *and* G [$\mathbb{Z}_2^3 \pm \mathbb{Z}_p$ *be regular subgroups of* Aut) + *isomorphic to* G. *Let us assume that there exists a* $\langle \mathcal{G}, G|$*-invariant partition* $\mathcal{C}$ [$\}B_1, B_2, \ldots, B_8\langle$ *of* V) +, *where* $\setminus B_i \setminus$[p *for every* i [$\}2, \ldots, 9\langle$. *In addition, we assume that* $\mathbb{Z}_p$ *is a subgroup of the base group of* $\mathbb{Z}_p$ $Sym)\mathcal{C}$+. *Then there is an automorphism* α *of the graph such that* $\mathcal{G}^\alpha$ [G.

3.1.4 Main result for p [6 and 8

In this section we will prove that $Q \pm \mathbb{Z}_5$, $Q \pm \mathbb{Z}_7$, $\mathbb{Z}_2^3 \pm \mathbb{Z}_5$ and $\mathbb{Z}_2^3 \pm \mathbb{Z}_7$ are CI-groups.

The whole section is based on the paper [L,L,P], so we will only modify the proof of Lemma 5.4 of [L,L,P].

Proposition 66. *Every Cayley graph of* $Q \pm \mathbb{Z}_5$, $Q \pm \mathbb{Z}_7$, $\mathbb{Z}_2^3 \pm \mathbb{Z}_5$ *and* $\mathbb{Z}_2^3 \pm \mathbb{Z}_7$ *is a CI-graph.*

We let R denote either Q or $\mathbb{Z}_2^3$, and let p [6 or 8. Let be a Cayley graph of $R \pm \mathbb{Z}_p$ and let A [Aut) + We denote by P a Sylow p-subgroup of A. Let us assume that A contains two copies of regular subgroups which we denote by $\mathcal{G}$ [$R \pm \mathbb{Z}_p$ and G [$R \pm \mathbb{Z}_p$. We can assume that is neither the empty nor the complete graph and both $\mathbb{Z}_p$ and $\mathbb{Z}_p$ are contained in P.

If the order of every orbit of P on V) +is p, then it is clear from Proposition 65 that is a CI-graph. Therefore P has an orbit $\Pi \to G$ such that $\setminus \Pi \setminus$ [p^2 since $p^3 > \setminus G \setminus$ The remaining orbits of P have order p since $3p^2 > 9p$.

It was proved in [L,L,P, Lemma 5.4] that the action of A on the vertices of the graph cannot be primitive so there is a nontrivial A-invariant partition $\mathcal{C} = \{B_0, B_1, \ldots, B_{t-1}\}$ of V) $+[$ G. The elements of the partition $\mathcal{C}$ have the same cardinality since the action of A is transitive on $\mathcal{C}$ so $|B_i| \geq 5p < p^2$ for every $i = 1, 2, \ldots, t-2$. The partition $\mathcal{C}$ is P-invariant so P acts on $\mathcal{C}$. Since P is a p-group, the order of every orbit of P is a power of p.

Let $\mathscr{C} = \{C_0, C_1, \ldots, C_{s-1}\}$ be an orbit of P on $\mathcal{C}$ such that $\Pi \leq \cap_{i=0}^{s-1} C_i$. We may assume that $B_i = C_i$ for $i = 1, 2, \ldots, s-2$. It is clear that s is a power of p. If $s \sim p^2$, then $|\cap_{i=0}^{s-1} C_i| \sim 3p^2 > 9p$ which is a contradiction. Since $|C_0| = |B_0| < p^2$, we cannot have $s = 2$. It follows that $2 < s < p^2$ which implies $s = p$.

For every $i < s$ and every $x \in P$ the following equalities hold for some $j < s$

$$)B_i \{ \Pi+^x = B_i^x \{ \Pi^x = B_j \{ \Pi.$$

This implies that

$$|B_0 \{ \Pi| = |B_i \{ \Pi|$$

for every $1 \geq i < s$. Therefore

$$p^2 = |\Pi| = |(\cap_{i=0}^{s-1})B_i \{ \Pi+| = s|B_0 \{ \Pi| = p|B_0 \{ \Pi|.$$

This gives $|B_0 \{ \Pi| = p$ so $|B_0|$ can only be p or 9 since $|B_0| = 9p$ and both $|B_0|$ and $t \sim s$ are at least p.

If $|B_0| = p$, then Π is the union of p elements of the A-invariant partition $\mathcal{C}$ and every orbit Π^∞ of P is an element of the partition $\mathcal{C}$ if $\Pi^\infty \cap \Pi$. For every orbit $\Pi^\infty \cap \Pi$ of P and for every $y \in \mathbb{Z}_p \cap \mathbb{Z}_p$ we have $y)\Pi^\infty+ = \Pi^\infty$. In particular, $y)B_7+ = B_7$. By Proposition 65 we may assume that there exists an element x^∞ in $\mathbb{Z}_p \cap \mathbb{Z}_p$ such that $x^\infty)B_0+ = B_j$ for some $j \in 1, 8$ and clearly $x^\infty)B_7+ = B_7$. Since both G and G are regular there exists $a \in C_A)x^\infty+$ such that $a)B_0+ = B_7$. Since a and x^∞ commute we have $a)B_j+ = B_7$, which contradicts the fact that $a)B_0+ = B_7$.

We must therefore have $|B_0| \geq 9$. Let x and y generate $\mathbb{Z}_p$ and $\mathbb{Z}_p$, respectively. Since G and G are regular we have that neither $x^{\mathcal{L}}$ nor $y^{\mathcal{L}}$ is the identity, so both x and y are regular on C. Since both $x^{\mathcal{L}}$ and $y^{\mathcal{L}}$ generate a transitive subgroup in $Sym(C)$ of prime order $p > 3$, and for every $r \in R \cap R$ the permutation $r^{\mathcal{L}}$ commutes with one of these two elements, we have $r^{\mathcal{L}} = id$. Since x and y are in the same Sylow p-subgroup of P we may assume that $x(B_i) = B_{i+1}$ and $y(B_i) = B_{i+1}$ for $i = 1, 2, \ldots, p-2$, where the indices are taken modulo p. By Proposition 65 we may also assume that $x \neq y$.

For every m there exists an l such that the action of $x^l y^{-l}$ is nontrivial on B_m since $x \neq y$. Therefore $A_{B_m}|_{B_m}$ contains a regular subgroup and a cycle of length p such that $p > \frac{|B_0|}{2}$. A theorem of Jordan on primitive permutation groups, which can be found in [Wie, Theorem 13.1], says that such a permutation group is 3-transitive and hence the induced subgraph of on B_m is either the complete or the empty graph for every m.

Lemma 67. *$B_m \subset B_n$ for $1 \geq m < n \geq p-2$.*

Proof. There exists a unique element $g \in \mathbb{Z}_p \leq P$ such that $g(B_m) = B_n$. We also have a unique element $h \in \mathbb{Z}_p \leq P$ with $g^{\mathcal{L}} = h^{\mathcal{L}}$. Since $\mathbb{Z}_p$ is a cyclic group of prime order and $x \neq y$ we have $g = h$. Moreover, we may also assume that $g|_{B_m} = h|_{B_m}$ since $g = h$ and the induced subgraphs of on $B_{m+c} \cap B_{n+c}$ are all isomorphic, where both $m-c$ and $n-c$ are taken modulo p.

Clearly, $g = hgh^{-1}$ is a cycle of length p on B_n. The vertices of $V(\Gamma) \setminus \Pi$ are contained in P-orbits of order p that contain the orbit of the vertex under x, so meet each B_i in a single vertex, so g fixes every vertex of the set $B_m \cap B_n \subset \Pi$ since $g^{\mathcal{L}} = id$.

Let $u \in B_m \subset \Pi$. It is enough to show that if u is adjacent to some $v \in B_n$, then u is adjacent to every vertex of B_n. We will prove that A is transitive on the following pairs: $\{(u, w) \mid w \in B_n\}$.

A is transitive on $\{u, w\} \cup w \in B_n \setminus supp(g)$ $\{u, w\} \cup w \in B_n \setminus \Pi$ since g fixes u. Therefore we may assume that $v \in B_n \setminus \Pi$ and we only have to find an element $a \in A$ such that $a(u) = u$ and $a(v) \in B_n \setminus \Pi$.

The restriction of g to B_n is a cycle of length p so g does not commute with $r|_{B_n}$, where r is an involution of R. Since r and g commute we have that there is a $u^\infty \in B_m$ such that $(rg)u^\infty = g(r)u^\infty$. Since the action of R is transitive on B_m there exists $a \in R$ such that $a(u) = u^\infty$. Then

$$(ra)(gu) = (rga)u = (rg)u^\infty = g(r)u^\infty = g(ra)u$$

so there exists $a^\infty \in A$ such that

$$a^\infty(gu) = ga^\infty u \tag{3.1}$$

Let us suppose that $v = gu$. Notice that gu is in a P-orbit of order p, so $gu \in \Pi$. Then the inequality (3.1) gives $a^\infty v = ga^\infty u$. Since $R|_{B_m}$ is regular on B_m there exists $a \in R$ such that $a(u) = a^\infty u$ and since a and g commute we have $a(v) = ag(u) = ga(u) = ga^\infty u$. Therefore $a(v) = a^\infty v$ and hence $a^{-1}a^\infty$ fixes u and $a^{-1}a^\infty v = v$ so we may assume that $v \neq gu$.

If $p = 8$, then $v \in B_n \setminus \Pi$.

Let us assume that $p = 6$. We claim that there exists $t \in R$ such that $t(u) \in B_m \cap \Pi = B_m \cap supp(g)$ while $t(v) \in B_n \setminus \Pi = B_n \setminus supp(g)$. It is clear that $g(B_m \setminus supp(g)) = B_n \setminus supp(g)$ and g commutes with each element of R. Therefore it is enough to show that if $u, v \in B_m \cap supp(g)$ with $u \neq v$, then there exists $t \in R$ such that $t(u) \in B_m \cap supp(g)$ and $t(v) \in B_m \setminus supp(g)$. This can easily be seen from the fact that $ide \setminus R \setminus 6 = 2$.

The permutations $t^{-1}g^l t$ fix the vertex u for $1 \geq l \geq 5$ and $t^{-1}g^{l_1}t(v) = t^{-1}g^{l_2}t(v)$ if $l_1 \equiv l_2 \pmod p$. At least one of the the four elements $t^{-1}gt$, $t^{-1}g^2t$, $t^{-1}g^3t$, $t^{-1}g^4t$ of A fixes u and maps v to an element of $B_n \setminus supp(g)$ $B_n \setminus \Pi$ since $|B_n \cap supp(g)| \setminus 4$, finishing the proof of the fact that $B_m \subset B_n$ for $1 \geq m < n \geq 8$. □

Every permutation of V) +which fixes B_m setwise for every m is an automorphism of so there is an a / A such that v^a [x. Applying Proposition 65 we get that there exists α / A such that $)R \pm \mathbb{Z}_p($ [$R \pm \mathbb{Z}_p$, finishing the proof of Proposition 66.

3.2 $\mathbb{Z}_p^3 \pm \mathbb{Z}_q$ is a DCI-group if $q > p^3$

In this section, for every prime $p > 4$ and for every prime $q > p^3$ we prove that $\mathbb{Z}_q \pm \mathbb{Z}_p^3$ is a DCI-group.

Most of the results we enumerate here have already been collected in Chapter 2 since we prove here that the direct product of an elementary abelian group ($\mathbb{Z}_p^3$) with a cyclic group ($\mathbb{Z}_q$) is a DCI-group. The cyclic group of order p, which is a DCI-group, can also be considered as an elementary abelian p-group of rank 2. The best general result was given by Hirasaka and Muzychuk [H,M] who proved that $\mathbb{Z}_p^4$ is a DCI-group for every prime p. For our investigation the following weaker results are also important. Dobson [Dob1] proved that $\mathbb{Z}_p^3$ is a CI-group for every prime p and Alspach and Nowitz showed [A,N] that $\mathbb{Z}_p^3$ is a CI-group with respect to Cayley color digraphs.

A new family of CI-groups was found by Kovács and Muzychuk [K,M], namely $\mathbb{Z}_p^2 \pm \mathbb{Z}_q$ is a CI-group for every prime p and q. Here we advance further.

Theorem 68. *For every prime p and every prime $q > p^3$ the group $\mathbb{Z}_p^3 \pm \mathbb{Z}_q$ is a DCI-group.*

Proof. We mimic the proof of Theorem 50. We use the same three steps but in different order.

Our technique is based on Lemma 8 again, so we fix a Cayley graph [$Cay)\mathbb{Z}_p^3 \pm \mathbb{Z}_q, S+$ Let A [Aut) +and G [$\mathbb{Z}_p^3 \pm \mathbb{Z}_q$ be another regular

subgroup of A isomorphic to $\mathbb{Z}_p^3 \pm \mathbb{Z}_q$. We have to find an α / A such that $\mathbb{G}^\alpha$ [$\mathbb{H}$ [$\mathbb{Z}_p^3 \pm \mathbb{Z}_q$.

Step 1

We may assume $\mathbb{Z}_q$ and $\mathbb{Z}_q$ lie in the same Sylow q-subgroup Q of $Sym)p^3q+$ Then both $\mathbb{Z}_p^3$ and $\mathbb{Z}_p^3$ are subgroups of $N_{Sym(p^3q)})Q+\{$ A so we may assume that $\mathbb{Z}_p^3$ and $\mathbb{Z}_p^3$ lie in the same Sylow p-subgroup of $N_{Sym(p^3q)})Q+\{$ A which is contained in a Sylow p-subgroup P of A.

The Sylow q-subgroup Q gives a partition $\mathcal{C}$ [$\}B_1, B_2, \ldots, B_{p^3}\langle$ of the vertices of , where $\backslash B_i \backslash$ [q for i [$2, \ldots, p^3$. It is easy to see that $\mathcal{C}$ is invariant under the action of $\mathbb{Z}_p^3$ and $\mathbb{Z}_p^3$ and hence $\rangle\mathbb{H}, \mathbb{G}| \geq Sym)q+Sym)p^3+$ Moreover, both $\mathbb{G}$ and $\mathbb{H}$ are regular so $\mathbb{Z}_p^3$ and $\mathbb{Z}_p^3$ induce regular action on $\mathcal{C}$ which we denote by H_1 and H_2, respectively. The assumption that $\mathbb{Z}_p^3$ and $\mathbb{Z}_p^3$ lie in the same Sylow p-subgroup of A implies that H_1 and H_2 are in the same Sylow p-subgroup of $Sym)p^3+$ what we denote by P_1.

Now, we reverse the order of the two remaining steps.

Step 2

Let us assume that $\mathbb{Z}_q$ { $\mathbb{Z}_q$ which is generated by p^3 disjoint q-cycles. We intend to find an element α / A such that $\mathbb{Z}_q^\alpha$ [$\mathbb{Z}_q$.

We define a graph $_0$ on $\mathcal{C}$ in the same way as in Section 3.1.3, which is an undirected Cayley graph of $\mathbb{Z}_p^3$.

We can define a colored graph $_1$ on $\mathcal{C}$ in the same way as in the previous case, which is again a Cayley color graph of $\mathbb{Z}_p^3$ and both H_1 and H_2 act regularly on $_1$.

We first prove a technical lemma.

Lemma 69. *Let us assume that H is a regular abelian subgroup of $Sym)p^n+$ and let $P \sim H$ be a Sylow p-subgroup of $Sym)p^n+$ Then H contains $Z)P+$*

Proof. It is well known that the center of P is a cyclic p-group. Let z be a generator of $Z)P+$ Then $\rangle H, z|$ is a transitive abelian group. Hence $\rangle H, z|$ is regular. Since H is also regular, we have that z is an element of H.

□

We also prove the following two lemmas what we will use several times in this step.

Lemma 70. *Let us assume that $C_1^\infty, C_2^\infty, \dots C_k^\infty$ are the set of the connected components of $V)\ _0+$ and let $C_i\ [\ \cap C_i^\infty \to V)\ +$ for every $i\ [\ 2, \dots, k$. Let α be a permutation on the vertex set $V)\ +$ such that for $2 \geq i \geq k$ the restriction $\alpha\backslash_{C_i}\ [\ \eta_i\backslash_{C_i}$ for some $\eta_i\ /\ Aut)\ +$ and $\alpha^{V(\Gamma_0)}$ is an automorphism of $\ _0$. Then α is an automorphism of $\ $.*

Proof. Let x and y be points in $V)\ +$ We have to prove that x is adjacent to y if and only if $\alpha)x+$is adjacent to $\alpha)y+$ This holds if x and y are in the same C_i for some $2 \geq i \geq k$ since $\alpha\backslash_{C_i}$ is defined by an automorphism of $\ $ on C_i. If $x\ /\ B_m$ and $y\ /\ B_n$, where $B_m \subset B_n$ and x is adjacent to y, then every element of B_m is adjacent to every element of B_n. Since $\alpha^{V(\Gamma_0)}\ /\ Aut)\ _0+$ the same holds for $\alpha)B_m+$and $\alpha)B_n+$and hence $\alpha)x+$is adjacent to $\alpha)y+$ Similar argument shows that if $x\ /\ B_m$ and $y\ /\ B_n$, where $B_m \subset B_n$ and x is not adjacent to y, then $\alpha)x+$is not adjacent to $\alpha)y+$

□

Lemma 71. *(i) Let A and B be two disjoint subsets of cardinality q of $V)\ +$ We write $A\ [\ \})a, x+\backslash x\ /\ \mathbb{Z}_q+\{$ and $B\ [\ \})b, x+\backslash x\ /\ \mathbb{Z}_q\langle$. Let us assume that g and $(g$ are automorphisms of the graph $\ $ with $g)a, x+[\ (g)a, x+[\ \ )a, x\,0\ 2+$, $g)b, x+[\ \ )b, x\,0\ 2+$and $(g)b, x+[\ \ )b, x\,0\ d+$ for some $1\ [\ d\ /\ \mathbb{Z}_q$ for all $x\ /\ \mathbb{Z}_q$. Furthermore, let us assume that α and $(\psi$ are automorphisms of the graph $\ $ with $\alpha)A+[\ (\psi)A+[\ B$ and α and $(\psi$ commute with g and $(g$, respectively. Then for $\alpha\ [\ (\psi\alpha^{\ 1}$ we have $(g^\alpha\backslash_B\ [\ g\backslash_B$.*

(ii) Let us assume that C [}$)c, x+\ x$ / $\mathbb{Z}_q$(*is a subset of* V) +*with* A { B [A { C [B. *We also assume that* g)$c, x+$[ ]c, x 0 $2+$*and* $(g)c, x+$[ ]c, x 0 $d+$*for every* x / $\mathbb{Z}_q$. *Let us assume that* $(\psi$ / $Aut)$ + *with* $(\psi)A+$[C *and we also assume that* $(g$ *and* $(\psi$ *commute. Then for* β [$(\psi\alpha$ ^{1} *we have* $(g^{\beta}\backslash_B$ [$g\backslash_B$.

