CAYLEY GRAPH ENUMERATION

by

Marni Mishna

BMath, University of Waterloo, 1998.

THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

IN THE DEPARTMENT

OF

MATHEMATICS &STATISTICS

SIMON FRASER UNIVERSITY

March 2000

APPROVAL

Name:	Marni Mishna
Degree:	Master of Science
Title of Thesis:	Cayley Graph Enumeration
Examining Committee:	Dr. R. Lockhart (Chair)

Dr. B. Alspach
Senior Supervisor

Dr. T. C. Brown

Dr. P. Hell

Dr. B. Stevens

External Examiner

Date Approved: March 3, 2000

Abstract

Pólya's Enumeration Theorem is a powerful method for counting distinct arrangements of objects. J. Turner noticed that circulant graphs have a sufficiently algebraic structure that Pólya's theorem can be used to determine the number of non-isomorphic circulants of order p for prime p. Recent results on CI-groups suggest that Turner's method can be used to enumerate a larger collection of circulants, circulant digraphs, and Cayley graphs and digraphs on $\mathbb{Z}_p^2$ and $\mathbb{Z}_p^3$.

Acknowledgments

Brian Alspach found me a nice enumeration problem and carefully read the work. NSERC and SFU provided me with the financial support that allowed this to be a quick project.

Big huge thanks to the wonderful, fun people that I have met while in Vancouver. I have been enlightened, entertained and inspired. I will leave here a better person than when I arrived.

Karen Meagher and Adam Fraser, my best friends, have continued to tolerate, support and encourage me. Karen offered some real killer suggestions and actually read the whole thing.

This one goes out to my family, especially my mom who even tried to understand what it meant.

it's an automatic toaster! brews delicious coffee automatically! does any mixing job!
by solving complex mathematical formulas

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Definitions and Notation

Determining the number of distinct graphs in a given family is one of the most basic questions one can ask about a family of graphs. Graph theorists have devoted much energy to searching for elegant answers to the graph isomorphism problem for many families of graphs. Pólya's theorem of enumeration, when it first became widely appreciated in the early 1960s, served as the main tool for many graph isomorphism problems. In 1967 J. Turner determined that a class of Cayley graphs was well suited to this approach. Cayley graphs are defined in relation to groups and consequently have a useful underlying structure. The Cayley graphs Turner considered possess a particular property, they are Cayley graphs on CI-groups, and recent work in this area has found more families with this characteristic, thereby opening up the possibility of applying his methods to these new families.

Throughout, Φ shall denote the Euler phi-function. Hence $\Phi(n)$ is defined over the natural numbers as the number of integers i, $1 \leq i \leq n$, coprime to n. The additive cyclic group of order n will be denoted by $\mathbb{Z}_n$, and $\mathbb{Z}_n^*$ will always denote the multiplicative group of units of the ring of integers modulo n. For a group G let $\mathrm{Aut}(G)$ denote the group of automorphisms of G. A graph automorphism is an adjacency preserving permutation of the vertex set. We will use similar notation $\mathrm{Aut}(X)$ to denote the graphs automorphisms of the

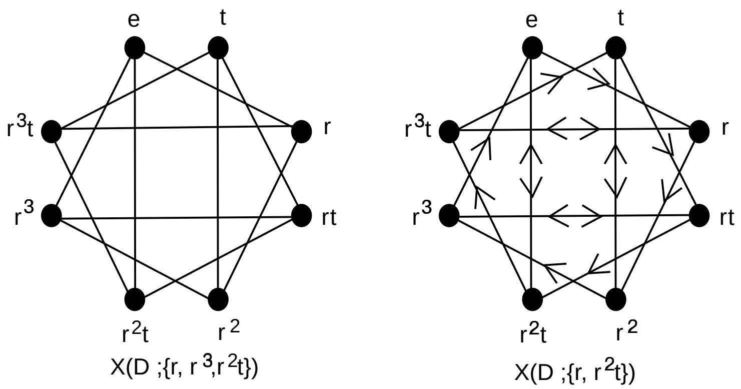

Figure 1.1: CAYLEY GRAPH $X(D_8, \{r, r^3, r^2t\})$ AND CAYLEY DIGRAPH $X(D_8, \{r, r^2t\})$

graph X.

The next two definitions describe a Cayley graph.

DEFINITION. A *Cayley subset* S of a group G is an inverse closed subset ($s \in S \implies s^{-1} \in S$) of G not containing the identity.

DEFINITION. A *Cayley Graph* is represented by $X(G; S)$ where G is a group, and S is a Cayley subset of G, also known as the *connection set*. The Cayley graph has vertex set G and edge set

$$\{(g_1, g_2)|g_1 = g_2 s, s \in S\}.$$

DEFINITION. A *Cayley digraph* $X(G; S)$ is defined on a group G and a set $S \subseteq G \setminus e$. It has vertex set G and there is a directed edge from g_1 to g_2 if and only if $g_2 = g_1 s$ for some $s \in S$.

EXAMPLE. The dihedral group $D_8 = \langle r, t | r^4 = t^2 = e, tr = r^{-1}t \rangle$ is a fine group upon which to define a Cayley graph and a Cayley digraph. Figure 1.1 provides an example of a Cayley graph and a Cayley digraph on D_8.

1.2 CI-Groups

Our ultimate goal is to provide some enumeration results for some families of Cayley graphs. This is most easily accomplished when there is a useful relationship between the isomorphisms of the graphs and automorphisms of the group.

If $\alpha \in \mathrm{Aut}(G)$, then for $S \subseteq G$, let $\alpha(S) = \{\alpha(s) | s \in S\}$. A group automorphism α of G can also be viewed as a map between two Cayley graphs on G upon considering the resulting action of α on the vertices G. That is, there exists a map between $X(G;S)$ and $X(G;\alpha(S))$. In fact, this action can be a graph isomorphism.

1.1 THEOREM. *Let $X = X(G;S)$ be a Cayley graph on the group G. If $\alpha \in \mathrm{Aut}(G)$, then α is an isomorphism from the graph X to the graph $X' = X(G;\alpha(S))$*

PROOF: By the definition of Cayley graph we have that $uv \in E(X)$ if and only if $v = us$ for some $s \in S$. Since α is a group automorphism, we have that $v = us$ if and only if $\alpha(v) = \alpha(u)\alpha(s)$. Thus $vu \in E(X)$ if and only if $\alpha(v)\alpha(u) \in E(X')$ so α is a graph isomorphism between the graphs X and X'.

⋆

Next we consider the reverse relationship. That is, in which cases does an isomorphism of the graph correspond to an automorphism of the group?

DEFINITION. Let G be a finite group, and let $X = X(G;S)$ and $X' = X(G;s')$ be Cayley graphs on G. S satisfies the *Cayley isomorphism property* if whenever X is isomorphic to X', there exists a group automorphism α of G such that α is also a graph isomorphism from X to X'. We abbreviate this as S is a *CI-subset*.

DEFINITION. If every Cayley subset of G is a CI-subset, then we say that G satisfies the *Cayley Isomorphism Property*, or succinctly, G is a *CI-group*.

This definition comes from a generalization of properties of circulant graphs. The relationship and motivation will soon become clear.

1.3 Some Known CI-Groups

The Cayley Isomorphism property is indeed a nice property, almost suspiciously so. It is in our best interests to determine which groups are CI-groups, indeed if any exist at all, as this will facilitate enumeration greatly.

The search for existence best begins with the cyclic groups. J. Turner [16] began the search with cyclic groups, and obtained results for cyclic groups of prime order. M. Muzychuk [9] settled the case for the cyclic groups in general.

1.2 THEOREM (Muzychuk). *The cyclic groups which are CI-groups are precisely those of order n where n is $8, 9, 18$ or $n = 2^e m$ where $e \in \{0, 1, 2\}$ and m is odd and square-free.*

The next obvious set to consider is the products of cyclic groups. We have the following results in this case. C. Godsil [4] managed a partial answer to the product of two cyclic groups.

1.3 THEOREM (Godsil). *The group $\mathbb{Z}_p^2, p$ prime, is a CI-group.*

The following result was determined independently by both T. Dobson [2] and M.-Y. Xu [17].

1.4 THEOREM (Dobson, Xu). *The group $\mathbb{Z}_p^3, p$ prime is a CI-group.*

It is these CI-groups that we shall consider in this thesis. We shall determine the number of isomorphism classes of Cayley graphs and Cayley digraphs of order n on these groups: $\mathbb{Z}_n$ with n as in Theorem 1.2, $\mathbb{Z}_p^2$ and $\mathbb{Z}_p^3$ for p prime.

Recently [8], it has been shown by J. Morris and T. Dobson that $\mathbb{Z}_p^4$ is also a CI-Group. The reader, at this point, may hypothesize that $\mathbb{Z}_p^n$ is a CI-Group for all n. In fact, L. Nowitz showed [10] that $\mathbb{Z}_2^6$ is not a CI-Group. However, for all n such that it is true, the methods presented in this work will determine the number of isomorphism classes of a given order.

Chapter 2

Circulants of Prime Order

Circulants are an interesting class of Cayley graphs well worth studying. They are Cayley graphs on the simplest of groups and thus may provide direction and insight into Cayley graphs on other groups, particularly finite groups. All finite vertex-transitive graphs of prime order are circulants, hence the study of vertex transitive graphs can gain from the study of circulants.

DEFINITION. A *circulant* is a Cayley graph on a cyclic group. We denote the circulant $X(\mathbb{Z}_n; S)$ by simply $X(n; S)$.

The complete set of circulants of order 5 is illustrated in Figure 2. Notice that $X(5; \{2, 3\})$ and $X(5; \{1, 4\})$ are isomorphic.

We shall begin with a known result about the number of circulants up to isomorphism

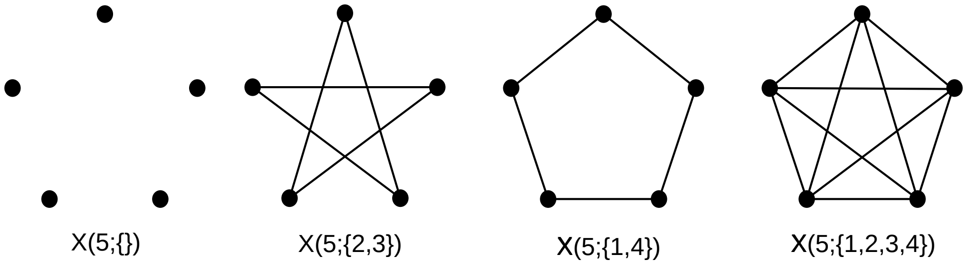

Figure 2.1: THE COMPLETE SET OF CIRCULANTS OF ORDER 5

of prime order p. A very elegant relationship, that of Theorem 1.2, exists between graph isomorphisms and group isomorphisms which allows us to use strong group theoretic tools. Further, these methods, notably Pólya's enumeration theorem, can be used to enumerate circulant graphs of other orders.

Enumerating the prime case directly offers sufficient insight that we include it. First we show that the prime circulants are the complete set of vertex-transitive graphs of prime order.

2.1 LEMMA. *Cayley graphs are vertex-transitive.*

PROOF: The action of a group G acting on itself by left multiplication is a permutation. This action clearly preserves adjacency in any Cayley graph defined on G. The permutation which takes u to v is left multiplication by $vu^{-1} \in G$.

⋆

Define the mapping $T_{a,b}$ acting on $\mathbb{Z}_n$ to be $T_{a,b}(x) = ax+b$. If $a \in \mathbb{Z}_n^*$, $T_{a,b}$ is a permutation of $\mathbb{Z}_n$. The notation $H < G$ indicates that H is a proper subgroup of G.

2.2 THEOREM (Burnside). *If G is a transitive permutation group acting on a prime number p of points, then either G is doubly transitive or*

$$G \cong \{T_{a,b} : a \in H < \mathbb{Z}_p^* \textit{ and } b \in \mathbb{Z}_p\}.$$

2.3 COROLLARY. *If G is a transitive permutation group acting on a prime number p of points and G is not doubly transitive, then G contains a unique subgroup of order p.*

PROOF: First we establish existence. The subgroup generated by $\langle T_{1,1} \rangle = \{T_{1,b} | b \in \mathbb{Z}_p\}$ is of order p and contained in G by Burnside's Theorem.

Consider $T_{a,b}(x) = ax + b$. Notice that if $a \neq 1$, $(a-1)$ is a unit and has an inverse in which case $(a-1)^{-1}(p-b)$ is a fixed point for $T_{a,b}(x)$. Since G is acting on p elements and the order of a permutation is the least common multiple of the cycle lengths in its disjoint cycle decomposition, an element of order p in G must be a p-cycle. Hence, an element of order p has no fixed points and the result follows from Theorem 2.2.

$\star$

2.4 THEOREM (Turner). *A graph X of order p is vertex-transitive if and only if X is a circulant graph.*

PROOF:[16] Since a circulant is a Cayley graph one direction follows from Lemma 2.1. Now suppose that X is a vertex-transitive graph of prime order p. If the automorphism group is doubly transitive, X is either the complete graph or the empty graph, both circulants. Otherwise, we may assume that $\mathrm{Aut}(X)$ is not doubly transitive, and thus has a unique subgroup of order p. We may consider a labelling of the vertices such that the generator of the this unique subgroup is $\rho = (0\ \ 1\ \ \ldots\ \ p-1)$. If i is adjacent to j in X, then they must be adjacent under the image of automorphism ρ, thus, $i+1$ is adjacent to $j+1$, and upon considering powers of ρ, $i+s$ is adjacent to $j+s$ for $0 \leq s \leq p-1$, with all computations modulo p. If we let S denote the set of vertices adjacent to the vertex labelled 0, we have i is adjacent to j if and only if $i-j$ and $j-i$ are adjacent to 0 if and only if $i-j \in S$ and $j-i \in S$. Clearly X is a circulant of order p with connection set S.

