Thesis for the Degree of Doctor of Philosophy

Cayley Graphs of Finite Cyclic Groups

by

Young-Won Kim

Department of Applied Mathematics

The Graduate School

Pukyong National University

August 2002

Cayley Graphs of Finite Cyclic Groups

유한 순환군의 케일리 그래프

Advisor : Hyo-Seob Sim

by

Young-Won Kim

A thesis submitted in partial fulfillment
of the requirements for the degree of

Doctor of Philosophy

in the Department Applied Mathematics, Graduate School
Pukyong National University

August 2002

김영원의 이학박사 학위논문을 인준함

2002년 6월 29일

주심	이학박사	백영길	인
부심	이학박사	조정래	인
위원	이학박사	송현종	인
위원	이학박사	박진한	인
위원	이학박사	심효섭	인

Cayley Graphs of Finite Cyclic Groups

A Dissertation

by

Young-Won Kim

Approved as to style and content by :

Chairman Young-Gheel Baik, Ph. D.

Member Jung-Rae Cho, Ph. D.

Member Hyun-Jong Song, Ph. D.

Member Jin Han Park, Ph. D.

Member Hyo-Seob Sim, Ph. D.

June 29, 2002

Contents

유한 순환군의 케일리 그래프

김영원

부경대학교 대학원 응용수학과

요 약

군(group) G 의 케일리 그래프는 G 의 원소를 꼭지점(vertex)으로 하고 G 의 단위원(identity) 1 을 포함하지 않는 주어진 부분집합 S 에 대하여 vu^{-1}가 S 의 원소가 되는 한 꼭지점 u 에서 다른 꼭지점 v 로 연결되는 변(edge)이 정하여지는 방향을 갖는 그래프로 1878년 Cayley에 의하여 추상군(abstract group)의 기하적 표현 방법으로 처음 도입되어 생성자(generators)와 관계식(relations)에 의하여 군(group)을 연구하는데 사용하였다. 한편 케일리 그래프는 그 자기동형사상군(automorphism group)이 꼭지점들의 집합 위에 추이적으로(transitively) 작용(acting)하므로 높은 대칭성을 갖는 꼭지점-추이적(vertex-transitive) 그래프들의 일종으로 특히, 유한군론을 이용한 케일리 그래프의 연구는 최근 그래프 이론에서 많은 주목을 받고 있다.

이 논문에서는 군 G 가 유한순환군인 경우, 즉 유한순환군의 케일리 그래프와 그 동형사상에 대하여 연구하였다. 특히, G 는 그 케일리 그래프의 자기동형사상군(automorphism group)의 정칙인(regular) 부분군(subgroup)으로 간주될 수 있는데 이 때, G 를 정규화하는(normalizing) 그래프의 자기동형사상군의 부분군이 변들의 집합 위에 추이적(transitive)으로 작용하는 경우를 중심으로 관찰하였다. 이러한 경우의 케일리 그래프를 정규(normal) 변-추이적(edge- transitive)이라고 한다. 특히, 유한순환군(finite cyclic group) G 에 대하여, 연결된 변-추이적(conected normal edge-transitive graph) 케일리 그래프의 분류문제를 해결하였고, 특히, 군 G 가 소수(prime)의 거듭제곱의 위수(order)를 갖는 유한순환군(finite cyclic group)일 때, 알려진 케일리 그래프들의 사전식곱(lexicographic product)에 의하여 G 의 정규 변-추이적 케일리 그래프를 완전히 결정하였다. 또한 유한순환군 G 의 케일리 동형사상 문제에 대한 부분적인 해결을 얻었다.

Chapter 1

Introduction

The notion of Cayley digraphs were ¯rst introduced by Cayley in 1878 as a graphical representation of abstract groups. The digraphs stem from a type of diagrams now called Cayley colour diagrams. Cayley colour diagrams were used by Coxeter and Moser [12] to investigate groups given by generators and relations. For a Cayley digraph X of a group G, the vertices correspond to the elements of the given group G. There is also a subset S of G which does not contain the identity element 1 of G. An ordered pair (u,v) of two vertices u and v is called an edge of X if and only if the element vu^{i1} in G belongs to S. In particular, if the inverse of each element of S also belongs to S, then the Cayley digraph is called undirected. Each undirected Cayley digraph gives rise to a graph by coalescing each pair of arc (x,y) and (y,x) into a single undirected edge $\{x,y\}$; the graph is called a Cayley graph. In this way, the undirected Cayley digraphs of G correspond to the Cayley graphs of G and vice versa.

Cayley (di)graphs are very important algebraic construction with many symmetries. In fact, the right multiplication on the vertices by each element of the group preserves the adjacency relation of the Cayley (di)graph and the group acts on the vertices regularly and so the group G may be viewed as a regular subgroup of the automorphism group of the Cayley (di)graph. In particular, the automorphism group $\mathrm{Aut}(X)$ of the Cayley (di)graph X acts transitively on the vertex set G. The normalizer $\mathrm{N}_{\mathrm{Aut}(X)}(G)$ of the regular subgroup G is the semidirect product:

$$\mathrm{N}_{\mathrm{Aut}(X)}(G) = G \cdot \mathrm{Aut}(G,S), \text{ where } \mathrm{Aut}(G,S) := \{\sigma \in \mathrm{Aut}(G) \mid S^{\sigma} = S\}.$$

A (di)graph X is said to be edge-transitive if its automorphism group $\mathrm{Aut}(X)$ is transitive on the edges. Also, for a graph X, the automorphism group $\mathrm{Aut}(X)$ is transitive on the ordered pairs of adjacent vertices, then X is said to be arc-transitive. It is difficult to find the full automorphism group of a (di)graph in general, and so this makes it difficult to decide whether it is edge-transitive, even for a Cayley (di)graph. As an accessible kind of edge-transitive digraphs, Praeger [35] focuses attention on those Cayley digraphs for which $\mathrm{N}_{\mathrm{Aut}(X)}(G)$ is transitive on the edges. Such a Cayley (di)graph is said to be normal edge-transitive. An approach to analyzing the family of Cayley (di)graphs for a finite group G was given by C.E. Praeger in 1999 which identifies normal edge-transitive Cayley (di)graphs as a sub-family of central importance.

Using the strategy in [35] to construct normal edge-transitive Cayley graphs from quotients, Houlis [18] was able to determine the isomorphism types of all connected normal edge-transitive Cayley graphs for Z_{pq}, where p, q are primes, and for $G = \mathrm{Z}_p \times \mathrm{Z}_p$, p is a prime, when $\mathrm{Aut}(G, S)$ acts reducibly on G.

In this thesis, we consider finite circulant digraphs, namely Cayley digraphs of finite cyclic groups. The main purpose of this thesis is to give a description of a classification of normal edge-transitive Cayley digraphs for finite cyclic groups.

Two Cayley digraphs $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(G, T)$ are said to be Cayley isomorphic if there exists $\alpha \in \mathrm{Aut}(G)$ such that $T = S^{\alpha}$. Cayley isomorphic Cayley digraphs are of course isomorphic. Ádám [1] conjectured that if two circulant digraphs $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(G, T)$ are isomorphic then they are Cayley isomorphic; the conjecture was shown to be false (see for example, [39]). It is known to be true if the number of vertices is either square-free or twice square-free (see [30, 31]).

Let $\mathrm{Z}_n = \{0, 1, ..., n-1\}$ denote the additive group of integers modulo a positive integer n, and let U_n denote the multiplicative group of units in Z_n. We may identify U_n with $\mathrm{Aut}(\mathrm{Z}_n)$. Denote the Cayley digraph of Z_n on the empty set by $n\mathrm{K}_1$.

We now state the main results of the thesis; the proofs will be given in chapter 4. The following theorem gives a determination of all connected normal edge-transitive circulant digraphs of order n.

Theorem 1.0.1. If S is a subgroup of U_n, then $\mathrm{Cay}(\mathrm{Z}_n, S)$ is connected normal edge-transitive. Every connected normal edge-transitive circulant digraph of order n is isomorphic to $\mathrm{Cay}(\mathrm{Z}_n, S)$ for some subgroup S of U_n. Let S and T be subgroups of U_n. Then $\mathrm{Cay}(\mathrm{Z}_n, S) \cong \mathrm{Cay}(\mathrm{Z}_n, T)$ if and only if $S = T$.

We focus our attention again on the special case when n is a prime power. Let p be an odd prime. For each positive divisor r of $p-1$, there is a unique subgroup of order r in the cyclic group U_{p^i}. The Cayley digraph of Z_{p^i} on the subgroup of order r in U_{p^i} is denoted by $X(p^i, r)$.

For $p = 2$, let $X(2^i, 1) = \mathrm{Cay}(\mathrm{Z}_{2^i}, \{1\})$, $X(2^i, 2) = \mathrm{Cay}(\mathrm{Z}_{2^i}, \{1, -1\})$, and $X(2^i, 3) = \mathrm{Cay}(\mathrm{Z}_{2^i}, \{1, -1+2^{i-1}\})$. Then we have:

Theorem 1.0.2. (i) For an odd prime p, every connected normal edge-transitive circulant digraph of order p^m is isomorphic to the lexicographic product $X(p^i, r)[p^{m-i}\mathrm{K}_1]$ for some positive divisor r of $p-1$ and an integer i with $1 \le i \le m$; different choices of i or r give nonisomorphic digraphs.

(ii) Every connected normal edge-transitive circulant digraph of order 2^m is isomorphic to the lexicographic product $X(2^i, j)[2^{m ¡ i}\mathrm{K}_1]$ for some integers i, j such that

$$1 \leq j \leq 3 \leq i \leq m \text{ or } 1 \leq j \leq i = 2 \text{ for } 3 \leq m,$$

and

$$1 \leq j \leq i = m \text{ for } m = 1, 2;$$

moreover, di®erent choices of i or j give nonisomorphic digraphs.

We note that the analogous result can be given for $n = 2p^m$ for an odd prime p.

We also consider Cayley Isomorphism Problem for ¯nite circulant digraphs. A Cayley digraph $\mathrm{Cay}(G, S)$ is called a CI-digraph of G if for each Cayley digraph $\mathrm{Cay}(G, T)$ isomorphic to $\mathrm{Cay}(G, S)$, there exists $\sigma \in \mathrm{Aut}(G)$ such that $S^\sigma = T$.

Let G be a ¯nite cyclic group, written additively and let S be a Cayley subset of G, namely a subset not containing the identity element 0. Let K be the set $\{a \in G \,|\, a + S = S\}$. Then it is easy to show that K is a subgroup of G. In fact, K is the largest subgroup of G such that S is a union of some cosets of K in G. We denote the subgroup by $\mathrm{Int}(S)$.

We also have the following theorem:

Theorem 1.0.3. Let G be a finite cyclic group and let S and T be Cayley subsets of G. If Cay$(G, S) \cong$ Cay(G, T), then Int(S) = Int(T) and Cay$(G/$Int$(S), S/$Int$(S)) \cong$ Cay$(G/$Int$(S), T/$Int$(S))$.

As a consequence of the above theorem, we have the following, which can be regarded as a complement to Huang and Meng's result in [19].

Corollary 1.0.4. Let Cay(G, S) be a Cayley digraph of a finite cyclic group G with Int(S) = K. If Cay$(G/K, S/K)$ is a CI-digraph of G/K, then Cay(G, S) is a CI-digraph of G.

We finally set up some general conventions and notation, which will be used frequently in this thesis.

Throughout this thesis actions of groups and most algebraic maps such as automorphisms, homomorphisms and isomorphisms are usually written as right operators. If g and h are elements of a group, the conjugate $h^{-1}gh$ is denoted by g^h.

The identity element of a multiplicative group is denoted by 1 and the same notation is also used for the trivial subgroup consisting of the identity element.

The kernel of a homomorphism φ of a group is denoted by kerφ.

Let G be a group. The automorphism group of the group G is denoted by $\mathrm{Aut}(G)$. If H is a subgroup of G, then the normalizer of H in G is denoted by $\mathrm{N}_G(H)$.

Let H, N be groups and $\phi : H \longrightarrow \mathrm{Aut}(N)$ a homomorphism. Then the homomorphism defines a semidirect product of H and N; we denote that semidirect product by $H \ltimes_\phi N$, or simply by $H \ltimes N$. We usually regard H and N as subgroups of $H \ltimes N$ via the natural identifications.

The cardinality of a set X is denoted by $|X|$.

The notation and terminology not defined in this thesis is standard and can be found in almost all standard books on related areas.

Chapter 2

Background results on group theory

In this chapter, we present some general facts that will be useful in this thesis. Some basic concepts and notation are also defined.

2.1 Some basic facts on general group theory

We first consider subgroups of direct product of groups in this section; the presentation here is in part based on the treatment of Suzuki (1982).

Let $G = H \times K$ be the direct product, let η and κ be the projection onto the factors H and K, respectively. We regard H and K as subgroups of G. Then we have the following lemma.

Lemma 2.1.1. Let U be a subgroup of G.

(1) $U \cap H \trianglelefteq U$, $U \cap K \trianglelefteq U$.

(2) The map $\varphi : u^{\eta} \mapsto u^{\kappa}(U \cap K)$ defines a homomorphism from U^{η} onto $U^{\kappa}/(U \cap K)$ with kernel $U \cap H$.

(3) $U = \{hk \,|\, h \in U^{\eta}, k \in U^{\kappa}, h^{\varphi} = k(U \cap K)\}$.

Proof. For each element g of G, we have $g = hk$ where $h = g^{\eta}$ and $k = g^{\kappa}$. If a subgroup U of G is given, U determine the four subgroups U^{η}, $U \cap H$, U^{κ}, and $U \cap K$. Since the direct factors H and K are normal subgroups of G, $U \cap H$ is normal in U; similarly, we have $U \cap K \trianglelefteq U$.