Proof. (i) Let us assume that α)$a, 1+$[ ]$b, b_0+$and $(\psi)a, 1+$[ ]$b, b_0^{\infty}+$for some b_0, b_0^{∞} / $\mathbb{Z}_q$. Using that α and g commute we get that α)$a, x+$[ )b, b_0 0 $x+$for every x / $\mathbb{Z}_q$ and similarly we have $(\psi)a, x+$[ ]b, b_0^{∞}0 $dx+$ Thus

$$\alpha)b, x+[\ \alpha)b, b_0\ 0\ )x\quad b_0++[\ (\psi)a, x\quad b_0+[\ )b, b_0^{\infty}0\ )x\quad b_0+d+$$
$$[\ )b,)b_0^{\infty}\quad db_0+0\ dx+.$$

It is easy to derive that α $^{1})b, x+[$ $\Big)b, \frac{x\ (b_0'\ db_0)}{d}\Big($. Using the previous two equations we get

$$\alpha\ ^{1}(g\alpha\backslash_B)b, x+[\ \alpha\ ^{1}(g\ )b,)b_0^{\infty}\quad db_0+0\ dx+$$
$$[\ \alpha\ ^{1})b,)b_0^{\infty}\quad db_0+0\ dx\ 0\ d+[\ \Big)b, \frac{)b_0^{\infty}\quad db_0+0\ dx\ 0\ d\quad)b_0^{\infty}\quad db_0+}{d}\Big\{$$
$$[\ )b, x\ 0\ 2+.$$

(ii) Let us assume that $(\psi)a, 1+$[ ]$c, c_0+$for some c_0 / $\mathbb{Z}_q$. Then $(\psi)a, x+$[ )c, c_0 0 $dx+$for all x / $\mathbb{Z}_q$ Thus

$$\begin{aligned}\beta)b, x+[\ (\psi\alpha\ ^{1})b, b_0\ 0\ )x\quad b_0++\\ [\ (\psi\ )a, x\quad b_0+[\ )c, c_0\ 0\ d)x\quad b_0++\end{aligned}\tag{3.2}$$

and hence β $^{1})c, x+$[ ]$b, \frac{x\ \ c_0+db_0}{d}+$ Using equation 3.2 we have

$$\beta\ ^{1}(g\beta\ )b, x+[\ \beta\ ^{1}(g\ )c, c_0\ 0\ d)x\quad b_0++[\ \beta\ ^{1})c, c_0\ 0\ d)x\quad b_0+0\ d+$$
$$[\ \Big)b, \frac{c_0\ 0\ d)x\quad b_0+0\ d\quad c_0\ 0\ db_0}{d}\Big\{\ [\ )b, x\ 0\ 2+.$$

□

The vertices of the graph Γ_0 and Γ_1 can be identified with the elements of $\mathbb{Z}_p^3$ and we may assume that the action of an element r of the Sylow p-subgroup P_1 is the following:

$$r)a,b,c+[\ )a\,0\ x,b\,0\ s_a,c\,0\ t_{a,b}+$$

where $s_a\ /\ \mathbb{Z}_p$ only depends on a and $t_{a,b}\ /\ \mathbb{Z}_p$ depends on a and b.

Let g and $\bar{g}$ denote the generator of $\mathbb{Z}_q$ and $\bar{\mathbb{Z}}_q$, respectively. We may assume that $g\backslash_{B_1}\ [\ \bar{g}\backslash_{B_1}$.

1. Let us assume first that Γ_0 is a connected graph.

   Using Lemma 57 (ii) we get that $g\backslash_{B_i}\ [\ \bar{g}\backslash_{B_j}$ if there exists a path in Γ_0 from B_i to B_j. This shows that $g\ [\ \bar{g}$ since Γ_0 is connected in this case.

2. Let us assume that Γ_0 is the empty graph.

   For every $B_m\ /\ \mathcal{C}$ there exist $a_m\ /\ \mathbb{Z}_p^3$ and $r_m\ /\ \bar{\mathbb{Z}}_p^3$ such that $a_m)B_1+[\ r_m)B_1+[\ B_m$.

   Let α be defined as follows

   $$\alpha\backslash_{B_1}\ [\ id$$
   $$\alpha\backslash_{B_m}\ [\ r_m a_m^{-1}\ \text{ for }\ 3 \geq m \geq p^3.$$

   It is easy to see that $\alpha^{\mathcal{L}}\ [\ id$ so using Lemma 70 we get that α is an automorphism of $\ $. Using Lemma 71 (i) we get that $\bar{g}^{\alpha}\ [\ g$.

3. Let us assume that the size of the connected components of Γ_0 is p.

   Let $C_1^{\infty}, C_2^{\infty}, \ldots, C_{p^2}^{\infty}$ denote the connected components of Γ_0 and for $2 \geq m \geq p^2$ let $C_m\ [\ \cap C_m^{\infty}$. For $C_2, \ldots, C_{p^2}$ we choose an element a_m of $\mathbb{Z}_p^3$ such that $a_m)C_1+[\ C_m$. We may assume that $B_1 \to C_1$. Since H_2 is regular on Γ_0, for every $3 \geq m \geq p^2$ there exists μ_m such that

$(u_m)B_1+[\ \ a_m)B_1+$ For $3 \geq m \geq p^2$ let $u_m\ [\ \ (u_m a_m^{\ 1}$. Now we define the following permutation:

$$\alpha_1\backslash_{C_1}\ [\ \ id$$
$$\alpha_1\backslash_{C_m}\ [\ \ u_m \text{ for } 3 \geq m \geq p^2.$$

Clearly, for $3 \geq m \geq p^2$ we have $u_m)B_j+[\ \ B_j$ for at least one $B_j \rightarrow C_m$. Since H_1 and H_2 are in the same Sylow p-subgroup of $Sym)p^3+$ the order of $u_m^{\mathcal{L}}$ is a power of p. We also have that C_m is the union of p elements of $\mathcal{C}$ for $2 \geq m \geq p^2$ hence $\alpha_1^{\mathcal{L}}\ [\ \ id$. We also have that $\alpha_1\backslash_{C_m}$ is the restriction of an automorphism of the graph for $m\ [\ \ 2, \ldots p$. Therefore by Lemma 70 α_1 is an automorphism of the graph .

Finally, Lemma 71 (ii) gives $(g^{\alpha_1}\ [\ \ g$.

4. Let us assume that the size of the connected components of $_0$ is p^2 and we denote them by $D_0^\infty, D_1^\infty, \ldots, D_{p\ 1}^\infty$. Let D_m denote the set of vertices of which belongs to the elements of D_m^∞ for $1 \geq m \geq p\ \ 2$.

Using Lemma 69 we get that $H_1\ \{\ H_2\ \{\ \ \}2\langle$. Let z be an element of order p of $H_1\ \{\ H_2$ and we denote by z_1 and z_2 the element of $\mathbb{Z}_p^3$ and $(\mathbb{Z}_p^3$ such that $z_1^{\mathcal{L}}\ [\ \ z_2^{\mathcal{L}}\ [\ \ z$, respectively. Then $)z_2^{\ i} z_1^i+^{\mathcal{L}}\ [\ \ id$ for $i\ [\ \ 2, \ldots, p\ \ 2$.

Let us assume first that $z_1)D_0+\{\ \ D_0$. We may assume that $z_1^i)D_0+[\ \ D_i$ for $i\ [\ \ 1, 2, \ldots, p\ \ 2$. We define α_2 in the following way:

$$\alpha_2\backslash_{D_0}\ [\ \ id$$
$$\alpha_2\backslash_{D_i}\ [\ \ z_2^i z_1^{\ i} \text{ for } 2 \geq i \geq p\ \ 2.$$

Since $z_1^{\mathcal{L}}\ [\ \ z_2^{\mathcal{L}}\ [\ \ z$ we have $\alpha_2^{\mathcal{L}}\ [\ \ id$. Using Lemma 70 again we get that $\alpha_2\ /\ Aut)\ +$and Lemma 71 gives $(g^{\alpha_2}\ [\ \ g$.

Therefore we may assume that $z_1)D_0+[\ \ D_0$. In this case the orbits of z give a $\rangle H_1, H_2|$-invariant partition $\mathcal{L}\ [\ \ \}E_{a,b}\ \backslash a, b\ /\ \mathbb{Z}_p\langle$ of $\mathcal{C}$.

Using that the elements of $\mathcal{C}$ [V) $_0$+can be identified with elements of $\mathbb{Z}_p^3$ we may assume that $E_{a,b}$ has the following form for every pair)a, b+/ $\mathbb{Z}_p^2$:

$$E_{a,b} \text{ [}\})a, b, c+/ \mathbb{Z}_p^3 \setminus c \text{ / } \mathbb{Z}_p\langle.$$

We may also assume that D_a^∞[$\cap_{b/\mathbb{Z}_p} E_{a,b}$ for all a / $\mathbb{Z}_p$.

Since H_1 acts regularly on $_0$, there exists h_1 / H_1 such that h_1)$E_{0,0}$+[$E_{0,1}$. Since H_2 is also regular, there exists h_2 / H_2 such that h_2)$E_{0,0}$+[h_1)$E_{0,0}$+ Since the order of h_1 and h_2 are p and h_1)D_0^∞+[h_2)D_0^∞+[D_0^∞ we have that h_1)D_i^∞+[h_2)D_i^∞+[$D_i^\infty$for i [$1, \ldots, p$ 2.

Since H_1 and H_2 are contained in the same Sylow p-subgroup we may assume that z, h_1 and h_2 act in the following way on $\mathbb{Z}_p^3$ which was identified with $\mathcal{C}$.

$$\begin{aligned} z)a, b, c+[\ )a, b, c\,0\ 2+ \\ h_1)a, b, c+[\ )a, b\,0\ 2, c+ \\ h_2)a, b, c+[\ )a, b\,0\ s_a, c\,0\ t_{a,b}+, \end{aligned}$$

where s_a and $t_{a,b}$ are in $\mathbb{Z}_p$. The assumption that h_1)$E_{0,0}$+[h_2)$E_{0,0}$+[$E_{0,1}$ gives that s_0 [2.

We claim that s_a [2 for $2 \geq a \geq p$ 2. Since H_2 is regular on $_0$ there exists k_2 / H_2 such that k_2)1, 1, 1+[ )a, 1, 1+ Since h_2 and k_2 commute we have that k_2)1, i, 1+[ )$a, s_a i, w_i$+for some w_i / $\mathbb{Z}_p$. If s_a { 2, then such an element cannot be in the Sylow p-subgroup P_1.

Therefore h_2)a, b, c+[ )a, b 0 2, c 0 $t_{a,b}$+for all)a, b, c+ / $\mathbb{Z}_p^3$, where $t_{a,b}$ / $\mathbb{Z}_p$ only depends on a and b.

Note that $E_{a,b}$ is a p-element subset of V) $_0$+for all a, b / $\mathbb{Z}_p$ so we may define the relation $\subset$ on subsets of vertices of $_0$ of the form $E_{a,b}$.

Lemma 72. *Let a [a^{∞}be elements of $\mathbb{Z}_p$ and we fix two more elements b and $b^{\infty}$of $\mathbb{Z}_p$. Then either $E_{a,b} \subset E_{a',b'}$ or $t_{a,b+n}$ [$t_{a',b'+n}$ for all n / $\mathbb{Z}_p$.*

Proof. Since s_a [2 for a / $\mathbb{Z}_p$ we have that for all m / $\mathbb{Z}_p$ the permutation $h_2^m h_1{}^m$ fixes $E_{a,b}$ and $E_{a',b'}$. Moreover,

$$\begin{aligned} h_2^m h_1{}^m)a,b,c+[\ )a,b,c\,0 \bigcup_{i=1}^{m} t_{a,b}{}_i+\text{and} \\ h_2^m h_1{}^m)a^{\infty},b^{\infty},c+[\ )a^{\infty},b^{\infty},c\,0 \bigcup_{i=1}^{m} t_{a',b'}{}_i+ \end{aligned} \tag{3.3}$$

One can see using Lemma 57 (ii) that if $\prod_{i=1}^{m} t_{a,b}{}_i$ { $\prod_{i=1}^{m} t_{a',b'}{}_i$ for some m / $\mathbb{Z}_p$, then $E_{a,b} \subset E_{a',b'}$. Using that p is a prime we obtain that if $\prod_{i=1}^{m} t_{a,b}{}_i$ [$\prod_{i=1}^{m} t_{a',b'}{}_i$ for all m / $\mathbb{Z}_p$, then $t_{a,b+n}$ [$t_{a',b'+n}$ for n / $\mathbb{Z}_p$.

□

For each a / $\mathbb{Z}_p$ we define the following function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$:

$$t_a)b+\ddagger t_{a,b}.$$

Lemma 73. *Let us assume that for some $a, a^{\infty}, b, b^{\infty}$/ $\mathbb{Z}_p$ we have $t_a)b0$ $n+[\ t_{a'})b^{\infty}0\ n+$for all n / $\mathbb{Z}_p$. We denote by k_2 the unique element of H_2 which maps $)a,b,1+$to $)a^{\infty},b^{\infty},1+$ Then $k_2)a,b\,0\ d,e+[\ )a^{\infty},b^{\infty}0\ d,e+$ for all d,e / $\mathbb{Z}_p$.*

Proof. Since k_2 and z commute we have $k_2)a,b,m+[\ )a^{\infty},b^{\infty},m+$for all m / $\mathbb{Z}_p$. We also have that k_2 and h_2 commute. Using the condition that $t_a)b\,0\ n+[\ t_{a'})b^{\infty}0\ n+$for all n / $\mathbb{Z}_p$ we obtain $k_2)a,b\,0\ d,e+[$ $)a^{\infty},b^{\infty}0\ d,e+$for all d,e / $\mathbb{Z}_p$.

□

Corollary 74. *If the conditions of Lemma 73 hold and k_1 is the unique element of H_1 such that $k_1)a, b, 1+[\ )a^{\infty}, b^{\infty}, 1+$, then $k_1\backslash_{E_{a,b}} [\ k_2\backslash_{E_{a,b}}$.*

We define an equivalence relation on the set $\}D_0^{\infty}, D_1^{\infty}, \ldots, D_{p\ 1}^{\infty}\langle$. We write $D_a^{\infty} \subseteq D_{a'}^{\infty}$ if and only if there exist b and b^{∞} in $\mathbb{Z}_p$ such that $t_{a,b+n} [\ t_{a',b'+n}$ for all $n\ /\ \mathbb{Z}_p$. We also write $D_a^{\infty} \subseteq D_{a'}^{\infty}$ if $D_a^{\infty} \subseteq D_{a'}^{\infty}$ does not hold.

Now we can choose a vertex $)a, b_a, 1+$ in every D_a^{∞} such that if $D_a^{\infty} \subseteq D_{a'}^{\infty}$, then $t_{a,b_a+n} [\ t_{a',b_{a'}+n}$ for all $n\ /\ \mathbb{Z}_p$. For every $2 \geq a \geq p\quad 2$ there exist $\mathfrak{a}_a\ /\ \mathbb{Z}_p^3$ and $(\psi_a\ /\ \mathbb{Z}_p^3$ such that $\mathfrak{a}_a^{\mathcal{L}})1, b_0, 1+[\ (\psi_a^{\mathcal{L}})1, b_0, 1+[\ )a, b_a, 1+$ since both H_1 and H_2 are regular on $\mathcal{C}$.

Now we can define the following permutation:

$$\alpha_3\backslash_{D_0} [\ id$$
$$\alpha_3\backslash_{D_a} [\ (\psi_a\mathfrak{a}_a{}^{1} \quad \text{for } 2 \geq a \geq p\quad 2.$$

Lemma 75. *α_3 is an automorphism of .*

Proof. We first prove that $\alpha_3^{\mathcal{L}}$ is an automorphism of the graph $_1$. If $B_i \cap B_j$ is contained in D_a^{∞} for some $a\ /\ \mathbb{Z}_p$, then α_3 is defined by the restriction of an automorphism of . Therefore we only have to investigate those pairs $)B_i, B_j+$ which are not in the same set D_a^{∞} for any $a\ /\ \mathbb{Z}_p$.

Let us assume that $B_i\ /\ E_{a,b}$ and $B_j\ /\ E_{a',b'}$. By the definition of α_3, for every $d\ /\ \mathbb{Z}_p$ at least one $E_{d,e}$ is fixed by $\alpha_3^{\mathcal{L}}$. Therefore $\alpha_3^{\mathcal{L}}$ fixes every set $E_{d,e}$ since the order of $\alpha_3^{\mathcal{L}}\backslash_{D'_d}$ is a power of p for every $d\ /\ \mathbb{Z}_p$.

Let us assume first that $D_a^{\infty} \subseteq D_{a'}^{\infty}$. Lemma 72 gives $E_{a,b} \subset E_{a',b'}$. Using also the fact that $\alpha_3^{\mathcal{L}}$ fixes $E_{a,b}$ and $E_{a',b'}$ setwise we get that B_i is adjacent to B_j if and only if $\alpha_3^{\mathcal{L}})B_i+$ is adjacent to $\alpha_3^{\mathcal{L}})B_j+$, proving the required property for an automorphism of $_1$.

Let us now assume that $D_a^\infty \subseteq D_{a'}^\infty$. We denote by the pair $)\psi_a \mathfrak{a}_a{}^1, \psi_a \mathfrak{a}_a{}^1+$ the restriction of the action of α_3 to $D_a^\infty \cap D_{a'}^\infty$. Since ψ_a and $\mathfrak{a}_a{}^1$ are automorphisms of the pair $))\psi_a \mathfrak{a}_a{}^1 \not\in,)\psi_{a'} \mathfrak{a}_{a'}{}^1 \not\in +$is an automorphism of the induced subgraph on $D_a^\infty \cap D_{a'}^\infty$ if and only $)id^{\mathcal{L}},)\psi_a{}^1 \psi_{a'} \mathfrak{a}_{a'}{}^1 \mathfrak{a}_a \not\in +$ is. Since both $\mathbb{Z}_p^3$ and $\mathbb{Z}_p^3$ are abelian we have

$$id^{\mathcal{L}},)\psi_a{}^1 \psi_{a'} \mathfrak{a}_{a'}{}^1 \mathfrak{a}_a \not\in [\ [\quad id^{\mathcal{L}},)\psi_{a'} \psi_a{}^1 \not\in) \mathfrak{a}_a \mathfrak{a}_{a'}{}^1 \not\in [\ .$$

It is clear that $)\mathfrak{a}_a \mathfrak{a}_{a'}{}^1 \not\in) a^\infty, b_{a'}, 1+[\ \ )a, b_a, 1+$and $)\psi_{a'} \psi_a{}^1 \not\in) a, b_a, 1+[$ $)a^\infty, b_{a'}, 1+$ Using Corollary 74 we get that

$$id^{\mathcal{L}},)\psi_{a'} \psi_a{}^1 \not\in) \mathfrak{a}_a \mathfrak{a}_{a'}{}^1 \not\in [\ [\quad id^{\mathcal{L}}, id^{\mathcal{L}} [$$

which is an automorphism on $D_a^\infty \cap D_{a'}^\infty$. This proves that $\alpha_3^{\mathcal{L}} \ / \ Aut)\ _1+$

If $B_i \subset B_j$, then $\alpha_3)B_i+\subset \alpha_3)B_j+$since $\alpha_3^{\mathcal{L}} \ / \ Aut)\ _1+$thus $p_i \ / \ B_i \to V)\ +$is adjacent to $p_j \ / \ B_j \to V)\ +$if and only if $\alpha_3)p_i+$is adjacent to $\alpha_3)p_j+$

If $B_i \nsim B_j$, then there exists $a \ / \ \mathbb{Z}_p$ such that B_i and $B_j \to D_a$. Since α_3 is defined on D_a by an automorphism of we have that $p_i \ / \ B_i$ is adjacent to $p_j \ / \ B_j$ if and only if $\alpha_3)p_i+$is adjacent to $\alpha_3)p_j+$ finishing the proof of Lemma 75.