$\star$

Having illustrated a motivation for studying circulants, we now return to the idea of enumeration. The next result is a specification of Muzychuk's Theorem to the prime case.

2.5 THEOREM (Turner). *Two circulant graphs $X = X(G;S)$, and $X' = X(G;S')$ of prime order p are isomorphic if and only if there exists some $a \in \mathbb{Z}_p^*$ such that $aS = S'$.*

PROOF: First suppose that there exists some $a \in \mathbb{Z}_p^*$ such that $S' = aS$. Left multiplication by a is a graph isomorphism from X to X'.

Now suppose that X and X' are isomorphic as graphs with isomorphism $f : V(X) \rightarrow V(X')$. If X is either the complete graph K_p or its complement $\bar{K_p}$, then $S = \{1, 2, \ldots, p-1\}$ or $\{\}$, respectively. In either of these cases $S' = S$. So, consider the case that X is neither K_p nor $\bar{K_p}$. For any circulant on vertices $0, 1, \ldots, p-1$ the rotation permutation $\rho = (0\ 1\ \ldots\ p-1)$ is a graph automorphism. The subgroup generated by ρ has order p.

Now, ρ is an automorphism of both X and X'. Further, since f is an isomorphism, $\sigma = (f(0)\ f(1)\ \ldots\ f(p-1))$ is also an automorphism of X' generating a subgroup of order p.

Since X is neither K_p nor $\bar{K_p}$ its automorphism group is not doubly transitive. Hence, by Corollary 2.3 we have that the group of permutations of X' contains a unique subgroup of order p. Thus, $\sigma \in \langle \rho \rangle$ and we have that

$$\begin{aligned} (f(0)\ f(1)\ \ldots\ f(p-1)) &= \rho^a \text{ for some } 1 \leq a \leq p-1 \\ &= (0\ a\ 2a \ldots (p-1)a). \end{aligned}$$

Thus, if we rewrite σ we can see that for some $0, \leq i \leq p-1$, $f(i) = 0, f(i+1) = a$ and in general $f(i+j) = aj$. We can now prove the theorem upon examining the adjacency criterion for circulants.

$$\begin{aligned} s \in S &\iff i \text{ is adjacent to } i+s \text{ in } X \text{ for all } i \in \mathbb{Z}_p \\ &\iff f(i) \text{ is adjacent to } f(i+s) \text{ in } X' \\ &\iff a(k+i) \text{ is adjacent to } a(k+i+s) \text{ in } X' \\ &\iff a(k+i) - a(k+i+s) \in S' \\ &\iff as \in S' \end{aligned}$$

Thus, $s \in S \iff as \in S'$, or, $S' = aS$.

⋆

2.1 Determining the Cycle Index

Theorem 2.5 provides the necessary information about the structure of circulants to appeal to Pólya's enumeration theorem.

In a framework suited to counting with the Pólya enumeration theorem, there is a domain for which one has an understanding of a permutation group, and a range of acceptable values. Pólya's theorem states that we can determine a generating function for the number of distinct functions from domain to the range, using the automorphism group and the generating function of the range.

Let the domain be set D and let the range be set R. Define R^D to be all of the functions from D to R. The theorem counts the number of distinct functions from D to R. A permutation group G acting on D will induce a permutation action on R^D. Pólya's theorem reduces counting the orbits of the induced action on R^D, that is, the number of distinct functions, to counting the distinct actions of G on D. The main tool is the cycle index of G, which holds the information of the permutations of D and which we define next.

Let G be a permutation group acting on a set Ω. Consider the disjoint cycle decomposition of $\sigma \in G$. Suppose it contains precisely b_k cycles of length k, for $1 \leq k \leq |\Omega|$. We define a monomial $\pi(\sigma)$ associated with the decomposition as follows: $\pi(\sigma) = x_1^{b_1} x_2^{b_2} \ldots x_m^{b_m}$, where $m = |\Omega|$. Note that $b_1 + 2b_2 + \ldots + kb_k = m$.

DEFINITION. The *cycle index* $\mathcal{Z}(G, \Omega)$ of the permutation group G acting on Ω is defined to be the polynomial in indeterminates $x_1, x_2, \ldots, x_m$

$$\mathcal{Z}(G, \Omega) = \frac{1}{|G|} \sum_{\sigma \in G} \pi(\sigma).$$

EXAMPLE. Let G be the permutation group generated by the 6-cycle $(0\ 1\ 2\ 3\ 4\ 5)$. The monomial corresponding to the identity permutation is $\pi(I_G) = x_1^6$. The monomial corresponding to a 6-cycle, of which there are two in G, is x_6^1. The two permutations which are products of two disjoint cycles of length three correspond to the monomial x_3^2. The remaining permutation is a product of three disjoint 2-cycles. The cycle index for G is thus

$$\mathcal{Z}(G, \{0,1,2,3,4,5\}) = \frac{1}{6}(x_1^6 + x_2^3 + 2x_3^2 + 2x_6^1).$$

The next example determines the cycle index of the group of automorphisms of a cyclic group acting on the cyclic group.

EXAMPLE. Let p be prime and let $\mathbb{Z}_p^*$, the multiplicative group of units of $\mathbb{Z}_p$, act on the set $\mathbb{Z}_p \setminus 0$ by multiplication. Theorem 2.6, illustrates that $a \in \mathbb{Z}_p^*$ generates a group of permutations of the elements of $\mathbb{Z}_p$. We can determine the cycle index of this action.

DEFINITION. Let $a, n \in \mathbb{Z}$ with $gcd(a,n) = 1$. We definite the *order of* a mod n to be the least positive integer $k(a)$ such that $a^{k(a)} \equiv 1 \pmod{n}$ and we denote this by $\mathrm{ord}_n(a)$. Notice that this is equivalent to saying that a has multiplicative order $k(a)$ in the group $\mathbb{Z}_n^*$

2.6 THEOREM. *Let G be a cyclic group of order n. The group $\mathrm{Aut}(G)$ of automorphisms of G is exactly the group of all automorphisms $\{\alpha_k : \alpha_k(g) = g^k, 1 \leq k < n,\ gcd(k,n) = 1\}$. Moreover, the mapping $k \mapsto \alpha_k$ is an isomorphism from $\mathbb{Z}_n^*$ to $\mathrm{Aut}(G)$.*

PROOF:[13] First we verify that $\alpha_k \in \mathrm{Aut}(G)$. We can see that α_k is a homomorphism of G, since for $g_1, g_2 \in G$, we have $\alpha_k(g_1 g_2) = (g_1 g_2)^k = g_1^k g_2^k = \alpha_k(g_1)\alpha_k(g_2)$. Let x be a generator of the group and let $g_1 = x^t$ and $g_2 = x^s, 0 \leq s, t < n$. Now suppose that $\alpha_k(g_1) = \alpha_k(g_2)$. Then we have that $x^{tk} \equiv x^{sk} \pmod{n}$. Thus, $tk \equiv sk \pmod{n}$. Since k and n are coprime, $t \equiv s \pmod{n}$. Given the possible values for s and t, they must be equal, and hence $g_1 = g_2$ and α_k is injective. Given x^t, clearly $\alpha_k(x^{k^{-1}t}) = x^t$, implying that α_k is surjective.

Next we verify that any element of $\mathrm{Aut}(G)$ is α_k for some $k, gcd(k,n) = 1$. Let x be a generator of G and let $\alpha \in \mathrm{Aut}(G)$. Since $\alpha(x^t) = (\alpha(x))^t$, the action of α is completely determined by its action on x. As $\alpha(x)$ must generate G as well, it has order n. Thus, $\alpha(x) = x^k$ for some k with $gcd(k,n) = 1$, as these are the generators. From this we see that for any element x^t of G, $\alpha(x^t) = \alpha(x)^t = (x^k)^t = \alpha_k(x^t)$.

⋆

2.7 LEMMA. *The number of elements of order k in $\mathbb{Z}_n$ is $\Phi(k)$ if $k|n$ and zero otherwise.*

PROOF: Certainly the order of an element must divide the order of the group and so we consider only those k which divide n. The elements of order n are precisely the integers in $\mathbb{Z}_n$ co-prime to n [13]. Thus, there are $\Phi(n)$ elements in the cyclic group of order n which have order n. If $a \in \mathbb{Z}_n$ is of order k, it generates a subgroup of $\mathbb{Z}_n$ of order k. From our remarks about n, there are at least $\Phi(k)$ elements of order k.

Now, $\mathbb{Z}_n$ is a cyclic group of order n, hence there exist subgroups of order k for each divisor k of n. Since for any positive integer n, $\sum_{k|n} \Phi(k) = n$, we can account for every element in $\mathbb{Z}_n$ upon considering the subgroup they generate. Hence, the number of elements of order k in $\mathbb{Z}_n$, for k a divisor of n, is $\Phi(k)$.

$\star$

2.8 THEOREM (Gauss, [14]). *The group of units of $\mathbb{Z}_p$ is a cyclic group, isomorphic to the cyclic group of order $p-1$.*

2.9 THEOREM. *The cycle index of $\mathbb{Z}_p^*$ acting on $\mathbb{Z}_p \setminus 0$ is*

$$\mathcal{Z}(\mathbb{Z}_p^*, \mathbb{Z}_p \setminus 0) = \frac{1}{p-1} \sum_{d|p-1} \Phi(d) x_d^{\frac{p-1}{d}},$$

where the sum is taken over all divisors of $p-1$.

PROOF: Let the order of a modulo p be $k(a)$. We know that for $a \geq 1$, $k(a) = (p-1)/gcd(a, p-1)$. If x is any element of $\mathbb{Z}_p \setminus 0$, then it is in the cycle $(x\ ax\ a^2x\ \ldots\ a^{k(a)-1}x)$. The permutation $g_a(x) = ax$ splits $\mathbb{Z}_p^*$ into cycles each of length $k(a)$. Since $k(a)$ must divide $p-1$, there are $(p-1)/k(a)$ cycles of length $k(a)$.

Summing over the elements of $\mathbb{Z}_p^*$, we have the cycle index

$$\begin{aligned}\mathcal{Z}(\mathbb{Z}_p^*, \mathbb{Z}_p \setminus 0) &= \frac{1}{p-1} \sum_{a \in \mathbb{Z}_p^*} x_{k(a)}^{\frac{p-1}{k(a)}} \\ &= \frac{1}{p-1} \sum_{a \in \mathbb{Z}_p^*} x_{\frac{p-1}{gcd(a,p-1)}}^{\gcd(a,p-1)} \\ &= \frac{1}{p-1} \sum_{d \mid p-1} \Phi(d) x_d^{\frac{p-1}{d}}.\end{aligned}$$

⋆

2.2 Enumerating Circulants of Prime Order

Pólya's Theorem brings together the three necessary components for counting in a very simple way. To establish context, first recall the Cauchy Fröbenius Lemma (also known by the Burnside Lemma). If G is a finite group of transformations acting on a finite set Ω of objects, and two objects are considered equivalent if one is transformed into the other by a transformation in G, then the number of inequivalent objects is $\frac{1}{|G|} \sum_{g \in G} fix(g)$, where $fix(g)$ is the number of points in Ω fixed by σ.

Pólya's Theorem generalizes this idea. Let D and R be finite sets. Let R^D denote the set of all functions from D to R, and let G be a permutation group acting on D. For each $\sigma \in G$ define a permutation $\bar{\sigma}$ acting on R^D by

$$\bar{\sigma}(f)(x) = f(\sigma(x))$$

for all $f \in R^D$ and all $x \in D$. The mapping taking σ to $\bar{\sigma}$ is a homomorphism of G to a permutation group $\bar{G}$.

2.10 THEOREM (Pólya). *With D, R, G, $\bar{G}$, and R^D as per the above discussion, the number of inequivalent $f \in R^D$ under $\bar{G}$ is determined by evaluating the cycle index of G with each variable set to $|R|$.*

The theorem is actually much stronger. A good discussion exists in either [1] or [12]. To summarize, if the weight of an element y in R is $w(y)$, then the generating function for R is then $g(u) \;= \sum_{y \in R} u^{w(y)}$. The generating function counting orbits of $f \in R^D$ under $\bar{G}$ is obtained by substituting $g(u^i)$ for x_i in the cycle index of G. In particular, the number of orbits of the permutation group $\bar{G}$ is given by setting all of the weights equal to one, essentially, evaluating the cycle index of G with each variable set to $|R|$.

We can apply Pólya's Theorem to count the number of circulant graphs of order p, p an odd prime. Let the domain D be the set of ordered pairs

$$\{\{1,-1\},\{2,-2\},\ldots,\{\frac{p-1}{2},\frac{p+1}{2}\}\}$$

with the range R chosen to be the set {0,1}. A function f_S in R^D corresponds to a circulant graph $X(n;S)$ in the following way. The set $\{i,-i\}$ is in S if and only if $f_S(\{i,-i\}) = 1$. The permutation group acting on D that we will consider is $\mathbb{Z}_p^*$ with the action of multiplication.