Let σ be the restriction of η on U. Then σ is a homomorphism from U onto U^{η}, and its kernel is $U \cap K$. Thus, we have $U^{\sigma} = U^{\eta} \cong U/(U \cap K)$. The homomorphism σ maps $U \cap H$ onto $U \cap H$. So $U \cap H \trianglelefteq U^{\eta}$. If $u^{\sigma} \in U \cap H$, then $u^{\sigma} = u^{\eta}$, from which we get $(u^{\sigma})^{-1}u = u^{\kappa}$. This implies that $u^{\kappa} \in U \cap K$. Conversely, if $u^{\kappa} \in U \cap K$, then $u^{\eta} = u^{\sigma} \in U \cap H$. Thus, we have $(U \cap H)^{\sigma^{-1}} = (U \cap H)(U \cap K)$. It follows that $U^{\eta}/(U \cap H) \cong U/(U \cap H)(U \cap K)$. Similarly, we get $U^{\kappa}/(U \cap K) \cong U/(U \cap K)(U \cap H)$. Therefore, we have a homomorphism from U^{η} onto $U^{\kappa}/(U \cap K)$ with kernel $U \cap H$; this is given by $\varphi : u^{\eta} \mapsto u^{\kappa}(U \cap K)$. In fact, if $u^{\eta} = v^{\eta}$ for two elements u and v of U, then $v^{-1}u = (v^{\kappa})^{-1}(v^{\eta})^{-1}u^{\eta}u^{\kappa} = (v^{\kappa})^{-1}u^{\kappa} \in U \cap K$. So, the function defined by $u^{\eta} \mapsto u^{\kappa}(U \cap K)$ is a homomorphism from U^{η} onto $U^{\kappa}/(U \cap K)$, and its kernel is $U \cap H$.

To prove (3), denote

$$V = \{hk \mid h \in U^{\eta}, k \in U^{\kappa}, h^{\varphi} = k(U \cap K)\}.$$

We can easily show that V is a subgroup of $G = H \times K$ and $U \leq V$. Clearly, we have $U^{\eta} = V^{\eta}$ and $U^{\kappa} = V^{\kappa}$. An element of $V \cap H$ is of the form $h1$ where $h^{\varphi} = 1(U \cap K)$. Since φ is a homomorphism from U^{η} onto $U^{\kappa}/(U \cap K)$ with kernel $U \cap H$, the element h must belong to $U \cap H$; so $U \cap H \geq V \cap H$ with $U \leq V$, this implies that $U \cap H = V \cap H$. Therefore $|U| = |V|$ and hence $U = V$. □

We here have some investigation about the automorphism groups of finite cyclic groups.

Let Z_n denote the additive group of integers modulo n for a positive integer n. The set U_n of integers m modulo n which are relatively prime to n forms an abelian group under multiplication modulo n. It is well-known that the automorphism group of a cyclic group of order n can be identified with this multiplicative group U_n.

Lemma 2.1.2. The automorphism group $\mathrm{Aut}(\mathrm{Z}_n)$ is isomorphic to U_n.

Proof. It follows from $i\alpha = (1\alpha)i$ that any automorphism α of Z_n is completely specified by 1α. Another easy fact is that $1\alpha_k = k$ determines an automorphism α_k of Z_n if k is non-zero and prime to n; and all the automorphisms of Z_n are determined by such values of k in 1 5 $k < n$. Consider the correspondence in which α_k is paired with k in U_n. That this is an isomorphism of $\mathrm{Aut}(\mathrm{Z}_n)$ with U_n is evident. □

It is now reasonable to ask for the structure of U_n in terms of the theory of finite abelian groups. The structure is well-known, see [29] for example. We here just state the special case when n is a power of a prime number.

Theorem 2.1.3. (1) If p is an odd prime, then U_{p^α} is the cyclic group of order $(p-1)p^{\alpha-1}$.

(2) If $p = 2$, then U_{2^α} is the direct product of the cyclic group $\langle 5 \rangle$ of order $2^{\alpha-2}$ and the cyclic group $\langle -1 \rangle$ of order 2 unless $\alpha = 1$, and U_2 is trivial.

We close this section with following well-known result, which is known as Dedekind Law.

Lemma 2.1.4. Let A, B and C be any subgroups of a group such that $A \le B$. Then $A(B \cap C) = B \cap AC$.

2.2 Permutation groups

We here present some basic concepts and fundamental results on permutation groups, which will be useful for our purpose. The presentation here is largely based on the treatments of [8] and [13].

Let X be a nonempty set. A permutation on X is a one-to-one correspondence $\alpha : X \longrightarrow X$. Two such permutations α and β can be composed to give the permutation $\alpha\beta$, which is defined by the rule $x(\alpha\beta) = (x\alpha)\beta$. Under the operation of composition the set of all permutations on X forms a group; we call it the symmetric group on X and denote by Sym(X). If X is the set $\{1, 2, ..., n\}$, we write S_n for Sym(X). A subgroup G of Sym(X) is called a permutation group on X; the cardinality of X is called the degree of G.

An action of a group G on a set X is defined as the rules:

(1) $x^1 = x$ for all $x \in X$;

(2) $(x^g)^h = x^{gh}$ for all $x \in X$ and $g, h \in G$.

If a group G acts on a nonempty set X, then to each element $g \in G$ we can associate a mapping $\overline{g}$ of X into itself, namely $x \mapsto x^g$. The mapping $\overline{g}$ is a bijection since it has $\overline{g^{-1}}$ as its inverse; hence we have a mapping $\rho : G \longrightarrow$ Sym(X) given by $x^\rho := \overline{x}$. Moreover we see that ρ is a group homomorphism. In general, every homomorphism of G into Sym(X) is called a permutation representation of G on X. Hence, we see that each action of G on X gives rise to a representation of G on X. The kernel of the action is the kernel of the permutation representation ρ; an action is faithful if $\ker \rho = 1$.

Each element g of a group G acts on the group G by right multiplication: $x^g := xg$ for all $x, g \in G$, and so g yields a permutation $R(g)$ of G, namely $R(g) : x \mapsto xg.$ Denote $R(G) := \{R(g) \,|\, g \in G\}$ and $R(G)$ is called the right regular representation of G. The action is faithful since the kernel $\{g \in G \,|\, xg = x$ for all $x \in G\}$ equals 1.

Let G be a finite group acting on a finite set X. The sets $x^G := \{x^g \,|\, g \in G\}$ for x in X are called the orbits of the action of G. Two orbits x^G and y^G are either equal or disjoint, and so the set of all orbits is a partition of X into mutually disjoint subsets. For each x in X, the set $G_x = \{g \in G \,|\; x^g = x\}$ forms a subgroup of G, which is called the stabilizer of x. The stabilizers of two points in the same orbit are conjugate; in fact, if $y = x^g$ for some $x \in X$ and $g \in G$, then $G_y = g^{-1}G_x g$. Moreover, for each $x \in X$ and $g, g' \in G$, $x^g = x^{g'}$ if and only if $(G_x)g = (G_x)g'$. The following result is fundamental and is often called `Orbit-Stabilizer Theorem'.

Theorem 2.2.1. Let G be a finite group acting on a finite set X. Then

$$|x^G| = |G|/|G_x|.$$

The proof of this theorem may be found in any standard text book on permutation group theory.

Definition 2.2.2. G acts transitively on X if there exist precisely one orbit in the action of G on X. Equivalently, G is transitive on X if for every pair of points $x, y \in X,$ there exists $g \in G$ such that $x^g = y$.

Definition 2.2.3. G acts regularly on X if G acts transitively on X and G_x is trivial.

If a finite group G acts transitively on a finite set X, then the following result follows immediately from Orbit-Stabilizer Theorem.

Theorem 2.2.4. Assume that G acts on X transitively. Then

(1) $|X| = |G|/|G_x|$.

(2) If G is finite, G acts on X regularly if and only if $|G| = |X|$.

The following result is also useful.

Lemma 2.2.5. Let G be a group acting transitively on a set X and let H be a subgroup of G. If $x \in X$, then $G = (G_x)H$ if and only if $G = H(G_x)$ if and only if H is transitive on X.

The number of orbits of G_x on X is independent of choices of x in X if G is transitive on X; the number is called the rank of the transitive group G on X.

In what follows we shall extend the action of G on X to 2^X by defining $Y^g := \{y^g \mid y \in Y\}$, for each $Y \subset X.$

Let G be a group acting transitively on a set X. A nonempty subset B is a block for G if for each $g \in G$ either $B^g = B$ or $B^g \cap B = \emptyset$.

Every group acting transitively on X has X and the singletons $\{x\}$ for $x \in X$ as blocks; these are called the trivial blocks. Any other block is called nontrivial.

Let B be a block for the transitive group G and put § := $\{B^g \mid g \in G\}$. Then § is a partition of X and each element of § is a block for G; we call § the system of blocks containing B.

Let G be a group which acts transitively on a set X. We say that G is primitive if G has no nontrivial blocks; otherwise, G is called imprimitive.

The following theorem on the normalizers of regular groups is well-known:

Theorem 2.2.6. If G is a regular subgroup of Sym(X), then N$_{\text{Sym}(X)}(G)$ is isomorphic to the semidirect product G n Aut(G) with the natural action of Aut(G) on G.

Chapter 3

Vertex-transitive (di)graphs

In this chapter we shall describe some basic concepts of vertex-transitive digraphs with a short survey on the study. Some properties on the vertex-transitive digraphs, which will be used in this thesis, will be also discussed.

3.1 Basic notation and concepts

We begin with the definition of digraphs.

By a digraph (or directed graph) we mean a pair $X = (V, E)$ where V is a set whose elements are called the vertices of X, and E is a subset of ordered pairs of distinct vertices whose elements are called the edges (or arcs) of X. Similarly a (undirected) graph is a pair $X = (V, E)$ where V is the set of vertices of X, and E is a subset of unordered pair of distinct vertices which are called the edges of X; the ordered pairs (x, y) of adjacent vertices that is those for which $\{x, y\} \in E$ are called the arcs of X. For a diagraph, edges and arcs are the same, but this is not the case for a graph. In particular, if $(x, y) \in E$ implies $(y, x) \in E$ for a diagraph $X = (V, E)$, then X is called undirected. Each graph $X = (V, E)$ with the arc set A defines a undirected diagraph $X^* = (V, A)$; conversely, each undirected digraph give rise to a graph by coalescing each pair of arc (x, y) and (y, x) into a single undirected edge $\{x, y\}$. In this way, the graphs correspond to the undirected digraphs and vice versa. The order of a finite (di)graph is the number of vertices.

The complement $\bar{X}$ of a graph X is the graph with the same vertex set with X but two points are adjacent in $\bar{X}$ if and only if they are not adjacent in X.

The complete graph K_n is the graph such that every unordered pair of distinct vertices is an edge of the graph. The complement of K_n is also denoted by $n\mathsf{K}_1$.

Given two (di)graphs X and Y, the lexicographic product, $X[Y]$ is defined as the (di)graph with vertex set $V(X) \times V(Y)$ and the following adjacency relation:

$$\begin{array}{lcl} (x, y) \text{ is adjacent to } (x', y') \text{ in } X[Y] & \Longleftrightarrow & \text{either } x \text{ is adjacent to } x' \text{ in } X, \\ & & \text{or } x = x',\ y \text{ is adjacent to } y' \text{ in } Y. \end{array}$$

Let X and Y be given two digraphs. If there exists a bijective map θ

from $V(X)$ onto $V(Y)$ such that $e \in E(X)$ implies $e^\theta \in E(Y)$, where $(x,y)^\theta = (x^\theta, y^\theta)$ for $e = (x,y)$ in a digraph, while $\{x,y\}^\theta = \{x^\theta, y^\theta\}$ for $e = \{x,y\}$ in a graph, then X and Y are said to be isomorphic and denoted by $X \cong Y$; such a bijective map θ is called an isomorphism from X onto Y.

Let $X = (V,E)$ be a (di)graph. An automorphism of X is an isomorphism from X onto X itself, and so an automorphism α of X is a permutation on V such that $e \in E(X)$ implies $e^\alpha \in E(X)$. The set of all automorphisms of X forms a subgroup of Sym(V); we call the subgroup the automorphism group of X and it is denoted by Aut(X). It is easy to see that for a digraph which is undirected, the automorphism group is that of the corresponding undirected graphs. The automorphism group of the complement of a graph X is the same with the automorphism group of X.

We now give some important summary properties.

Definition 3.1.1. A (di)graph $X = (V,E)$ is called vertex-transitive if Aut(X) is transitive on V.

A vertex-transitive (di)graph is not necessarily edge-transitive, and vice versa. In a vertex-transitive (di)graph, all vertices have the same properties with respect to the structure of the (di)graph. In particular, for a vertex-transitive graph, each vertex is contained in the same number of edges; such a number is called the valency of the vertex and the graph itself is said to be regular.

An automorphism α of a (di)graph X acts on the edge set E in a natural way.

Definition 3.1.2. A (di)graph $X = (V, E)$ is called edge-transitive if Aut(X) is transitive on E.

Definition 3.1.3. A graph X is arc-transitive if Aut(X) is transitive on the arc set of X.

So if a digraph X is undirected, then X is edge-transitive if and only if the corresponding undirected graph is arc-transitive. A graph which is vertex-transitive and edge-transitive is not necessarily arc-transitive. Note that an arc-transitive graph must be vertex-transitive and edge-transitive.

Definition 3.1.4. A graph X is called half-transitive if X is vertex-transitive and edge-transitive but not arc-transitive.