□

Finally, one can see using Lemma 71 (ii) that $\mathcal{G}^{\alpha_3} [\ \mathcal{G}$.

Step 3

Let us assume that for the generators of the cyclic groups $\mathcal{G} \ / \ \mathbb{Z}_q$ and $\mathcal{G} \ / \ \mathbb{Z}_q$ we have $\mathcal{G} [\ \mathcal{G}$.

Since $\mathcal{G} [\ \mathcal{G}$ we have that $\mathbb{Z}_p^3$ and $\mathbb{Z}_p^3$ are contained in $C_A)\mathcal{G}+$ Using Sylow's theorem again we may assume that $\mathbb{Z}_p^3$ and $\mathbb{Z}_p^3$ are in the same

Sylow p-subgroup of $C_A(g)$. Using all these assumptions we prove the following Lemma.

Lemma 76. *(i)* $\mathbb{Z}_p^3 \leq \mathbb{Z}_q \wr Sym(p^3)$.

(ii) If $\mathbb{Z}_p^3 \leq \mathbb{Z}_q \wr Sym(p^3)$, *then for every* $\mu \in \mathbb{Z}_p^3$ *we have* $(\mu)^b = id$.

Proof. (a) $\mathbb{Z}_p^3 \leq \mathbb{Z}_q \wr Sym(p^3)$ since the elements of $\mathbb{Z}_p^3$ and g commute.

(b) Let $A^\infty = A \wr Sym(p^3)$. We have already assumed that $\mathbb{Z}_p^3$ and $\mathbb{Z}_p^3$ lie in the same Sylow p-subgroup of A^∞, which is generated by p^3 disjoint q-cycles. Let μ be an arbitrary element of $\mathbb{Z}_p^3$. For every $(b, s) \in \mathbb{Z}_p^3 \wr \mathbb{Z}_q$ we have $(\mu)^{b,s} = (c, s)$ t for some $c \in \mathbb{Z}_p^3$ and $t \in \mathbb{Z}_q$, where t only depends on μ and b since $\mu \in \mathbb{Z}_q \wr Sym(p^3)$. The permutation group G is transitive, hence there exist $a_1, a_2 \in \mathbb{Z}_p^3$ such that $a_1 = (1, s)(b, s)$ and $a_2 = (c, s)$ $t = (1, s)$ t. The order of $a_2 \mu a_1$ is a power of p since a_2, μ and a_1 lie in a Sylow p-subgroup. Therefore $t = 1$ and hence $(\mu)^b = id$.

□

Lemma 76 says that for every $\mu \in \mathbb{Z}_p^3$ we have $(\mu)^b = id$. We use again the graph $_1$ defined on $\mathcal{C}$. It is clear that H_1 and H_2 are regular subgroups in $Aut(_1)$ and they are isomorphic to $\mathbb{Z}_p^3$. Since $\mathbb{Z}_p^3$ is a DCI$^{(2)}$-group [A,N] we have that there exists $\mu \in \langle H_1, H_2 \rangle^{(2)}$ such that $H_2^\mu = H_1$.

Let $\eta = \mu id_{\mathcal{L}}$ be an element of the wreath product $\mathbb{Z}_q \wr Sym(p^3)$. Clearly, $\eta \in \langle G, \mathbb{G} \rangle^{(2)}$ and hence η is an automorphism of $_0$, which conjugates $\mathbb{Z}_p^3$ to $\mathbb{Z}_p^3$. Moreover, the base group part of η is the identity so $\eta \in C_A(g)$. This proves that $G^\eta = G$, finishing the proof of Theorem 68.

□

Our method also gives the following general theorem.

Theorem 77. *Let H be a finite p-group which is a $DCI^{(2)}$-group and q be a prime with $q > |H|$. Then $G = H \times \mathbb{Z}_q$ is a $(q-2)$-DCI-group.*

Proof. Let Γ be a Cayley graph of G. Let us assume first that Γ is connected. Let $\mathcal{G} = \mathcal{H} \times \mathcal{Z}_q$ and $\mathcal{G}' = \mathcal{H}' \times \mathcal{Z}_q'$ be two regular subgroups of A isomorphic to G, where $A = Aut(\Gamma)$. We would like to find $\alpha \in A$ with $\mathcal{G}^\alpha = \mathcal{G}'$.

Using the same argument as in Step 1 in the previous two cases we may assume that $\mathcal{Z}_q$ and $\mathcal{Z}_q'$ lie in the same Sylow q-subgroup of $Sym(G)$, which gives a partition $\mathcal{C} = \{B_1, B_2, \ldots, B_{|H|}\}$. Clearly, we have $\langle \mathcal{G}, \mathcal{G}' \rangle \geq Sym(q) \wr Sym(H)$ and we may also assume that $\mathcal{H}$ and $\mathcal{H}'$ are contained in the same Sylow p-subgroup. The regular action induced by $\mathcal{H}$ and $\mathcal{H}'$ on $\mathcal{C}$ will be denoted by H_1 and H_2, respectively.

Since the degree of the vertices of Γ_0 is less than q we have $B_i \nsim B_j$ if there exists an edge between B_i and B_j. This shows that Γ_0 (the same graph as in the previous cases) is connected since Γ is connected. Lemma 57 (ii) shows that $\mathcal{Z}_q = \mathcal{Z}_q'$.

It is easy to see that $\langle \mathcal{H}, \mathcal{H}' \rangle \geq \mathcal{Z}_q \wr Sym(H)$ and similar argument as in Lemma 76 (ii) shows that for every element of $g \in \langle \mathcal{H}, \mathcal{H}' \rangle^{(2)}$ we have $(g)_{\Gamma_0} = id$. Since H is a DCI$^{(2)}$-group and Γ_1 is a Cayley graph of H containing the regular subgroups H_1 and H_2, there exists an element of $\eta \in \langle H_1, H_2 \rangle^{(2)}$ such that $H_2^\eta = H_1$. It is easy to verify that η lifts to an automorphism of Γ by $\alpha = \eta id_{\mathcal{L}}$, where $\eta id_{\mathcal{L}}$ is an element of the wreath product $\mathcal{Z}_q \wr Sym(H)$ with $(\eta id_{\mathcal{L}})_{\Gamma_0} = id_{\mathcal{L}}$. It is easy to verify that $\mathcal{G}^\alpha = \mathcal{G}'$, finishing the proof of the theorem for connected graphs.

Now, let us assume that $\Gamma = Cay(G, S)$ is not connected. Every connected component of a Cayley graph of G is isomorphic to a connected Cayley graph of $G_1 \geq G$. Either $G_1 \geq H$ or G_1 is of the form $H_1 \times \mathbb{Z}_p$,

where $H_1 \geq H$. The connected Cayley graphs in both cases are CI-graph so if $Cay)G, S+\subsetneq Cay)G, T+$, then there exists $\alpha \ / \ Aut)G_1+$with $\alpha)S+[\ \ T$. Finally, it is easy to verify that for every p-group listed in Theorem 31 each automorphism of G_1 extends to an automorphism of G, finishing the proof of Theorem 77. □

4. EXPANDER GRAPHS

4.1 Definition of expander graph series

Let be an arbitrary undirected graph with vertex set $V)$ + Let $S \leq V)$ + We define the *boundary* of S, which we denote by $\partial)S+$, to be the set of vertices in $V)$ +ر S with at least one neighbour in S. For a graph the *vertex isoperimetric number* or the *vertex expansion ratio* $h)$ +is defined by

$$h) \ +[\ min \left\{ \frac{\backslash \partial)S+\backslash}{\backslash S \backslash} \right(S \rightarrow V) \ +, 1 < \backslash S \backslash \geq \frac{\backslash V) \ +\backslash}{3} \left(.$$

Similarly, the *edge isoperimetric number* or the *edge expension ratio* is

$$h_e) \ +[\ min \left\{ \frac{\backslash \partial_e)S+\backslash}{\backslash S \backslash} \right(S \rightarrow V) \ +, 1 < \backslash S \backslash \geq \frac{\backslash V) \ +\backslash}{3} \left(,$$

where $\partial_e)S+$, what we call the *edge boundary*, denotes the set of edges leaving S. A graph is called an ϵ-*expander* if $h) \ +\sim \epsilon$, and a series of graphs $_n$ is called an *expander family* if there is a constant $\epsilon > 1$ such that for every n the graph $_n$ is an ϵ-expander. Denoting the maximum degree by d it is easy to see that

$$\frac{h_e) \ +}{d} \geq h) \ +\geq h_e) \ +,$$

so we could have used $h_e) \ +$to define expander family for graphs of bounded degree. Sometimes we drop the subscripts n and we omit to mention the fact that we are talking about an infinite sequence of graphs. We will only restrict our attention to undirected d-regular graphs. We shall say that d-regular expander graphs are finite graphs which are highly connected and sparse in some sense.

The theory of expander graphs is a fast developing area of mathematics and expander graphs have many different applications in pure and applied mathematics as well. The original definition of expander graphs was introduced by Pinsker [Pin]. Pinsker proved the existence of d-regular bipartite expander graph series using a simple probabilistic proof. Recently, it was discovered that an equivalent definition was formulated earlier by Barzdin and Kolmogorov [B,K].

4.2 Spectral expansion, Mixing lemma

We will exhibit a series of non-expander Cayley graphs of special type in Section 4.4. Therefore we only briefly collect some important properties of expander graphs.

The *adjacency matrix* M of a graph on vertices labeled by $2, \ldots, n$ is defined by $M_{i,j}$ [\}e / E) +from i to $j\langle$\ The *normalized adjacency* matrix of a d-regular graph is simply N [$\frac{M}{d}$, which can also be considered as the transition matrix of the random walk on . Since M is symmetric it has n real eigenvalues. It is clear that)2, . . . , 2+/ $\mathbb{R}^n$ is an eigenvector of the adjacency matrix with eigenvalue d and all the eigenvalues lie in the interval] d, d^. The eigenvalues of the graph are denoted in the following way:

$$d\,[\ \lambda_1)\ +\sim \lambda_2)\ +\sim \ldots \sim \lambda_n)\ +\sim\ d.$$

Many properties of the graph can be derived from its *spectrum*, which is the set of eigenvalues of the corresponding adjacency matrix. For example, a d-regular graph is connected if and only if $\lambda_2)$ +< d and G is bipartite if and only if $\lambda_n)$ +[d. Moreover the multiplicity of d is equal to the number of connected components. However it is not too hard to construct *cospectral graphs*, which are non-isomorphic graphs with the same spectrum, but we have already seen that the isomorphism classes of Cayley graphs of $\mathbb{Z}_p$ are determined by the spectrum, see [Tur].

The difference between the two biggest eigenvalues $d \quad \lambda_2)G+$is called the *spectral gap* and $\lambda) \ +$denotes o c˜ $\}\backslash\lambda_2) \ \dashv, \backslash\lambda_n) \ \dashv\backslash$. The following inequalities, proved independently by Dodziuk [Dod] and by Alon [Alo], relate the spectral gap and the isoperimetric numbers:

$$\frac{d \quad \lambda_2) \ +}{3} \geq h_e) \ + \geq \quad \overline{3d)d \quad \lambda_2) \ +}.$$

This theorem shows that $_n$ is an expander family if and only if the spectral gaps $d \quad \lambda_2) \ _n+$of these graphs are bounded from below by some positive constant.

A combinatorial way to describe expander graphs is the Expander Mixing Lemma, which was first proved by Alon and Chung. [A,C].

Lemma 78 (Alon, Capalbo)**.** *Let be a d-regular graph. Then*

$$\left| E)S,T\dashv \quad \frac{d\backslash S\backslash\backslash T\backslash}{\backslash V) \ \dashv} \right| \geq \lambda) \ + \ \overline{\backslash S\backslash\backslash T\backslash} \tag{4.1}$$

for all $S,T \to V) \ +$, *where* $E)S,T+$*denotes the number of edges connecting a vertex in* S *with a vertex in* T*.*

Note that the ratio $\frac{d\backslash S\backslash\backslash T\backslash}{\backslash V(\Gamma)\backslash}$ is the expected value of the edges between sets of cardinality $\backslash S\backslash$ and $\backslash T\backslash$ in a random d-regular graph on n vertices. The eigenvalues of the adjacency matrix can also be estimated with the difference which appears on the left side of equation (4.1). This statement, proved by Bilu and Linial [B,L], is usually called the converse of the Expander Mixing Lemma.

Lemma 79. *Let be a d-regular graph. Suppose that there exists some positive constant c such that* $\left| E)S,T\dashv \quad \frac{d\backslash S\backslash\backslash T\backslash}{\backslash V(\Gamma)\backslash} \right| \geq c \quad \overline{\backslash S\backslash\backslash T\backslash}$ *for every* $S \{ T [\ \mathcal{B}$. *Then* $\lambda) \ + \geq Kc)2\,0 \ l\text{o}g_2)\frac{d}{\lambda(G)}+$.

The distance $d)x,y+$of two vertices x and y in a graph is the length of the shortest path connecting these vertices and the *diameter* of a graphs is

o c˜ $_{x,y/V(\Gamma)}$ $d)x, y+$ Clearly, one of the most important properties of expander graphs is that they have small diameter. More precisely, for a fixes $\epsilon > 1$, an ϵ-expander graph on n vertices has diameter $O)$ npi $n+$

Finally, we mention again that the normalized adjacency matrix of a graph can be considered as the transition matrix of a Markov chain, which is called the random walk on . A random walk is a sequence of random vertices $v_1, v_2, \ldots$ of the graph, where v_{i+1} is chosen uniformly at random from the neighbours of v_i. The choices in different steps are independent.

It is well known that if is connected and non-bipartite with $\backslash V) \dashv \backslash [\ n$, then the random walk converges to the to the uniform distribution on $V) +$ what we denote by u_n. The rate of convergence can be estimated by $\lambda) +$ We choose an arbitrary *initial distribution vector* $p [\ p_1, p_2, \ldots, p_n$ such that $\prod_{i=1}^{n} p_i [\ 2$, then we get the following.

Lemma 80. *Let be a graph on n vertices and let p be the initial distribution vector as above. We denote by N the normalized adjacency matrix of . Then* $\backslash\backslash N^k p \quad u_n \backslash\backslash_2 \geq \left)\frac{\lambda(\Gamma)}{d}\right($ *.*

4.3 Existence of expanders

As we have already mentioned before, the existence of expander graph series can be proved using the probabilistic method. What is more, using a suitable random graph model, there exists an $\epsilon > 1$ such that the probability that a randomly chosen d-regular graph on n vertices is an ϵ-expander tends to 2 as n tends to infinity if $d \sim 4$.

The first explicit series of expander graphs was constructed by Margulis [Mar]. Let G be a locally compact group and let H be a Hilbert space. We say that a unitary representation $\pi = G \backslash\!\!\!\otimes U)H +$ has *almost invariant vectors* if there exist $v_n \ / \ H$ with $\backslash\backslash v_n \backslash\backslash [\ 2$ such that for every compact subset K of G we have that $\text{uxs}_{g/K} \backslash\backslash \pi)g \dashv v_n + \ v_n \backslash\backslash$ tends to zero as n tends to infinity.

The group G is said to have *property (T)* if every unitary representation of G having almost invariant vectors has a non-zero G-invariant vector. It was proved by Kazhdan [Kaz] that $SL)n, K+$has property (T) if K is a locally compact non-discrete field. Note that $SL)n, \mathbb{R}+$does not have property (T). It was also proved that lattices in real simple groups of rank at least 3 (e.g. $SL)d, \mathbb{Z}+$ where $d \sim 4$) also have property (T). It was proved by Margulis [Mar] that if G is a group generated by a finite set S and G has Kazhdan property $)T+$and $\mathcal{M}$is a set of finite index subgroups of G, then the Cayley graphs $\}Cay)G/N, S+\backslash N \ / \ \mathcal{M}$(form a family of ϵ^{∞}expanders for some $\epsilon^{\infty} > 1$. This result gave the first explicit example for a family of expander graphs.

One explicit example avoiding the use heavy machinery of infinite group theory was found by Reingold, Vadhan and Wigderson [R,V,W]. Their construction is based on the Zig-Zag graph product. Given an m-regular graph $_1$ and a d-regular graph $_2$ on n and m vertices, respectively. The Zig-Zag product $_1 \equiv _2$ of $_1$ and $_2$ is a d^2-regular graph on nm vertices. The advantage of the Zig-Zag product is that the spectral gap of the product can be estimated from below by a function of the spectral gaps of $_1$ and $_2$. Using such a method, d-regular graphs on d^{4n} vertices were constructed for every n and $d \sim 4$ with isoperimetric number bounded from below by some positive constant which does not depend on n.

For more information and more applications of expander graphs we refer the reader to the survey of Lubotzky [Lub2] and the paper of Hoory, Linial and Wigderson [H,L,W].

4.4 *Non-expander Cayley graphs of finite simple groups*

In this section, for every infinite sequence of simple groups of Lie type of growing rank we exhibit connected Cayley graphs of degree at most 21 such that the isoperimetric number of these graphs converges to 1. This proves

that these graphs do not form a family of expanders.