Since multiplication by a is the same as multiplication by $-a$ with respect to D, in this case the permutation group can be pared down to $\mathbb{Z}_{p-1}/\{1,-1\} \cong \mathbb{Z}_{\frac{p-1}{2}}$.

2.11 THEOREM (Turner). *Let p be a prime. The number of circulant graphs of order p, to within isomorphism, is*

$$\frac{2}{p-1}\sum_{d|\frac{p-1}{2}} \Phi(d)2^{\frac{p-1}{2d}}.$$

PROOF: We have by Theorem 2.5 that two circulant graphs $X(Z_p;S)$, and $X'(Z_p;T)$ are isomorphic if and only if their connection sets satisfy $S = aT$ for some $a \in Z_p^*$. Consider the action of a in the cyclic group of order $(p-1)/2$ on D. This maps the set $\{i,-i\}$ to $\{ia,-ia\}$. This induces an action $\bar{a}$ on R^D defined by $\bar{a}(f)(x) = f(ax)$. Notice that $f(\{ai,-ai\}) = 1$ if and only if $\bar{a}(f)(\{i,-i\}) = 1$ for each $i \in Z_p^*$. Since $\bar{a}(f) \in R^D, a(f_S) = f_T$ for some $T \subseteq D$, with $S = aT$. Thus, counting the number of orbits of this group simultaneously counts the number of isomorphism classes. The cyclic index of the latter group is

$$\frac{2}{p-1}\sum_{d|\frac{p-1}{2}} \Phi(d)x_d^{\frac{p-1}{2d}}$$

We now substitute $2 = |R|$ for each variable, according to Pólya's Theorem, and obtain the desired result.

⋆

EXAMPLE. To illustrate this result consider the circulants on five vertices. There is the empty graph, the five-cycle and the complete graph; the choices of valency 0, 2 and 4, respectively. If we now consider the number of classes according to the formula, we have

$$\frac{2}{4}(\Phi(1)2^2 + \Phi(2)2) = 3,$$

as is consistent with Figure 2.

EXAMPLE. To illustrate the power of the formula we consider a more impressive result. Let $p = 53$. The cycle index for this case is

$$\frac{2}{52}(x_1^{26} + x_2^{13} + 12x_{13}^2 + 12x_{26}),$$

and it follows that the number of non-isomorphic circulant graphs of order 53 is

$$\frac{1}{26}(2^{26} + 2^{13} + 12 \cdot 2^2 + 12 \cdot 2) = 2\ 581\ 428.$$

2.3 Circulant Digraphs of Prime Order

The enumeration of digraphs is simpler than the enumeration of graphs, yet has not previously been investigated. Theorem 2.5 holds in the digraph case as well, and hence we can use the same method. However, in this situation the connection sets can be any subset of $\mathbb{Z}_p \setminus 0$, so we need not concern ourselves with dealing with pairs $\{i, -i\}$. Instead we simply determine the cycle index of $\mathbb{Z}_p^*$ acting on $\mathbb{Z}_p$ by left multiplication as calculated in Theorem 2.9. When the order of a circulant is prime there is not much difference between the directed and the undirected case. However, the results for digraphs are typically simpler than the results for graphs.

2.12 THEOREM. *The number of non-isomorphic circulant digraphs of order p, p prime, is*

$$\frac{1}{p-1}\sum_{d|p-1}\Phi(d)2^{(p-1)/d}.$$

EXAMPLE. We can contrast the earlier result with the number of circulant digraphs on five vertices. The number of non-isomorphic digraphs on 5 vertices is

$$\frac{1}{4}(2^4+2^2+2\cdot 2)=6.$$

EXAMPLE. It is just as simple to determine the same information of a circulant digraph of a larger order. Consider $p=29$. The number of non-isomorphic circulant digraphs of order 29 is

$$\frac{1}{28}\sum_{d|28}\Phi(d)2^{\frac{28}{d}}=9\ 587\ 580.$$

2.4 Counting Regular Cayley Graphs

One of the charms of this counting method, as opposed to, say, directly appealing to the Cauchy-Fröbenius Lemma, is that we can obtain even more relevant information. In fact, we have not made use of the true power of the more general version of Pólya's Theorem at all. The results so far could just as easily have been computed with the Cauchy-Fröbenius Lemma.

Instead of producing the number of orbits, which in this case yields the number of non-isomorphic graphs, we can greate a generating function which gives us more information about these graphs. For example, since Cayley graphs are vertex transitive they are regular, that is every vertex has the same valency. We can use Pólya's Theorem to create a generating function $F(x)$ where the coefficient of u^k is the number of non-isomorphic graphs which are $k-$regular. A Cayley graph is $k-$regular when the connection set is of size k.

To get the desired generating function from Pólya's theorem we need a suitable generating function for $R=\{0,1\}$. Recall that $f_S(a)=1$ if and only if $\{a,-a\}\subseteq S$. Since the valency of a graph is the size of its connection set S, and for each choice of 1 for a function the size of S is incremented by 2, the element 1 in R should have a weight of 2, and 0 a weight of 0. Thus, the generating function for R is $G(u) = 1 + u^2$. According to Pólya's theorem if we substitute $G(u^k)$ for x_k in the cycle index, the result will be a generating function for the number of $k - regular$ graphs of a given valency.

EXAMPLE. In the case of circulants of order 5, we had the cycle index of $\frac{1}{2}(x_1^2 + x_2)$. Thus, upon replacing each x_i with $1+u^{2i}$ we have the generating function $\frac{1}{2}((1+u^2)^2+(1+u^4)) = 1 + u^2 + u^4$. This suggests a circulant each of valency 0, 2, and 4, which was also evident from Figure 2.

If two Cayley graphs are isomorphic their complements are isomorphic under the same isomorphism. Thus, for a given group G, if there are m non-isomorphic, k-regular, Cayley graphs on G of order n, there are also m non-isomorphic Cayley graphs on G of order n of valency $n - k$. Thus one only needs half the terms in the generating function to get the complete picture.

EXAMPLE. In an earlier example we calculated that there were over two million circulants of order 53. The valency generating function,

$$1+13u^2+13u^4+100u^6+578u^8+2530u^{10}+8866u^{12}+25300u^{14}+60115u^{16}+120175u^{18}+\ldots$$

indicates how they are distributed. For example, there are 25 300 14-regular circulants of order 53.

We can even determine this formula in general. If we denote the coefficient of u^n in a polynomial $f(u)$ by $[u^n]f(u)$, then the number of circulants of order p and valency k is

$$\begin{aligned} & [u^k]\frac{2}{p-1}\sum_{d|(p-1)/2}\Phi(d)(1+u^{2d})^{\frac{p-1}{2d}} \\ = \; & [u^k]\frac{2}{p-1}\sum_{d|(p-1)/2}\Phi(d)\sum_{i=0}^{(p-1)/(2d)}\binom{(p-1)/(2d)}{i}u^{2id} \\ = \; & \sum_{d|gcd(k,(p-1))/2}\Phi(d)\binom{(p-1)/(2d)}{k/(2d)}. \end{aligned}$$

For example, the number of circulants of prime order p of valency two is always 1. The number of valency 4, is $(p-1)/4$ if four divides $p-1$ and $(p-3)/4$ otherwise.

We can use this same technique in the case of digraphs to count the graphs of a given out-valency.

The number of circulant digraphs of order p and out-valency n is

$$\begin{aligned} & [u^n]\frac{1}{p-1}\sum_{d|p-1}\Phi(d)(1+u^d)^{\frac{p-1}{d}} \\ = & [u^n]\frac{1}{p-1}\sum_{d|p-1}\sum_{i=0}^{(p-1)/(2d)}\Phi(d)\binom{(p-1)/(2d)}{i}u^{2id} \\ = & \sum_{d|gcd(n,p-1)}\Phi(d)\binom{(p-1)/d}{n/d}. \end{aligned}$$

Chapter 3

Circulants and Circulant Digraphs

The case of counting circulants of prime order is so pleasingly solved it would be satisfying if the composite case follows as nicely. The cycle index in this case is slightly more complicated.

Theorem 1.2, implies that we can enumerate a larger collection of circulants using Pólya's theorem and Turner's clever method. Thus, we can enumerate the circulant of order 8, 9, 18 and $2^e m$ where $e \in \{0, 1, 2\}$ and m is odd and square-free. Here we consider only the case where m is odd and square-free. The formulae for the remaining values will follow from the results from this and the next chapter.

Working with the group of units of $\mathbb{Z}_n$ when n is not prime is not as straightforward as the prime case. However, we can show that a group of units is as straightforward as working with product of cyclic groups.

3.1 LEMMA. *Let $U(R)$ denote the units of a ring R. If $S = R_1 \oplus R_2 \oplus \ldots \oplus R_t$, for rings $R_i, 1 \leq i \leq t$, with multiplicative identities 1_{R_i}, then*

$$U(S) = U(R_1) \times U(R_2) \times \ldots \times U(R_t).$$

PROOF:[14] Addition and multiplication are defined in the natural way, that is, componentwise. We have that

$$(r_1, r_2, \ldots, r_t)(s_1, s_2, \ldots, s_t) = (r_1 s_1, r_2 s_2, \ldots, r_t s_t).$$

Thus, $(r_1, r_2, \ldots, r_t)$ has an inverse if and only if r_i has an inverse for each i from 1 to t. Thus the group of units of $R_1 \oplus R_2 \oplus \ldots \oplus R_t$ is precisely $U(R_1) \times U(R_2) \times \ldots \times U(R_t)$.

⋆

3.2 THEOREM (Chinese Remainder Theorem). *Suppose that $m = m_1 m_2 \ldots m_t$ and that $gcd(m_i, m_j) = 1$ for $i \neq j$. Let $b_1, b_2, \ldots, b_t$ be integers and consider the system of congruences:*

$$x \equiv b_i \pmod{m_i}, \text{ for } i = 1 \ldots t.$$

There exists a unique solution to this problem, modulo m.

The Chinese Remainder Theorem allows us to prove a well known result.

3.3 THEOREM. *Let $m = m_1 m_2 ... m_t$, where the m_i are pairwise co-prime. Then*

$$\mathbb{Z}_m^* \quad \cong \quad \mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \ldots \times \mathbb{Z}_{m_t}^*$$

PROOF:[14] Let ψ_i denote the natural homomorphism $x \mapsto x \pmod{m_i}$ from $\mathbb{Z}$ to $\mathbb{Z}_{m_i}$ for $i = 1, \ldots, t$. These form a natural map ψ from $\mathbb{Z}_m$ to $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_t}$ defined by : $\psi(n) = (\psi_1(n), \psi_2(n), \ldots, \psi_t(n))$ for all $n \in \mathbb{Z}_m$. This is a ring homomorphism as each ψ_i is itself a homomorphism. Further, it is an isomorphism because the Chinese Remainder Theorem guarantees a well defined inverse function. The inverse of ψ takes $(x_1, x_2, \ldots, x_t)$ to the unique solution modulo m of $x \equiv x_i \pmod{m_i}, i = 1 \ldots t$. This gives us an isomorphism between $\mathbb{Z}_m$ and $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_t}$ and from Lemma 3.1, $\mathbb{Z}_m^* \cong \mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \ldots \times \mathbb{Z}_{m_t}^*$.

⋆

3.1 Circulants

We first consider circulants that have an order that is a product of two distinct primes. It will become clear how to generalize this to the larger case. Circulants of the form $X(pq; S)$

with p, q prime can be enumerated in a manner similar to the circulants of prime order. Each circulant will be associated with a function from

$$D = \{\{1,-1\},\{2,-2\},\ldots\{\frac{pq-1}{2},\frac{pq+1}{2}\}\}$$

to $R = \{0,1\}$ defined by

$$f_S(\{i,-i\}) = \begin{cases} 1 & \{i,-i\} \in S \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 1.2 tells us, that as in the case of prime order circulants, the group action to consider is multiplication by an element a in $\mathbb{Z}_{pq}^*$. Functions, and consequently connection sets, which can be mapped to each other under this action yield isomorphic circulants.

As before $a \in \mathbb{Z}_{pq}^*$ acts on D by mapping $\{i,-i\}$ to $\{ai,-ai\}$. Thus a and $-a$ perform the same action. Hence, the group of permutations we consider is $\mathbb{Z}_{pq}^*/\{1,-1\}$. By Theorem 3.3 this group is isomorphic to $(\mathbb{Z}_p^* \times \mathbb{Z}_q^*)/\{(1,1),(-1,-1)\}$ which we denote by $\mathcal{P}_{pq}$.

The cycle index is calculated by examining the action of the permutation group on the domain.