We are now concerned with the relationship between transitive permutation groups and vertex-transitive digraphs. The vertex-transitivity of digraphs corresponds to the transitivity of permutation group, and edge-transitive digraphs correspond to the so called orbital digraphs of a transitive permutation group, while symmetric graphs correspond to the orbital graphs associated with so called symmetric orbital, which we shall give an explicit description here. The presentation is basically from the treatment of [8].

Let us suppose that a transitive permutation group G on V is given; then there is an induced action of G on $V \times V$, defined by

$$(x, y)^g = (xg, yg).$$

Since G is transitive, the diagonal $\Delta = \{(x, x) \mid x \in V\}$ is an orbit; we shall write D_0 instead of Δ. Suppose that G has r orbits $D_0, D_1, \cdots, D_{r-1}$ on $V \times V$; each D_i is called an orbital of G. For a fixed $x \in V$, and put $D_i(x) = \{y \in V \mid (x, y) \in D_i\}$ for $i = 1, 2, ..., r-1$. Then $D_0(x), D_1(x), \cdots, D_{r-1}(x)$ are precisely the orbits of G_x on V. Hence r is the rank of G.

Each orbital D_i associates with the digraph $X_i = (V, D_i)$; this digraph is called an orbital digraph associated with D_i. It is obvious that each orbital digraph is edge-transitive. Conversely, each edge-transitive digraph X must be an orbital digraph of the transitive group Aut(X).

We have the following characterization of primitivity in terms of the associate digraphs.

Theorem 3.1.5. Let G be a transitive permutation group on V. Then G is primitive on V if and only if the orbital digraph X_i associated with each orbit $D_i (\neq D_0)$ of G on $V \times V$ is connected.

Each orbit D different from D_0 is `paired' with its transpose:

$$D^t = \{(x,y) \mid (y,x) \in D\}.$$

In general, D and D^t are different. When $D = D^t$, we say that D is self-paired or symmetric. If D is symmetric, the orbital digraph associated with D is undirected; the graph associated with each symmetric orbital D is called an orbital graph associated with D. It is obvious that the orbital graph associated with symmetric orbital is arc-transitive. On the other hand, each arc-transitive graph X must be an orbital graph of the transitive group X.

Similarly, if we call a union of several orbitals of a transitive permutation group G generalized orbital of G; the associated digraph with a generalized orbital is called a generalized orbital digraph. The undirected graph associated with a symmetric generalized orbital is called a generalized orbital graph. Then all generalized orbital (di)graphs are vertex-transitive; and all vertex-transitive (di)graphs X are generalized orbital (di)graphs for the transitive groups Aut(X).

3.2 Arc-transitive graphs

In this section we shall give an exposition of some known results on classifications of some special classes of arc-transitive graphs. Recall that a undirected graph $X = (V, E)$ is said to be arc-transitive if Aut(X) is transitive on the arcs of X; that is, Aut(X) acts transitively on the set of ordered adjacent pair of vertices of X. It is easy to see that X is arc-transitive if and only if Aut(X) acts transitively on V and for a fixed vertex x, the stabilizer G_x of x in Aut(X) is transitive on the set of vertices adjacent to x.

The earliest work in this direction was done by C.Y. Chao. In 1971 he classified all arc-transitive graphs with a prime order. The result may be summarized as follows:

Let $Z_p = \{0, 1, ..., p-1\}$ denote the cyclic group of order p written additively. The automorphism group Aut(Z_p) of Z_p is isomorphic to Z_{p-1}. For a positive divisor r of $p-1$, let H_r denote the unique subgroup of Aut(Z_p) of order r. The graph $G(p, r)$ of order p is defined for each even positive divisor r of $p-1$ by

$$V = Z_p, \quad E = \{\{x, y\} \mid x - y \in H_r\}.$$

Chao [10] proved the following:

Theorem 3.2.1. Let p be an odd prime.

(1) If X is a arc-transitive graph of order p then either $X = pK_1$ or $X = G(p, r)$ for some even divisor r of $p-1$.

(2) Conversely pK_1 and each of the graphs $G(p, r)$ is arc-transitive of order p.

In 1987, Y. Chang and J. Oxley [11] determined all arc-transitive graphs of order $2p$, for a prime p. It was possible because the classification of the primitive groups of degree mp , $m < p$ was given in 1985 by M.W. Libeck and J. Saxl [28].

In 1993, C. Praeger and M. Xu [36, 37] was be able to give a classification of the vertex-primitive arc-transitive graph of order a product of two distinct primes. The imprimitive case was done by C. Praeger, R. Wang and M. Xu [36] in the same year.

A undirected graph X is said to be half-transitive, it is vertex-transitive and edge-transitive, but not arc-transitive. W.T. Tutte was the first who considered half-transitive graphs. He proved

Theorem 3.2.2. If a graph X is vertex-transitive and edge-transitive and if it has odd valency, then X is arc-transitive.

He asked whether there are such graphs of even valency. In 1970, I.Z. Bouwer [9] gave an affirmative answer for Tutte's question; he constructed a half-transitive graph of valency n for each even number $n \geq 4$. The smallest graph in this family was order 54 and valency 4. In 1981, D.F. Holt [17] found another half-transitive graph which has valency 4 and order 27.

Since 1990 several authors have done much work on half-transitive graphs; they are B. Alspach, M. Conder, C. Li, D. Marusic, L. Nowitz, C. Praeger, H. Sim, D. Taylor and M. Xu. For these results, the reader is referred to a survey paper [26] and [41].

3.3 Cayley (di)graphs of finite groups

The class of vertex-transitive (di)graphs is very interesting to especially group theorist. One of the most important classes of vertex-transitive (di)graphs is so-called Cayley (di)graphs of finite groups.

The concept of Cayley graphs was introduced by A. Cayley in 1878 as a graphical representation of abstract groups. Cayley graphs (Cayley colour diagrams) were used by Coxeter and Moser to investigate groups given by generator and relations. However, in the last forty years, the theory of Cayley graphs has been developed to a rather big branch of algebraic graph theory.

We give a definition of a Cayley (di)graph of a finite group.

Let G be a finite group. A subset S of G is called a Cayley subset if S does not contain the identity element 1 of G. A Cayley subset S is called symmetric if $S = S^{-1}$ where $S^{-1} := \{s^{-1} \mid s \in S\}$.

Definition 3.3.1. The Cayley digraph of a group G on a Cayley subset S is the digraph with vertex set G and (x, y) is an edge if and only if $yx^{-1} \in S$.

If S is symmetric then the adjacency relation is symmetric and thus the Cayley digraph is undirected; the corresponding graph is called the Cayley graph of G on S. We denote the Cayley digraph of G on S by Cay(G, S); abusing notation, we also denote the corresponding Cayley graph by the same notation.

A Cayley (di)graph of a cyclic group is called a circulant (di)graph, or simply a circulant.

We observe some elementary properties about Cayley (di)graphs.

Lemma 3.3.2. Let G be a finite group and let S be a Cayley subset. Then Cay(G, S) is connected if and only if S generates G.

Proof. Suppose that the Cayley digraph is connected and let g be an element of G. Then there exists a sequence of vertices $1 = v_0, v_1, ..., v_n = g$ such that either (v_i, v_{i+1}) is an edge or (v_{i+1}, v_i) is an edge. Write s_i for $v_i v_{i-1}^{-1}$ for $i = 1, ..., n$. Then either $s_i \in S$ or $s_i^{-1} \in S$ and $g = s_n s_{n-1} \cdots s_2 s_1$. So S generates G. Suppose that S generates G. Since G is finite, for each g we have $g = s_n s_{n-1} \cdots s_2 s_1$ for some s_i in S. Then $(1, s_1), (s_1, s_2 s_1), ..., (s_{n-1} \cdots s_1, g)$ is a sequence of edges connecting 1 and g. This implies that Cay(G, S) is connected. The proof is similar for the undirected case. □

Since $yx^{-1} \in S$ implies $(yg)(xg)^{-1} \in S$ for every x, y and g in G, the right regular representation $R(G)$ of the group G is a subgroup of the automorphism group of every Cayley digraph of G, which acts regularly. The same is true for undirected Cayley digraphs.

Thus we have the following lemma.

Lemma 3.3.3. The automorphism group of a Cayley graph of a group G contains a regular subgroup isomorphic to G. In particular, every Cayley (di)graph of a group G is vertex-transitive.

The converse of the above result is also well-known; in fact, the Cayley graphs of a group G can be characterized by the following lemma; see [8].

Lemma 3.3.4. A digraph X is a Cayley digraph of G if and only if Aut(X) contains a regular subgroup isomorphic to G.

The following lemma is a consequence of Lemma 3.3.3 and Lemma 2.2.5.

Lemma 3.3.5. Let X = Cay(G, S) be a Cayley graph, A = Aut(X), and A_1 the subgroup of A consisting of those automorphisms that fix the identity element 1 of G. Then $A = R(G)\,A_1$ and $R(G) \cap A_1 = 1$.

We have shown that the right regular representation $R(G)$ of G is a regular subgroup of the automorphism group A of a Cayley graph X = Cay(G, S) of G. We now determine the normalizer of the regular subgroup $R(G)$ in the automorphism group A of X.

Let X = Cay(G, S) be a Cayley graph of G; we first set up the following notation.

Notation 3.3.6. $\mathrm{Aut}(G,S) := \{\alpha \in \mathrm{Aut}(G) : S^\alpha = S\}$.

Obviously, $\mathrm{Aut}(X) \geq R(G)\,\mathrm{Aut}(G,S)$. Write $A := \mathrm{Aut}(X)$. We have

Lemma 3.3.7. $\mathrm{N}_A(R(G)) = R(G)\,\mathrm{Aut}(G,S)$.

Proof. Since the normalizer of $R(G)$ in the symmetric group $\mathrm{Sym}(G)$ is the holomorph of G. By Theorem 2.2.6, that is $\mathrm{N}_{\mathrm{Sym(G)}}(R(G)) = R(G)\mathrm{Aut}(G)$, we have

$$\mathrm{N}_A(R(G)) = R(G)\mathrm{Aut}(G) \cap A = R(G)(\mathrm{Aut}(G) \cap A).$$

Obviously, $\mathrm{Aut}(G) \cap A = \mathrm{Aut}(G,S)$. Thus $\mathrm{N}_A(R(G)) = R(G)\,\mathrm{Aut}(G,S)$. □

Corollary 3.3.8. $R(G)$ is normal subgroup of A if and only if $A_1 = \mathrm{Aut}(G,S)$ if and only if every automorphism of X that fixes the identity of G is an automorphism of G.

Some work has been devoted to characterizing Cayley graphs $\mathrm{Cay}(G,S)$ in terms of $\mathrm{Aut}(G)$. The problem of determining the full automorphism group of a Cayley (di)graph is very difficult in general; Since a Cayley (di)graph of G is defined by G, natural approach to the problem is to understand the relationship between the full automorphism group and G, for example, whether or not G, as regular subgroup, is normal in the automorphism of the Cayley graph. We refer to [41, 7, 27] for some studies of those Cayley graphs for which the regular subgroup $R(G)$ is normal in A. The extreme case where $A = R(G)$ has received considerable attention, see [4, 16, 22, 25].

Cayley (di)graphs form a proper subclass of vertex-transitive graphs. The Petersen graph is the smallest vertex-transitive graph which is not a Cayley graph. Mckay and Praeger conjecture that most vertex-transitive graphs are Cayley graphs, see [35].

3.4 Cayley Isomorphisms of Cayley (di)graphs

The isomorphism problem for Cayley (di)graphs is to decide whether two given Cayley (di)graphs are isomorphic or not. The problem is a fundamental problem in graph theory. We here give a brief survey on the study of the problem. The presentation is in part based on [23].

The Cayley (di)graph Cay(G, S) is determined completely by G and S. However, since it is very difficult problem to decide whether or not any given two Cayley (di)graphs are isomorphic in general. If σ is an automorphism of G such that $S^\sigma = T$, then σ gives rise to an isomorphism from Cay(G, S) onto Cay(G, T). Such an isomorphism is called a Cayley isomorphism. It is of course possible for two Cayley (di)graphs Cay(G, S) onto Cay(G, T) to be isomorphic but no Cayley isomorphisms map S to T.

Definition 3.4.1. A Cayley (di)graph Cay(G, S) is called a CI-(di)graph of

G if for each Cayley (di)graph Cay(G,T) isomorphic to Cay(G,S), there exists $\sigma \in$ Aut(G) such that $S^\sigma = T$. The group G is called a DCI-group if every Cayley digraph of G is a CI-digraph; G is called a CI-group if every Cayley graph of G is a CI-graph.

We discuss some basic properties about CI-(di)graphs.

For a finite group G and a Cayley subset S of G, if Cay(G,S) is disconnected then

$$\text{Cay}(G,S) \cong \frac{|G|}{|\langle S\rangle|}\text{Cay}(\langle S\rangle,S)$$

so that for any Cayley subset T of G,

$$\text{Cay}(G,S) \cong \text{Cay}(G,T) \text{ if and only if } \text{Cay}(\langle S\rangle,S) \cong \text{Cay}(\langle T\rangle,T).$$

Let H,L be two subgroups of G, and let S,T be Cayley subsets such that $\langle S\rangle = H$, $\langle T\rangle = L$ and Cay$(H,S) \cong$ Cay(L,T). Then Cay$(G,S) \cong$ Cay(G,T). If Cay(G,S) is a CI-(di)graph, then $S^\sigma = T$ for some $\sigma \in$ Aut(G). Thus $H^\sigma = \langle S\rangle^\sigma = \langle S^\sigma\rangle = \langle T\rangle = L$, that is H is conjugate under Aut(G) to L, and in particular, $H \cong L$. Therefore we have:

Proposition 3.4.2. Let G be finite group and let Cay(G,S) be a CI-(di)graph of G.