The study of series of Cayley graphs of finite simple groups has received great attention. It was announced by Kassabov, Lubotzky and Nikolov in [K,L,N] that there exist $k \in \mathbb{N}$ and $1 < \epsilon \in \mathbb{R}$ such that every non-abelian finite simple group which is not a Suzuki group has a set of generators S of size at most k for which $Cay(G, S)$ is an ϵ-expander. The details of the proof of this result are given in a series of papers ([Kas1],[K,N],[Kas2],[Lub3],[Nik]), and the theorem has been extended by Breuillard, Green and Tao in [B,G,T1] to the Suzuki groups. These results motivate a question which was asked by Lubotzky in [L,Z] - is every family of Chevalley groups of bounded rank a family of uniformly expanding groups? Recently, Breuillard, Green, Guralnick and Tao [B,G,G,T] proved the folllowing theorem:

Theorem 81 (Breuillard, Green, Guralnick, Tao)**.** *Let G be a finite simple group of Lie type of rank n. Suppose that a and b are elements of G selected uniformly at random. Then the probability that $Cay(G, \{a, b, a^{-1}, b^{-1}\})$ is an ϵ-expander is at least $2 - C|G|^{-\delta}$, where C and δ only depend on ϵ and n.*

In [Lub2], Lubotzky also suggested that one should investigate families of simple groups of unbounded rank, and wrote that it seems likely that if G_n is a sequence of non-abelian simple groups of Lie type such that the rank of G_n is unbounded, then for every n there exists a generating set $T_n \subset G_n$ such that the graphs $Cay(G_n, T_n)$ do not form a family of expanders. An explicit example (see [Lub1, p.31]) of a non-expander family of Cayley graphs of special linear groups was given by Luz. The diameter of the graphs given by Luz was investigated by Kassabov and Riley, and it was proved in [K,R] that there exists $c \in \mathbb{R}$ such that the diameter of the graphs is smaller than $c \log(|SL(n, p)|)$.

Similarly, the symmetric group S_n is generated by $\gamma = (2, 3)$ and $\sigma_n = (2, 3, \ldots, n)$ for every $n \in \mathbb{N}$ and the corresponding sequence of isoperimetric

numbers $h)Cay)S_n, \}\gamma, \sigma_n\langle +$+tends to 1. Moreover, one can find a set of generators of S_n such that the diameter of the corresponding Cayley graphs is $^{-})n^2+$which shows that these Cayley graphs do not form a family of expanders, see [Lub1, Proposition 6.1.8].

One of the breakthroughs in solving questions on growth in groups is due to Helfgott (see [Hel]), who proved that for a generating set $A \to SL)3, p+$ we have either $\backslash A^3\backslash \sim \backslash A\backslash^{1+\delta}$ or $)A \cap A^{\ 1} \cap e\dot{+}^{k}$ [$SL)3, p\dot{+}$ where $\delta > 1$ and $k \sim 2$ are absolute constants. Complete generalizations of this result to all finite simple groups of Lie type of bounded rank were given by Pyber and Szabó (see [P,Sz]) and by Breuillard, Green and Tao (see [B,G,T2]). For every $n \sim 4$, an explicit example of a generating set A of $SL)n, 4+$was also given by Pyber and Szabó (see [P,Sz]) such that $\backslash A^3\backslash \geq 211\backslash A\backslash$ and it is mentioned that large families of generating sets of constant growth, which are union of a few cosets of some subgroup, can also be given for $SL)n, q\dot{+}$ where $q > 3$. Similar counterexamples for growth in symmetric groups were given in [P,P,S,Sz] and in [Spi5].

For every prime power q we will investigate 8 series $A_l)q\dot{+}, B_l)q\dot{+}, C_l)q\dot{+}$ $D_l)q\dot{+}, {}^2A_{2n\ 1})q^2\dot{+}, {}^2A_{2n})q^2\dot{+}, {}^2D_n)q^2+$of finite simple groups of Lie type. These are the series of groups of Lie type of fixed type for which the rank of the groups tends to infinity. In order to define generators and subgroups of these groups we will use the generators given by Steinberg in [Ste] and we will use the notation and several results from the book of Carter [Car].

For these 8 series of finite simple groups of Lie type we construct Cayley graphs and subsets such that the number of neighbours of these subsets depends on the rank of the group. Moreover, the isoperimetric number of these graphs tends to 1. This proves the conjecture of Lubotzky concerning the series of Cayley graphs of simple groups of unbounded rank. More precisely, we prove the following:

Theorem 82 ([Som2]). *(a) Let G be a Chevalley group of rank l of type*

A_l, B_l, C_l or D_l. For every $l \sim 6$ and for every finite field $GF)q+$there exists a generating set T of cardinality at most 21 and a subset of the vertices $S \to V)Cay)G, T++$with $\backslash S\backslash \geq \frac{\backslash G\backslash}{2}$ such that $\frac{\backslash \partial(S)\backslash}{\backslash S\backslash} \geq \frac{6}{l\ 3}$.

(b) Let G be a twisted group of type ${}^2A_{2n\ 1}$, ${}^2A_{2n}$ or ${}^2D_n$. For every $n \sim 6$ and for every finite field $GF)q+$there exists a generating set $T^\infty$of cardinality at most 9 and $S^\infty \to V)Cay)G, T^\infty++$with $\backslash S^\infty\backslash \geq \frac{\backslash G\backslash}{2}$ such that $\frac{\backslash \partial(S')\backslash}{\backslash S'\backslash} \geq \frac{6}{n\ 2}$.

In Section 4.4.1 we give all necessary definitions and we collect some important facts concerning the construction of simple groups of Lie type. The proof of Theorem 82 (a) is contained in Section 4.4.2, and Theorem 82 (b), which is the case of twisted groups, will be handled in Section 4.4.7. Finally, in Section 4.4.11 we present the construction for $PSL)n, q+$in terms of matrices.

4.4.1 Preliminaries

In this section we collect important facts about finite simple groups of Lie type and we build up the notation we will use throughout this chapter.

Let $K\ [\ GF)q+$be a finite field. We denote by Ω the system of roots and $\Omega\ [\ \Omega^+ \cap \Omega\ $ is the union of the positive and negative roots. We also choose $\Phi\ [\ \}r_1, r_2, \ldots, r_l\langle \to \Omega^+$ which is the set of fundamental roots.

The Weyl group W is generated by the reflections w_r, where $r\ /\ \Omega$. It is well known that W is generated by the fundamental reflections w_r, where $r\ /\ \Phi$. In order to simplify notation we denote by w_i the fundamental reflection w_{r_i}, where $r_i\ /\ \Phi$. We denote by $x_r)t+$the standard generators of the Chevalley group G, where $r\ /\ \Omega$ and $t\ /\ K$. If $r\ [\ r_i$ for some $r_i\ /\ \Phi$, then we denote by $x_i)t+$the standard generator $x_{r_i})t+$ The subgroups $X_r\ [\ \}x_r)t+\backslash t\ /\ K\langle$ for $r\ /\ \Omega$ are called root subgroups of G.

Let $n_r)t+[\ x_r)t+x_{\ r})\ \ t^{\ 1}+x_r)t+$ and set $n_r\ [\ n_r)2+$ Clearly, $n_r)t+$ is an element of the subgroup generated by the root subgroups X_r and $X_{\ r}$ for every $t\ /\ K$ and $r\ /\ \Omega$. It is well known that $n_r x_s)t+n_r^{\ 1}\ [\ x_{w_r(s)})\eta_{r,s}t+$ for some $\eta_{r,s}\ /\ K$ depending only on r and s, see [Car, p.101]. Let $h_r)t+[\ n_r)t+n_r)\ \ 2+$ It is easy to see that $h_r)t+/\ \rangle X_r, X_{\ r}|$.

We denote by H the subgroup generated by the elements $h_r)t+$ for all $r\ /\ \Omega$ and $t\ /\ K$ and let N be the subgroup of G generated by H and the elements n_r for all $r\ /\ \Omega$. The elements of H can be written in the form $h)\chi+$, where χ is a K-character of $\mathbb{Z}\Omega$, see [Car, p.97]. The K-character corresponding to $h_r)t+$ is denoted by $\chi_{r,t}$ and $\chi_{r,t})a+[\ t^{\frac{2(a,r)}{(r,r)}}$. H is a normal subgroup of N and $n_w h)\chi+n_w^{\ 1}\ [\ h)\chi^{\infty}+$ where $\chi^{\infty})r+[\ \chi)w^{\ 1})r++$, see [Car, p.102].

The Weyl group W is isomorphic to N/H and every element of the Weyl group W acts on the root system Ω. Using this isomorphism, the cosets of H in N can be written as $n_w H$ with $n_{w_r}\ [\ n_r$ for all $r\ /\ \Omega$.

4.4.2 Chevalley groups

In this section we construct series of Cayley graphs for 5 different series of Chevalley groups. For these Chevalley groups we need 7 series of Cayley graphs. The six different constructions are similar but we will treat them separately.

We first prove the following technical lemma.

Lemma 83. *Let $w\ [\ w_1 w_2 \dots w_l$ be a Coxeter element of the Weyl group W. Fix an $2 \geq i \geq l\ \ 2$ and let us assume that the fundamental root r_i is orthogonal to r_j if $i\,0\ 2 < j \geq l$ and r_{i+1} is orthogonal to r_k if $2 \geq k \geq i\ \ 2$. We also assume that r_i and r_{i+1} have the same length and $w_i)r_{i+1}+[\ r_i 0\ r_{i+1}$. Then $w)r_i+[\ r_{i+1}$.*

Proof. Since r_i is orthogonal to r_j for every $j > i\,0\ 2$ we have that $w)r_i+[$

$w_1w_2\dots w_iw_{i+1})r_i+$ The elements w_k are reflections through the hyperplane perpendicular to r_k. Thus $w_k)r_k+[\quad r_k$ for every $2 \geq k \geq l$ and $w_{i+1})r_i+[$ $r_i\ 0\ r_{i+1}\ [\ \ w_i)r_{i+1}+$since r_i and r_{i+1} have the same length. It follows that $w_iw_{i+1})r_i+[\ \ w_i)r_i\ 0\ r_{i+1}+[\ \ w_i)r_i+0\ w_i)r_{i+1}+[\quad r_i\ 0\ )r_i\ 0\ r_{i+1}+[\ \ r_{i+1}$. Hence $w)r_i+[\ \ w_1w_2\dots w_{i\ \ 1})r_{i+1}+[\ \ r_{i+1}$ since r_{i+1} is orthogonal to r_k for $2 \geq k \geq i\quad 2$.

□

4.4.3 A_l

Let G be a Chevalley group of type A_l. The Dynkin diagram of the corresponding root system is the following:

One can see from the Dynkin diagram that $w_i)r_{i+1}+[\ \ r_i0\ r_{i+1}\ [\ \ w_{i+1})r_i+$ for $i\ [\ \ 2,\dots,l\quad 2$.

Let $w\ [\ \ w_1w_2\dots w_l$ be a Coxeter element of the Weyl group. We choose λ to be a generator of the multiplicative group of $GF)q+$

Lemma 84. *$x_1)2+$, n_w and $h_{r_1})\lambda+$generate the Chevalley group G.*

Proof. It was proved in [Ste, Theorem 3.11] that $x_1)2+n_w$ and $h_{r_1})\lambda+$generate G if $q > 4$, and $x_1)2+$and n_w generate G if $q \geq 4$.

□

For every $l \sim 6$ we define the following undirected Cayley graph:

$$_a\ [\ \ Cay)G, \}x_1)2+, n_w, h_{r_1})\lambda+, x_1)2+^{\ 1}, {n_w}^{\ 1}, h_{r_1})\lambda+^{\ 1}\langle +$$

Let K_a be the subgroup of the Chevalley group G generated by the root subgroups $X_{r_1}, X_{\ r_1}, X_{r_2}, X_{\ r_2}, \dots, X_{r_{l-1}}, X_{\ r_{l-1}}$. Clearly, $K_a \subsetneq A_{l\ \ 1})q+$ Let

$$S_a\ [\ \ \sqrt{\vphantom{x}}^{l\ \ 1}_{i=0} K_a n_w^i.$$

Lemma 85. *The orbit of w which contains r_1 is the following:*

$$\longrightarrow r_1 \xrightarrow{w} r_2 \xrightarrow{w} r_3 \xrightarrow{w} \cdots \xrightarrow{w} r_{l-1} \xrightarrow{w} r_l \xrightarrow{w} r_1 \quad \ldots \quad r_l \xrightarrow{w}$$

This can be formulated as follows:

$$w)r_i+[\ r_{i+1} \text{ for } 2 \geq i \geq l \quad 2$$
$$w)r_l+[\ r_1 \quad \ldots \quad r_l$$
$$w)\ r_1 \quad r_2 \quad \ldots \quad r_l+[\ r_1$$

Proof. Lemma 83 gives that $w)r_i+[\ r_{i+1}$ for $2 \geq i \geq l \quad 2$ and

$$w)r_l+[\ w_1w_2\ldots w_l)r_l+[\ w_1w_2\ldots w_{l-1})\ r_l+[\ w_1w_2\ldots w_{l-1})r_l+$$

since w is a linear transformation of the vector space spanned by the roots. We also have $w_j)r_{j+1}\,0\ \times\times\times 0\ r_l+[\ r_j\,0\ r_{j+1}\,0\ \times\times\times 0\ r_l$ for $2 \geq j \geq l \quad 2$. Therefore

$$w_1w_2\ldots w_{l-1})r_l+[\ w_1w_2\ldots w_{l-2})r_{l-1}\,0\ r_l+$$
$$[\ w_1w_2\ldots w_{l-3})r_{l-2}\,0\ r_{l-1}\,0\ r_l+[\ \times\times\times[\ r_1\,0\ r_2\,0\ \ldots 0\ r_l.$$

This shows that

$$w)r_l+[\ \ )r_1\,0\ r_2\,0\ \ldots 0\ r_l+ \tag{4.2}$$

Using again the linearity of w and equation (4.2) we get

$$w)r_1\,0\ r_2\,0\ \ldots 0\ r_l+[\ r_2\,0\ r_3\,0\ \ldots 0\ r_l \quad)r_1\,0\ r_2\,0\ \ldots 0\ r_l+[\ \ r_1.$$

This gives $w) \quad)r_1\,0\ r_2\,0\ \ldots 0\ r_l++[\ r_1$, finishing the proof Lemma 85.

□

It follows from the proof of Lemma 85 that if $2 \geq i \geq l \quad 2$, then $n_w^i K_a n_w{}^i$ contains $n_w^i X_{r_{l-i}} n_w{}^i\ [\ X_{r_l}$. Therefore $n_w^i K_a n_w{}^i\ \{\ K_a$ which shows that $n_w^i\ /\ K_a$ for every $2 \geq i \geq l \quad 2$. This implies that $K_a, K_a n_w, \ldots, K_a n_w^{l-1}$ are different right cosets of K_a so S_a is the union of l pairwise disjoint subsets of the vertices of $_a$ and these subsets have the same cardinality.

Lemma 86. $\frac{|\partial(S_a)|}{|S_a|} \geq \frac{6}{l}$

Proof. S_a is the union of l right cosets of K_a so $|S_a| = l|K_a|$. It is clear from the definition of S_a that $K_a n_w^i n_w \subset S_a$ for every $1 \geq i \geq l-3$ and similarly $K_a n_w^i n_w^{-1} \subset S_a$ if $2 \geq i \geq l-2$. Therefore those neighbours of S_a which are not in S_a can only be obtained as an element of the following subset of the vertices of $_a$:

$$K_a n_w^l \cup K_a n_w^{-1} \bigcup_{i=1}^{l-1} K_a n_w^i h_{r_1}(x_1) \cup \bigcup_{i=1}^{l-1} K_a n_w^i h_{r_1}(x_1)^{-1} \bigcup_{i=1}^{l-1} K_a n_w^i h_{r_1}(x_{r_1}) \cup \bigcup_{i=1}^{l-1} K_a w^i h_{r_1}(x_{r_1})^{-1}.$$

K_a is a subgroup of G so $K_a n_w^i x \subset K_a n_w^i$ if and only if $n_w^i x n_w^{-i} \in K_a$. We first apply this observation to $x_1(x_{r_1})$ and $x_1(x_{r_1})^{-1} \subset x_1(x_{r_1})$. It is easy to see from Lemma 85 that $n_w^i x_1(x_{r_1}) n_w^{-i}$ is of the form $x_{w^i(r_1)}(\alpha) \subset x_{i+1}(\alpha)$ for some $\alpha \in GF(q)^*$ if $1 \geq i \geq l-2$. It follows that $n_w^i x_1(x_{r_1}) n_w^{-i} \in X_{r_{i+1}} \subset K_a$ if $i \leq l-2$.

Using the fact that $h_r(\lambda)$ and $h_r(\lambda)^{-1}$ are in the subgroup $\langle X_r, X_{-r} \rangle$ we get that $n_w^i h_{r_1}(\lambda) \subset n_w^i \in \langle X_{w^i(r_1)}, X_{-w^i(r_1)} \rangle \subset \langle X_{r_{i+1}}, X_{-r_{i+1}} \rangle \subset K_a$ if $i \leq l-2$.

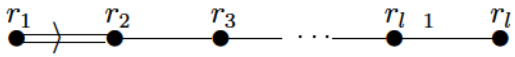
Now, $\partial(S_a) \subseteq K_a n_w^l \cap K_a n_w^{-1} \cap K_a n_w^{l-1} x_1(2) \cap K_a n_w^{l-1} x_1(-2) \cap K_a n_w^{l-1} h_{r_1}(\lambda) \cap K_a n_w^{l-1} h_{r_1}(\lambda^{-1})$. All of these subsets are right cosets of K_a so they have the same cardinality which proves that $|\partial(S_a)| \geq 7|K_a|$, while $|S_a| = l|K_a|$. □

Remark 87. In order to prove Theorem 82 (a) we repeat the previous construction several times. In every single case the chosen generating set of the Cayley graph will consist of a few standard generators of the Chevalley group, an element of the form n_w, where $w = w_1 w_2 \dots w_l$ is a Coxeter element of the corresponding Weyl group, and an element of the group H. If G is of rank

l we will choose a subgroup of G which is isomorphic to a Chevalley group of rank l 2 and which is of the same type. The subset of the vertices for which the isoperimetric number is sufficiently small will be a union of cosets of the subgroup of rank l 2.

4.4.4 B_l

Let G be a Chevalley group of type B_l. The Dynkin diagram of a Chevalley group of type B_l is the following:



It is easy to see from the Dynkin diagram that $w_1)r_2+[\ r_20\ 3r_1$ and $w_2)r_1+[\ r_1\,0\ r_2$. Set $w\ [\ w_1\ldots w_l$.