3.4 THEOREM. *The cycle index of $\mathcal{P}_{pq}$ acting on D is*

$$\mathcal{Z}(\mathcal{P}_{pq},D) = \frac{2}{p-1}\sum_{d|p-1}\sum_{e|q-1/2}\Phi(d)\Phi(e)x_{L(d,e)}^{\frac{\Phi(pq)}{2L(d,e)}}x_{H(d)}^{\frac{p-1}{2H(d)}}x_{H(e)}^{\frac{q-1}{2H(e)}}$$

where

$$H(a) = \begin{cases} a & a \textit{ is odd} \\ a/2 & \textit{otherwise} \end{cases}$$

and

$$L(d_1,d_2) = \begin{cases} \operatorname{lcm}(d_1,d_2)/2 & d_1,d_2 \textit{ both even and divisible by the same power of 2} \\ \operatorname{lcm}(d_1,d_2) & \textit{otherwise.} \end{cases}$$

PROOF: Let us denote the element $\{m, -m\}$ of D by m, with $0 < m \leq n/2$. An element of $\mathcal{P}_{pq}$ is of the form $\{(a,b), (-a,-b)\}$. We can represent it uniquely by $g_{(a,b)}$, with $0 \leq a < p$ and $0 \leq b \leq q/2$. We have that $g_{(a,b)}$ acts on m in the following way: $g_{(a,b)}(m) = x$ where $x \equiv am \pmod{p}, x \equiv bm \pmod{q}$. The Chinese Remainder Theorem guarantees a unique value for x. Notice that $g^2_{(a,b)}(m) = x$ where $x \equiv a^2m \pmod{p}$, $x \equiv b^2m \pmod{q}$ and in general, $g^i_{(a,b)}(m)$ is the solution to $x \equiv a^im \pmod{p}$, $x \equiv b^im \pmod{q}$. Also notice that if m is a multiple of p this system reduces to $x \equiv 0 \pmod{p}$, $x \equiv b^im \pmod{q}$. Thus multiples of p are mapped to other multiples of p. In fact we can partition D into three parts, multiples of p, multiples of q and those coprime to pq. Since a multiple of p is necessarily coprime to q, there are $\Phi(q)/2$ members in the first part, $\Phi(p)/2$ members of the second part, and $\Phi(pq)/2$ members of the third part.

To determine the cycle index we must find the cycle structure of each permutation. Consider $m \in D$. We have already determined that the permutations permute m within the part to which it belongs. Hence, lets consider the action of a general permutation on m and consider the three parts separately. Let $k_a = k_a$ and $k_b = \mathrm{ord}_p(b)$.

First, let m be a multiple of p. Let $g_{(a,b)}$ be a general action from $\mathcal{P}_{pq}$. The length of the cycle in which m is contained under the action $g_{(a,b)}$ is the least k for which either $g^k_{(a,b)}(m) = m$ or $g^k_{(a,b)}(m) = -m$. That is, the least k for which $b^k \equiv 1 \pmod{q}$ or $b^k \equiv -1 \pmod{q}$ respectively. The second case occurs exactly when k_a is even, and in this case k is $k_a/2$. In the first case $k = k_a$. There are $\Phi(q)/2 = (q-1)/2$ multiples of p in D, and each is contained in a cycle of length k. This will have the effect of contributing an $x_k^{\frac{q-1}{2k}}$ to the cyclic monomial of $g_{(a,b)}$. The case for multiples of q is identical. There are $\frac{p-1}{2k}$ cycles of length k, where k is k_b if k_b is even and k is k_b otherwise.

If m is coprime to both p and q, then we must contend with the double equivalence. The element m is contained in a cycle of length k, where k is the smallest integer such that $g^k_{(a,b)}(m) = m$ or $g^k_{(a,b)}(m) = -m$. The first case occurs when $a^k \equiv 1 \pmod{p}$, and $b^k \equiv 1 \pmod{q}$. The smallest k for which this can happen is $k = \mathrm{lcm}(k_a, k_b)$.

The second case happens only when $a^k \equiv -1 \pmod{p}$, and $b^k \equiv -1 \pmod{q}$. From discussion on multiples of p that would imply that this case occurs when k_b and k_a are both even, and hence $k = \mathrm{lcm}(k_a, k_b)/2$. However, if $k_b|\mathrm{lcm}(k_a, k_b)/2$ then $b^{\frac{\mathrm{lcm}(k_a,k_b)}{2k}} \equiv 1 \pmod{q}$. Hence, this case occurs exactly when k_b and k_a are both even, and neither $k_b|\mathrm{lcm}(k_a, k_b)/2$ nor $k_a|\mathrm{lcm}(k_a, k_b)/2$. The latter two occur when one of k_b and k_a contains a power of two higher than the other. In the latter two cases, $k = \mathrm{lcm}(k_a, k_b)$.

So there are $\Phi(pq)/2 = (p-1)(q-1)/2$ members of this part, each contained in a cycle of length k, thus under $g_{(a,b)}$ there are $(p-1)(q-1)/(2k)$ cycles of length k.

Let $k_a = ord_p(a)$, and $k_b = ord_q(b)$. Putting all three cases together,

$$\pi(g_{(a,b)}) = \begin{cases} x_{lcm(k_a,k_b)}^{\frac{\phi(pq)}{2lcm(k_a,k_b)}} x_{k_a}^{\frac{p-1}{2k_a}} x_{k_b}^{\frac{q-1}{2k_b}} & k_a, k_b \text{ both odd} \\ x_{lcm(k_a,k_b)}^{\frac{\phi(pq)}{2k}} x_{k_a}^{\frac{p-1}{2k_a}} x_{k_b/2}^{\frac{q-1}{k_b}} & k_a, k_b \text{ both even} \\ x_{lcm(k_a,k_b)}^{\frac{\phi(pq)}{2k}} x_{k_a/2}^{\frac{p-1}{k_a}} x_{k_b}^{\frac{q-1}{2k_b}} & k_a \text{ even, } k_b \text{ odd} \\ x_{lcm(k_a,k_b)/2}^{\frac{\phi(pq)}{\mathrm{lcm}(k_a,k_b)}} x_{k_a/2}^{\frac{p-1}{2k_a}} x_{k_b/2}^{\frac{q-1}{2k_b}} & k_a \text{ even, } k_b \text{ even and divisible by the same powers of 2} \\ x_{lcm(k_a,k_b)}^{\frac{\phi(pq)}{2\mathrm{lcm}(k_a,k_b)}} x_{k_a/2}^{\frac{p-1}{2k_a}} x_{k_b/2}^{\frac{q-1}{2k_b}} & \text{otherwise} \end{cases}$$

Now that the possible cycle actions are summarized, it remains to determine the number of permutations of each cycle type. These can be counted by enumerating through the possible orders of elements in $\mathbb{Z}_p$ and $\mathbb{Z}_q$.

To begin, consider the following observation.

3.5 LEMMA. *The multiplicative order of $-a$ in $\mathbb{Z}_p$, p prime, depends on the residue of* $\mathrm{ord}_p(a)$ *modulo 4. If* $\mathrm{ord}_p(a)$ *is congruent to 0 modulo four, then* $\mathrm{ord}_p(-a) = ord_p(a)$. *If* $\mathrm{ord}_p(a)$ *is odd, then* $\mathrm{ord}_p(-a) = 2\mathrm{ord}_p(a)$. *Otherwise,* $\mathrm{ord}_p(-a) = \mathrm{ord}_p(a)/2$.

PROOF: Notice that if $\mathrm{ord}_p(a) = k(a)$, then $(-a)^{2k(a)} \equiv (-1)^{2k(a)} a^{2k(a)} \equiv 1 \pmod{p}$. Hence, $\mathrm{ord}_p(-a)|2k(a)$. By symmetry, $k(a)|2\mathrm{ord}_p(-a)$. Thus, $\mathrm{ord}_p(-a) \in \{k(a), \frac{k(a)}{2}, 2k(a)\}$.

Let $k(a)$ be divisible by four. Then, $(-a)^{k(a)/2} = (-1)^{k(a)/2}a^{k(a)/2} \equiv -1 \pmod{p}$. Hence, $\mathrm{ord}_p(-a) = k(a)$. Next, if $k(a)$ is congruent to 2 modulo 4, then $(-a)^{k(a)/2} = (-1)^{k(a)/2}a^{k(a)/2} \equiv 1 \pmod{p}$, and the order of $-a$ is $k(a)/2$. Lastly, if $k(a)$ is odd, then $(-a)^{k(a)} = (-1)^{k(a)}a^{k(a)} \equiv -1 \pmod{p}$, hence the order of $-a$ is $2k(a)$.

⋆

Now, the number of elements of order k modulo p is $\Phi(k)$. Lemma 3.5 gives us a way to count the number of elements a of order k modulo q where $0 \leq a < q/2$. Now, recall that if $x \in \mathbb{Z}_{pq}$ is in a cycle of length $2k$ under multiplication by a, the corresponding element of D, $\{x, -x\}$, will be in a cycle of length k under the permutation associated with a in P. If x is a multiple of q, this cycle length will be $k_a = \mathrm{ord}_p(a)$. Now, if k_a is divisible by 4, $-a$ will result in a cycle of the same length. Hence, there are $\Phi(k_a)/2 = \Phi(k_a/2)$ elements between 0 and $q/2$ which will put an element in a cycle of order k_a. If k_a is even, but not divisible by 4, then it will still put $\{x, -x\}$ in a cycle of length $k_a/2$. In this case the order of $-a$ modulo p is $k_a/2$, so will also put the element of D in a cycle of length $k_a/2$. Thus, the number of elements between 0 and $q/2$ with order k_a is $\Phi(k_a/2)$.

Just by considering only even orders, we can account for all of the orders of elements between 0 and $q/2$.

We have that

$$\begin{aligned}
\mathcal{Z}(\mathcal{P}, \mathcal{D}) &= \frac{2}{\Phi(pq)} \sum_{g_{(a,b)} \in \mathcal{P}} \pi(g_{(a,b)}) \\
&= \frac{2}{\Phi(pq)} \sum_{d|p-1} \sum_{\substack{e|q-1 \\ 2|e}} \Phi(d)\Phi(e/2) x_{H(d)}^{\frac{p-1}{2H(d)}} x_{e/2}^{\frac{q-1}{e}} x_{L(d,e)}^{\frac{\Phi(pq)}{2L(d,e)}}
\end{aligned}$$

We can split the final sum up into different cases based on the parity of the first divisor.

$$\begin{aligned}
& \frac{2}{\Phi(pq)} \sum_{\substack{d|p-1 \\ 2\nmid d}} \sum_{e|(q-1)/2} \Phi(d)\Phi(e) x_d^{\frac{p-1}{2d}} x_e^{\frac{q-1}{2e}} x_{\mathrm{lcm}(d,2e)}^{\frac{\Phi(pq)}{2\mathrm{lcm}(d,2e)}} \\
+ \; & \frac{2}{\Phi(pq)} \sum_{\substack{d|p-1 \\ 4|d}} \sum_{\substack{e|q-1 \\ 2|e}} \Phi(d)\Phi(e) x_{d/2}^{\frac{p-1}{d}} x_e^{\frac{q-1}{2e}} x_{\mathrm{lcm}(d,e)}^{\frac{\Phi(pq)}{2\mathrm{lcm}(d,e)}} \\
+ \; & \frac{2}{\Phi(pq)} \sum_{\substack{d|p-1 \\ 2|d}} \sum_{\substack{e|q-1 \\ d,e\text{have same powers} \\ \text{of 2 as factors}}} \Phi(d)\Phi(e) x_{d/2}^{\frac{p-1}{d}} x_e^{\frac{q-1}{2e}} x_{\mathrm{lcm}(d/2,e)}^{\frac{\Phi(pq)}{2\mathrm{lcm}(d/2,e)}}
\end{aligned}$$

⋆

3.6 COROLLARY. *Let p, q be prime. The number of circulant graphs of order $n = pq$ up to isomorphism is*

$$\frac{2}{\Phi(pq)} \sum_{d|p-1} \sum_{\substack{e|q-1 \\ e \text{ even}}} \Phi(d)\Phi(e/2) 2^{\frac{p-1}{2H(d)}} 2^{\frac{q-1}{e}} 2^{\frac{\Phi(pq)}{2L(d,e)}}.$$

PROOF: This value is achieved by substituting $|R| = 2$ into every value of x.

⋆

Consider now some examples for some small primes.

EXAMPLE. We can calculate the number of circulants of order 6. According to Theorem 3.6, this number is

$$2^3 = 8$$

since the cycle index is x_1^3, which is evident from Figure 3.1.

EXAMPLE. We can calculate the number of circulants any large suitable order. The number of graphs of order 35 is 11 144. We can also determine the number of each valency. Recall that to determine the generating function where the weight is valency we simply substitute $1 + u^{2i}$ for x_i in the cycle index. In this case we get,

$$1 + 3u^2 + 14u^4 + 62u^6 + 208u^8 + 530u^{10} + 1052u^{12} + 1648u^{14} + 2054u^{16} + \ldots.$$

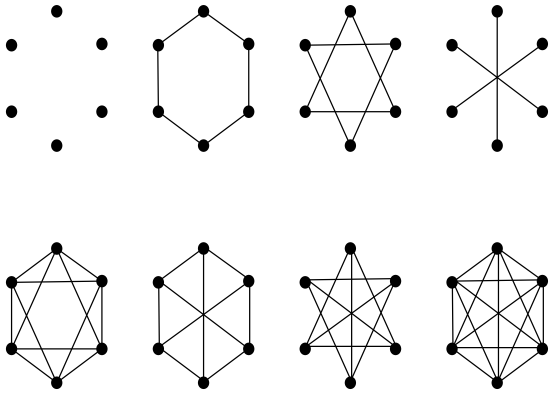

Figure 3.1: THE EIGHT ISOMORPHISM CLASSES OF CIRCULANTS OF ORDER 6

We can generalize the enumeration formula with some help from notation. Let $\mathrm{lcm}(\{a_i\})$ denote the least common multiple of a set. That is, for each $a_i \in \{a\}$, $a_i | \mathrm{lcm}(\{a\})$, and it is the smallest integer with this property. If the set consists of a single element a, then $\mathrm{lcm}(a) = a$.