(1) For each Cayley subset T of G, if Cay$(\langle S\rangle,S) \cong$ Cay$(\langle T\rangle,T)$ then $\langle S\rangle$ is conjugate under Aut(G) to $\langle T\rangle$, in particular, $\langle S\rangle \cong \langle T\rangle$.

(2) All subgroups of G isomorphic to $\langle S\rangle$ are conjugate under Aut(G).

A criterion for CI-graphs due to Babai [5] plays an important role. We state it as follows:

Theorem 3.4.3. Let $X = \mathrm{Cay}(G,S)$ be a Cayley (di)graph of a finite group G. Then X is a CI-(di)graph of G if and only if for every $\sigma \in \mathrm{Sym}(G)$ with $\sigma R(G)\sigma^{-1} \leq \mathrm{Aut}(X)$, there exists an $a \in \mathrm{Aut}(X)$ such that $aR(G)a^{-1} = \sigma R(G)\sigma^{-1}$.

We present a proof of this fundamental theorem which is essentially the same as Babai [5].

Proof. Assume that there is a $\sigma \in \mathrm{Sym}(G)$ such that $\sigma R(G)\sigma^{-1} \leq \mathrm{Aut}(X)$. Without loss of generality, we assume that σ fixes 1. Let X^σ be the digraph with vertex set G and edge set $\{(g^\sigma,(sg)^\sigma)\,|\,g \in G,\ s \in S\}$. Then we have $\mathrm{Aut}(X^\sigma) = \sigma^{-1}\mathrm{Aut}(X)\sigma$. Thus we have $\mathrm{Aut}(X^\sigma) \geq R(G)$, which implies that X^σ is also a Cayley digraph of G. Since the neighborhood of 1 in X^σ is S^σ, we see that $X^\sigma = \mathrm{Cay}(G,S^\sigma)$. Since $\mathrm{Cay}(G,S)$ is CI, there exists an $\alpha \in \mathrm{Aut}(G)$ such that $S^\alpha = S^\sigma$, and so $S^{\sigma\alpha^{-1}} = S$ and $\sigma\alpha^{-1} = a \in \mathrm{Aut}(X)$. Since α normalizes $R(G)$, we have

$$aR(G)a^{-1} = \sigma\alpha^{-1}R(G)\alpha\sigma^{-1} = \sigma R(G)\sigma^{-1}.$$

Conversely, let σ be an isomorphism from X to another Cayley digraph $Y = \mathrm{Cay}(G,T)$ such that $1^\sigma = 1$. Then $S^\sigma = T$ and $Y = X^\sigma$. Hence $\mathrm{Aut}(Y) \geq R(G)$. This yields that there is an $a \in \mathrm{Aut}(X)$ such that

$\sigma R(G)\sigma^{-1} = aR(G)a^{-1}$, and we may also assume that $1^a = 1$. Thus we have $\alpha = a^{-1}\sigma$ normalizes $R(G)$ and $1^\alpha = 1$. Therefore, $\alpha \in \mathrm{Aut}(G)$ and $S^\alpha = S^{a^{-1}\sigma} = S^\sigma = T$. □

Next we use the Sylow Theorem to investigate CI-graphs of prime-power order. Let G be a p-group for a prime p. Suppose that X is a connected Cayley graph of G of valency less than p. Let $A = \mathrm{Aut}(X)$. Then $A = R(G)A_1$ such that $p \nmid |A_1|$. Thus $R(G)$ is a Sylow p-subgroup of A. By the Sylow theorem, all regular subgroups of A are conjugate, and so X is a CI-graph by Theorem 3.4.3. This simple property was first observed by Babai in [5] and is slightly extended for undirected graphs in [24] as follows.

Proposition 3.4.4. Let p be a prime and let G be a p-group. Then G is a connected $(p-1)$-DCI- and $(2p-2)$-CI-group. In particular, the cyclic group $\mathbb{Z}_p$ is a DCI-group.

A well-known open question about Cayley (di)graphs is which Cayley (di)graphs for a group G are CI-(di)graphs. This question has received considerable attention, and has been investigated under various conditions in the literature. Interest in this question stems from a conjecture of Ádám in 1967 that all circulant graphs were CI-graphs of the corresponding cyclic groups. This conjecture was disproved by Elspas and Turner [15] in 1970, and since then a lot of work has been devoted to seeking CI-graphs. Ádám's conjecture asserts that every finite cyclic group is DCI-group.

The following theorem outlines the main results in this direction.

Theorem 3.4.5. Let n be an integer greater than 1.

(1) The cyclic group Z_n is a DCI-group if and only if $n = k, 2k,$ or $4k$ where k is odd square-free.

(2) The cyclic group Z_n is a CI-group if and only if either $n = 8, 9, 18$, or $n = k, 2k,$ or $4k$ where k is odd square-free.

For the case $n = p$, a prime, the result was obtained by Turner [39] in 1967; for the case where $n = pq$ is a product of two distinct primes, by Alspach and Parsons [3] in 1979; for the case when $(n, \varphi(n)) = 1$, by Pálfy in 1987; for the form of n of this theorem, by Muzychuk [30, 31] in 1995 and 1997. For the `only if' part of the theorem, the results were mainly obtained by Babai and Frankl [6].

Next theorem is about the CI-property of elementary abelian p-groups.

Theorem 3.4.6. Let p be a prime. Then

(1) Z_p^2 and Z_p^3 are CI-groups (see [2, 14])

(2) Z_p^6 is not a CI-group(see [33])

We state a conjecture made by Toida (1977) regarding a special class of circulant graphs. Let $G = Z_n$ be a cyclic group of order n, and let V_n be the set of elements of G of order n.

Conjecture 3.4.7. If $S \subset V_n$, then Cay(G, S) is a CI-graph.

Very recently, the conjecture was proved independently in [21] and [32].

Chapter 4

Cayley (di)graphs of cyclic groups

4.1 Normal edge-transitive Cayley (di)graphs

A Cayley (di)graph $X = \mathrm{Cay}(G, S)$ is said to be edge-transitive if its automorphism group $\mathrm{Aut}(X)$ is transitive on the edges. It is difficult to find the full automorphism group of a graph in general, and so this makes it difficult to decide whether it is edge-transitive, even for a Cayley graph. As an accessible kind of edge-transitive (di)graphs, Praeger [34] focuses attention on those (di)graphs for which $\mathrm{N}_{\mathrm{Aut}(X)}(G)$ is transitive on edges.

Definition 4.1.1. A Cayley (di)graph $X = \mathrm{Cay}(G, S)$ is said to be normal edge-transitive if $\mathrm{N}_{\mathrm{Aut}(X)}(G)$ is transitive on edges.

Praeger gave an approach to analyzing normal edge-transitive Cayley (di)graphs as a subfamily of central importance. In this section, we give a preliminary discussion of normal edge-transitive (di)graphs of finite groups.

As established in Chapter 2, we denote $\mathsf{Aut}(G,S) := \{\alpha \in \mathsf{Aut}(G) : S^{\alpha} = S\}$. By Lemma 3.3.7, $\mathsf{N}_A(R(G)) = R(G)\,\mathsf{Aut}(G,S)$, where elements of $\mathsf{Aut}(G,S)$ have the natural conjugation action on the normal subgroup $R(G)$, and also acts naturally as permutations of $R(G)$.

We first characterize normal edge-transitivity in terms of the action of $\mathsf{Aut}(G,S)$.

Theorem 4.1.2. Let $X = \mathsf{Cay}(G,S)$ be a Cayley digraph of a finite group G on a Cayley subset S. Then X is normal edge-transitive if and only if $\mathsf{Aut}(G,S)$ is transitive on S.

Proof. Suppose that X is normal edge-transitive. Let $s, s_1 \in S$. Then $(1,s)^{\sigma} = (1,s_1)$, for some $\sigma \in R(G)\mathsf{Aut}(G,S)$. We set $\sigma = \beta R(g)$, where $R(g) \in R(G)$ and $\beta \in \mathsf{Aut}(G,S)$. Then $(1,s)^{\sigma} = (1,s)^{\beta R(g)} = (1^{\beta}, s^{\beta})^{R(g)} = (1,s^{\beta})^{R(g)} = (g, s^{\beta}g) = (1,s_1)$. So $g = 1$ and $s^{\beta}g = s_1$. Hence $s_1 = s^{\beta}$ for some $\beta \in \mathsf{Aut}(G,S)$. Therefore $\mathsf{Aut}(G,S)$ is transitive on S.

Conversely, suppose that $\mathsf{Aut}(G,S)$ is transitive on S. Let (x,y) and (x_1,y_1) are edges in $X = \mathsf{Cay}(G,S)$. Then $yx^{-1} = s$ and $y_1x_1^{-1} = s_1$, for some $s, s_1 \in S$. Since $\mathsf{Aut}(G,S)$ is transitive on S, $s_1 = s^{\alpha}$ for some $\alpha \in \mathsf{Aut}(G,S)$. We have $(x,y)^{R(x^{-1})\alpha R(x_1)} = (1, yx^{-1})^{\alpha R(x_1)} = (1,s)^{\alpha R(x_1)} =$

$(1^\alpha, s^\alpha)^{R(x_1)} = (1, s_1)^{R(x_1)} = (1, y_1x_1^{-1})^{R(x_1)} = (x_1, y_1)$.

Hence $(x, y)^{R(x^{-1})\alpha R(x_1)} = (x_1, y_1)$, for some $R(x^{-1})\alpha R(x_1) \in R(G)\mathrm{Aut}(G, S)$. Therefore X is normal edge-transitive. □

Theorem 4.1.3. Let $X = \mathrm{Cay}(G, S)$ be a Cayley graph of a finite group G on a Cayley subset S such that $S = S^{-1}$. Then X is normal edge-transitive if and only if either $\mathrm{Aut}(G, S)$ is transitive on S or S is the disjoint union of sets T and T^{-1} where both T and T^{-1} are orbits of $\mathrm{Aut}(G, S)$.

Proof. Suppose that X is normal edge-transitive. Assume that $\mathrm{Aut}(G, S)$ is not transitive on S. Then $s^{\mathrm{Aut}(G,S)}$ is an orbit of $\mathrm{Aut}(G, S)$ for some $s \in S$. We set $T = s^{\mathrm{Aut}(G,S)}$ and let $s_1 \in S - T$. Since X is normal edge-transitive, there exists $\alpha \in R(G)\mathrm{Aut}(G, S)$ such that $\{1, s\}^\alpha = \{1, s_1\}$. So $\{1, s\}^\alpha = \{1, s\}^{R(g)\delta} = \{g, sg\}^\delta = \{g^\delta, (sg)^\delta\} = \{1, s_1\}$ for some $R(g) \in R(G)$ and $\delta \in \mathrm{Aut}(G, S)$. (1) if $g^\delta = 1$, then $g = 1$. Therefore $s_1 = (sg)^\delta = s^\delta \in T$. This is contradiction to the fact that $s_1 \in S - T$. (2) if $(sg)^\delta = 1$, then $sg = 1$. So $s_1 = g^\delta = (s^{-1})^\delta = (s^\delta)^{-1} \in T^{-1}$. Hence $S - T \subset T^{-1}$. Since $T^{-1} = (s^{-1})^{\mathrm{Aut}(G,S)}$ is $\mathrm{Aut}(G, S)$ orbit and $S - T = T^{-1}$, it follows that $T \cap T^{-1} = \emptyset$ and $S = T \cup T^{-1}$.

Conversely, let $\{x, y\}, \{x_1, y_1\}$ be any two edges of $X = \mathrm{Cay}(G, S)$. Then $yx^{-1} = s$ and $y_1x_1^{-1} = s_1$, for some $s, s_1 \in S$. We continue by taking each case separately:

We assume that $\mathrm{Aut}(G, S)$ is transitive on S. Then $\{x, y\}^{R(x^{-1})} = \{1, s\}$

and $\{x_1, y_1\}^{R(x_1^{-1})} = \{1, s_1\}$. Since Aut$(G, S)$ is transitive on S, there exists $\alpha \in$ Aut(G, S) such that $\{1, s\}^\alpha = \{1^\alpha, s^\alpha\} = \{1, s_1\}$. Thus $\{x, y\}^{R(x^{-1})\alpha R(x_1)} = \{1, s\}^{\alpha R(x_1)} = \{1, s_1\}^{R(x_1)} = \{x_1, y_1\}$. That is $\{x, y\}^{R(x^{-1})\alpha R(x_1)} = \{x_1, y_1\}$, for some $R(x^{-1})\alpha R(x_1) \in R(G)Aut(G, S)$. Therefore X is normal edge-transitive. We assume that $S = T \cup T^{-1}$ and that Aut(G, S) is transitive on T. Suppose first that both $s, s_1 \in T$. Since Aut(G, S) is transitive on T there exists $\alpha \in$ Aut(G, S) such that $s^\alpha = s_1$. So $\{x, y\}^{R(x^{-1})\alpha R(x_1)} = \{1, s\}^{\alpha R(x_1)} = \{1^{R(x_1)}, s_1^{R(x_1)}\} = \{x_1, y_1\}$. That is $\{x, y\}^{R(x^{-1})\alpha R(x_1)} = \{x_1, y_1\}$, for some $R(x^{-1})\alpha R(x_1) \in R(G)Aut(G, S)$. Therefore X is normal edge-transitive. If $s, s_1 \in T^{-1}$, uses the same arguments. Now let $s \in T$ and $s_1 \in T^{-1}$. That is $yx^{-1} \in T$ and $y_1 x_1^{-1} \in T^{-1}$. Then $\{x, y\}^{R(x^{-1})} = \{1, yx^{-1}\}$ $= \{1, s\}$ and $\{1, s\}^{R(s^{-1})} = \{s^{-1}, 1\}$. Since Aut$(G, S)$ is transitive on T^{-1} and $s^{-1}, s_1 \in T^{-1}$, there exists $\alpha \in$ Aut(G, S) such that $\{1, s^{-1}\}^\alpha = \{1, s_1\}$. Hence $\{x, y\}^{R(x^{-1})R(s^{-1})\alpha R(x_1)} = \{x_1, y_1\}$, for some $R(x^{-1})R(s^{-1})\alpha R(x_1)$ $\in R(G)$Aut(G, S). Therefore X is normal edge-transitive. □

Lemma 4.1.4. Let $X =$ Cay(G, S) be a Cayley graph of a finite abelian group G on a Cayley subset S such that $S = S^{-1}$ and let X^* be the corresponding Cayley digraph of X. Then X is normal edge-transitive if and only if X^* is normal edge-transitive.