One can see using Lemma 83 that

$$w)r_i+[\ w_1w_2\ldots w_l)r_i+[\ r_{i+1}\ \text{ for } 3\geq i\geq l\ 2. \tag{4.3}$$

The fundamental roots $r_3,\ldots,r_l$ are orthogonal to r_1. Therefore $w)r_1+[\ w_1w_2)r_1+[\ w_1)r_1\,0\ r_2+[\ r_1\,0\ )r_2\,0\ 3r_1+[\ r_1\,0\ r_2$. We also have that w is linear so using equation (4.3) we have that if $3\geq j\geq l\ 2$, then

$$w)r_10\ r_20\ldots0\ r_j+[\ w)r_1+0\ w)r_2+0\ldots0\ w)r_j+[\ r_10\ r_20\ r_30\ldots0\ r_{j+1}. \tag{4.4}$$

Using these observations we conclude that the following picture represents a part of the $\rangle w|$-orbit of r_1:

$$r_1\xrightarrow{w}r_1\,0\ r_2\xrightarrow{w}r_1\,0\ r_2\,0\ r_3\xrightarrow{w}\cdots\longrightarrow r_1\,0\ r_2\,0\ \ldots0\ r_l\xrightarrow{w}$$

This can be formulated as follows:

$$w^i)r_1+[\ r_1\,0\ r_2\,0\ \ldots0\ r_{i+1}\ \text{for } i\ [\ 2,\ldots,l\ 2. \tag{4.5}$$

The orbit of $\rangle w|$ containing these elements contains $w)r_1\,0\ r_2\,0\ \ldots 0\ r_l+$ as well. It is easy to see that $w_i)r_{i+1}\,0\ r_{i+2}\,0\ \ldots 0\ r_l+[\ r_i\,0\ r_{i+1}\,0\ \ldots 0\ r_l$ if $3 \geq i \geq l\quad 2$. We also have $w_1)r_2+[\ 3r_1\,0\ r_2$ hence

$$\begin{aligned} w)r_l+[\ & w_1 \ldots w_{l\ 1}w_l)r_l+[\quad w_1 \ldots w_{l\ 1})r_l+ \\ & [\quad w_1 \ldots w_{l\ 2})r_{l\ 1}\,0\ r_l+[\ \times\times[\quad w_1)r_2\,0\ \ldots 0\ r_l+ \\ & [\quad)r_l\,0\ \ldots 0\ r_2\,0\ 3r_1+ \end{aligned}$$

This implies using equation (4.4) that

$$w)r_1\,0\ \ldots 0\ r_l+[\ w)r_1\,0\ \ldots 0\ r_{l\ 1}+0\ w)r_l+[\quad r_1. \tag{4.6}$$

One can easily describe the remaining elements of the orbit since w is linear.

We also investigate the action of $\rangle w|$ on $3r_1\,0\ r_2\,0\ \ldots 0\ r_l$ and $r_2\,0\ \ldots 0\ r_l$. Using equation (4.6) and the linearity of w we get that $w)3r_1\,0\ r_2\,0\ \ldots 0\ r_l+[$ $w)r_1+0\ w)r_1\,0\ r_2\,0\ \ldots 0\ r_l+[\ r_1\,0\ r_2\quad r_1\ [\ r_2$. It follows using equation (4.3) that

$$w^i)3r_1\,0\ r_2\,0\ \ldots 0\ r_l+[\ r_{i+1} \text{ for } 2 \geq i \geq l\quad 2. \tag{4.7}$$

One can also prove using equation (4.5) and equation (4.7) that

$$w^i)r_2\,0\ \ldots 0\ r_l+[\quad 3)r_1\,0\ r_2\,0\ \ldots 0\ r_{i+1}+0\ r_{i+1} \text{ for } 2 \geq i \geq l\quad 2. \tag{4.8}$$

$$Char)K+> 3$$

Let us assume that $char)K+> 3$.

Lemma 88. *$x_1)2+$, n_w and $h_t)\lambda+$, where $t\ [\ 3r_1\,0\ r_2\,0\ \times\times 0\ r_l$, generate the Chevalley group G of type B_l if the characteristic of the underlying field is not 3.*

Proof. It was proved in |Ste, Theorem 3.11| that $x_1)2+$ and n_w and $h_t)\lambda+$generate the Chevalley group G if $char)K+\{\ 3$ and $\backslash K\backslash\{\ 4$, and $x_1)2+$and n_w generate G is $\backslash K\backslash[\ 4$.

□

We define again a sequence of connected Cayley graphs. Let

$$_b [\ Cay \ G, \}x_1)2+,x_1) \ \ 2+,n_w, n_w{}^1, h_t)\lambda+,h_t)\lambda+{}^1\langle [,$$

where $G [\ B_l$ and $w [\ w_1w_2 \dots w_l$. Similarly to the previous case let

$$K_b [\ \rangle X_{r_1}, X \ _{r_1}, X_{r_2}, X \ _{r_2}, \dots, X_{r_{l-1}}, X \ _{r_{l-1}}|$$

and let

$$S_b [\ \sum_{i=0}^{l \ 2} K_b n_w^i. \tag{4.9}$$

Lemma 89. $\frac{\backslash \partial(S_b)\backslash}{\backslash S_b \backslash} \geq \frac{4}{l \ 1}$

Proof. We claim that S_b is the union of pairwise disjoint right cosets of K_b. We only have to show that $n_w^i \ / \ K_b$ if $2 \geq i \geq l \quad 3$. Straightforward calculation shows using equation (4.3) that $n_w^i X_{r_{l-i}} n_w{}^i [\ X_{r_l}$ if $2 \geq i \geq l \quad 3$. Therefore $X_{r_l} \rightarrow n_w^i K_b n_w{}^i \{ \ K_b$ if $2 \geq i \geq l \quad 3$ which gives that $n_w^i \ / \ K_b$. Thus S_b is the union of $l \quad 2$ pairwise disjoint right cosets of K_b.

Using the definition of the Cayley graph $_b$ we have that $\partial)S_b+$is a subset of the following set:

$$\sum_{i=0}^{l \ 2})K_b n_w^i+n_w \sum_{i=0}^{l \ 2})K_b n_w^i+n_w{}^1 \sum_{i=0}^{l \ 2})K_b n_w^i+x_1)2+\sum_{i=0}^{l \ 2})K_b n_w^i+x_1) \ \ 2+$$
$$\sum_{i=0}^{l \ 2})K_b n_w^i+h_t)\lambda+\sum_{i=0}^{l \ 2})K_b n_w^i+h_t)\lambda+{}^1.$$

By the definition of S_b the subsets $K_b n_w^i n_w$ are contained in S_b if $1 \geq i \geq l \quad 4$ and $K_b n_w^i n_w{}^1 \rightarrow S_b$ if $2 \geq i \geq l \quad 3$.

Using equation (4.5) we have $n_w^i x_1) \circ 2+n_w{}^i [\ x_{r_1+r_2+\dots+r_{i+1}})u+$for some $u \ / \ K^{\pm}$. If $1 \geq i \geq l \quad 3$, then $x_{r_1+r_2+\dots+r_{i+1}})u+ / \ K_b$ since $r_1 \, 0 \ r_2 \, 0 \ \dots 0 \ r_{i+1}$ is in the root system generated by the fundamental roots $r_1, r_2, \dots, r_{l \ 1}$ and

K_b is the Chevalley group of type $B_{l\ 1}$ generated by the corresponding root subgroups. Therefore $K_b n_w^i x_1)\circ 2+[\ \ K_b n_w^i \to S_b$ if $1 \geq i \geq l\quad 3$.

The elements $h_t)\lambda+$and $h_t)\lambda+^{\ 1}[\ \ h_t)\lambda\ ^{1}+$are in the subgroup generated by X_t and $X_{\ t}$. Equation (4.7) shows that $n_w^i X_t {n_w}^i[\ \ X_{w^i(t)}[\ \ X_{r_{i+1}}$ and by the linearity of w we have $n_w^i X_{\ r} {n_w}^i[\ \ X_{\ r_{i+1}}$ for $i[\ \ 2,3,\ldots,l\quad 3$. Thus $n_w^i h_t)\lambda+{n_w}^i$ and $n_w^i h_t)\lambda\ ^{1}+{n_w}^i$ are in $\rangle X_{r_{i+1}}, X_{\ r_{i+1}}| \geq K_b$ if $2 \geq i \geq l\quad 3$.

It follows that $\partial)S_b+\longrightarrow K_b n_w^{l\ 1}\cap K_b {n_w}^1\cap K_b h_t)\lambda+\cap K_b h_t)\lambda\ ^{1}+$which gives $\frac{\setminus\partial(S_b)\setminus}{\setminus S_b\setminus} \geq \frac{4\setminus K_b\setminus}{(l\ \ 1)\setminus K_b\setminus}[\ \ \frac{4}{l\ \ 1}$.

□

$Char)K+[\ \ 3$

Lemma 90. *$x_s)2+$, $x_{\ r_1})2+$, n_w and $h_t)\lambda+$, where $s[\ \ r_2\ 0\ \times\times 0\ r_l$ and $t[\ \ 3r_1\ 0\ r_2\ 0\ \times\times 0\ r_l$, generate the Chevalley group G of type B_l if $char)K+[\ \ 3$.*

Proof. It was proved in [Ste, Theorem 3.14] that $x_s)2+x_{\ r_1})2+n_w$ and $h_t)\lambda+$ generate G if $\setminus K\setminus > 3$ and $x_s)2+x_{\ r_1})2+$and n_w generate G if $\setminus K\setminus[\ \ 3$.

□

Let

$$\overset{\infty}{b}[\ \ Cay\ \ G, \}x_s)2+, x_{\ r_1})2+, n_w^{\subseteq 1}, h_t)\lambda+^{\subseteq 1}\langle\ [\ .$$

The set S_b, which is defined as in equation (4.9), can be considered as a subset of $V)\ \overset{\infty}{b}+$so we claim the following.

Lemma 91. $\frac{\setminus\partial(S_b)\setminus}{\setminus S_b\setminus} \geq \frac{5}{l\ \ 1}$

Proof. It was proved in Lemma 89 that $\setminus S_b\setminus[\ \ )l\quad 2+\setminus K_b\setminus$

Similarly, the proof of Lemma 89 shows that $K_b n_w^i h_t)\lambda+^{\subseteq 1}\to S_b$ if $2 \geq i \geq l\quad 3$. By the definition of S_b we have $K_b n_w^i n_w \to S_b$ if $1 \geq i \geq l\quad 4$ and $K_b n_w^i {n_w}^1 \to S_b$ if $2 \geq i \geq l\quad 3$.

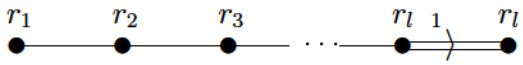
Using $w)\ r_1+[\ \ w)r_1+$and equation (4.5) we get that $n_w^i x\ _{r_1})2+n_w{}^i\ /\ K_b$ if $1 \geq i \geq l\ \ 3$ since $w^i)r_1+[\ \ r_1 0\ r_2 0\ \ldots 0\ r_{i+1}$ by equation (4.5). Hence $K_b n_w^i x\ _{r_1})2+[\ \ K_b n_w^i \to S_b$.

Equation (4.8) shows that $n_w^i x_s)2+n_w{}^i$ is in K_b if $2 \geq i \geq l\ \ 3$. Therefore $\cap_{i=1}^{l\ 2} K_b n_w^i [\ x_s)2+\longrightarrow S_b$. Finally, we conclude that $\partial)S_b+\longrightarrow K_b n_w{}^1 \cap K_b n_w^{l\ 1} \cap K_b h_t)\lambda+\cap K_b h_t)\lambda+{}^1 \cap K_b x_s)2+$

□

4.4.5 C_l

The Dynkin diagram is the following in this case:



It can easily be verified using the Dynkin diagram that $w_{l\ 1})r_l+[\ \ r_l 0\ 3r_{l\ 1}$ and $w_l)r_{l\ 1}+[\ \ r_{l\ 1} 0\ r_l$.

Using Lemma 83 one can see that $w)r_i+[\ \ r_{i+1}$ for $i\ [\ \ 2,3,\ldots,l\ \ 3$. We also have

$$w)r_{l\ 1}+[\ \ w_1 w_2 \ldots w_l)r_{l\ 1}+[\ \ w_1 w_2 \ldots w_{l\ 1})r_l 0\ r_{l\ 1}+$$
$$[\ \ w_1 w_2 \ldots w_{l\ 2})r_l 0\ r_{l\ 1}+$$

Since r_l is orthogonal to the remaining roots $r_1, r_2, \ldots, r_{l\ 2}$ we have

$$w)r_{l\ 1}+[\ \ r_l 0\ w_1 w_2 \ldots w_{l\ 2})r_{l\ 1}+$$

Since $w_i)r_{i+1} 0\ \ldots 0\ r_{l\ 1}+[\ \ r_i 0\ r_{i+1} 0\ \ldots 0\ r_{l\ 1}$ for $i\ [\ \ 2 \ldots l\ \ 3$ we also have

$$w_1 w_2 \ldots w_{l\ 2})r_{l\ 1}+[\ \ w_1 w_2 \ldots w_{l\ 3})r_{l\ 2} 0\ r_{l\ 1}+[\ \ r_1 0\ \ldots 0\ r_{l\ 2} 0\ r_{l\ 1}.$$

This gives $w)r_{l\ 1}+[\ \ r_1 0\ r_2 0\ \ldots 0\ r_l$.

Using all these observations we can determine a part of the orbit of $\rangle w|$ containing r_1, which is the following:

$$\rightarrow r_1 \xrightarrow{w} r_2 \xrightarrow{w} \dots \xrightarrow{w} r_{l\ 1} \xrightarrow{w} r_l\, 0\ r_{l\ 1}\, 0\ r_{l\ 2}\, 0\ \dots 0\ r_1 \rightarrow$$

Lemma 92. *$x_1)2+$, n_w and $h_{r_1})\lambda+$generate the Chevalley group G.*

Proof. The proof can be found in |Ste, Theorem 3.11|. □

The construction is almost the same as in the case A_l. Let

$$_c[\ \ Cay\ \ G, \}x_1)2+, x_1)\ \ 2+, n_w, n_w{}^1, h_{r_1})\lambda+, h_{r_1})\lambda+{}^1\langle[.$$

Let

$$K_c[\ \ \rangle X_{r_2}, X_{\ r_2}, X_{r_3}, X_{\ r_3}, \dots, X_{r_l}, X_{\ r_l}|$$

and let

$$S_c[\ \ \sqrt{\ }_{i=0}^{l\ \ 2} K_c n_w^i.$$

Lemma 93. $\frac{\partial(S_c)}{S_c} \geq \frac{6}{l\ \ 1}$

Proof. As in the previous cases, $n_w{}^i K_c n_w^i$ contains $n_w{}^i X_{r_{i+1}} n_w^i\ [\ \ X_{r_1}$ for $2 \geq i \geq l\ \ \ 3$ which gives that n_w^i is not in K_c if $2 \geq i \geq l\ \ \ 3$. This proves that $S_c[\ \ )l\ \ \ 2+K_c$

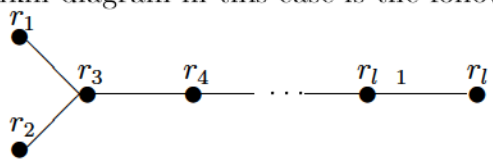
Again, $K_c n_w^i n_w \rightarrow S_c$ if $2 \geq i \geq l\ \ \ 4$ and $K_c n_w^i n_w{}^1 \rightarrow S_c$ if $i\ [\ \ 1$.

It is also easy to verify that $n_w^i x_1)2+\subseteq 1 n_w{}^i\ [\ \ )x_{i+1})u+\subseteq 1$ for some $u\ /\ GF)q+$. Therefore $n_w^i x_1)2+\subseteq 1 n_w{}^i\ /\ X_{r_{i+1}}$ and $n_w^i h_{r_1})\lambda+\subseteq 1 n_w{}^i$ are in the subgroup generated by $X_{r_{i+1}}$ and $X_{\ r_{i+1}}$ for $i\ [\ \ 2, \dots, l\ \ \ 3$. Thus the elements of the right cosets $K_c n_w^i x_1)2+\subseteq 1$ and $K_c n_w^i h_{r_1})\lambda+\subseteq 1$ are in S_c if $2 \geq i \geq l\ \ \ 3$. This proves that $\partial)S_c+\leq K_c n_w^l{}^1 \cap K_c n_w{}^1 \cap K_c x_1)2+\cap K_c x_1)2+{}^1 \cap K_c h_{r_1})\lambda+\cap K_c h_{r_1})\lambda+{}^1$, which is the union of 7 right cosets of K_c. Thus $\partial)S_c+\geq 7K_c$

□

4.4.6 D_l

The Dynkin diagram in this case is the following:



Lemma 94. *1.* $x_{r_1})2+, n_w$ *and* $h_{r_1})\lambda+$*generate the Chevalley group* G *if the rank of* G *is odd.*

2. $x_{\ r_1})2+, x_{r_1})2+, x_3)2+, n_w$ *and* $h_{r_1})\lambda+$*generate the Chevalley group* G *if the rank of* G *is even.*

Proof. The proof can be found in [Ste, Theorem 3.11 and Theorem 3.13]. □

First, we describe a part of the orbit of $\rangle w|$ which contains r_1. The root r_1 is orthogonal to $r_4, \ldots, r_l$ hence $w)r_1+[\ w_1w_2w_3)r_1+$so we have

$$w_1w_2w_3)r_1+[\ w_1w_2)r_1\,0\ r_3+[\ w_1)r_1\,0\ r_2\,0\ r_3+[\ r_1\,0\ r_2\,0\ r_3\,0\ r_1\ [\ r_2\,0\ r_3$$

and similarly

$$w)r_2+[\ w_1w_2w_3)r_2+[\ w_1w_2)r_2\,0\ r_3+[\ w_1)\ r_2\,0\ r_3\,0\ r_2+[\ r_3\,0\ r_1.$$

Using Lemma 83 we get $w)r_i+[\ r_{i+1}$ for $i\ [\ 4, \ldots, l\ 2$. This gives that both $w^i)r_1+$and $w^i)r_2+$are of the form

$$r_{i+2}\,0\ r_{i+1}\,0\ \ldots 0\ r_3\,0\ y, \tag{4.10}$$

where $y\ [\ r_1$ or $y\ [\ r_2$.

Odd case

Let us assume that l is odd.

Let

$$_d[\ \ Cay\ \ G,\}x_{r_1})2+,x_{r_1})2+^1,n_w,n_w{}^1,h_{r_1})\lambda+,h_{r_1})\lambda+^1\langle[.$$

Let

$$K_d[\ \ \rangle X_{r_1},X_{\ r_1},X_{r_2},X_{\ r_2},\ldots,X_{r_{l-1}},X_{\ r_{l-1}}|$$

and let

$$S_d[\ \ \sqrt[l\ \ 3]{\ }_{i=0}K_dn_w^i.$$

Lemma 95. $\frac{\setminus\partial(S_d)\setminus}{\setminus S_d\setminus}\geq\frac{2}{l\ \ 2}$

Proof. It is clear that if $1\geq i\geq l\ \ \ 4$, then $n_w^ix_{r_1})2+\subset^1n_w{}^i[\ \ x_{w^i(r_1)})u+\subset^1\ /K_d$ for some $u\ /GF)q+\neq$ since by (4.10) the root $w^i)r_1+$is a linear combination with integer coefficients of the fundamental roots $r_1,r_2,\ldots,r_{l\ \ 1}$ and similarly $n_w^ih_{r_1})\lambda+\subset^1n_w{}^i\ /K_d$. It follows that $\partial)S_d+\leq K_dn_w^{l\ \ 2}\cap K_dn_w{}^1$.