3.7 THEOREM. *Let $p_1, p_2, \ldots, p_t$ be a collection of distinct, odd primes. The cycle index of the group action of $\mathbb{Z}^*_{p_1 p_2 \ldots p_t}/\{1,-1\}$ acting on $\mathbb{Z}_{p_1 p_2 \ldots p_t}/\{1,-1\} \setminus 0$ by right multiplication is*

$$\begin{aligned} &\mathcal{Z}(\mathbb{Z}^*_{p_1 p_2 \ldots p_t}/\{1,-1\}, \mathbb{Z}_{p_1 p_2 \ldots p_t}/\{1,-1\} \setminus 0) \\ = \;& \frac{2}{\phi(p_1 p_2 \ldots p_t)} \sum_{\substack{(d_1, d_2, \ldots, d_t) \\ d_i | p_i - 1 \\ d_t | (p_t - 1)/2}} \Phi(d_1) \ldots \Phi(d_t) \prod_{\substack{I \subseteq \{1,2,\ldots,t\} \\ I \neq \{\}}} x_{L(\{d_i\}_{i \in I})}^{\frac{P(I)}{2L(\{d_i\}_{i \in I})}}, \end{aligned}$$

where H and L are as in Theorem 3.4 and $P(I) = \prod_{i \in I}(p_i - 1)$.

PROOF: The proof is very similar to Theorem 3.4. Theorem 1.2 holds in this case and we use the same isomorphism and action from the group to the set. An element of $\mathbb{Z}_{p_1 p_2 \ldots p_t}/\{1,-1\} \setminus 0$ can be represented by m with $0 < m < p_1 p_2 \ldots p_t/2$. An element of the group $a \in \mathbb{Z}^*_{p_1 p_2 \ldots p_t}$ is represented by $g_{(a_1, a_2, \ldots, a_t)} = g_{\bar{a}}$ with $a_i \equiv a \pmod{p_i}$ and $0 \leq a_t \leq p_t/2$. Each $g_{\bar{a}}$ acts on m as $g_{\bar{a}}(m) = x$ where x is the unique solution modulo

$p_1 p_2 \dots p_t$ to the system of congruences $x = a_i m \pmod{p_i}$. Thus, $g_{\bar{a}}^2(m)$ is the solution to $x = a_i^2 m \pmod{p_i}$ and in general $g_{\bar{a}}^k(m)$ is the solution x to $x = a_i^k m \pmod{p_i}$.

In the case of $t = 2$ three cases were evident. The possibilities were either that m is coprime to both p_1 and p_2 or to exactly one of p_1 or p_2. In the general case, m may be coprime with some subset of the p_i. The length of the cycle in which m is contained will depend on this subset. Say without loss of generality that m is coprime with exactly $p_1, p_2, \dots, p_s$, for $1 \leq s \leq t$. Consider the action under $g_{\bar{a}}$. For $i > s$, $a_i m \equiv 0 \pmod{p_i}$. This means if $k = \operatorname{lcm}(\{ord_{p_i}(a)\}), i = 1 \dots s$, we have $g_{\bar{a}}^k(m) = m$. Thus, the cycle length of $g_{\bar{a}}$ divides k. This will be the order of the cycle unless there exists a k' for which $g_{\bar{a}}^{k'}(m) = -m$. Such a $k' < k$ exists, as before, if and only if, each $\operatorname{ord}_{p_i}(a)$ is even and not all are divisible by 4. If such a k' exists it is $k' = \operatorname{lcm}(\{ord_{p_i}(a)\})/2$.

It is not difficult determine the number of m coprime with exactly the set $\{p_1, p_2, \dots, p_s\}$, or indeed any subset of the p_i in general. There are $\Phi(p_i)$ elements of $\mathbb{Z}_{p_1 p_2 \dots p_t}$ coprime with p_i, hence there are $\prod_{i=1}^s \Phi(p_i)/2$ possible values for m, each coprime with exactly $p_1 p_2 \dots p_s$.

As before, we sum over the possible orders to achieve the result.

⋆

3.8 COROLLARY. *The number of circulants of order $p_1 p_2 \dots p_t$ with each p_i a distinct odd prime is*

$$\frac{2}{\phi(p_1 p_2 \dots p_t)} \sum_{\substack{(d_1, d_2, \dots, d_t) \\ d_i | p_i - 1 \\ d_t | (p_t - 1)/2}} \Phi(d_1) \dots \Phi(d_t) \prod_{\substack{I \subseteq \{1,2,\dots,t\} \\ I \neq \{\}}} 2_{L(\{d_i\}_{i\in I})}^{\frac{P(I)}{2L(\{d_i\}_{i\in I})}} .$$

3.2 Circulant Digraphs

The digraph case is simpler. As we are not looking at the quotient group, by merely determining the cycle index of $\mathbb{Z}_n^*$ acting on $\mathbb{Z}_n$, we can count the classes. This removes the awkward terms that result from determining the parity of orders. Though, in reality in the circulant case we have hidden this awkwardness in notation.

3.9 THEOREM. *Let $p_1, p_2, \ldots, p_t$ be a collection of distinct, odd primes. The cycle index of the group action of $\mathbb{Z}^*_{p_1p_2\ldots p_t}$ acting on $\mathbb{Z}_{p_1p_2\ldots p_t} \setminus 0$ by left multiplication is*

$$\mathcal{Z}(\mathbb{Z}^*_{p_1p_2\ldots p_t}, \mathbb{Z}_{p_1p_2\ldots p_t} \setminus 0) = \frac{1}{\phi(p_1p_2\ldots p_t)} \sum_{\substack{(d_1,d_2,\ldots,d_t)\\ d_i|p_i-1}} \Phi(d_1)\ldots\Phi(d_t) \prod_{\substack{I\subseteq\{1,2,\ldots,t\}\\ I\neq\{\}}} x_{L(\{d_i\}_{i\in I})}^{\frac{P(I)}{\mathrm{lcm}(\{d_i\}_{i\in I})}},$$

where L is as in Theorem 3.7.

3.10 COROLLARY. *The number of digraphs of order $p_1p_2\ldots p_t$, with each p_i prime, $i = 1\ldots t$ is*

$$\frac{1}{\phi(p_1p_2\ldots p_t)} \sum_{\substack{(d_1,d_2,\ldots,d_t)\\ d_i|p_i-1}} \Phi(d_1)\ldots\Phi(d_t) \prod_{\substack{I\subseteq\{1,2,\ldots,t\}\\ I\neq\{\}}} 2^{\frac{P(I)}{\mathrm{lcm}(\{d_i\}_{i\in I}}}.$$

EXAMPLE. The number of non-isomorphic circulant digraphs of order 15 is

$$\frac{1}{8}\sum_{d|2}\sum_{e|4}\Phi(d)\Phi(e)2^{2/d+4/e+8/lcm(d,e)} = 2212.$$

Chapter 4

Unit Circulants

The question remains, what of the circulants of other orders? If we are relying on this technique, we can say nothing of the orders which fall outside of those that satisfy Muzychuk's Theorem. However, the recent proof [8] of the following conjecture of Toida [15] allows us to continue in the same fashion to count a family of circulants with no restriction on order.

4.1 THEOREM (Dobson, Morris). *For any $S \subseteq \mathbb{Z}_n^*$, whenever $X(n;S')$ is isomorphic to $X(n;S)$, there exists an $a \in \mathbb{Z}_n^*$ satisfying $S' = aS$.*

This result allows us to enumerate the circulants $X(n;S)$ of order n whose Cayley subset is a subset of $\mathbb{Z}_n^*$. We shall call such a circulant a *unit circulant*. Notice that the circulants of prime order are all unit circulants. We can also define the class of *unit circulant digraphs*. These are the digraphs with the analogous property, that is, circulant digraphs of order n with the connection set a subset of $\mathbb{Z}_n^*$.

EXAMPLE. If $n = 6$, then the Cayley subsets which yield unit circulants are the empty set and $\{1, 5\} = \mathbb{Z}_6^*$, as depicted in Figure 4.

In the model we have used so far we use the domain of $\mathbb{Z}_n^*$ in the case of digraphs and $\mathbb{Z}_n^*/\{1, -1\}$ in the case of graphs. Theorem 4.1 implies that the permutation group to use in Pólya's Theorem is $\mathbb{Z}_n^*$. Hence we are essentially looking at $\mathbb{Z}_n^*$ acting on itself. To use Pólya's enumeration result we need to determine the cycle index of this action.

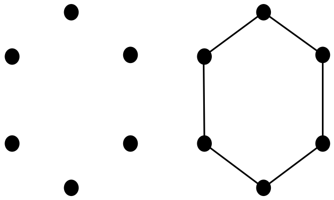

Figure 4.1: THE COMPLETE FAMILY OF UNIT CIRCULANTS ON 6 VERTICES

The difficulty lies in determining the order of an arbitrary element in $\mathbb{Z}_n^*$. Fortunately, the structure of $\mathbb{Z}_n^*$ is well studied and we can make use of an isomorphism of $\mathbb{Z}_n^*$ to a product of cyclic groups to determine the cycle index.

4.1 Odd Prime Powers

We know from Theorem 2.8 that $\mathbb{Z}_p^*$ is isomorphic to the cyclic group of order $p-1$ when p is prime. To determine the the group of units for other orders, we will require some number theoretic tools.

DEFINITION. An integer a is called a *primitive root* mod n, if a generates the group $\mathbb{Z}_n^*$. Equivalently, a is a primitive root mod n if a is of order $\Phi(n)$ modulo n. If there exists some primitive root modulo a given n, then we have that $\mathbb{Z}_n^*$ is cyclic.

EXAMPLE. To see that 2 is a primitive root mod 5 notice $2^2 \equiv 4 \pmod 5, 2^3 \equiv 3 \pmod 5$, and $2^4 = 1$. On the other hand, 8 has no primitive root as $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$.

4.2 LEMMA. *If $t \geq 1$ and $a \equiv b \pmod{p^t}$, then $a^p \equiv b^p \pmod{p^{t+1}}$.*

4.3 COROLLARY. *If $t \geq 2$ and $p \neq 2$, then $(1+ap)^{p^{t-2}} \equiv 1 + ap^{t-1} \pmod{p^t}$ for all $a \in \mathbb{Z}$. Further, if p does not divide a, then p^{t-1} is the order of $1+ap$ modulo p^t.*

PROOF: We can prove this result by induction on t. The result is trivially true when $t = 2$. Next, say it is true for $2 \leq t = n$. Then we have

$$\begin{aligned} (1+ap)^{p^{n-2}} &\equiv 1 + ap^{n-1} \pmod{p^n} \\ (1+ap)^{p^{n-1}} &\equiv (1+ap^{n-1})^p \pmod{p^{n+1}} \quad \text{by Lemma 4.2} \\ &\equiv 1 + \binom{p}{1} ap^{n-1} + B \pmod{p^{n+1}} \end{aligned}$$

where each term in B contains p^{n+1} as a factor since it contains a power of p^{n-1} greater than 1. Hence, the result holds for $t = n+1$ and the result follows by induction. Now, this implies that $(1+ap)^{p^{t-1}} \equiv 1 \pmod{p^t}$, since the order of $1+ap$ divides p^{t-1}. However, $(1+ap)^{p^{t-2}} \equiv 1 + ap^{t-1} \pmod{p^t}$, and hence as p does not divide a, this is not 1. Thus the order of $1+ap$ is greater than p^{t-2}, and hence is p^{t-1}.

⋆

4.4 THEOREM. *If p is an odd prime and $t \in \mathbb{Z}^+$, then $\mathbb{Z}^*_{p^t}$ is cyclic.*

PROOF:[14] To prove the result, it is sufficient to establish the existence of an element of $\mathbb{Z}^*_{p^t}$ with order $\Phi(p^t) = (p-1)p^{t-1}$. The case $t = 1$ was proven in Theorem 2.8, hence we may choose an element $x \in \mathbb{Z}_p$ with order $p-1$. If $x^{p-1} \not\equiv 1 \pmod{p^2}$, then we can, and momentarily shall, illustrate that x is the desired element of order $\Phi(p^t)$. If $x^{p-1} \equiv 1 \pmod{p^2}$, then $x+p$ is also an element of order $p-1$ mod p and

$$(x+p)^{p-1} \equiv x^{p-1} + (p-1)x^{p-2}p \equiv 1 + (p-1)x^{p-2}p \pmod{p^2}.$$

The expression $(p-1)x^{p-2}$ is clearly not divisible by p, thus $(x+p)^{p-1} \not\equiv 1 \pmod{p^2}$.

We can assume without loss of generality that $x^{p-1} \not\equiv 1 \pmod{p^2}$. We can write x^{p-1} as $1+ap$, where p does not divide a. The multiplicative order of $1+ap$ modulo p^t is p^{t-1} by Corollary 4.3.

Now, consider any whole number n such that $x^n \equiv 1 \pmod{p^t}$. Thus, $(x^n)^{p-1} \equiv (1+ap)^n \equiv 1 \pmod{p^t}$, and p^{t-1} must divide n. Further, $x^n = 1 + bp^t$ for some integer

b, so $x^n \equiv 1 \pmod{p}$. If we write $n = p^{t-1}m$, then since $x^p \equiv x \pmod{p}$, $1 \equiv x^n \equiv x^m \pmod{p}$. Since the order of x modulo p is $p-1$, $p-1$ divides m. Thus, for any n such that $x^n \equiv 1 \pmod{p^t}$, $\Phi(p^t)$ divides n. We have illustrated a primitive root modulo p^t, implying that $\mathbb{Z}_{p^t}$ is cyclic for prime p.