Proof. Suppose that X is normal edge-transitive Cayley graph for a finite abelian group G. Then by Theorem 4.1.3, for $s \in S$, the orbit $s^{\mathrm{Aut}(G,S)}$

either be equal to S or equal to T such that $S = T \cup T^{-1}$ and $T \cap T^{-1} = \emptyset$. But since G is abelian we have the mapping $\alpha : x \mapsto x^{-1}$ is an automorphism of G. Also α preserves the Cayley subset S because $S^{\alpha} = S^{-1} = S$ and in the case $S = T \cup T^{-1}$ it interchanges T and T^{-1}. Thus $\alpha \in \mathrm{Aut}(G, S)$ and the second case does not arise, and so $\mathrm{Aut}(G, S)$ is transitive on S. By Theorem 4.1.2, X^* is normal edge-transitive.

Conversely, suppose that X^* is normal edge-transitive. Then $\mathrm{Aut}(G, S)$ is transitive on S by Theorem 4.1.2. Therefore X is normal edge-transitive by Theorem 4.1.3. □

We close this section with some observation of lexicographic products of digraphs. We recall again the definition of lexicographic product of two digraphs:

Given two digraphs X and Y the lexicographic product $X[Y]$ is defined as the digraph with vertex set $V(X) \times V(Y)$ and the following adjacency relation:

$$(x, y) \text{ is adjacent to } (x', y') \text{ in } X[Y] \iff \begin{array}{l} \text{either } x \text{ is adjacent to } x' \text{ in } X, \\ \text{or } x = x',\ y \text{ is adjacent to } y' \text{ in } Y. \end{array}$$

We then have following basic result; for the proof see, for example [18].

Lemma 4.1.5. Let $X = \mathrm{Cay}(G, S)$ be a Cayley digraph for a finite group G with $S \neq \emptyset$. If S is a union of cosets of a normal subgroup M of G, then $X \cong \mathrm{Cay}(G/M, S/M)[|M|\mathrm{K}_1]$, where S/M denotes the set of cosets

$Ms,\ s \in S$.

Proof. Let T be a set of coset representatives for M in $G,$ that is for any $g \in G,$ there exists a unique $t \in T$ such that $Mg = Mt$ (or $gt^{-1} \in M$). Let $\gamma : G \longrightarrow G/M \times M$ defined by $g^\gamma = (Mg, gt^{-1})$ where $Mg = Mt, t \in T.$ We claim that γ is an isomorphism from X to Cay$(G/M, S/M)[|M|$K$_1]$. (1) if $g \neq g_1$ and $Mg = Mg_1,$ then we will obtain two distincts vertices $(Mg, gt^{-1}), (Mg_1, g_1t^{-1})$ because $gt^{-1} \neq g_1t^{-1}$. (2) if $g \neq g_1$ and $Mg \neq Mg_1,$ then $g^\gamma \neq {g_1}^\gamma.$ By (1) and (2) γ is injective. Also γ is onto because if $(Mg, x) \in G/M \times M$ with $g, x \in G$ then there exist $t \in T$ such that $Mg = Mt.$ Set $g_1 = xt \in G$, so that $Mg_1 = Mxt = Mt = Mg$ because $x \in M.$ Hence $(Mg, x) = (Mg_1, x) = (Mg_1, g_1t^{-1}) = {g_1}^\gamma.$ Therefore γ is bijective from G to $G/M \times M.$ Finally we must show that γ is preserves adjacency and nonadjacency. Since S is a union of cosets of M in G and $1 \notin S,$ $M \cap S = \emptyset$ because $1 \in M.$ This means $Ms \in S/M$ if and only if $s \in S.$ So (g, g_1) is an edge in $X =$ Cay(G, S) if and only if $g_1g^{-1} \in S$ if and only if $Mg_1g^{-1} \in S/M$ if and only if (Mg, Mg_1) is an edge in Cay$(G/M, S/M)$ if and only if $((Mg, gt^{-1}), (Mg_1, g_1t_1^{-1}))$ is an edge in Cay$(G/M, S/M)[|M|$K$_1]$ where $t, t_1 \in T$ such that $Mg = Mt$ and $Mg_1 = Mt_1.$ Therefore γ is an isomorphism. □

4.2 Normal edge-transitive circulant (di)graphs

Using the strategy in [34] to construct normal edge-transitive Cayley graphs from quotients, Houlis [18] was able to determine the isomorphic types of all connected normal edge-transitive Cayley graphs for Z_{pq}, where p, q primes; for $G = \mathrm{Z}_p \times \mathrm{Z}_p$, p a prime, Houlis also made a classification which gives all normal edge-transitive Cayley graphs $\mathrm{Cay}(G, S)$ such that $\mathrm{Aut}(G, S)$ acts reducibly on G. In this section, we consider finite circulant (di)graphs, namely Cayley (di)graphs of finite cyclic groups.

Two Cayley (di)graphs $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(G, T)$ are said to be Cayley isomorphic if there exists $\alpha \in \mathrm{Aut}(G)$ such that $T = S^{\alpha}$. Cayley isomorphic Cayley (di)graphs are of course isomorphic. Ádám [1] conjectured that if two circulant (di)graphs $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(G, T)$ are isomorphic then they are Cayley isomorphic; the conjecture was shown to be false (see for example, [39]). It is known to be true if the number of vertices is either square-free or twice square-free (see [30, 31]).

Let $\mathrm{Z}_n = \{0, 1, ..., n-1\}$ denote the additive group of integers modulo a positive integer n, and let U_n denote the multiplicative group of units in Z_n. We may identify U_n with $\mathrm{Aut}(\mathrm{Z}_n)$. Denote the Cayley graph of Z_n on the empty set by $n\mathrm{K}_1$. The following theorem gives a determination of all connected normal edge-transitive circulant digraphs of order n.

Theorem 4.2.1. If S is a subgroup of U_n, then $\mathsf{Cay}(\mathsf{Z}_n, S)$ is connected normal edge-transitive. Every connected normal edge-transitive circulant digraph of order n is isomorphic to $\mathsf{Cay}(\mathsf{Z}_n, S)$ for some subgroup S of U_n.

Proof. For the ¯rst part of the theorem, let S be a subgroup of U_n. Since $1 \in S$, we have $\mathsf{Z}_n = \langle S \rangle$ and so $\mathsf{Cay}(\mathsf{Z}_n, S)$ is connected by Lemma 3.3.2. Identifying U_n with $\mathsf{Aut}(\mathsf{Z}_n)$, S as an automorphism group acts transitively on the subset S of Z_n; the action is realised by multiplication. Since $\mathsf{Aut}(\mathsf{Z}_n, S) = \{a \in \mathsf{U}_n \mid S^a = S\}$, we have $\mathsf{Aut}(\mathsf{Z}_n, S) = S$, and therefore $\mathsf{Aut}(\mathsf{Z}_n, S)$ is transitive on S. It follows from Theorem 4.1.2 that $\mathsf{Cay}(\mathsf{Z}_n, S)$ is normal edge-transitive.

For the second part, let X be a connected normal edge-transitive circulant digraph of order n. Then X is isomorphic to $\mathsf{Cay}(\mathsf{Z}_n, T)$ for some subset T of Z_n. By Theorem 4.1.2, $\mathsf{Aut}(\mathsf{Z}_n, T)$ is transitive on T. Write S for $\mathsf{Aut}(\mathsf{Z}_n, T)$. Then we may regards S as a subgroup U_n. Since $\langle T \rangle = \mathsf{Z}_n$, there exists t in $T \cap \mathsf{U}_n$. It follows that $T = St$. Therefore the map $i \mapsto it$, $i \in \mathsf{Z}_n$ yields an Cayley isomorphism from $\mathsf{Cay}(\mathsf{Z}_n, S)$ onto $\mathsf{Cay}(\mathsf{Z}_n, T)$. This completes the proof. □

For normal edge-transitive circulant graphs, we only need to consider the corresponding circulant digraphs by the virtue of Lemma 4.1.4. A normal edge-transitive circulant digraph of order n is undirected if only if it isomorphic to $\mathsf{Cay}(\mathsf{Z}_n, S)$ for some subgroup S of U_n containing -1.

If n is square-free or twice square-free, then different choices of S give nonisomorphic digraphs. In addition to this trivial case, the following theorem gives an answer for the isomorphism problem of normal edge-transitive circulant digraphs of finite order.

Theorem 4.2.2. Let S and T be subgroups of U_n. Then $\mathrm{Cay}(Z_n, S) \cong \mathrm{Cay}(Z_n, T)$ if and only if $S = T$.

We focus our attention again on the special case when n is a prime power. Let p be an odd prime. For each positive divisor r of $p-1$, there is a unique subgroup of order r in the cyclic group U_{p^i}. The Cayley digraph of Z_{p^i} on the subgroup of order r in U_{p^i} is denoted by $X(p^i, r)$.

For $p = 2$, let $X(2^i, 1) = \mathrm{Cay}(Z_{2^i}, \{1\})$, $X(2^i, 2) = \mathrm{Cay}(Z_{2^i}, \{1, -1\})$, and $X(2^i, 3) = \mathrm{Cay}(Z_{2^i}, \{1, -1+2^{i-1}\})$. Then we have:

Theorem 4.2.3. (i) For an odd prime p, every connected normal edge-transitive circulant digraph of order p^m is isomorphic to the lexicographic product $X(p^i, r)[p^{m-i}K_1]$ for some positive divisor r of $p-1$ and an integer i with $1 \le i \le m$; different choices of i or r give nonisomorphic digraphs.

(ii) Every connected normal edge-transitive circulant digraph of order 2^m is isomorphic to the lexicographic product $X(2^i, j)[2^{m-i}K_1]$ for some integers i, j such that

$$1 \le j \le 3 \le i \le m \text{ or } 1 \le j \le i = 2 \text{ for } 3 \le m,$$

and

$$1 \leq j \leq i = m \text{ for } m = 1, 2;$$

moreover, different choices of i or j give nonisomorphic digraphs.

We note that the analogous result can be given for $n = 2p^m$ for odd prime p. The result can be stated as follows:

For each positive divisor r of $p-1$, there is a unique subgroup of order r in the cyclic group U_{2p^i}. The Cayley digraph of Z_{2p^i} on the subgroup of order r in U_{2p^i} is denoted by $X(p^i, r)$.

Theorem 4.2.4. For an odd prime p, every connected normal edge-transitive circulant digraph of order $2p^m$ is isomorphic to the lexicographic product $X(p^i, r)[p^{m-i}\mathrm{K}_1]$ for some positive divisor r of $p-1$ and an integer i with $1 \leq i \leq m$, different choices of i or r giving nonisomorphic digraphs.

4.3 The isomorphism problem

First consider the case when $n = 2^m$. We assume that $m \geq 3$. It is well known that $\mathrm{U}_{2^m} = \langle -1 \rangle \cdot \langle 5 \rangle \cong \mathrm{Z}_2 \times \mathrm{Z}_{2^{m-2}}$. For each $i = 2, 3, ..., m,$ let

$$S_i = \{1 + k2^i \mid k = 0, 1, ..., 2^{m-i}-1\}.$$

Then $S_2, S_3, ..., S_m$ consist of all subgroups of $\langle 5 \rangle$. For each $i = 2, ..., m-1$, let

$$T_i = S_{i+1} \cup \{ -1 + k2^i \mid 1 \le k \le 2^{m ¡ i}-1,\ k: \text{ odd} \}.$$

Then T_i is a subgroup of U_{2^m} such that $|T_i| = |S_i| = 2^{m ¡ i}$. Let T be a subgroup of U_{2^m}, and let π be the natural projection from U_{2^m} onto $\langle 5 \rangle$. Then $T^{\pi} = S_i$, for some $i = 2, 3, ..., m$. Then there exits a homomorphism θ from S_i to $\langle -1 \rangle / \langle -1 \rangle \cap T$ such that $T = \{ st \mid s^{\theta} = t \cdot \langle -1 \rangle \cap T,\ s \in S_i \}$. If T contains -1, then the only such homomorphism is trivial; therefore T is the direct product of S_i and $\langle -1 \rangle$. Suppose that T does not contain -1. If $S_i^{\theta} = \langle 1 \rangle$, then θ is the trivial homomorphism, and hence $T = S_i$. If $S_i^{\theta} = \langle -1 \rangle$, it follows from $\mathrm{Ker}\theta = S_{i+1}$ and $S_i^{\theta} = \langle -1 \rangle \cong \mathrm{Z}_2$ that $T = T_i$ for some $i = 2, ..., m-1$.

Consequently, we have the following lemma.

Lemma 4.3.1. $\{ S_i, T_j, \langle -1 \rangle \cdot S_i \mid i = 2, 3, ..., m,\ j = 2, 3, ..., m-1 \}$ is the set of all subgroups of U_{2^m}.