It remains to show that S_d is the union of $l\ \ \ 4$ pairwise disjoint cosets of K_d. Again, $n_w^iK_dn_w{}^i$ contains the subgroup $n_w^iX_{r_{l-i}}n_w{}^i[\ \ X_{r_l}$ if $2\geq i\geq l\ \ \ 4$ which shows that $n_w^i\ /K_d$.

□

Even case

Let us assume that l is even.

Let

$$_d^\infty[\ \ Cay\ \ G,\}x_{\ r_1})\circ 2+,x_{\ r_1})\circ 2+,x_{r_3})\circ 2+,n_w,n_w{}^1,h_{r_1})\lambda+,h_{r_1})\lambda+^1\langle[.$$

Let

$$K_d^\infty[\ \ \rangle X_{r_1},X_{\ r_1},X_{r_2},X_{\ r_2},\ldots,X_{r_{l-1}},X_{\ r_{l-1}}|$$

and let

$$S_d^{\infty}[\bigvee_{i=0}^{l\ 4} K_d^{\infty} n_w^i.$$

Lemma 96. $\frac{\partial(S'_d)}{S'_d} \geq \frac{2}{l\ 3}$

Proof. It is clear that $w^i)\ \ r_1+[\ \ w^i)r_1+$and hence $w^i)\ \ r_1+$is in the root system generated by the roots $r_1, r_2, \ldots, r_{l\ 1}$ if $2 \geq i \geq l\ \ 5$. This shows that $n_w^i x_{\subseteq r_1})\circ 2+n_w{}^i\ [\ \ x_{w^i(\subseteq r_1)})u+/\ K_d^{\infty}$for some $u\ /\ GF)q+$.

It was proved in Lemma 95 that $n_w^i h_{r_1})\lambda+^{\subseteq 1} n_w{}^i\ /\ K_d^{\infty}$if $1 \geq i \geq l\ \ 5$. Finally, by Lemma 83 $n_w^i x_{r_3})\circ 2+n_w{}^i\ [\ \ x_{r_{3+i}})t+$for some $t\ /\ K^{\pm}$ which is in K_d^{∞}if $1 \geq i \geq l\ \ 5$. It follows that $\partial)S_d^{\infty}+\leq K_d^{\infty} n_w^{l\ 3} \cap K_d^{\infty} n_w{}^1$.

It remains to show that $S_d^{\infty}$is the union of $l\ \ 4$ pairwise disjoint cosets of K_d^{∞}. This is clear since if $2 \geq i \geq l\ \ 5$, then $n_w^i K_d^{\infty} n_w{}^i$ contains the subgroup X_{r_l} which shows that $n_w^i\ /\ K_d^{\infty}$.

□

4.4.7 Twisted groups

The twisted groups can be obtained as subgroups of Chevalley groups. In order to define twisted groups we need to find a non-trivial symmetry ρ of the Dynkin diagram. We restrict our attention to those twisted groups which are defined using a symmetry of order 3 and we also assume that the roots in Ω have the same length. It is well known that such a symmetry ρ can be extended to a unique isometry τ of the vector space spanned by Ω. We assume that $Aut)K+$contains an element f of order 3, where $K\ [\ \ GF)q+$. Then the Chevalley group G has an automorphism of order 3, which we denote by α such that $x_r)k+^{\alpha}\ [\ \ x_{\overline{r}})\overline{k}+$for every $r\ /\ \circ\ \Phi$ and $k\ /\ K$, where $\overline{k}\ [\ \ f)k+$and $\overline{r}\ [\ \ \tau)r+$. Furthermore, $x_r)k+^{\alpha}\ [\ \ x_{\overline{r}})\gamma_r\overline{k}+$for every $r\ /\ \Omega$ and $k\ /\ K$ with $\gamma_r\ [\ \ \circ\ 2$.

Let U be the subgroup of G generated by the elements $x_r)t+$for all $r \,/\, \Omega^+$ and $t \,/\, K$ and let V be generated by the elements $x_r)t+$for all $r \,/\, \Omega$ and $t \,/\, K$. The subgroup U^1 is the set of elements $u \,/\, U$ such that $u^\alpha \,[\, u$ and similarly $V^1 \,[\, \}v \,/\, V \setminus v^\alpha \,[\, v\langle$. The twisted group G^1 is generated by U^1 and V^1. The subgroups H^1 and N^1 are defined as the intersection of G^1 with H and N, respectively, where H and N are defined in Section 4.4.1. We denote by W^1 the elements w of the Weyl group W such that $\tau w \tau^{\,1} \,[\, w$. There is a natural isomorphism of the group W^1 to N^1/H^1 and we denote by n_w^1 an element of $N^1 \geq N$ which corresponds to $w^1 \,/\, W^1$.

The set of positive roots Ω^+ has a partition where the elements of the partition are of the following form:

$$
\begin{aligned}
&Z \,[\, \}r \setminus r \,/\, \Omega^+ \text{ and } \overline{r} \,[\, r\langle \\
&Z \,[\, \}r, \overline{r} \setminus r \,/\, \Omega^+ \text{and } r \,0\, \overline{r} \,/\, \Omega\langle \\
&Z \,[\, \}r, \overline{r}, r \,0\, \overline{r} \setminus r \,/\, \Omega^+ \text{and } r \,0\, \overline{r} \,/\, \Omega\langle\,.
\end{aligned}
$$

We denote by Φ^1 the collection of sets which are elements of the partition. For each set Z in the partition there is a unique element $w_Z \,/\, W^1$, which is an element of the subgroup generated by w_r for $r \,/\, Z$, such that $w_Z)Z+[\quad Z$. These elements are the following:

$$
\begin{aligned}
&w_Z \,[\, w_r \text{ if } Z \,[\, \}r \setminus r \,/\, \Omega^+ \text{ and } \overline{r} \,[\, r\langle \\
&w_Z \,[\, w_r w_{\overline{r}} \text{ if } Z \,[\, \}r, \overline{r} \setminus r \,/\, \Omega^+ \text{and } r \,0\, \overline{r} \,/\, \Omega\langle \\
&w_Z \,[\, w_{r+\overline{r}} \,[\, w_r w_{\overline{r}} w_r \text{ if } Z \,[\, \}r, \overline{r}, r \,0\, \overline{r} \setminus r \,/\, \Omega^+ \text{and } r \,0\, \overline{r} \,/\, \Omega\langle\,.
\end{aligned}
$$

Every element of Φ^1 can be obtained as $w)Z+$, where $w \,/\, W^1$ and Z contains a fundamental root. Those sets which contain a fundamental root are called fundamental sets. Moreover, W^1 is generated by $\}w_Z \setminus Z \,/\, \Phi^1\langle$.

For every $Z \,/\, \Phi^1$ we denote by X_Z the subgroup generated by the root subgroups X_r for $r \,/\, Z$, and we set $X_Z^1 \,[\, X_Z \,\{\, G^1$.

4.4.8 ${}^2A_{2n\ 1}$

The fundamental sets in this case are the following:

$$Z_n [\ \}r_n\langle\ ,\ Z_i [\ \}r_i, r_{2n\ i}\langle \text{ for } 2 \geq i \geq n\quad 2,$$

and the corresponding elements of the Weyl group W^1 are:

$$w_{Z_n} [\ \ w_n, \text{ and } w_{Z_i} [\ \ w_i w_{2n\ i} \text{ for } 2 \geq i \geq n\quad 2.$$

We may assume (see [Car, p.233]) that the subgroups defined above are of the following form:

$$X^1_Z [\ \}x_r)t+\backslash t [\ \bar{t}\langle \text{ if } Z [\ \}r\langle$$
$$X^1_Z [\ \}x_r)t+x_{\overline{r}})\bar{t}+\backslash t\ /\ K\langle \text{ if } Z [\ \}r, \overline{r}\langle.$$

Let $n^1_w [\ \ n_{w^1_1} n_{w^1_2} \ldots$ and $h_e [\ \ h_{r_1})\lambda+h_{\overline{r_1}})\overline{\lambda}+$ where λ generates the multiplicative group of the finite field $K [\ GF)q+$ In the following in order to simplify notation we write n_w instead of n^1_w.
We also define $x_e [\ \ x_{r_1})2+x_{r_{2n-1}})2+$which is an element of $X^1_{Z_1}$ and which can also be written as $x_{r_1})2+x_{r_1})2+^{\alpha} [\ \ x_{r_1})2+x_{\overline{r_1}})2+$

Lemma 97. *x_e, n_w and h_e generate the group G^1.*

Proof. The proof can be found in [Ste, Theorem 4.1]. □

Let

$${}_e [\ \ Cay\ \ G, \}x_e, x_e{}^1, n_w, n_w{}^1, h_e, h_e{}^1\langle [.$$

Let

$$K_e [\ \ \rangle X^1_{Z_2}, X^1{}_{Z_2}, X^1_{Z_3}, X^1{}_{Z_3}, \ldots, X^1_{Z_n}, X^1{}_{Z_n}|$$

and let

$$S_e [\ \ \sqrt{\ }_{i=0}^{n\ \ 2} K_e n^i_w.$$

K_e can be considered as a twisted group which is a subgroup of the Chevalley group generated by the root subgroups $X_{r_2}, X_{r_2}, \ldots, X_{r_{2n-2}}, X_{r_{2n-2}}$. The corresponding set of fundamental roots is ρ-invariant and we denote by Ω_{2n-3} the root system generated by these roots. The restriction of ρ to the set $\{r_2, r_3, \ldots, r_{2n-2}\}$ gives a symmetry of the Dynkin diagram of these roots which extends to an isometry. This isometry is the restriction of τ. This gives that for $Z \subset \Phi^1$ the subgroup X_Z^1 is a subgroup of K_e if and only if $Z \subset \Omega_{2n-3}$. Clearly, $h_r(t)$is in $\langle X_Z^1, X^1{}_Z \rangle \subset G^1$ if $Z \cap \{r\}$ with $r \cap \overline{r}$. If $Z \cap \{r, \overline{r}\}$, then there is a homomorphism of $SL_2(K)$onto $\langle X_Z^1, X^1{}_Z \rangle \subset G^1$ which shows that $x_r(t)x_{\overline{r}}(\overline{t}) \in G^1$ and $h_r(t)h_{\overline{r}}(\overline{t}) \in G^1$.

Conjugating by $n_w^i \in N^1$ we get the following:

$$n_w{}^i X_Z^1 n_w^i \cap n_w{}^i) X_Z \subset G^1) n_w^i \cap n_w{}^i X_Z n_w^i \subset n_w{}^i G^1 n_w^i \cap X_{w^{-i}(Z)} \subset G^1 \cap X^1_{w^{-i}(Z)}. \tag{4.11}$$

Lemma 98. $\frac{|\partial(S_e)|}{|S_e|} \geq \frac{6}{n-1}$

Proof. We claim that S_e is the union of $n-2$ disjoint subsets. $K_e n_w^j \cap K_e n_w^{j'}$ if and only if $n_w^{j-j'} \in K_e$ so we have to show that $n_w^i \notin K_e$ if $2 \geq i \geq n-3$. We claim that $w^i)r_1 \in \{r_{i+1}$ if $2 \geq i \geq n-3$. If $k \geq n-4$, then

$$w)r_k \in \{w_1 w_{2n-1} \ldots w_k w_{2n-k} w_{k+1})r_k \in$$

since r_k is orthogonal to r_j if $j \sim k \pm 3$. Therefore

$$\begin{aligned} w)r_k \in \{w_1 w_{2n-1} \ldots w_k)r_k \pm r_{k+1} \in \\ \cap w_1 w_{2n-1} \ldots w_{k-1})r_{k+1} \in \{r_{k+1} \end{aligned}$$

since r_{k+1} is orthogonal to the roots $r_{2n-k}, \ldots, r_{2n-1}$ and r_{k+1} is orthogonal to $r_1, \ldots, r_{k-1}$. It follows that $w^{-i})Z_{i+1} \in \{Z_1$ and hence by equation (4.11) $X_{Z_1}^1 \subset n_w{}^i K_e n_w^i$ if $2 \geq i \geq n-3$. This proves that $n_w^i \notin K_e$ if $2 \geq i \geq n-3$ hence $|S_e| \cap (n-2)|K_e|$

It is easy to see that S_e contains $K_e n_w^i n_w$ if i [$1, 2, \ldots, n \quad 4$ and S_e contains $K_e n_w^i n_w{}^1$ if i [$2, 3, \ldots, n \quad 3$.

We use again the fact that $K_e n_w^i g$ [$K_e n_w^i$ if and only if $n_w^i g n_w{}^i$ / K_e. Since $n_w^i x_{r_1})2 + n_w{}^i$ [$x_{w^i(r_1)})\xi+$for some ξ / K and x_e [$x_{r_1})2 + x_{r_1})2 +^\alpha$ we have

$$n_w^i x_{r_1})2 + x_{r_1})2 +^\alpha n_w{}^i \; [\; n_w^i x_{r_1})2 + n_w{}^i n_w^i x_{r_1})2 +^\alpha n_w{}^i$$
$$[\; n_w^i x_{r_1})2 + n_w{}^i) n_w^i x_{r_1})2 + n_w{}^i +^\alpha \; [\; x_{w^i(r_1)})\xi + x_{w^i(r_1)})\xi +^\alpha \; [\; x_{r_{i+1}})\xi + x_{r_{i+1}})\xi +^\alpha.$$

This shows that $n_w^i x_e n_w{}^i$ / $X^1_{Z_{i+1}}$ which proves that if i [$2, 3, \ldots, n \quad 3$, then $n_w^i x_e^{\subseteq 1} n_w{}^i$ / K_e and hence $K_e n_w^i x_e^{\subseteq 1}$ [$K_e n_w^i$ since $Z_{i+1} \to \Omega_{2n \; 3}$.

We also have $n_w^i h_{r_1})\lambda + h_{\overline{r_1}})\overline{\lambda} + n_w{}^i$ [$h_{r_{i+1}})\theta + h_{w^i(\overline{r_1})})\theta^\infty +$for some θ, θ^∞/ K. Using the fact that w / W^1 we have $w^i)\overline{r_1}+$[$\overline{w^i)r_1}+$so $h_{r_{i+1}})\theta + h_{w^i(\overline{r_1})})\theta^\infty +$[$h_{r_{i+1}})\theta + h_{\overline{r_{i+1}}})\theta^\infty +$. Clearly, $n_w^i h_e n_w{}^i$ / H^1. Thus θ^∞[$\overline{\theta}$ and $n_w^i h_e^{\subseteq 1} n_w{}^i$ [$\Big) h_{r_{i+1}})\theta + h_{\overline{(r_{i+1})}})\overline{\theta} + \Big(^{\subseteq 1}$ / K_e since r_{i+1} / $\Omega_{2n \; 3}$ if i [$2, \ldots, n \quad 3$. This proves that $K_e n_w^i h_e^{\subseteq 1}$ [$K_e n_w^i$ if i [$2, \ldots, n \quad 3$ and hence $\partial) S_e + \longrightarrow K_e n_w^n{}^1 \cap K_e n_w{}^1 \cap K_e x_e \cap K_e x_e{}^1 \cap K_e h_e \cap K_e h_e{}^1$, finishing the proof of Lemma 98.

□

4.4.9 ^2D_n

The fundamental sets in this case are the following:

$$Z_1 \; [\; \}r_1, r_2\langle\,, \; Z_i \; [\; \}r_{i+1}\langle \text{ for } 3 \geq i \geq n \quad 2,$$

and the corresponding elements of the Weyl group W^1 are:

$$w_{Z_1} \; [\; w_1 w_2, \text{ and } w_{Z_i} \; [\; w_{i+1} \text{ for } 3 \geq i \geq n \quad 2.$$

Let n_w [$n_{w_1^1} n_{w_2^1} \ldots n_{w_{n-1}^1}$ and h_f [$h_{r_1})\lambda + h_{\overline{r_1}})\overline{\lambda}+$, where λ generates $K^\pm$. We also define x_f [$x_{r_1})2 + x_{r_2})2+$which can also written as $x_{r_1})2 + x_{r_1})2 +^\alpha$ [$x_{r_1})2 + x_{\overline{r_1}})2+$

Lemma 99. *x_f, n_w and h_f generate the group G^1.*

Proof. The proof can be found in [Ste, Theorem 4.1]. □

Let

$$_f = Cay(G, \{x_f, x_f^{-1}, n_w, n_w^{-1}, h_f, h_f^{-1}\}).$$

Let

$$K_f = \{X^1_{Z_1}, X^{-1}{}_{Z_1}, X^1_{Z_2}, X^{-1}{}_{Z_2}, \ldots, X^1_{Z_{n-2}}, X^{-1}{}_{Z_{n-2}}\}$$

and let

$$S_f = \bigcup_{i=0}^{n-3} K_f n_w^i.$$

We denote by Ω_{n-1} the root system generated by the fundamental roots $r_1, r_2, \ldots, r_{n-1}$.

Lemma 100. $\frac{|\partial(S_f)|}{|S_f|} \geq \frac{2}{n-2}$

Proof. The Coxeter element in this case is exactly the same as in Section 4.4.6. This gives that $n_w^i(r_{n-i}) = r_n$ for $1 \leq i \leq n-4$. The fundamental sets $Z_2, Z_3, \ldots, Z_{n-1}$ consist of only one element thus $n_w^i S_f n_w^{-i}$ contains $X^1_{w^i(Z_{n-1-i})} = X_{w^i(r_{n-i})} = X_{r_n} = X^1_{Z_{n-1}}$ if $2 \leq i \leq n-4$ since S_f contains X^1_{n-i}. This proves that if $2 \leq i \leq n-4$, then $n_w^i \in K_f$. Thus S_f is the union of $n-3$ disjoint subsets of the same cardinality. Therefore $|S_f| = (n-3)|K_f|$

Using the definiton of S_f one can see that $K_f n_w^i n_w \subseteq S_f$ if $i = 1, \ldots, n-5$ and $K_f n_w^i n_w^{-1} \subseteq S_f$ if $i = 2, \ldots, n-4$.

The elements $n_w^i x_f n_w^{-i}$ are of the form $x_r(t)x_{\bar{r}}(-\bar{t})$ for some $r \in \Omega$ and $t \in K^{\pm}$. In order to prove that these elements are in K_f for $i = 1, 2, \ldots, n-4$ we only have to show that $r \in \Omega_{n-1}$. Using the fact that the Coxeter element in this case is the same as in Section 4.4.6 we have that both $w^i(r_1)$ and $w^i(r_2)$ are of the form $r_1 + r_3 + r_4 + \ldots + r_{i+1}$ or $r_2 + r_3 + r_4 + \ldots + r_{i+1}$. These roots are clearly in the root system generated by the fundamental roots $r_1, r_2, \ldots, r_{l-1}$

if $i \geq n$ 3. This proves that $n_w^i x_f^{\subseteq} n_w{}^i$ is in K_f if $1 \geq i \geq n$ 4 and hence $S_f x_f^{\subseteq} \to S_f$.