$\star$

It remains to determine the cycle index of $\mathbb{Z}^*_{p^t}$ on itself. Once we have established this result, the enumeration formula will fall from it. From this point on assume that D and R are as they have been to this point.

4.5 THEOREM. *If p be is an odd prime, then*

$$\mathcal{Z}(\mathbb{Z}^*_{p^t}, \mathbb{Z}^*_{p^t}) \quad = \quad \frac{1}{\Phi(p^t)} \sum_{d|\Phi(p^t)} \Phi(d) x_d^{\Phi(p^t)/d}.$$

PROOF: The group action of $a \in \mathbb{Z}^*_{p^t}$ acting on itself is $\alpha_a(x) = ax \pmod{p^t}$. Hence, an arbitrary element $x \in \mathbb{Z}^*_{p^t}$ is contained in the cycle

$$(x \;\; ax \;\; a^2x \;\; \ldots \;\; a^{k-1}x)$$

where k is the multiplicative order of a in $\mathbb{Z}_{p^t}$. The size of $\mathbb{Z}^*_{p^t}$ is $\Phi(p^t)$, hence each a contributes a term of $x_k^{\frac{\Phi(p^t)}{k}}$.

The fact that the group is cyclic implies that there are $\Phi(k)$ elements of order k in the group.

$\star$

4.2 Products of Odd Prime Powers

Next we consider the product of odd prime powers.

4.6 THEOREM. *Let p and q be distinct odd primes and let $n = p^r q^s$. The cycle index of $\mathbb{Z}_n^*$ acting on itself is*

$$\mathcal{Z}(\mathbb{Z}_{p^rq^s}^*, \mathbb{Z}_{p^rq^s}^*) = \frac{1}{\Phi(p^rq^s)} \sum_{d_1|\Phi(p^r)} \sum_{d_2|\Phi(q^s)} \Phi(d_1)\Phi(d_2) x_{lcm(d_1,d_2)}^{\frac{\Phi(p^rq^s)}{lcm(d_1,d_2)}}$$

PROOF: We have so far that the automorphism group is isomorphic to $\mathbb{Z}_{p^r}^* \times \mathbb{Z}_{q^s}^*$. Given $(a,b) \in \mathbb{Z}_{p^r}^* \times \mathbb{Z}_{q^s}^*$, the corresponding action $g_{(a,b)}$ on $\mathbb{Z}_n$ maps $m \in \mathbb{Z}_n^*$ to the unique solution x modulo n of

$$\begin{aligned} x &\equiv am \pmod{p^r} \\ x &\equiv bm \pmod{q^s}. \end{aligned}$$

It follows that $g_{(a,b)}^i(m)$ is the unique solution x modulo n of

$$\begin{aligned} x &\equiv a^i m \pmod{p^r} \\ x &\equiv b^i m \pmod{q^s}. \end{aligned}$$

Hence, the general element $m \in Z_{p^rq^s}^*$ is contained in the cycle

$$(m \;\; g_{(a,b)}(m) \;\; g_{(a,b)}^2(m) \;\; \ldots \;\; g_{(a,b)}^{k-1}(m)),$$

where k is the smallest integer such that $m \equiv ma^k \pmod{p^r}$ and $m \equiv mb^k \pmod{q^s}$. It must be that $k = lcm(k(a), k(b))$. We have already illustrated that there are $\Phi(k(a))$ elements of order $k(a)$ in $\mathbb{Z}_{p^r}$, thus the number of pairs (a,b) with a, b of orders $k(a), k(b)$ respectively is $\Phi(k(a))\Phi(k(b))$.

$\star$

4.7 COROLLARY. *If $n = p_1^{r_1} p_2^{r_2} \ldots p_t^{r_t}$ where each p_i is a distinct odd prime, then*

$$\mathcal{Z}(\mathbb{Z}_n^*, \mathbb{Z}_n^*) = \frac{1}{\Phi(n)} \sum_{\substack{(d_1,d_2,\ldots,d_t) \\ d_i|\Phi(p_i^{r_i})}} \Phi(d_1)\ldots\Phi(d_t) x_{lcm\{d_i\}}^{\Phi(n)/lcm\{d_i\}}.$$

4.3 Unit Circulants of All Orders

Powers of two are only slightly more complicated to incorporate.

4.8 THEOREM. *Primitive roots exist modulo 2^t for $t = 1$ and 2, hence $\mathbb{Z}_2$ and $\mathbb{Z}_4$ are cyclic. If $t > 2$, then $\mathbb{Z}^*_{2^t} \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{t-2}}$.*

PROOF: [14] The first statement follows from the observation that 1 is a primitive root modulo 2 and 3 is a primitive root modulo 4. Henceforth let $t \geq 3$. We show the equivalent statement that $A = \{(-1)^a 5^b | a = 0, 1 \text{ and } 0 \leq b < 2^{t-2}\}$ is a reduced residue system modulo 2^t. That is, every element in $Z^*_{2^t}$ is equivalent to an element in A modulo 2^t. We prove by induction that

$$5^{2^{t-3}} \equiv 1 + 2^{t-1} \pmod{2^t}. \tag{4.1}$$

This is clearly true for $t = 3$. Now assume it is true for $t = n$. We have,

$$\begin{aligned} & 5^{2^{n-3}} && \equiv 1 + 2^{n-1} \pmod{2^n} \\ \Longrightarrow\quad & 5^{2^{n-2}} && \equiv (1 + 2^{n-1})^2 \pmod{2^{n+1}} \text{ by Lemma 4.2} \\ & && \equiv 1 + 2^n + 2^{2n-2} \pmod{2^{n+1}} \\ & && \equiv 1 + 2^n \mod 2^{n+1} \end{aligned}$$

since $2n - 2 \geq n + 1$ when $n \geq 3$. We have established (4.1) by induction. In proving the claim we have established the multiplicative order of 5 in $\mathbb{Z}_{2^t}$ to be 2^{t-2}.

We next show that the members of A are distinct in in $\mathbb{Z}_{2^t}$. If they are distinct, A will cover all of $\mathbb{Z}_{p^t}$ since we have already discovered an injective relationship.

Say that $-5^b \equiv 5^{b'} \pmod{2^t}$. That would imply that

$$\begin{aligned} & 5^{b-b'} && \equiv -1 \pmod{2^t} \\ \Longrightarrow\quad & 2(b - b') && \equiv 0 \pmod{2^{t-2}} \\ \Longrightarrow\quad & (b - b') && \equiv 2^{t-3} \pmod{2^{t-2}} \\ \Longrightarrow\quad & 5^{2^{t-3}} && \equiv -1 \pmod{2^t} \end{aligned}$$

contradicting (4.1). If $5^b \equiv 5^{b'} \pmod{2^t}$, then

$$\begin{aligned} 5^{b-b'} &\equiv 1 \pmod{2^t} \\ \Longrightarrow \quad (b-b') &\equiv 0 \pmod{2^{t-2}} \\ \Longrightarrow \quad b &= b'. \end{aligned}$$

Since $((-1)^a 5^b)^{2^{t-2}} \equiv 1 \pmod{2^t}$, no element in $\mathbb{Z}_{2^t}^*$ has order higher than 2^{t-2}, and thus there could be no primitive roots of 2^t, for $t \geq 3$.

$\star$

We can now close the story on the unit circulants and unit circulant digraphs. Theorem 4.1 establishes the connection between the permutation group of the connection sets and isomorphism classes as was the case for circulants and circulant digraphs of prime order.

4.9 THEOREM. *Let $n = 2^{r_1} p_2^{r_2} \ldots p_t^{r_t}$ where each p_i is a distinct odd prime. The number of unit circulants of order n is*

$$\frac{2}{\Phi(n)} \sum_{\substack{(d_0,d_1,d_2,\ldots,d_t) \\ d_1 | 2^{r_1-3} \\ d_i | \Phi(p_i^{r_i}) \\ d_0 | 2}} \Phi(d_1) \cdots \Phi(d_t) 2^{\frac{\Phi(n)}{2\mathrm{lcm}(\{d_i\},d_0)}},$$

when $r_1 \geq 3$,

$$\frac{2}{\Phi(n)} \sum_{\substack{(d_1,d_2,\ldots,d_t) \\ d_1 | 2^{r_1-1} \\ d_i | \Phi(p_i^{r_i})}} \Phi(d_1) \cdots \Phi(d_t) 2^{\frac{\Phi(n)}{2\mathrm{lcm}\{d_i\}}}$$

when $0 < r_1 < 3$, and

$$\frac{2}{\Phi(n)} \sum_{\substack{(d_1,d_2,\ldots,d_t) \\ d_i | \Phi(p_i^{r_i}), 1<i\leq t}} \Phi(d_1) \cdots \Phi(d_t) 2^{\frac{\Phi(n)}{2\mathrm{lcm}\{d_i\}}}$$

otherwise.

PROOF: We proceed in a manner identical to the enumeration of circulants of prime order. This is justified by Theorem 4.1. A substitution of 2 into each x_i of the cycle index gives the result.

$\star$

4.10 THEOREM. *If $n = 2^{r_1} p_2^{r_2} p_3^{r_3} \ldots p_t^{r_t}$, where each p_i is a distinct odd prime, then the number of unit circulant digraphs of order n is*

$$\frac{1}{\Phi(n)} \sum_{\substack{(d_1,d_2,\ldots,d_t)\\ d_1|2^{r_1}\\ d_i|\Phi(p_i^{r_i}),1<i\leq t}} \Phi(d_1)\cdots\Phi(d_t)2^{\frac{\Phi(n)}{\mathrm{lcm}\{d_i\}}}$$

when $r \leq 2$, and

$$\frac{1}{\Phi(n)} \sum_{\substack{(d_0,d_1,\ldots,d_t)\\ d_0|2\\ d_1|2^{r_1-2}\\ d_i|\Phi(p_i^{r_i}),1<i\leq t}} \Phi(d_1)\cdots\Phi(d_t)2^{\frac{\Phi(n)}{\mathrm{lcm}(\{d_i\},d_0)}}$$

otherwise.

To illustrate these, it is best we end this section with a couple of examples.

EXAMPLE. Consider the unit circulants of order 16. The formula yields

$$\frac{2}{8}\sum_{d|4}\Phi(d)x_d^{\frac{8}{2d}} = \frac{1}{4}(2^4+4+4) = 6,$$

as one can see from Figure 4.3.

EXAMPLE. We can use the formula from Theorem 4.9 to count the number of unit circulants of order 35 to compare with the number of circulants. The number of unit circulants is

$$\begin{aligned}\frac{2}{24}\sum_{d|3}\sum_{e|4}\Phi(d)\Phi(e)2^{\frac{12}{\mathrm{lcm}(d,e)}} &= \frac{1}{12}(2^{12}+2^6+2\cdot 2^3+2\cdot 2^4+2\cdot 2^2+4\cdot 2)\\ &= 352.\end{aligned}$$

This is a small portion of the 11 144 total number of circulants of order 35.

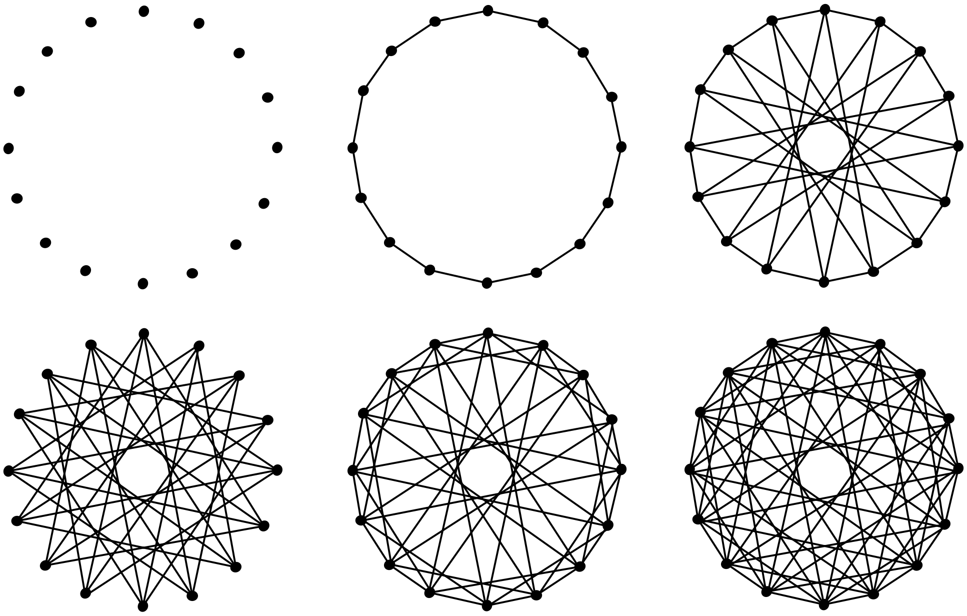

Figure 4.2: Non-Isomorphic Unit Circulants of Order 16

By way of contrast we can also calculate the number of unit circulant digraphs of order 35. The number of non-isomorphic circulant digraphs of order 35 is

$$\frac{1}{24}\sum_{d|6}\sum_{e|4}\Phi(d)\Phi(e)2^{\frac{24}{\mathrm{lcm}(d,e)}} \quad = \quad 699\,616.$$

Chapter 5

Cayley Graphs over $\mathbb{Z}_p \times \mathbb{Z}_p$ with p prime.