Let S be a subset of Z_{2^m}. For each positive integer l, define $¢_l(S)$ by

$$¢_l(S) := \{ (s_1, s_2, ..., s_l) \mid s_1, s_2, ..., s_l \in S,\ s_1 + s_2 + \cdots + s_l = 0 \text{ in } \mathrm{Z}_{2^m} \}.$$

Let θ: Cay(Z_{2^m}, S) $\longrightarrow$ Cay(Z_{2^m}, T) be an isomorphism with $0^{\theta} = 0$, and let

$$x_0 = 0,\ x_1 = s_1,\ x_2 = s_1 + s_2, ...,\ x_l = s_1 + s_2 + \cdots + s_l.$$

Define $t_i = x_i^\theta - x_{i\,¡\,1}^\theta$ for each $i = 1, 2, ..., l.$ Then $(t_1, t_2, ..., t_l) \in$ ¢$_l(T).$ The map $(s_1, s_2, ..., s_l) \mapsto (t_1, t_2, ..., t_l)$ defines a bijective map between ¢$_l(S)$ and ¢$_l(T).$

To each subset S of $Z_{2^m},$ we assign a positive number $g(S)$ defined by

$$g(S) = \min\{\, l \mid ¢_l(S) \neq \emptyset \,\}.$$

Then we have:

Lemma 4.3.2. If Cay$(Z_{2^m}, S) \cong$ Cay(Z_{2^m}, T) then $|¢_l(S)| = |¢_l(T)|$ and $g(S) = g(T)$ for each l.

We now calculate $g(S_i)$ and $g(T_i)$. We recall that

$$S_i = \{\, 1 + k2^i \mid k = 0, 1, 2, ..., 2^{m\,¡\,i}-1 \,\}.$$

Since $1 + k2^i \equiv 1 \bmod 2^i,$ it follows that $g(S_i) \equiv 0 \bmod 2^i,$ that is, $g(S_i) \geq 2^i$. We observe that

$$2^m = (2^i - 1) + (1 + (2^{m\,¡\,i}-1)2^i) = 1 + 1 + \cdots + 1 + (1 + (2^{m\,¡\,i}-1)2^i).$$

Therefore $g(S_i) \leq 2^i$, and so $g(S_i) = 2^i$.

We then consider $g(T_i)$. We also recall that
$T_i = \{1 + k2^i \mid 0 \leq k \leq 2^{m\,¡\,i}-1,\ k:$ even$\} \cup \{-1 + k2^i \mid 0 \leq k \leq 2^{m\,¡\,i}-1,\ k:$ odd$\}.$
Since $-1 + k2^i \equiv 1 \bmod 2$ and $1 + k2^i \equiv 1 \bmod 2$, we have $g(T_i) \equiv 0 \bmod 2$. If $t_1, t_2 \in T_i$ and $t_1 + t_2 \equiv 0 \bmod 2^m$, then $-1 = t_1 t_2^{¡1}$ in T_i; this yields a

contradiction since T_i does not contain -1. Therefore $g(T_i) \geq 4$. However, since

$$1 + 1 + (-1 + 2^i) + (-1+(2^{m-i}-1)2^i) = 2^m,$$

we get $g(T_i) = 4$.

We summarize this observation as follows.

Lemma 4.3.3. (i) $g(S_i) = 2^i$; (ii) $g(T_i) = 4$; (iii) $g(S_i) = g(T_i) \iff i = 2$.

Fixing m, we denote

$$U := \{\, (a,b,c,d) \mid a+b+c+d = k2^{m-2},\ 0 \leq a,b,c \leq 2^{m-2}-1,\ a,b,c,d,k: \text{ integers}\,\},$$

$$X := \{(a,b,c,0) \in U\}, \quad Y := \{(a,b,c,2^{m-2}) \in U\,\},$$

$$Z := \{(a,b,c,d) \in U \mid 1 \leq d \leq 2^{m-2}-1\}.$$

Let $\lambda\colon X \longrightarrow Y$ be a map defined by $(a,b,c,0)^\lambda = (a,b,c,2^{m-2})$. Then λ is bijective, and so

$$|X| = |Y|.$$

Let (a,b,c,d) be an element of $Y \cup Z$. Then $1+4a$, $1+4b$, $1+4c$, $1+4(d-1)$ are contained in S_2 and $(1+4a) + (1+4b) + (1+4c) + (1+4(d-1)) = k2^m = 0$ in Z_{2^m}. Therefore, we have that $(1+4a,\ 1+4b,\ 1+4c,\ 1+4(d-1)) \in ¢_4(S_2)$. The map $\mu : Y \cup Z \longrightarrow ¢_4(S_2)$ defined by

$$(a,b,c,d)^\mu = (1+4a,\ 1+4b,\ 1+4c,\ 1+4(d-1))$$

is bijective, and hence $|Y \cup Z|$ = $|¢_4(S_2)|$.

Let (x_1, x_2, x_3, x_4) be an element of $¢_4(T_2)$. Since $x_1 + x_2 + x_3 + x_4 = k2^m$ and either $x_i \equiv 1 \bmod 4$ or $x_i \equiv -1 \bmod 4$, there exists a permutation σ on $\{1, 2, 3, 4\}$ such that $x_{\sigma(1)} \equiv x_{\sigma(2)} \equiv 1 \bmod 4$, and $x_{\sigma(3)} \equiv x_{\sigma(4)} \equiv -1 \bmod 4$. Define

$$y_1 = (x_{\sigma(1)} - 1)/4, \; y_2 = (x_{\sigma(2)} - 1)/4, \; y_3 = (x_{\sigma(3)} + 1)/4, \; y_4 = (x_{\sigma(4)} + 1)/4.$$

The map $(x_1, x_2, x_3, x_4) \mapsto (y_{\sigma i 1(1)}, y_{\sigma i 1(2)}, y_{\sigma i 1(3)}, y_{\sigma i 1(4)})$ defines an injective map from $¢_4(T_2)$ into $X \cup Z$. Since (y_1, y_2, y_3, y_4) cannot be equal to $(0, 0, 0, 0)$, this map is not surjective. Therefore $|¢_4(T_2)| < |X \cup Z| = |Y \cup Z| = |¢_4(S_2)|$.

Thus we have:

Lemma 4.3.4. $|¢_4(S_2)| > |¢_4(T_2)|$.

Even though, it is not necessary to give the exact values of $|¢_4(S_2)|$ and $|¢_4(T_2)|$ for the proof of the isomorphism theorem, we calculate the numbers here:

Remark 4.3.5. (1) $|¢_4(S_2)| = 2^{3m i 6}$; (2) $|¢_4(T_2)| = 3 \cdot 2^{3m i 8}$.

Proof. (1) Let $S(m, k) = \{(x_1, x_2, x_3, x_4) \,|\, x_1 + x_2 + x_3 + x_4 = k2^{m i 2} - 1, 0 \le x_1, x_2, x_3, x_4 \le 2^{m i 2} - 1\}$ and let $H(m, k) = \{(x_1, x_2, x_3, x_4) \,|\, x_1 + x_2 + x_3 + x_4 = k2^{m i 2} - 1, \; 0 \le x_1, x_2, x_3, x_4 \le k2^{m i 2} - 1\}$.

Then it is well-known that $|H(m,k)| ={}_{2+k2^{\text{m ¡ 2}}}C_{k\text{¢}2^{\text{m ¡ 2}}\text{ ¡ }1}$.

Let $a = 1 + 4x_1$, $b = 1 + 4x_2$, $c = 1 + 4x_3$, $d = 1 + 4x_4$. Then $a + b + c + d = 4 + 4(x_1 + x_2 + x_3 + x_4) = k \cdot 2^m, k = 1, 2, 3$. Since

$$\text{¢}_4(S_2) = \{(a, b, c, d) \,|\, a, b, c, d \in S_2,\ a + b + c + d = 0 \text{ in } \mathrm{Z}_{2^{\mathrm{m}}}\},$$

where $S_2 = \{1 + 4k \,|\, 0 \le k \le 2^{m\,\text{¡}\,2} - 1\}$, it follows that $(a, b, c, d) \in \text{¢}_4(S_2)$ if and only if

$x_1 + x_2 + x_3 + x_4 = k2^{m\,\text{¡}\,2} - 1$, where $0 \le x_1, x_2, x_3, x_4 \le 2^{m\,\text{¡}\,2} - 1$, $k = 1, 2, 3$. Thus

$$|\,\text{¢}_4(S_2)| = |S(m, 1)| + |S(m, 2)| + |S(m, 3)|.$$

By the straightforward calculation, we see that

$$H(m, 1) = S(m, 1),\ |H(m, 2)| = |S(m, 2)| + 4|S(m, 1)| \text{ and}$$

$$|H(m, 3)| = |S(m, 3)| + 4|S(m, 2)| + 10|S(m, 1)|.$$

This yields that $|\,\text{¢}_4(S_2)| = |S(m, 1)| + |S(m, 2)| + |S(m, 3)| = 2^{3m\,\text{¡}\,6}$.

(2) Recall that $\text{¢}_4(T_2) = \{(x_1, x_2, x_3, x_4) \,|\, x_1, x_2, x_3, x_4 \in T_2, x_1 + x_2 + x_3 + x_4 = 0, \text{ in } \mathrm{Z}_{2^{\mathrm{m}}}\}$, where $T_2 = \{1 + 4k \,|\, 0 \le k \le 2^{m\,\text{¡}\,2} - 1,\ k \text{ is even }\} \cup \{-1 + 4k \,|\, 0 \le k \le 2^{m\,\text{¡}\,2} - 1,\ k \text{ is odd }\}$.

Let $T_2(e) = \{1 + 4k \,|\, 0 \le k \le 2^{m\,\text{¡}\,2} - 1,\ k \text{ is even }\}$ and let

$T_2(o) = \{-1 + 4k \,|\, 0 \le k \le 2^{m\,\text{¡}\,2} - 1,\ k \text{ is odd }\}$. Then $T_2 = T_2(e) \cup T_2(o)$. Therefore, if $(x_1, x_2, x_3, x_4) \in \text{¢}_4(T_2)$, then two elements of $\{x_1, x_2, x_3, x_4\}$ are in $T_2(e)$ and two elements of $\{x_1, x_2, x_3, x_4\}$ are in $T_2(o)$.

Define

$$y_i = \begin{cases} \frac{x_i - 1}{4} & \text{if } x_i \in T_2(e) \\ \frac{x_i + 1}{4} & \text{if } x_i \in T_2(o) \end{cases}$$

If $(x_1, x_2, x_3, x_4) \in \Delta_4(T_2)$, then we have $x_1 + x_2 + x_3 + x_4 = k2^m$, where $x_1, x_2, x_3, x_4 \in T_2$, $k = 1, 2, 3$ and so $x_1+x_2+x_3+x_4 = 4(y_1+y_2+y_3+y_4) = k2^m$, where $0 \leq y_1, y_2, y_3, y_4 \leq 2^{m-2} - 1$, $k = 1, 2, 3$.

Therefore $y_1 + y_2 + y_3 + y_4 = k2^{m-2}$, where $0 \leq y_1, y_2, y_3, y_4 \leq 2^{m-2} - 1$, $k = 1, 2, 3$, two elements of $\{y_1, y_2, y_3, y_4\}$ are even, and two elements of $\{y_1, y_2, y_3, y_4\}$ are odd.

Define

$H(m, k) = \{(x_1, x_2, x_3, x_4) \,|\, x_1+x_2+x_3+x_4 = k2^{m-2},\ 0 \leq x_1, x_2, x_3, x_4 \leq k2^{m-2}\}$,

$T(m, k) = \{(y_1, y_2, y_3, y_4) \,|\, y_1+y_2+y_3+y_4 = k2^{m-2},\ 0 \leq y_1, y_2, y_3, y_4 \leq 2^{m-2}-1\}$,

$T_e(m, k) = \{(y_1, y_2, y_3, y_4) \in T(m, k) \,|\, y_1, y_2, y_3, y_4$: even $\}$ and

$T_o(m, k) = \{(y_1, y_2, y_3, y_4) \in T(m, k) \,|\, y_1, y_2, y_3, y_4$: odd $\}$.

Then $|\Delta_4(T_2)| = \sum_{k=1} |T(m, k)| - \sum_{k=1} |T_e(m, k)| - \sum_{k=1} |T_o(m, k)|$ and

$$|H(m, k)| = {}_{3+k2^{m-2}} C_{k2^{m-2}}.$$

With the straightforward calculation, we have

$$|H(m, 1)| = |T(m, 1)| + 4,\ |H(m, 2)| = |T(m, 2)| + 4|T(m, 1)| + 10$$

and $|H(m, 3)| = |T(m, 3)| + 4|T(m, 2)| + 10|T(m, 1)| + 20$.

We then have $\sum_{k=1} |T(m, k)| = 2^{3m-6} - 1$.

We now consider $\sum_{k=1} |T_e(m,k)|$. Let $z_1 = \frac{y_1}{2}, z_2 = \frac{y_2}{2}, z_3 = \frac{y_3}{2}, z_4 = \frac{y_4}{2}$. Then $z_1 + z_2 + z_3 + z_4 = k2^{m-3},\ 0 \le z_1, z_2, z_3, z_4 \le 2^{m-3} - 1$. Hence

$|T_e(m,k)|$

$= |\{(z_1,z_2,z_3,z_4) \mid z_1 + z_2 + z_3 + z_4 = k2^{m-3},\ 0 \le z_1, z_2, z_3, z_4 \le 2^{m-3} - 1\}|$

$= |T(m-1,k)|$.

Therefore $\sum_{k=1} |T_e(m,k)| = \sum_{k=1} |T(m-1,k)| = 2^{3(m-1)-6} - 1 = 2^{3m-9} - 1$.