Similarly, the elements $n_w^i h_f n_w{}^i$ are of the form $h_r)t+\overline{h_r})\overline{t}+$for some $r \ / \ \Omega$ and $t \ / \ K^{\pm}$and it is easy to see that $r \ / \ \Omega_{n\ 1}$ if $1 \geq i \geq n$ 4. This proves that $n_w^i h_f^{\subseteq} n_w{}^i$ is in K_f if $1 \geq i \geq n$ 4 and hence $S_f h_f^{\subseteq} \to S_f$.

Therefore $\partial)S_f+\leq K_f n_w^{n\ 2} \cap K_f n_w{}^1$, which shows that $\frac{\backslash \partial(S_f) \backslash}{\backslash S_f \backslash} \geq \frac{2 \backslash K_f \backslash}{(n\ 2) \backslash K_f \backslash}$, finishing the proof of Lemma 100.

□

4.4.10 $^2A_{2n}$

The fundamental sets are the following:

$$Z_1 [\ \} r_n, r_{n+1}, r_n\, 0\ r_{n+1}\langle\ ,\ Z_i [\ \} r_{n+1\ i}, r_{n+i}\langle\ \text{for } 3 \geq i \geq n.$$

Let $n_w^1 [\ n_{w_1^1} n_{w_2^1} \dots n_{w_n^1}$ and $h_g [\ h_{r_n})\lambda+\overline{h_{r_n}})\overline{\lambda}+$ where λ generates $K^{\pm}$. We also define $x_g [\ x_{r_n})2+x_{r_{n+1}})2+x_{r_n+r_{n+1}})k+$with $k\, 0\ \overline{k} [\ 2$.

Lemma 101. *x_g, n_w and h_g generate the group G^1.*

Proof. The proof can be found in [Ste, Theorem 4.1].

□

Let

$$_g [\ Cay\ G, \} x_g, x_g{}^1, n_w, n_w{}^1, h_g, h_g{}^1 \langle [\ .$$

Let

$$K_g [\ \rangle X_{Z_1}^1, X^1{}_{Z_1}, X_{Z_2}^1, X^1{}_{Z_2}, \dots, X_{Z_{n-1}}^1, X^1{}_{Z_{n-1}} |$$

and let

$$S_g [\ \sqrt{}_{i=0}^{n\ 2} K_g n_w^i.$$

Lemma 102. $\frac{\backslash \partial(S_g) \backslash}{\backslash S_g \backslash} \geq \frac{2}{n\ 1}$

Proof. First, we show that S_g is the union of $n \quad 2$ disjoint subsets of the same cardinality. It is enough to show that $n_w^i \not/ K_g$ for $i [\quad 2, \dots, n \quad 3$. This will be done by proving that $X_{Z_n}^1$ is contained in $n_w^i K_g n_w{}^i$. Using equation (4.11) we only have to show that $w^i) Z_{n \ i} + [\quad Z_n$ for $i [\quad 2, \dots n \quad 3$.

The fundamental root r_{k+1} is contained in $Z_{n \ k}$. Let us assume that $2 \geq k \geq n \quad 3$.

$$\begin{aligned} w) r_{k+1} + [\quad & w_n w_{n+1} w_n w_{n \ 1} w_{n+2} \dots w_1 w_{2n}) r_{k+1} + \\ [\quad & w_n w_{n+1} w_n w_{n \ 1} w_{n+2} \dots w_{k+1} w_{2n \ k} w_k) r_{k+1} + \end{aligned}$$

since r_{k+1} is orthogonal to the roots r_j if $j > n$ or $j < k \quad 2$. Clearly, $w_{k+1} w_{2n \ k} w_k) r_{k+1} + [\quad r_k$ so

$$w) r_{k+1} + [\quad w_n w_{n+1} w_n \dots w_{k+2} w_{2n \ k \ 1}) r_k + [\quad r_k$$

since the remaining reflections fix r_k.

One can see by induction that $w^i) r_{i+1} + [\quad r_1$ for $i [\quad 2, \dots n \quad 3$ and since $w \not/ W^1$ we have $w^i) \overline{r_{i+1}} + [\quad \overline{w^i) r_{i+1}} + [\quad r_{2n}$ and hence $w^i) Z_{n \ i} + [\quad Z_n$. This proves that for $i [\quad 2, \dots, n \quad 3$ the subgroup $n_w^i) K_g + n_w{}^i$ contains $X_{Z_n}^1$. Therefore $\backslash S_g \backslash [\quad) n \quad 2 + \backslash K_g \backslash$.

The definition of S_g shows that $K_g n_w^i n_w \to S_g$ if $i \{ \quad n \quad 3$ and $K_g n_w^i n_w{}^1 \to S_g$ if $i \{ \quad 1$. It remains to investigate the elements of the form $n_w^i x_{\overline{g}}^{\subset} n_w{}^i$ and $n_w^i h_{\overline{g}}^{\subset} n_w{}^i$.

We claim that $w^i) r_n + [\quad r_n \, 0 \ r_{n \ 1} \, 0 \ \dots \, 0 \ r_{n \ i}$ if $i \geq n \quad 3$. Using the orthogonality of the fundamental roots r_j, r_k, where $\backslash j \quad k \backslash \sim 3$ we get the following:

$$\begin{aligned} w) r_n + [\quad & w_n w_{n+1} w_n w_{n \ 1} w_{n+2} \dots w_1 w_{2n}) r_n + \\ [\quad & w_n w_{n+1} w_n w_{n \ 1}) r_n + [\quad w_n w_{n+1}) r_{n \ 1} + [\quad r_{n \ 1} \, 0 \ r_n. \end{aligned} \tag{4.12}$$

Similarly, if $2 \geq k \geq n \quad 3$, then

$$\begin{aligned} w)r_{n\ k}+[\ & w_n w_{n+1} w_n w_{n\ 1} w_{n+2} \dots w_1 w_{2n})r_{n\ k}+ \\ [\ & w_n w_{n+1} w_n \dots w_{n\ k} w_{n+k+1} w_{n\ k\ 1})r_{n\ k}+ \\ [\ & w_n w_{n+1} w_n \dots w_{n\ k+1})r_{n\ k\ 1}+[\ r_{n\ k\ 1}. \end{aligned} \tag{4.13}$$

Since w is linear we get using (4.12) and (4.13) that

$$w^i)r_n+[\ r_n\, 0\ r_{n\ 1}\, 0\ \dots 0\ r_{n\ i}. \tag{4.14}$$

From equation (4.14) one can see that if i [$1, \dots, n \quad 3$, then both r_1 and r_{2n} are orthogonal to $w^i)r_n+$, and similarly r_1 and r_{2n} are orthogonal to $w^i)r_{n+1}+[\ w^i)\overline{r_n}+[\ \overline{w^i)r_n}+[\ r_{n+i+1}$. This shows that for

$$w^{\propto}[\ w_n w_{n+1} w_n w_{n\ 1} w_{n+2} \dots w_2 w_{2n\ 1}$$

we have $w^i)r_n+[\ )w^{\propto i})r_n+$and $w^i)r_{n+1}+[\ )w^{\propto i})r_{n+1}+$. Therefore $w^i)r_n\, 0\ r_{n+1}+[\ )w^{\propto i})r_n\, 0\ r_{n+1}+$. Moreover, $n^i_w x_g n_w{}^i$ [$n^i_{w'} x_g n_{w'}{}^i$ and $n^i_w h_g n_w{}^i$ [$n^i_{w'} h_g n_{w'}{}^i$.

Clearly, $n_{w'}$ / K_g and hence the elements $n^i_{w'} x_{\overline{g}}^{\subset} n_{w'}{}^i$ and $n^i_{w'} h_{\overline{g}}^{\subset} n_{w'}{}^i$ are in K_g if i [$1, 2, \dots, n \quad 3$.

□

In order to finish the proof of Theorem 82 we have to verify that for those sets S for which the boundary $\partial)S+$is relatively small we have $\backslash S\backslash \geq \frac{\backslash G\backslash}{2}$. The order of the investigated simple groups is the following:

$$\begin{aligned} A_l)q+= & \quad \tfrac{1}{(l+1,q\ 1)} q^{\frac{l(l-1)}{2}} \textstyle\bigcup_{i=1}^{l})q^{i+1} \quad 2+ \\ B_l)q+= & \quad \tfrac{1}{(2,q\ 1)} q^{l^2} \textstyle\bigcup_{i=1}^{l})q^{2i} \quad 2+ \\ C_l)q+= & \quad \tfrac{1}{(2,q\ 1)} q^{l^2} \textstyle\bigcup_{i=1}^{l})q^{2i} \quad 2+ \\ D_l)q+= & \quad \tfrac{1}{(4,q^l\ 1)} q^{\frac{l(l-1)}{2}} \textstyle\bigcup_{i=1}^{l})q^{2i} \quad 2+ \\ {}^2A_l)q^2+= & \ \tfrac{1}{(l+1,q+1)} q^{\frac{l(l-1)}{2}} \textstyle\bigcup_{i=1}^{l}\Big)q^{i+1} \quad) \quad 2+^{i+1}\Big(\\ {}^2D_l)q^2+= & \ \tfrac{1}{(4,q^l+1)} q^{l(l\ 1)} \quad q^l\, 0\ 2[\textstyle\bigcup_{i=1}^{l})q^{2i} \quad 2+ \end{aligned}$$

It is easy to see that such a simple group cannot have a subgroup of index at most $3l$, finishing the proof of Theorem 82.

4.4.11 Identification

In this section we give explicit generators of the groups that we investigated in Sections 4.4.2 and 4.4.7. We also show how to find the subsets of the vertices S for which $\partial)S+$is relatively small. We only handle the case of special linear groups which can easily be transformed to the case of the projective special linear groups which is clearly the easiest one. This example includes the original idea which was extended to several different series of simple groups. In order to show the simplicity of the original construction we forget about the machinery which was built up before.

Let

$$A_l\,[\,\left(\begin{array}{ccccc} 2 & 2 & & & \\ & 2 & & & \\ & & 2 & & \\ & & & \ddots & \\ & & & & 2 \end{array}\right)^{\wr},$$

where $A_l\ /\ GF)q+^{(l+1)*\,(l+1)}$. Let

$$B_l\,[\,\left(\begin{array}{ccccccc} 1 & 1 & 1 & \dots & 1 & 1 &) \\ 2 & 1 & 1 & \dots & 1 & 1 & 1 \\ 1 & 2 & 1 & \dots & 1 & 1 & 1 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots \\ 1 & 1 & \dots & 2 & 1 & 1 & 1 \\ 1 & 1 & \dots & 1 & 2 & 1 & 1 \\ 1 & 1 & \dots & 1 & 1 & 2 & 1 \end{array}\right)^{2+l\wr}.$$

We denote by C_l the diagonal matrix $diag)\frac{1}{\lambda}, \lambda, 2, 2, \dots, 2+/\ GF)q+^{(l+1)*\,(l+1)}$, where λ generates $GF)q+^{\pm}$.

We denote by $e_{i,j}$ the matrix with 2 in the (i,j)-th position and zeros everywhere else and let $T_{i,j}(\delta) = I + \delta e_{i,j}$, where I denotes the identity matrix and $\delta \in K$. Using this notation we can write $A_l = T_{1,2}(1)$.

The standard generator $x_{r_1}(1)$ of the Chevalley group given in Section 4.4.3 corresponds to the matrix A_l and the Coxeter element n_w can be identified with B_l. Finally, C_l plays the role of $h_{r_1}(\lambda)$.

Clearly, $T_{i,j}(\alpha)T_{i,j}(\beta) = T_{i,j}(\alpha+\beta)$ and $[T_{i,j}(\alpha), T_{j,k}(\beta)] = T_{i,k}(\alpha\beta)$ if $i \neq k$, where $[g,h] = g^{-1}h^{-1}gh$ denotes the commutator of g and h.

Lemma 103. *For every $l \in \mathbb{N}$ the set $\{A_l, B_l, C_l\}$ forms a generating set of $SL(l, 2, q)$.*

Proof. We fix the size of the matrices and hence we can write $A = A_l$, $B = B_l$ and $C = C_l$. Let $H = \langle A, B, C\rangle$. It is enough to verify that $T_{i,j}(\delta) \in H$ for every $i \neq j$ and $\delta \in GF(q)$.

It is easy to see that $A^{C^k} = T_{1,2}(1)^{C^k} = T_{1,2}(\lambda^{2k})$. Using $T_{1,2}(\alpha)T_{1,2}(\beta) = T_{1,2}(\alpha+\beta)$ we get that $T_{1,2}(\delta) \in \langle A, C\rangle \leq H$ for every $\delta \in GF(q)$. For $i \neq j$ we have $B^k T_{i,j}(\delta) B^{-k} = T_{i+k,j+k}(\delta)$, where the indices are taken modulo l and hence $T_{i,i+1}(\delta) \in H$ for every $2 \geq i \geq l$ and for every $\delta \in GF(q)$. This implies that for every $2 < l \geq l$ and for every $\delta \in GF(q)$

$$[\ldots[[T_{1,2}(\delta), T_{2,3}(1)], T_{3,4}(1)], \ldots, T_{l-1,l}(1)] = T_{1,l}(\delta) \in H.$$

Using again the fact that $B^k T_{1,l}(\delta) B^{-k} = T_{1+k,l+k}(\delta)$ we get that $T_{i,j}(\delta) \in H$ for every $i \neq j$ and for every $\delta \in GF(q)$.

□

Let

$$S_0 = \left\{ \begin{pmatrix} D & 1 \\ 1 & 2 \end{pmatrix} \in SL(l, 2, q) \mid D \in SL(l, q) \right\}.$$

For every $2 \geq i \geq l$ we define

$$S_i = S_0 B^i.$$

Finally, let

$$S [\sqrt[l]{\prod_{i=0}^{1} S_i}.$$

It is easy to see that $\backslash S \backslash < \frac{\backslash SL(l+1,q) \backslash}{2}$ if $l \sim 2$.

Lemma 104. $\frac{\backslash \partial(S) \backslash}{\backslash S \backslash} \geq \frac{6}{l}$

Proof. Every element of S has exactly l columns with 1 in the last row, and exactly 2 column with 1 in the first l rows and 2 in the last row. The sets S_i are pairwise disjoint since an invertible matrix can not have a column with only zero entries. Furthermore, they all have the same cardinality since S_0 is a subgroup of $SL)l\,0\ \ 2, q+$and S_i are right cosets of S_0 in $SL)l\,0\ \ 2, q+$

It is easy to see that $SB \wr\ S \leq S_0 B^l [\ \ S_l$ and $SB\ ^1 \wr\ S \leq S_0 B\ ^1$. The remaining elements of $\partial)S+$are of the form MA, MC and $MA\ ^1$, $MC\ ^1$ where $M\ /\ S$.

Let us assume that $M\ /\ S_i$. Then

$$M [\left)\begin{matrix} D & 1 & D^{\infty} \\ 1 & 2 & 1 \end{matrix}\right[$$

for some $D\ /\ GF)q\frac{l}{+}^{l\ \ i}$ and $D^{\infty}/\ GF)q\frac{l}{+}^{i}$. Multiplying a matrix M by A or $A\ ^1$ from the right only modifies the second column of M. Therefore if $M\ /\ S_i$ with $i \{\ \ l, l\ \ \ 2$, then it is easy to see that $MA, MA\ ^1\ /\ S_i$.

Multiplying a matrix M by C or $C\ ^1$ from the right only modifies the first and the second columns of M thus if $M\ /\ S_i$ with $i \{\ \ l, l\ \ \ 2$, then $MC^{\subseteq 1}\ /\ S_i$.

This gives that $\partial)S+\leq S_l \cap S_0 B\ ^1 \cap S_l\ _1 A \cap S_l\ _1 A\ ^1 \cap S_l\ _1 C \cap S_l\ _1 C\ ^1$ since $S [\ \ \cap_{i=0}^{l}\ ^1 S_i$.

□

BIBLIOGRAPHY

[Alo] N. Alon. Eigenvalues and expanders. Combinatorica, **6** (2) (1986), 83-96.

[A,C] N. Alon, F. R. K. Chung, Explicit construction of linear sized tolerant networks, Discrete Math. **72** (1988), 15-19. **1** (2) (2004), 151-163 .

[A,N] B. Alspach, L. A. Nowitz, Elementary Proofs that Z_p^2 and Z_p^3 are CI-groups, Eur. J. Combin. **20** (1999), 607-617.

[A,P] B. Alspach, T. D. Parsons, Isomorphism of circulant graphs and digraphs, Discrete Math. **25** (1979), 97-108.

[Ádá] A. Ádám, Research Problem 2-10, J. Combin. Theory, **2** (1967), 393.

[Bab1] L. Babai, Isomorphism problem for a class of point-symmetric structures, Acta Math. Acad. Sci. Hungar. **29** (1977), 329-336.

[Bab2] L. Babai, On a conjecture of M. E. Watkins on graphical regular representations of finite groups, Comp. Math, **37** 3 (1978), 291-296.

[Bab3] L. Babai, Finite digraphs with given regular automorphism groups, Period. Math. Hungar. **11** (1980), 257-270.

[Bab4] L. Babai, Infinite digraphs with given regular automorphism groups, J. Combin. Theory, **25** (1978), 26-46.

[B,F1] L. Babai, P. Frankl, Isomorphisms of Cayley graphs I, Colloqzeria Mathematica Societatis János Bolyai, **18** Combin. Keszthely, 1976, North-Holland, Amsterdam (1978), 35-52.

[B,F2] L. Babai, P. Frankl, Isomorphisms of Cayley graphs II, Acta Math. Acad. Sci. Hung. **34** (1979), 177-183.

[B,G] L. Babai, C. Godsil, On the Automorphism Groups of almost all Cayley Graphs, Eur. J. Combin. **3** (1982), 9-15.

[B,K] Y. M. Barzdin, A. N. Kolmogorov, On the realization of nets in 4-dimensional space, Probl. Kybernet, **8** (1967), 261-268.

[B,L] Y. Bilu, N. Linial, Lifts, discrepancy and nearly optimal spectral gap, Combinatorica **26** (5) (2006), 495-513.

[B,T] F. Boesch, R. Tindell, Circulants and their connectivities, J. Graph Theory **8** (1984), 487-499.

[B,G,G,T] E. Breuillard, B. Green, R. Guralnick, T. Tao, Expansion in finite simple groups of Lie type, arxiv: 1309.1975.

[B,G,T1] E. Breuillard, B. Green, T. Tao, Suzuki groups as expanders, Groups Geom. Dyn. **5** (2011), 281-299.

[B,G,T2] E. Breuillard, B. Green, T. Tao, Approximate subgroups of linear groups, Geom. Funct. Anal. **21** (4) (2011), 774-819.

[Car] R. W. Carter, Simple groups of Lie type, John Wiley & Sons, New York, Reprint of the 1972 original; A Wiley-Interscience Publication (1989).