The strategy of appealing to Pólya's Theorem to count isomorphism classes can be used to count the Cayley graphs on $\mathbb{Z}_p \times \mathbb{Z}_p$, since this is another family of CI-groups. However, the automorphism group of $\mathbb{Z}_p \times \mathbb{Z}_p$ is the general linear group and hence our methods to determine the cycle index are quite different than for determining the cycle index of a cyclic group.

We consider $\mathbb{Z}_p \times \mathbb{Z}_p$ as an additive group, and consequently think of $\mathbb{Z}_p \times \mathbb{Z}_p$ as a two dimensional vector space over $\mathbb{Z}_p^*$. In general we consider of $\mathbb{Z}_p^n$ to be an $n - dimensional$ vector space over $\mathbb{Z}_p$. With this view in mind, the group of automorphisms is clear.

5.1 THEOREM. *The automorphism group of $\mathbb{Z}_p^n$ is isomorphic to $GL(n, p)$, the group of invertible $n \times n$ matrices over Z_p.*

PROOF: Define $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, with the 1 in the i^{th} position. Since $\mathbb{Z}_p^n$ is generated by the set of $e_i, 1 \leq i \leq n$, the action of any automorphism is determined by its action on $\{e_i, i = 1 \ldots n\}$.

We can construct a general automorphism α, and in the process count the number of possible automorphisms. We have $p^n - 1$ non-zero elements to which we can map e_1.

Our only constraint in determining the value of $\alpha(e_2)$ is linearly independence with e_1, and hence none of the p scalar multiples of $\alpha(e_1)$ leaving $p^n - p$ possibilities. Likewise, the choice for $\alpha(e_3)$ cannot be in the span of $\alpha(e_1)$ and $\alpha(e_2)$, thus $p^n - p^2$ possibilities. In general, there are $p^n - p^{i-1}$ choices to which one may assign $\alpha(e_i)$. Thus the total number of possible automorphisms α of the group $\mathbb{Z}_p^n$ is

$$|\mathrm{Aut}(Z_p^n)| = \prod_{i=0}^{n-1} p^n - p^i$$

which we shall denote $[\ p\ ]_n$.

Now, clearly the action of any $A \in GL(n,p)$ is an automorphism of Z_p^n and hence $GL(n,p) \subseteq \mathrm{Aut}(Z_p^n)$. As the sizes of the two sets are equal, the two sets are equal.

$\star$

The problem of determining the cycle structure of linear transformations over a finite field was first tackled by Kung in [6]. His aim was to determine characteristics of random matrices. His main tool was a vector space analog of the Pólya cycle index, hence we will require effort beyond his work. Recently, Fripertinger [3] calculated the Pólya cycle index of the general linear group (as well as affine and projective groups) and used the cycle index to enumerate isometry classes of linear codes.

The cycle index as Fripertinger calculated it is suitable to enumerate digraphs, but requires modification to be useful for the undirected graph case. Furthermore, since we are first interested in specifying $n = 2$, we can write the expression in a far more explicit, though less compact, form.

5.1 Rational Normal Form

In this context we are regarding the matrices as permutations. Recall that permutations which are conjugate have the same cycle structure. This is the essence of our strategy. As each matrix is in a single conjugacy class, we can determine the cycle index by determining the size of each conjugacy class and the cycle structure of a representative. This section defines the rational normal form and illustrates its suitability as a representative.

Let V be a vector space of finite dimension n over field F. An automorphism is a bijective linear transformation of V to itself. Let A be such a linear transformation of V over F throughout. The notation $\mathbb{F}_p$ indicates the finite field of p elements. The vector space we will consider is $\mathbb{Z}_p^n$, hence, we have $A \in GL(n,p)$. However, these results hold over any field and hence we shall present them in full generality when this is reasonable.

DEFINITION. The space V is *cyclic with respect to* A if there is some $v \in V$ such that $\{v, A(v), A^2(v), ..., A^{n-1}(v)\}$ forms a basis for V.

DEFINITION. A polynomial $\phi(x) \in F[x]$ is an *annihilating polynomial in* V *of* A if and only if $\phi(A)v = 0$ for every $v \in V$. We call $\phi(x)$ the *minimal polynomial of* A if $\phi(x)$ is the monic annihilating polynomial of minimum degree. A is guaranteed to possess an annihilating polynomial, and consequently a minimal polynomial, since the Cayley-Hamilton Theorem states that the characteristic polynomial $det(A - Ix)$, of a matrix A is annihilating.

DEFINITION. Let $\phi(x) = a_0 + a_1x + \ldots + a_rx^r \in \mathbb{F}[x]$. The *companion matrix* of $\phi(x)$ is the $r \times r$ matrix

$$C(\phi) = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ -a_0 & -a_1 & -a_2 & \ldots & -a_{n-1} \end{pmatrix}$$

Notice that the minimal polynomial of $C(\phi)$ is $\phi(x)$.

If V is an n-dimensional vector space cyclic with respect to linear transformation A and the minimal polynomial of A is $\phi(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n$, then there is a basis of V over F such that in this basis the matrix of A is $C(\phi)$. The rational normal form is a generalization of a companion matrix.

A vector space V can always be broken down into cyclic subspaces. Recall [5] that given a linear transformation A of V over F, with minimal polynomial $\phi(x) = \prod_i \phi_i(x)^{c_i}$, with each $\phi_i(x)$ monic, irreducible, and unique, then A decomposes V into a direct sum of n_i-dimensional cyclic subspaces, each invariant under $\phi_i(x)^{c_i}$ for some i. Notice that $\sum_i n_i c_i = n$.

DEFINITION. The *primary decomposition* of A is a unique representation of V as a direct sum of A-invariant subspaces U_i such that U_i is the kernel of $\phi_i(A)^{c_i}$.

Each A-invariant subspace U_i can be further decomposed into a direct sum of subspaces $U_{i,j}$ such that A restricted to $U_{i,j}$ is cyclic. Each $U_{i,j}$ is the kernel of $\phi_i(A)^j$ for $j \leq c_i$.

DEFINITION. A *partition* of n is an unordered set of integers which sum to n. We can summarize a partition with a partition vector $\lambda = (\lambda_1, \lambda_2, \lambda_3, \ldots)$, a sequence of non-negative integers with finitely many non-zero terms such that $n = \lambda \cdot (1, 2, 3, ...) = 1\lambda_1 + 2\lambda_2 + 3\lambda_3 + \ldots$. Henceforth partitions will refer to the vectors and $|\lambda|$ will denote the size, which is n.

DEFINITION. Given the $r \times r$ companion matrix $C(\phi)$ we can define the associated $kr \times kr$ matrix known as the *hypercompanion matrix* $\phi^{(k)}$ by

$$\phi^{(k)} = \begin{pmatrix} C(\phi) & 0_r & 0_r & \ldots & 0_r \\ E_{ir} & C(\phi) & 0_r & \ldots & 0_r \\ 0_r & E_{ir} & C(\phi) & \ldots & 0_r \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0_r & 0_r & 0_r & \ldots & C(\phi) \end{pmatrix}$$

where $E_{ir} = (e_{ij})_{i \leq r, j \leq r}$ with $e_{ij} = 1$, if $(i, j) = (1, r)$ and 0 otherwise, and 0_r is the $r \times r$ 0-matrix. Notice that $\phi^{(1)} = C(\phi)$ and that the minimal polynomial of $\phi^{(k)}$ is $\phi(x)^k$.

DEFINITION. Given a monic, irreducible polynomial $\phi(x)$ of degree d, and a partition λ we define the $d|\lambda| \times d|\lambda|$ matrix $D(\phi, \lambda)$ as the diagonal block matrix

$$D(\phi, \lambda) = diag[\underbrace{\phi^{(1)}, \ldots, \phi^{(1)}}_{\lambda_1 \text{times}}, \underbrace{\phi^{(2)}, \ldots, \phi^{(2)}}_{\lambda_2 \text{times}}, \ldots, \underbrace{\phi^{(i)}, \ldots, \phi^{(i)}}_{\lambda_i \text{times}}, \ldots].$$

5.2 THEOREM. *Suppose A is a linear transformation of an n-dimensional space with minimal polynomial $\psi(x) = \phi(x)^c$, with $\phi(x)$ monic, irreducible and of degree d. There exists a partition λ with $|\lambda| d = n$ such that A is similar to $D(\phi, \lambda)$.*

The partition comes from the way A decomposes V into cyclic subspaces. That is, λ_i is the number of cyclic subspaces of V of dimension i.

5.3 COROLLARY. *Let A be a linear transformation in the n-dimensional vector space V over F with minimal polynomial $\phi(x) = \prod_{i=1} \phi_i(x)^{c_i}$ with each ϕ_i unique, monic and irreducible and d_i the degree of ϕ_i. There exists a sequence of partitions $(\lambda^{(1)}, \lambda^{(2)}, \ldots)$ with $\sum_i |\lambda^{(i)}| d_i = n$, and an ordered basis of V such that A relative to that basis is*

$$\bar{A} = diag[D(\phi_1, \lambda^{(1)}), D(\phi_2, \lambda^{(2)}), \ldots, D(\phi_i, \lambda^{(i)}), \ldots]$$

DEFINITION. The matrix $\bar{A}$ of A as described in the above corollary is the *rational normal form of A*. Each matrix is similar to a matrix in rational normal form unique up to the ordering of the blocks.

To determine the rational normal form for a matrix A, first factor its minimal polynomial $\phi(x)$ into $\phi(x) = \prod_i \phi_i(x)^{c_i}$ where each ϕ_i is an irreducible minimal polynomial. Determine the primary decomposition of V into $U_1 \oplus U_2 \oplus \cdots \oplus U_t$ where U_i is the kernel of $\phi_i^{c_i}(A)$. For each i determine the number $\lambda_{n_j}^{(i)}$ of subspaces of U_i with dimension $c_i n_j$ which are cyclic with respect to the restriction of A on U_i. This will correspond to the number of spaces which are contained in the kernel of $\phi^{n_j}(A)$ but not the kernel of $\phi^{n_j-1}(A)$. The sum of all dimensions of all cyclic subspaces must total n, the dimension of V, that is, $\sum_i |\lambda^{(i)}| d_i = n$.

EXAMPLE. To illustrate this process consider the following $A \in GL(3,5)$. Let $A = \left(\begin{smallmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 2 & 3 & 0 \end{smallmatrix}\right)$. The minimum polynomial of A is $(x-2)^2(x-4)$. The space spanned by $(A-2I_3)^2$ is equal to the space spanned by $\left(\begin{smallmatrix} 1 & 2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$. and hence the kernel is two dimensional. The kernel of $A - 2I_3$ contains only the zero vector since it is of full rank. Hence, the kernel of $(A - 2I_3)^2$ is cyclic. Thus, $\lambda^{(1)} = (0,1)$. On the other hand, the kernel of $(A - 4I_3)$ is one dimensional and so $\lambda^{(2)} = (1)$. This gives a rational normal form of

$$D[x-2,(0,1)]D[x-4,(1)] = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

EXAMPLE. To construct an $n \times n$ matrix in rational normal form one needs only a collection of irreducible polynomials $\phi_1, \phi_2, \ldots, \phi_t$ of degrees $d_1, d_2, \ldots, d_t$ each less than n, respectively, and a set of t partitions $\lambda^{(i)}$ such that $\sum_i |\lambda^{(i)}|d_i = n$. When $n = 2$ it is not a strain to imagine all of the possibilities. Let $V = \mathbb{Z}_p \times \mathbb{Z}_p$. We will consider the various definitions and consequences in this context.

The irreducible polynomials of degree at most two are of the form $x^2 + ax + b$ and $x - a$, with $a, b \in \mathbb{Z}_p$.

If a matrix has an irreducible, degree two, minimal polynomial $\phi(x) = x^2 + ax + b$, then clearly all of V is annihilated by $\phi(A)$. Thus, the partition $\lambda^{(1)} = 1$, since there is one cyclic subspace of dimension $2 \cdot 1$. The rational normal form is

$$D[x^2 + ax + b, (1)] = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix}.$$

If the minimal polynomial factors as $\phi_1(x)\phi_2(x) = (x - a)(x - b)$, then the primary decomposition will split V into $U_1 \oplus U_2$ where $U_1 = kernel(A - aI_2)$ and $U_2 = kernel(A - bI_2)$. These are both of dimension at least one and since the dimension of V is 2 there are both of dimension exactly 1, and hence cyclic. Thus, $\lambda^{(1)} = (1)$ and $\lambda^{(2)} = (1)$. The rational normal form is

$$D[x - a, (1)]D[x - b, (1)] = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}.$$

Next consider $x - a$. There are two possible partitions of 2, (2) and $(0, 1)$. The first implies that there are two cyclic subspaces of dimension 1 hence $A - aI_2$ annihilates all of V and $x - a$ is the minimum polynomial. This gives rise to a rational normal form of

$$D[x - a, (2)] = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

In the other case, there is one cyclic subspace with respect to the matrix, of dimension 2. Thus, $(x - a)^2$ is the minimum polynomial and the rational normal form is

$$D[x - a, (0, 1)] = \begin{pmatrix} a & 0 \\ 1 & a \end{pmatrix}.$$

5.2 The Size of a Conjugacy Class

Kung [6] determined the size of a conjugacy class in $GL(n,p)$. Let $\phi(x) \in \mathbb{F}_p[x]$ be a monic, irreducible polynomial of degree d, and let $\lambda = (\lambda_1, \lambda_2, \ldots)$ be a partition.