We want to know $\sum_{k=1} |T_o(m,k)|$.

Let $z_1 = \frac{y_1-1}{2}, z_2 = \frac{y_2-1}{2}, z_3 = \frac{y_3-1}{2}, z_4 = \frac{y_4-1}{2}$. Then we have

$$z_1 + z_2 + z_3 + z_4 = k2^{m-3} - 2,\ 0 \le z_1, z_2, z_3, z_4 \le 2^{m-3} - 1.$$

We observe that $|T_o(m,1)| = |H(m-1,1)|$. Since

$|T_o(m,2)|$

$= |\{(z_1,z_2,z_3,z_4) \mid z_1 + z_2 + z_3 + z_4 = 2^{m-2} - 2,\ 0 \le z_1, z_2, z_3, z_4 \le 2^{m-3} - 1\}|$,

$|H(m-1,2)| = 4|T_o(m,1)| + |T_o(m,2)|$. If $k = 3$, then

$|T_o(m,3)|$

$= |\{(z_1,z_2,z_3,z_4) \mid z_1 + z_2 + z_3 + z_4 = 3 \cdot 2^{m-3} - 2,\ 0 \le z_1, z_2, z_3, z_4 \le 2^{m-3} - 1\}|$,

and so $|H(m-1,3)| = |T_o(m,3)| + 4|T_o(m,2)| + 10|T_o(m,1)|$.

Therefore, we have $\sum_{k=1} |T_o(m,k)| = 2^{3m-9}$.

Since $|\Delta_4(T_2)| = \sum_{k=1} |T(m,k)| - \sum_{k=1} |T_e(m,k)| - \sum_{k=1} |T_o(m,k)|$, we have

$$|\Delta_4(T_2)| = 2^{3m-6} - 1 - (2^{3m-9} - 1) - 2^{3m-9} = 2^{3m-6} - 2^{3m-8} = 3 \cdot 2^{3m-8}.$$

Consequently, $|¢_4(S_2)| = 4 \cdot 2^{3m ¡ 8} > 3 \cdot 2^{3m ¡ 8} = |¢_4(T_2)|$. □

We are now ready to give the proof of Theorem 4.2.2 for the case when $n = 2^m, p^m$ or $2p^m$ for an odd prime p.

We first consider the case when $n = 2^m$, $m \geq 3$. Let S and T be subgroups of U_n. Suppose that the corresponding Cayley digraphs are isomorphic. Then of course $|S| = |T|$. If the Cayley digraphs are undirected, then both S and T contain -1, and hence $S = T = \langle -1 \rangle S_i$ for some $i = 2, 3, ..., m$, by Lemma 4.3.1. We then assume that the Cayley digraphs are not undirected. Then neither $-1 \in S$ nor $-1 \in T$. Suppose that $S \neq T$. From Lemma 4.3.1, we may assume that $S = S_i$ and $T = T_i$ for some $i = 2, 3, ..., m-1$. If $i > 2$ then $g(S) = 2^i > 4 = g(T)$ by Lemma 4.3.3; this is a contradiction to Lemma 4.3.2. Therefore $i = 2$. By Lemma 4.3.4, $|¢_4(S_2)| \neq |¢_4(T_2)|$, which yields a contradiction by Lemma 4.3.2. Consequently $S = T$.

We now consider the other cases when $n = 2,\ 4,\ p^m$, or $2p^m$ for odd prime p. In these cases U_n is cyclic. Therefore if $|S| = |T|$ then $S = T$. This completes the proof.

The method we applied for this special case may not be applied to yield a proof for general case, namely for arbitrarily given number n. Our isomorphism problem was solved in the author's joint paper [38] by using some basic properties of Schur ring theory, and we describe it here.

We will prove the following:

Lemma 4.3.6. If two connected normal edge-transitive circulant digraphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isomorphic, then they are Cayley isomorphic.

We note that Klin and Pöschel in [20] first applied the method of Schur rings to solve isomorphism problems of circulant digraphs and they succeeded in solving the isomorphism problem for circulant digraphs of odd prime-power order in [20]. We also note that our isomorphism theorem may be an immediate consequence of Toida Conjecture; after the first version of this thesis was written, we just realized that Toida Conjecture was very recently proved.

Let $G = \mathbb{Z}_n$ be the cyclic group order n. For the conveniency, we shall use the multiplicative notation for the cyclic group $\mathbb{Z}_n$. So 1, rather than 0, denotes the identity element of $\mathbb{Z}_n$. We also choose a generator x, so that $G = \mathbb{Z}_n = \{1, x, x^2, ..., x^{n-1}\}$.

Let $X = \mathrm{Cay}(G, S)$ be a Cayley digraph of G on a subset S. Let A be the automorphism group of the digraph X and let A_1 be the subgroup of all automorphisms of X that fix 1. Let S_1, $S_2, ..., S_k$ be all orbits of the natural action of A_1 on G. Let $\mathbb{Z}[G]$ be the group ring of G over the integer ring $\mathbb{Z}$, which consists of the formal sums $\sum_{g \in G} c_g g$, where c_g are integers.

For each subset $T = \{t_1, t_2, ..., t_s\}$ of G, we denote $t_1 + t_2 + \cdots + t_s$ by $\underline{T}$ and call it a simple quantity. Then the transitivity module $\mathbb{Z}(G, A_1)$

belonging to A_1 is the module generated by $\underline{S_1}, \underline{S_2}, ..., \underline{S_k}$, which are called the basic quantities. It is known as Schur's fundamental theorem (see [40]) that the transitivity module is a subring of the group ring.

Let X = Cay(G, S) and Y = Cay(G, T) be isomorphic circulant digraphs with automorphism groups A and B, respectively. Let $\lambda : G \longrightarrow G$ be an isomorphism of X onto Y such that $1^\lambda = 1$. Since A is vertex-transitive we can choose such λ. Obviously, we have $B = \lambda^{\text{i}1} A \lambda$ and $B_1 = \lambda^{\text{i}1} A_1 \lambda$ is the group of all automorphisms of Y that ¯x 1. The isomorphism λ extends to a linear operator of Z(G, A_1) onto Z(G, B_1). Of course λ sends each simple quantity of Z(G, A_1) to a simple quantity of Z(G, B_1). Let y be an element of G and let $R(y)$ be the right regular representation of y de¯ned by $z^{R(y)} = zy$ for all z in G.

Then $(S_i y)^\lambda = (S_i)^{R(y)\lambda R((y^{\cdot})^{\text{i}1})\lambda^{\text{i}1}\lambda R(y^{\cdot})} = (S_i)^{\alpha\lambda R(y^{\cdot})} = (S_i)^\lambda y^\lambda$ where $\alpha = R(y)\lambda R((y^\lambda)^{\text{i}1})\lambda^{\text{i}1}$ is an automorphism of X such that $1^\alpha = 1$. Since $(\underline{S_i} \cdot \underline{y})^\lambda = \underline{(S_i y)^\lambda}$, we have $(\underline{S_i} \cdot \underline{y})^\lambda = (\underline{S_i})^\lambda \cdot (\underline{y})^\lambda$. This implies that the linear operator λ preserves multiplication of the subring, and so λ is a ring-isomorphism between Z(G, A_1) and Z(G, B_1).

Let a be an automorphism of G. Let $\underline{S} = s_1 + s_2 + \cdots + s_t$. Then we denote $\underline{S}^a = {s_1}^a + {s_2}^a + \cdots + {s_t}^a$, and we also denote $\underline{S}^{(m)} = s_1^m + s_2^m + \cdots + s_t^m$ for each positive integer m. We want to show $(\underline{S}^a)^\lambda = (\underline{S}^\lambda)^a$ for each simple quantity $\underline{S}$ of Z(G, A_1) by using the same idea of the proof of Theorem 23.9(a) in [40].

It is enough to prove that $(\underline{S}^{(p)})^{\lambda}$ = $(\underline{S}^{\lambda})^{(p)}$ for each prime p in U_n. Since $(\underline{S})^p \equiv \underline{S}^{(p)}$ mod p, we have $(\underline{S}^{\lambda})^p$ = $(\underline{S}^p)^{\lambda} \equiv (\underline{S}^{(p)})^{\lambda}$ mod p. On the other hand, $\underline{S^{\lambda}}$ is a simple quantity of Z(G, B_1) and hence $(\underline{S}^{\lambda})^p \equiv (\underline{S}^{\lambda})^{(p)}$ mod p. Thus $(\underline{S}^{\lambda})^{(p)} \equiv (\underline{S}^{(p)})^{\lambda}$ mod p. We know that both sides of the congruence are simple quantities. Therefore $(S^{\lambda})^{(p)}$ = $(S^{(p)})^{\lambda}$ and so we have done. Since S^{λ} = T, we have the following immediate consequence of this observation.

Lemma 4.3.7. If Cay(Z$_n, S$) and Cay(Z$_n, T$) are isomorphic, then the following holds. Aut(Z$_n, S$) = Aut(Z$_n, T$).

Now let X = Cay(Z$_n, S$) and Y = Cay(Z$_n, T$) be isomorphic connected normal edge-transitive circulant digraphs. From the proof of Theorem 4.2.1 we have known that X and Y are Cayley isomorphic to Cay(Z$_n, S^0$) and Cay(Z$_n, T^0$) respectively for some subgroups S^0 and T^0 of U$_n$. Then by Lemma 4.3.7, Aut(Z$_n, S^0$) = Aut(Z$_n, T^0$), that is S^0 = T^0. This completes the proof of Lemma 4.3.6, and so Theorem 4.2.2 is now proved.

Now we will give a proof of Theorem 4.2.3.

Let p be an odd prime. Then U$_{p^{\mathrm{m}}}$ is a cyclic group of order $(p-1)p^{m\,\mathrm{i}\,1}$. Let S be a subgroup of U$_{p^{\mathrm{m}}}$ and let B be the Sylow p-subgroup of S. Then B = $\{1 + kp^i \mid k$ = $0, 1, 2, ..., p^{m\,\mathrm{i}\,i}-1\}$ for some integer i = $1, 2, ..., m$ and $|B|$ = $p^{m\,\mathrm{i}\,i}$.

Let M := $\{kp^i \mid k$ = $0, 1, 2, ..., p^{m\,\mathrm{i}\,i}-1\}$. Then M is the subgroup of

Z$_{p^{\mathrm{m}}}$ of order $p^{m\,\mathrm{i}\,i}$, and B = 1 + M. We see that

$$S = \cup_{a2S}\ aB = \cup_{a2S}\ a(1 + M) = \cup_{a2S}\ (a + M).$$

So S is a union of coset of M in Z$_{p^{\mathrm{m}}}$. Let r denote $|S/B|$, which is a divisor of $p{-}1$. If $a + M = a^0 + M$ for some a, a^0 in S, then $a^{\mathrm{i}\,1}a^0 \in 1 + M = B$, and so $aB = a^0B$. Therefore $|S/M| = r$. By Lemma 4.1.5, we have

$$\mathrm{Cay}(\mathrm{Z}_{p^{\mathrm{m}}}, S) = \mathrm{Cay}(\mathrm{Z}_{p^{\mathrm{m}}}/M, S/M)[p^{m\,\mathrm{i}\,i}\mathrm{K}_1].$$

We want to show that

$$\mathrm{Cay}(\mathrm{Z}_{p^{\mathrm{m}}}/M, S/M) \cong X(p^i, r).$$

Let θ : Z$_{p^{\mathrm{m}}}$ $\longrightarrow$ Z$_{p^{\mathrm{i}}}$ be the natural homomorphism, namely $x^\theta \equiv x$ mod p^i. Then Kerθ = M and S^θ is a subgroup of U$_{p^{\mathrm{i}}}$ since θ preserves the multiplication as well. The homomorphism θ induces the isomorphism $\overset{1}{\theta}$ from Z$_{p^{\mathrm{m}}}/M$ onto Z$_{p^{\mathrm{i}}}$. Note that $(S/M)^{\overset{1}{\theta}} = S^\theta$. Therefore $\overset{1}{\theta}$ is also an isomorphism between Cay(Z$_{p^{\mathrm{m}}}/M, S/M$) and Cay(Z$_{p^{\mathrm{i}}}, S^\theta$). Since S^θ is the unique subgroup of order r in U$_{p^{\mathrm{i}}}$, it follows that Cay(Z$_{p^{\mathrm{i}}}, S^\theta$) = $X(p^i, r)$. The proof of (i) of the theorem is now complete.

We then consider (ii) of the theorem. We first assume that $m \geq 3$. Let S be a subgroup of U$_{2^{\mathrm{m}}}$. Then S is one of those listed in Lemma 4.3.1. Write B for $S \cap \langle 5 \rangle$. Then $B = \{1 + k2^i \mid k = 0, 1, ..., 2^{m\,\mathrm{i}\,i}{-}1\}$ for some $i = 2, 3, ..., m$. Let $M := \{k2^i \mid k = 0, 1, 2, ..., 2^{m\,\mathrm{i}\,i}{-}1\}$. Then

M is a subgroup of order 2^{m-i} of Z_{2^m}. Since $B = 1 + M$, S is a union of some cosets of M in Z_{2^m}. In fact either i) $S = 1 + M$, or ii) $S = (1 + M) \cup (-1 + M)$, or iii) $S = (1 + M) \cup (-1 + 2^{i-1} + M)$, $3 \leq i \leq m$ from Lemma 4.3.1. Let $\theta : \mathrm{Z}_{2^m} \longrightarrow \mathrm{Z}_{2^i}$ be the natural homomorphism such that $x^\theta \equiv x \bmod 2^i$. Then $\mathrm{Ker}\theta = M$, and $S^\theta = \{1\}$ for i), $S^\theta = \{1, -1\}$ for ii) and $S^\theta = \{1, -1 + 2^{i-1}\}$, $3 \leq i \leq m$ for iii). Since $\mathrm{Cay}(\mathrm{Z}_{2^m}/M, S/M) \cong \mathrm{Cay}(\mathrm{Z}_{2^i}, S^\theta)$, it follows from Lemma 4.1.5 that $\mathrm{Cay}(\mathrm{Z}_{2^m}, S) \cong \mathrm{Cay}(\mathrm{Z}_{2^i}, S^\theta)[2^{m-i}\mathrm{K}_1]$, where i varies from 2 to m for i) and ii), while i does from 3 to m for iii).