[C,L] M. Conder, C. H. Li, On isomorphism of Cayley graphs, Eur. J. Combin. **19** (1998), 911-919.

[D,F,M] C. Delorme, O. Favaron, M. Mahéo, Isomorphisms of Cayley Multigraphs of Degree 4 on Finite Abelian Groups, Eur. J. Combin. **13** (1992), 59-61.

[Dob1] E. Dobson, Isomorphism problem for Cayley graphs of $\mathbb{Z}_p^3$, Discrete Math. **147** (1995), 87-94.

[Dob2] E. Dobson, J. Morris, Quotients of CI-groups are CI-groups, Graphs and Combin. (2013), 1-4.

[Dob3] E. Dobson, The isomorphism problem for Cayley ternary relational structures for some abelian groups of order 8p, Dicrete Math. **310** (2010), 2895-2909.

[Dob3] E. Dobson, Asymptotic automorphism groups of Cayley digraphs and graphs of abelian groups of prime-power order, Ars Math. Contemp. **3** (2010), 201-214.

[D,S2] E. Dobson, P. Spiga, CI-groups with respect to ternary relational structures: new examples, Ars Math. Contemp. **6** (2013), 351-364.

[D,S,V] E. Dobson, P. Spiga, G. Verret, Cayley graphs on abelian groups, arXiv: 1306.3747.

[Dod] J. Dodziuk, Difference equations, isoperimetric inequality and transience of certain random walks. Trans. Amer. Math. Soc, **284** (2) (1984), 787-794.

[Dj] D. Ž. Djoković, Acta Math. Acad. Sci. Hungar. **21**, Issue 3-4 (1970), 267-270.

[E,M] V. N. Egorov, A. I. Markov, On Adam's conjecture for graphs with circulant adjacency matrices (Russian), Doklady Akad. Nauk SSSR **249** (1979), 529-532. = Soviet Math. Dokl. **20** (1979), 1292-1296.

[E,T] B. Elspas, J. Turner, Graphs with circulant adjacency matrices, J. Combin. Theory, **9** (1970), 297-307.

[F,X] X. G. Fang, M. Y. Xu, On isomorphisms of Cayley graphs of small valency, Algebra Colloq. **1** (1994), 67-76.

[God1] C. Godsil, GRR's for non-solvable groups, Algebraic methods in graph theory, Vol. I, II Szeged (1978), pp. 221-239, Colloq. Math. Soc. János Bolyai, Amsterdam-New York (1981) I

[God2] C. Godsil, On Cayley graph isomorphisms, Ars Combin. **15** (1983), 231-246.

[Hel] H. A. Helfgott. Growth and generation in $SL_2)Z/pZ+$, Ann. of Math. (2), **167** (2) (2008), 601-623.

[Het] D. Hetzel, Über regulate graphische Darstellung yon auflösbaren Gruppen, Technisehe UniversitEt, Berlin (1976) (Diplomarbeit)

[Hig] G. Higman, Enumerating p-groups I, Proc. Lond. Math. Soc. **10** (1960), 24-30.

[H,M] M. Hirasaka, M. Muzychuk, An elementary abelian group of rank 4 is a CI-group, J. Combin. Theory, Ser. A **94**(2) (2001), 339-362.

[H,L,W] S. Hoory, N. Linial, A. Wigderson, Expander graphs and their applications, Bull. (New Series) Amer. Math. Soc. **43** (4), October (2006), 439-561.

[Huf1] W. C. Huffman, The equivalence of two cyclic objects on pq elements, Discrete Math. **154** (1996), 103-127.

[Huf2] W. C. Huffman, V. Job, V. Pless, Multipliers and Generalized Multipliers of Cyclic Objects and Cyclic Codes, J. Combin. Theory, Ser. A **62** (1993), 183-215.

[Imr] W. Imrich, Graphs with transitive abelian automorphism group, Combinatorial theory and its applications, Coll. Math. Soc. János Bolyai **4**, Balatonfüred, Hungary (1969), 651-656.

[Jos] A. Joseph, The isomorphism problem for Cayley digraphs on groups of prime-squared order, Discrete Math. **141** (1995), 173-183.

[Kas1] M. Kassabov, Universal lattices and unbounded rank expanders, Invent. Math. **170** no. 2 (2007), 297-326.

[Kas2] M. Kassabov, Symmetric groups and expander graphs, Invent. Math. **170** no. 2 (2007), 327-354.

[K,L,N] M. Kassabov, A. Lubotzky, N. Nikolov, Finite Simple Groups as Expanders, Proc. Natl. Acad. Sci. USA **103** no. 16 (2006), 6116-6119.

[K,N] M. Kassabov, N. Nikolov, Universal lattices and property tau, Invent. Math. **165** no. 1 (2006), 209-224.

[K,R] M. Kassabov, R. Riley, Diameters of Cayley graphs of Chevalley groups, Eur. J. Comb. **28** (3) (2007), 791-800.

[Kaz] D. A. Kazhdan, Connection of the dual space of a group with the structure of its close subgroup, Func. Anal. Appl. **1** (1) (1967), 63-67.

[K,P1] M. H. Klin, R. Pöschel, 'The isomorphism problem for cyclic graphs with p^2 or pq vertices', Abstract presented at the A. A. Zykov Seminar on Graph Theory, Odessa, 1975 (Russian).

[K,P2] M. H. Klin, R. Pöschel, 'The Konig problem, the isomorphism problem for cyclic graphs and the characterization of Schur rings', Preprint, AdWd DDR, ZIMM, Berlin, March 1978.

[K,P3] M. H. Klin, R. Pöschel, 'The isomorphism problem for circulant digraphs with pn vertices', Preprint P-34/80, Akademie der Wissenschaften der DDR, ZIMM, Berlin, 1980.

[K,P4] M. H. Klin, R. Pöschel, 'The Konig problem, the isomorphism problem for cyclic graphs and the method of Schur rings', Algebraic methods in graph theory, Szeged, 1978, Colloquia Mathematica Societatis János Bolyai **25** (North-Holland, Amsterdam, (1981) 405-434.

[K,M] I. Kovács, M. Muzychuk, The group $\mathbb{Z}_{p^2} \pm \mathbb{Z}_q$ is a CI-group, Comm. Alg. **37** (2009), 3500-3515.

[K,M,P] M. H. Klin, M. Muzychuk, R. Pöschel, The isomorphism problem for circulant graphs via Schur ring theory, Dimacs Ser. in Discrete Math. and Theor. Comp. Sci, **56** (2001), 241-264.

[Li1] C.H. Li, "On Cayley isomorphism of finite Cayley graphs- A survey" Discrete Math. **256**(1/2) (2002), 301-334.

[Li2] C.H. Li, Isomorphisms of connected Cayley digraphs, Graphs Combin. **14** (1998), 37-44.

[Li3] C. H. Li, Finite CI-groups are soluble, Bull. London Math. Soc. **31** no. 4 (1999), 419-423.

[Li4] C. H. Li, On isomorphisms of finite Cayley graphs- a survey, Discrete Math. **256** (2002), 301-334.

[L,P] C. H. Li, C. E. Praeger, The finite simple groups with at most two fusion classes of every order, Comm. Algebra **24** (1996), 3681-3704.

[L,L,P] C. H. Li, Z. P. Lu, P. P. Pálfy, Further restrictions on the structure of finite CI-groups, J. Algebr. Combin. **26** (2007), 161-181.

[Lub1] A. Lubotzky, Discrete groups, expanding graphs and invariant measures, with an appendix by J. D. Rogawski, Reprint of the 1994 edition. Modern Birkhauser Classic. Birkhäuser Verlag, Basel, (2010).

[Lub2] A. Lubotzky, Expander Graphs in Pure and Applied Mathematics, Bull. Amer. Math. Soc. **49** (2012), 113-162.

[Lub3] A. Lubotzky, Finite simple groups of Lie type as expanders, J. Eur. Math. Soc. **13** (2011), 1331-1341.

[L,Z] A. Lubotzky, A. Zuk, On Property (τ), monograph in preparation.

[Mar] G. A. Margulis, Explicit constructions of expanders. (Russian) Problemy Peredači Informacii **9** (1973), no. 4, 71-80. English translation: Problems of Information Transmission **9** no. 4, (1973), 325-332 .

[M,X] J. X. Meng, M. Y. Xu, On the isomorphism problem of Cayley graphs of abelian groups, Discrete Math. **187** (1998), 161-169.

[Mor1] J. Morris, Isomorphic Cayley Graphs on different Groups, J. Graph Theory, **31** no. 4 (1999), 345-362.

[Mor2] J. Morris, Results towards showing $\mathbb{Z}_p^{2p\ 1}$ is a CI-group. In: Proceedings of the Thirty-third Southeastern International Conference on Combinatorics, Graph Theory and Computing, Boca Raton, FL, 2002. Congr. Numer, **156** (2002), 143-153.

[Mor3] J. Morris, Elementary proof that $\mathbb{Z}_p^4$ is a DCI-group, arXiv: 1403.4557.

[Muz1] M. Muzychuk, Ádám's conjecture is true in the square-free case, J. Combin. Theory, Ser. A, **72** (1995), 118-134.

[Muz2] M. Muzychuk, On Ádám's conjecture for circulant graphs, Discrete Math. **167/168** (1997), 497-510; corrigendum **176** (1997), 285-298.

[Muz3] M. Muzychuk, An elementary abelian group of large rank is not a CI-group, Discrete Math. **264**(1-3) (2003), 167-185.

[Muz4] M. Muzychuk, A solution of the isomorphism problem for circulant graphs, Proc. London Math. Soc. (3) **88** (2004), 1-41.

[Nik] N. Nikolov, A product decomposition for the classical quasisimple groups, J. Group Theory **10** (2007), 43-53.

[Now] L. A. Nowitz, A non-Cayley-invariant Cayley graph of the elementary abelian group of order 64, Discrete Math. **110** (1992), 223-228.

[N,W1] L. A. Nowitz, M. E. Watkins, On graphical regular representations of non-abelian groups I, Canad. J. Math. **24** (1972), 993-1008.

[N,W2] L. A. Nowitz, M. E. Watkins, On graphical regular representations of non-abelian groups II, Canad. J. Math. **24** (1972), 1009-1018.

[Pál1] P. P. Pálfy, Isomorphism Problem for Relational Structures with a Cyclic Automorphism, Eur. J. Combin. **8** (1987), 35-43.

[Pál2] P. P. Pálfy, On regular pronormal subgroups of symmetric groups, Acta Math. Hungar. **34**, Issue 3-4, (1979), 287-292.

[Pin] M. S. Pinsker, On the complexity of a concentrator, 7th International Teletraffic Conference, Stockholm, pages (1973), 318/1-318/4.

[P,P,S,Sz] Ch. E. Praeger, L. Pyber, P. Spiga, E. Szabó, Graphs with automorphism groups admitting composition factors of bounded rank, Proc. Amer. Math. Soc. **140** (7), (2012) 2307- 2318.

[P,Sz] L. Pyber, E. Szabó, Growth in finite simple groups of Lie type of bounded rank, Submitted, Available at arxiv.org: 1005.1881.

[R,V,W] O. Reingold, S. Vadhan, A. Wigderson, Entropy waves, the zig-zag graph product, and new constant-degree expanders, Ann. of Math. (2) **155** no. 1 (2002), 157-187.

[Roy] G. Royle, Constructive enumeration of graphs, PhD Thesis, University of Western Australia, (1987).

[Sim] C. C. Sims, Enumerating p-groups, Proc. Lond. Math. Soc. **15** (1965), 151-166.

[Som] G. Somlai, Elementary abelian p.groups of rank $3p\ 0\ 4$ are not CI-groups, J. Algebr. Combin. **34** (2011), 323-335.

[Som2] G. Somlai, Non-expander Cayley graphs of simple groups, Communications in Algebra, DOI:10.1080/00927872.2013.865041, (accepted paper).

[Spi1] P. Spiga, Elementary abelian p-groups of rank greater than or equal to 4p-2 are not CI-groups, J. Algebr. Combin. **26** (2007), 343-355.

[Spi2] P. Spiga, On the Cayley isomorphism problem for a digraph with 24 vertices, Ars Math. Contemp. 1 no. 1, (2008), 38-43.

[Spi3] P. Spiga, Enumerating Groups Acting Regularly on a d-dimensional Cube, **37** Issue 7 (2009), 2540-2545.

[Spi4] P. Spiga, CI-property of elementary abelian 4-groups, Discrete Math. **309** (2009), 3393-3398.

[Spi5] P. Spiga. Two local conditions on the vertex stabiliser of arc-transitive graphs and their effect on the Sylow subgroups, J. Group Theory 15 (1), (2012) 23-35.

[Ste] R. Steinberg, Generators for simple groups, Canad. J. Math. **14** (1962), 277-283.

[Toi] S. Toida, A note on Ádáms conjecture, J. Combin. Theory, Ser. B, **23** (1977), 239-246.

[Tur] J. Turner, Point-Symmetric Graphs with a Prime Number of Points, J. Austral. Math. Soc, Ser. A **44** (1988), 389-396.

[Wat1] M. E. Watkins, On the Action of Non-Abelian Groups on Graphs, J. Combin. Theory **11** (1971), 95-104.

[Wat2] M. E. Watkins, Graphical regular representations of alternating, symmetric and miscellaneous small groups, Aequat. Math, **11** (1974), 40-50.

[Wat3] M. E. Watkins, On graphical regular representations of $C_n \pm Q$, Graph Theory and its Applications, Lecture Notes in Mathematics **03**, Springer, Berlin (1972), 305-311.

[Wie] H. Wielandt, Finite permutation groups, Academic Press, London-New York, (1964).

[Xu] M. Y. Xu, Some work on vertex-transitive graphs by Chinese mathematicians, Group Theory in China, Kluwer Academic Publishers, Dordrecht, (1996), 224-254.

[X,X,S,B] M. Y. Xu, F. Xingiu, H. S. Sim, Y. G. Baik, On a conjecture of Li and Praeger concerning the isomorphisms of Cayley graphs of A_5, Science in China, Ser. A **44** (2001), 1502-1508.

[X,X] M. Y. Xu, S. Xu, Symmetry properties of Cayley graphs of small valencies on the alternating group A_5, Science in China, Ser. A Math. **47** No. 4 (2004), 593-604.

Summary

Two major topics are discussed in this thesis. The central objects we investigate in both of them are the Cayley graphs of finite groups. First, we shortly define Cayley graphs and we collect basic facts about them.

Chapter 1, 2 and 3 are devoted to the investigation of Cayley graphs corresponding to the same group. More precisely, Chapter 1 can be considered as an introduction to the isomorphism problem of Cayley graphs, where we recall the concepts of CI-graphs and CI-groups and related notions.

In Chapter 2 we construct non-CI-graphs for elementary abelian p-groups which are the most important candidates for CI-groups. Improving earlier results of Muzychuk [Muz3] and Spiga [Spi1], for every prime $p > 3$ we exhibit a Cayley graph on $\mathbb{Z}_p^{2p+3}$ which is not a CI-graph.

On the positive side, in Chapter 3, for every prime $p > 4$ we prove that $Q \pm \mathbb{Z}_p$ is a DCI-group, where Q denotes the quaternion group of order 9. This gives a new infinite family of non-abelian CI-groups, which are really rare. Using the same method we reprove that $\mathbb{Z}_2^3 \pm \mathbb{Z}_p$ is a CI-group for every prime $p > 4$, which was first obtained by Dobson and Spiga [D,S2]. Our new result completes the description of CI-groups of order $9p$. We also apply our method to prove that for every prime $p > 4$ the group $\mathbb{Z}_q \pm \mathbb{Z}_p^3$ is a DCI-group if q is also a prime with $q > p^3$. Finally, we prove that if G is p-group which is a $\mathrm{DCI}^{(2)}$-group, then $G \pm \mathbb{Z}_q$ is a)q 2+DCI-group if q is a prime with $q > \backslash G \backslash$

In Chapter 4 we solve a problem which was a conjecture of Lubotzky [Lub2] about the Cayley graphs of series of finite simple groups. For every infinite sequence of simple groups of Lie type of growing rank we exhibit connected Cayley graphs of degree at most 21 such that the isoperimetric number of these graphs converges to 1. This proves that these graphs do not form a family of expanders.

Összefoglaló

Az értekezés két témát dolgoz fel. Mindkét esetben véges csoportok Cayley gráfjaival kapcsolatos problémákra keressük a választ. Elsőként definiáljuk a Cayley gráfokat, és összegyűjtjük a legelemibb tulajdonságaikat.

Az első három fejezetben nagyrészt egyazon csoport különböző Cayley gráfjainak vizsgálatával foglalkozunk. Ezek közül az elsőben ismertetjük a Cayley gráfok izomorfizmusproblémáját, ahol is bevezetjük a CI-gráfok, CI-csoportok és ehhez kapcsolódó fogalmak definícióját.

A második fejezetben elemi Abel p-csoportokhoz konstruálunk nem-CI-gráfokat. Ezek a csoportok a legfontosabb jelöltek CI-csoportokra. Belátjuk, hogy a $\mathbb{Z}_p^{2p+3}$ nem CI-csoport, ha p kettőnél nagyobb prím. Ez az eredmény Muzychuk [Muz3] és Spiga [Spi1] korábbi eredményét javítja meg.

A harmadik fejezetben CI-csoportokkal kapcsolatos pozitív eredményeket bizonyítunk. Belátjuk, hogy $Q \pm \mathbb{Z}_p$ is DCI-csoport minden $p > 4$ prímszámra, ahol Q a kvaterniócsoportot jelöli, gazdagítva ezzel az ismert nem kommutatív CI-csoportok halmazát. Ezzel párhuzamosan Dobson és Spiga [D,S2] egy eredményére ($\mathbb{Z}_2^3 \pm \mathbb{Z}_p$ egy CI-csoport) is új bizonyítást kapunk. Ezek az eredmények lezárják a $9p$ rendű CI-csoportok vizsgálatát. A kidolgozott módszert alkalmazva belátjuk, hogy $\mathbb{Z}_p^3 \pm \mathbb{Z}_q$ is DCI-csoport, ahol q egy p^3-nél nagyobb prímszám. Végül a Cayley gráfok fokszámát korlátozva kapjuk a következőt. Legyen G egy DCI$^{(2)}$-csoport, ami ráadásul p-csoport. Továbbá q egy G rendjénél nagyobb prímszám, akkor $G \pm \mathbb{Z}_q$ egy $)q \quad 2+ \quad DCI$-csoport.

Az utolsó fejezetben egy Lubotzky [Lub2] által felvetett egyszerű csoportok Cayley gráfjainak sorozataival kapcsolatos kérdésre adunk választ. Lie-típusú egyszerű csoportok tetszőleges végtelen sorozatához, ahol a csoportok rendje tart a végtelenbe konstruálunk legfeljebb tizedfokú Cayley gráfokat, amiknek az izoperimetrikus száma nullához tart. Az ilyen tulajdonságú gráfok nem alkotnak expander gráfsorozatot.