We observe that $\mathrm{Cay}(\mathrm{Z}_{2^i}, S^\theta) = X(2^i, 1)$, $2 \leq i \leq m$ for i), $\mathrm{Cay}(\mathrm{Z}_{2^i}, S^\theta) = X(2^i, 2)$, $2 \leq i \leq m$ for ii), and $\mathrm{Cay}(\mathrm{Z}_{2^i}, S^\theta) = X(2^i, 3)$, $3 \leq i \leq m$ for iii). Consequently $\mathrm{Cay}(\mathrm{Z}_{2^m}, S) \cong X(2^i, j)[2^{m-i}\mathrm{K}_1]$ where $3 \leq i \leq m$, $1 \leq j \leq 3$, or $i = 2$, $j = 1, 2$. For $m = 2$ or 1, $S = \{1\}$, or $S = \{1, -1\}$, and so $\mathrm{Cay}(\mathrm{Z}_{2^m}, S) = X(2^m, j)$ where $1 \leq j \leq m$. This proves (ii) of the theorem.

4.4 Cayley Isomorphisms for circulant digraphs

In this section, we consider Cayley Isomorphism Problem for finite circulant digraphs. We recall that a Cayley digraph $\mathrm{Cay}(G, S)$ is called a CI-digraph of G if for each Cayley digraph $\mathrm{Cay}(G, T)$ isomorphic to $\mathrm{Cay}(G, S)$, there exists $\sigma \in \mathrm{Aut}(G)$ such that $S^\sigma = T$.

We outline the Huang and Meng's observation in [19] with slightly different elucidation.

Let G be a finite cyclic group, written additively and let S be a Cayley subset of G, namely a subset not containing the identity element 0. Let K be the set $\{a \in G \mid a + S = S\}$. Then it is easy to show that K is a subgroup of G. In fact, K is the largest subgroup of G such that S is a union of some cosets of K in G. We denote the subgroup by $\mathrm{Int}(S)$.

Let M be a subgroup of the cyclic group G. A partition $S = S_1 \cup S_2$ of a Cayley subset S is called an M-partition if M is a subgroup of $\mathrm{Int}(S_1)$ and M contains S_2. An M-partition is maximal if S has no M-partition for all subgroup containing M.

The following theorem has been given by Huang and Meng in [19].

Theorem 4.4.1. Let G be a finite cyclic group and let S be a Cayley subset of G. If $S = S_1 \cup S_2$ is a maximal M-partition for a nontrivial subgroup M of G, then $\mathrm{Cay}(G, S)$ is a CI-digraph of G if and only if both $\mathrm{Cay}(G, S_1)$ and $\mathrm{Cay}(G, S_2)$ are CI-digraphs of G and $\langle \mathrm{Aut}(G, S_1), \mathrm{Aut}(G, S_2) \rangle = \mathrm{Aut}(G)$.

It is unhappy that this theorem does not tell us anything if $S_2 = ?$; the case is, in fact, when $\mathrm{Int}(S) = M$ is nontrivial. To complement it we observe the following theorem.

Theorem 4.4.2. Let G be a finite cyclic group and let S and T be a Cayley subset of G. If Cay$(G, S) \cong$ Cay(G, T), then Int(S) = Int(T) and Cay$(G/\text{Int}(S), S/\text{Int}(S)) \cong$ Cay$(G/\text{Int}(S), T/\text{Int}(S))$.

Proof. Let $\varphi :$ Cay$(G, S) \longrightarrow$ Cay(G, T) be an isomorphism from the Cayley digraph Cay(G, S) onto the Cayley digraph Cay(G, T) with $0^\varphi = 0$. Let $K :=$ Int(S). Then Int$(T) = K^\varphi$. Since G is cyclic, of course $K^\varphi = K$, and so Int(S) = Int(T); in particular, $K^\alpha = K$ for each α in Aut(Cay(G, S)) with $0^\alpha = 0$. Note that $\alpha_0 := R(x)\varphi R(-x^\varphi)\varphi^{-1}$ for each x in G is an automorphism of Cay(G, S) such that $0^{\alpha_0} = 0$. Therefore, $K^{\alpha_0} = K$. Thus

$$(K + x)^\varphi = K^{R(x)\varphi R(-x^\varphi)\varphi^{-1}\varphi R(x^\varphi)} = K^{\alpha_0 \varphi R(x^\varphi)} = K + x^\varphi.$$

Consequently, φ maps each coset of K to a coset of K. This implies that φ induces an isomorphism from Cay$(G/K, S/K)$ onto Cay$(G/K, T/K)$. □

As a consequence of the above theorem, we have the following, which complements Huang and Meng's Theorem:

Corollary 4.4.3. Let Cay(G, S) be a Cayley digraph of a finite cyclic group G with Int$(S) = K$. If Cay$(G/K, S/K)$ is a CI-digraph of G/K, then Cay(G, S) is a CI-digraph of G.

Proof. Let $G = \mathrm{Z}_n$ be a cyclic group of order n, written additively. Assume that Cay$(G/K, S/K)$ is a CI-digraph of G/K. Let Cay(G, T) be a Cayley digraph such that Cay$(G, S) \cong$ Cay(G, T). From the above theorem, we have

Cay$(G/K, S/K) \cong$ Cay$(G/K, T/K)$. Since Cay$(G/K, S/K)$ is a CI-digraph, we have $(S/K)^\alpha = T/K$ for some α in Aut(G/K). Then $(K+1)^\alpha = K + r$ for some positive integer r relatively with $m := |G/K|$. It is routine to show that the map $1 \mapsto r$ induces an automorphism β of G such that $S^\beta = T$. Consequently, Cay(G, S) is a CI-digraph of G. □

Bibliography

[1] A. Ádám, `Research problem 2-10', J. Combin. Theory 2 (1967), 393.

[2] B. Alspach and L. Nowitz, `Elementary proofs that $Z_p{}^2$ and $Z_p{}^3$ are CI-groups', European J. Combin., 19 (1999), 607-617.

[3] B. Alspach and T. D. Parsons, `Isomorphisms of circulant graphs and digraphs', Discrete Math., 25 (1979), 97-108.

[4] L. Babai, `Finite digraphs with given regular automorphism groups', Period. Math. Hungar., 11 (1980), 257-270.

[5] L. Babai, `Isomorphism problem for a class of point-symmetric structures', Acta Math. Acad. Sci. Hungar., 29 (1977), 329-336.

[6] L. Babai and P. Frankl, `Isomorphisms of Cayley graphs I', Combinatorics, (Keszthely, 1976),35-52; Colloq. Math. Soc. J. Bolyai,18, North-Holland, Amsterdam, (1978),

[7] Y. G. Baik, Y. Q. Feng, H. S. Sim and M. Y. Xu, `On the normality of Cayley graphs of Abelian groups', Algebra Colloq., 5 (1998), 297-304.

[8] N. L. Biggs and A. T. White, Permutation Groups and Combinatorial Structure, Cambridge University Press (1979).

[9] I. Z. Bouwer, `Vertex and edge-transitive but not 1-transitive graphs', Canad. Math. Bull., 13 (1970), 231-237.

[10] C. Y. Chao, `On the classification of symmetric graphs with a prime number of vertices', Trans. Amer. Math. Soc. 158 (1971), 247-256.

[11] Y. Cheng and J. Oxley, `On weakly symmetric graphs of order twice a prime', J. Combin. Theory Ser. B 4 (1987), 196-211.

[12] H. S. M. Coxeter and W. O. J. Moser, Generators and Relations for Discrete Groups, Springer-Verlag (1972).

[13] J. D. Dixon and B. Mortimer, Permutation Groups, Springer-Verlag (1991).

[14] E. Dobson, `Isomorphism problem for Cayley graph of $Z_p{}^3$', Discrete Math., 147 (1995), 87-94.

[15] B. Elspas and J. Turner, `Graphs with circulant adjacency matrices', J. Combin. Theory 9 (1970), 297-307.

[16] G. D. Godsil, `GRR's for non-solvable groups', Colloq. Math. Soc. Jannos Bolyai, 25 (1978), 221-239.

[17] D. F. Holt, `A graph which is edge transitive but not arc-transitive', J. Graph Theory, 5 (1981), 201-204.

[18] P. Houlis, Quotients of normal edge-transitive Cayley graphs, M.Sc. Thesis (University of Western Australia, 1998).

[19] Q. Huang and J. Meng, `A classi¯cation of DCI(CI)-subsets for cyclic group of odd prime power order', Journal of Combinatorial Theory, Series, 78 (2000), 24-34.

[20] M. H. Klin and R. PÄschel, `The isomorphism problem for circulant digraphs with p^n vertices', Preprint P-34/80 Akad. derWiss. der DDR, ZIMM, Berlin, (1980).

[21] C. H. Li, `Finite permutation groups containing cyclic regular subgroups, circulant graphs, and regular Cayley maps', Preprint, (2001).

[22] C. H. Li, `The solution of problem of Godsil on cubic Cayley graphs', J. Combin. Theory Ser. B, 72 (1998), 140-142.

[23] C. H. Li, `On Cayley Isomorphisms of Finite Cayley graphs - a survey', Discrete Math., To appear.

[24] C. H. Li, `On isomorphisms of connected Cayley graphs', Discrete Math., 178 (1998), 109-122.

[25] C. H. Li and H. S. Sim, `The graphical regular representations of metacyclic p-groups', Europ. J. Combin., 21 (2000), 917-925.

[26] C. H. Li and H. S. Sim, `On half-transitive metacirculant graphs of prime-power order', J. Combin. Theory Ser. B, 81 (2001), 45-57.

[27] C. H. Li and H. S. Sim, `Automorphisms of Cayley graphs of metacyclic groups of prime-power order', J. Austral. Math. Soc., 71 (2001), 223-231.

[28] M. W. Liebck and Saxl, `Primitive permutation groups containing an element of large prime order', J. London Math. Soc. (2) 31 (1985), 237-249.

[29] Ian D. Macdonald, The Theory of Group, Oxford University Press (1968).

[30] Mikhail Muzychuk, `¶Ad¶am's conjecture is true in the square-free case', J. Combin. Theory Ser. A 72 (1995), 118-134.

[31] Mikhail Muzychuk, `Corrigendum: On ¶Ad¶am's conjecture for circulant graphs', Discrete Mathematics 176 (1997), 285-298.

[32] Mikhail Muzychuk, Mikhail Klin, and Reinhard PÄoschel, `The isomorphism problem for circulant graphs via Schur ring theory', DIMACS Series in Discrete Mathematics and Theoretical Computer Science, AMS, 56 (2001), 241-264.

[33] L. A. Nowitz, `A nonCayley-invariant Cayley graph of the elementary Abelian group of order 64', Discrete Math., 110 (1992), 223-228.

[34] C. E. Praeger, `Finite normal edge-transitive Cayley graphs', Bull. Austral. Math. Soc. 60 (1999), 207-220.

[35] C. E. Praeger, `Finite transitive permutation groups and finite vertex-transitive graphs', Graph Symmetric: Algebraic Methods and Applications, NATO ASI Ser. C 497 (1997), 277-318.

[36] C. E. Praeger, R. J. Wang and M. Y. Xu, `Symmetric graphs of order a product of two distinct primes', J. Combin. Theory Ser. B, 58 (1993), 299-318.

[37] C. E. Praeger and M. Y. Xu, `Vertex primitive graphs of order a product of two distinct primes', J. Combin. Theory Ser. B, 59 (1993), 245-266.

[38] H. S. Sim and Y. W. Kim, `Normal edge-transitive circulant graphs', Bull. Korean Math. Soc., 38 (2001), 317-324.

[39] J. Turner, `Point-symmetric graphs with a prime number of points', J. Combin. Theory , 3 (1967), 136-145.

[40] Helmut Wielandt, Finite Permutation Group, Academic Press (1968).

[41] Ming-Yao Xu, Lecture Notes on Some Work about Vertex-Transitive Graphs by Chinese Mathematicians, Pohang U. Science and Technology (2000).

감사의 글

본 논문이 완성되기까지 항상 학문에의 연구 매진을 독려하시고 밝은 가르침과 날카로운 깨우침으로 이끌어주신 심효섭 지도 교수님, 언제나 자상하신 모습으로 지도와 편달을 아끼시지 않으시던 백영길 교수님께 먼저 머리 숙여 감사드립니다.

저의 졸고에 대해 아낌없는 질책과 편달로 더 아름다운 논문을 요구하시며 마지막까지 정성을 쏟을 수 있게 지도해 주신 심사위원 조정래교수님, 송현종교수님, 박진한교수님, 부경대학교 응용수학과의 여러 교수님들 그리고 음으로 양으로 도움을 주신 신우택선생님, 박성준선생님, 박진근선생님, 서유덕선생님, 나호준선생님에게도 감사의 뜻을 전하고 싶습니다.

본인이 학위과정을 마칠 수 있도록 헌신적인 내조를 아끼지 않은 아내와 사랑스런 딸 한슬 아들 지환이와도 이 기쁨을 함께하며, 지금까지 뒷바라지 해 주신 부모님께 이 영광을 바칩니다.