5.4 THEOREM ([6]). *The size of the centralizer of $D(\phi,\lambda)$ in $GL(|\lambda|d, p)$ is*

$$b(\lambda, d, p) = \prod_{i=1}^{|\lambda|}\prod_{j=1}^{\lambda_i}(p^{d\mu_i} - p^{d(\mu_i - j)})$$

where

$$\mu_i = \sum_{k=1}^{i} k\lambda_k + \sum_{k=i+1}^{|\lambda|} i\lambda_k.$$

A key thing to notice here is that the number depends on d and the partition, not the polynomial itself.

5.5 COROLLARY. *The number of matrices $A \in GL(n,p)$ with rational normal form*

$$\bar{A} = diag[D(\phi_1, \lambda^{(1)}), D(\phi_2, \lambda^{(2)}), \ldots, D(\phi_i, \lambda^{(i)}), \ldots]$$

is

$$\frac{[\,p\,]_n}{\prod_{i=1}^{s} b(\lambda^{(i)}, d, p)}.$$

PROOF: Every matrix is conjugate to a unique matrix in rational normal form. As conjugacy defines an equivalence relation, to count the number of matrices with a given rational normal form we can determine the size of a conjugacy class. The cardinality of a conjugacy class in a group G containing a fixed element g is the order of G divided by the order of the centralizer of g in G. It is thus sufficient to show that the order of the centralizer of $\bar{A}$, a matrix in rational normal form, is $\prod_{i=1}^{s} b(\lambda^{(i)}, d, p)$. It is a block matrix hence the centralizer is the direct product of the centralizers of each block. The order of a block is given by Theorem 5.4.

$\star$

EXAMPLE. Again we examine the $n = 2$ case to clarify.

Consider the number of matrices with rational normal form $D[x - a, (2)]$. These are the scalar multiples of the identity. We would expect exactly one each of these since these matrices commute with any other and are the only matrices with produce an effect of scalar multiplication. We calculate $\mu_1 = 2$, and $b((2), 1, p) = (p^2 - p)(p^2 - p)$. This is exactly $[\ p\ ]_2$ hence the number of matrices in a conjugacy class with $D[x - a, (2)]$ is exactly one. Similarly we can calculate the values for the other classes and they work out as follows.

Minimal polynomial	Rational normal form	Number in a class
$(x - a)$	$D[x - a, (2)]$	1
$(x - a)^2$	$D[x - a, (0, 1)]$	$p^2 - 1$
$(x - a)(x - b), a \neq b$	$D[x - a, (1)]D[x - b, (1)]$	$p(p + 1)$
$x^2 + ax + b$, irreducible	$D[x^2 + ax + b, (1)]$	$p^2 - p$

Table 5.1: Sizes of Conjugacy Classes in $GL(2, p)$

5.3 The Cycle Index of $GL(2, p)$

The cycle index of $GL(2, p)$ acting on $\mathbb{Z}_p \times \mathbb{Z}_p \setminus (0, 0)$ is nearly at hand. The previous examples have illustrated the complete set of conjugacy classes and their sizes. To finish we require the cycle structure of each class acting as a permutation.

Observe that in general, the action of an $n \times n$ diagonal block matrix on $\mathbb{Z}_p^n$ can be decomposed into a product of actions of the blocks on vectors of the appropriate length. Now, Pólya observed [11] that given groups G and H acting on sets X and Y, respectively, the cycle index of the induced action of the product $G \times H$ on $X \times Y$, $(g, h)(x, y) = (gx, hy)$, can be expressed

$$\mathcal{Z}(G \times H) = \mathcal{Z}(G)\mathcal{Z}(H).$$

A matrix $\bar{A}$ in rational normal form is a block diagonal matrix. Each block is a hypercompanion matrix of a monic, irreducible polynomial ϕ_i of degree d_i over $\mathbb{Z}_p$. We can decompose this into an action of the direct product of hypercompanion matrices,

$$\prod_{i=1}^{s}\prod_{j=1}^{|\lambda^{(i)}|}\prod_{k=1}^{\lambda_j^{(i)}}\phi_i^{(j)}$$

acting on

$$\prod_{i=1}^{s}\prod_{j=1}^{|\lambda^{(i)}|}\prod_{k=1}^{\lambda_j^{(i)}}\mathbb{Z}_p^{jd_i}.$$

Hence the problem of determining the cycle index of any matrix reduces to determining the cycle structure of hypercompanion matrices of monic irreducible polynomials.

To determine the cycle structure of just such a matrix, consider the connection between the hypercompanion matrix and its polynomial.

DEFINITION. Given $A \in GL(n, p)$, we define the *order* of A to be the least integer $k > 0$ such that $A^k = I_n$, the $n \times n$ identity matrix.

DEFINITION. Let $\phi \in \mathbb{F}_p[x]$ be a polynomial of degree m such that $\phi(0) \neq 0$. The *order* of ϕ, denoted $\operatorname{ord}(\phi)$ or $\operatorname{ord}(\phi(x))$, is the least integer $k > 0$ such that $\phi(x)$ divides $x^k - 1$. It can be shown that some $k \leq p^m - 1$ exists. If $\phi(0) = 0$, we can define the order of ϕ by writing $\phi(x) = x^n\psi(x)$ such that $n \in \mathbb{N}$, $\psi(0) \neq 0$, and define $\operatorname{ord}(\phi) = \operatorname{ord}(\psi)$.

5.6 THEOREM ([7]). *Let $\phi \in \mathbb{F}_p[x]$ be an irreducible polynomial over $\mathbb{F}_p$ of degree m with $\phi(0) \neq 0$. Then $\operatorname{ord}(\phi)$ is equal to the order of any root of ϕ in the multiplicative group $\mathbb{F}_{p^m}^*$.*

5.7 COROLLARY ([7]). *Let $\phi \in \mathbb{F}_p[x]$ be an irreducible polynomial over $\mathbb{F}_p$ of degree m with $\phi(0) \neq 0$. Then $\operatorname{ord}(\phi)$ divides $p^m - 1$.*

The following provides a very useful summary regarding the number of irreducible polynomials of a given degree.

5.8 THEOREM ([7]). *The number of monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree m and order k is equal to $\Phi(k)/m$ if $k \geq 2$ and m is the multiplicative order of p modulo k. It is 2 if $m = k = 1$ and 0 in all other cases.*

If $m = 2$, then for all positive k such that $k|(p^2 - 1)$ and $p \not\equiv 1$ modulo k, k is the order of $\Phi(k)/2$ irreducible polynomials in $F_p[x]$.

We can determine the order of reducible polynomials with the following two results.

5.9 THEOREM ([7]). *Given irreducible polynomials $\phi_1, \phi_2 \in \mathbb{F}_p[x]$ with $\phi_1(0) \neq 0, \phi_2(0) \neq 0$, $\operatorname{ord}(\phi_1\phi_2) = \operatorname{lcm}(\operatorname{ord}(\phi_1), \operatorname{ord}(\phi_2))$.*

5.10 THEOREM ([7]). *If $\phi \in F_p[x]$ is an irreducible polynomial of degree m with $\phi(0) \neq 0$, then $\operatorname{ord}(\phi^k) = p^b \operatorname{ord}(\phi)$, where b is the smallest integer with $p^b \geq m$.*

For our purposes, since $p > 2$ and $m = 2$, b will be 1.The connection between the companion matrices and the polynomials is direct.

5.11 LEMMA. *If $\phi(x)$ be an irreducible polynomial in $\mathbb{F}_p[x]$ with $\phi(0) \neq 0$, then $ord(\phi^{(1)}) = ord(\phi)$.*

5.12 COROLLARY ([7]). *Let $\phi(x)$ be an irreducible polynomial in $\mathbb{F}_p[x]$ with $\phi(0) \neq 0$. Then $ord(\phi^{(k)}) = ord(\phi(x)^k) = p^b ord(\phi(x))$ where b is the smallest integer with $p^b \geq m$.*

5.13 THEOREM. *Let V be cyclic with respect to linear transformation A. Let $\phi(x)$ be an irreducible, monic polynomial and the minimal polynomial of A. As a permutation of the non-trivial elements of V, A is a product of cycles of a length* $\operatorname{ord}(\phi)$.

PROOF: Since V is cyclic with respect to A, there is some $v \in V$ such that any $w \in V$ can be written as $w = \psi(A)v$ for some $\psi \in \mathbb{F}[x]$ of degree less than or equal to the degree of $\phi(x)$. Now, let $\operatorname{ord}(\phi) = k$. Hence $\phi(x)|(x^k - 1)$, and thus $A^k - I = 0$. For any $w \in V$, $(A^k - I)w = 0 \implies A^k w = w$ and w is in a cycle of length at most k.

Now say $A^m w = w$ for some integer $m > 0$. We write $w = \psi(A)v$, and hence $A^m\psi(A)v = \psi(A)v$ and $(A^m - I)\psi(A)v = 0$. Any polynomial which annihilates v annihilates V and thus $\phi(x)$ will divide it. Hence, $\phi(x)|((x^m - 1)\psi(x))$. Since $\phi(x)$ is irreducible it must divide either $\psi(x)$ or $x^m - 1$. In the first case, $\psi(x) = \phi(x)$ since the degree of $\psi(x)$ is at most the degree of $\phi(x)$. In this case $w = 0$. Otherwise, $\phi(x)|(x^m - 1)$ which implies that $m \geq k$ by the definition of order of a polynomial. Thus $m = k$ and all elements in the space are in cycles of length $\mathrm{ord}(\phi)$.

$\star$

5.14 THEOREM. *The cycle index of $GL(2,p)$ acting on $\mathbb{Z}_p \times \mathbb{Z}_p \setminus (0,0)$ is*

$$\begin{aligned}
& \mathcal{Z}(GL(2,p), \mathbb{Z}_p \times \mathbb{Z}_p \setminus (0,0)) && (5.1)\\
= \ & \frac{1}{(p^2-p)(p^2-1)} \sum_{d|(p-1)} \Phi(d) x_d^{(p^2-1)/d} && (5.2)\\
+ \ & \frac{1}{2(p^2-1)} \sum_{\substack{d|(p^2-1)\\ p\not\equiv 1 \pmod{d}}} \Phi(d) x_d^{(p^2-1)/d} && (5.3)\\
+ \ & \frac{1}{p^2-p} \sum_{d|p-1} \Phi(d) x_d^{(p-1)/d} x_{pd}^{(p-1)/d} && (5.4)\\
+ \ & \frac{1}{(p-1)^2} \sum_{d|(p-1)} \sum_{\substack{e|(p-1)\\ e\leq d}} \Phi'(d,e) x_d^{\frac{p-1}{d}} x_e^{\frac{p-1}{e}} x_{\mathrm{lcm}(d,e)}^{\frac{(p-1)^2}{\mathrm{lcm}(d,e)}} && (5.5)
\end{aligned}$$

where $\Phi'(d,e) = \Phi(d)\Phi(e)$ if $d \neq e$ and $\Phi(d)^2 - 1$ otherwise.

PROOF: If we consider $A \in GL(n,p)$ as a permutation $\alpha_A(x)$, it is a product of disjoint permutations $\alpha_{A_1}\alpha_{A_2}\ldots\alpha_{A_m}$ where each A_i is a hypercompanion matrix. The vector space $V = \mathbb{Z}_p \times \mathbb{Z}_p$ is divided into subspaces W_i such that W_i is cyclic with respect to A_i for each i. An element x in $\mathbb{Z}_p \times \mathbb{Z}_p$ can be uniquely expressed as $w_1 \oplus w_2 \oplus \ldots \oplus w_m$ with $w_i \in W_i$. If $x \in W_i$ for some i, then by Theorem 5.13, under α_A it is in a cycle of length $\mathrm{ord}(A_i)$. If it is the direct sum of non-trivial elements from more than one subspace, say $W_1', W_2', \ldots, W_l'$, it is in a cycle of length $\mathrm{lcm}(\mathrm{ord}(A_1'), \mathrm{ord}(A_2'), \ldots, \mathrm{ord}(A_l'))$.

To determine the cycle index we sum over the different types of rational normal forms as uncovered in the previous discussion. The first summand, (5.2), gives us the cycle inventory for elements with the rational normal form $A = D[x - a, (2)]$. As noted earlier, matrices of this form have the effect of scalar multiplication. Hence the cycle structure is straightforward. The number of transformations for each order is the number of elements in $\mathbb{Z}_p$ with order $\mathrm{ord}(a)$, or $\Phi(\mathrm{ord}(a))$ by Lemma 2.7.

V is also cyclic with respect to transformations with rational normal form $D[x^2 + ax + b, (1)]$ for irreducible polynomials $x^2 + ax + b$. Theorem 5.8 gives us the number of polynomials of degree two with a given order, hence we have (5.3) to account for these types of transformations.

The third summand, (5.4), accounts for the matrices with rational normal form $A = D[x - a, (0, 1)]$. There are two cyclic subspaces, one with order $\mathrm{ord}(a)$ and a second of order $\mathrm{ord}((x-a)^2) = p\ \mathrm{ord}(a)$, by Theorem 5.10. Both subspaces have p elements, but the remaining elements in the subspace also have order $p\ \mathrm{ord}(a)$, since that is the least common multiple of the pair.

The last, and most complicated, type of rational normal form comes from matrices with the remaining normal form, $D[x - a, (1)]D[x - b, (1)]$ when $a \neq b$. Here there are two cyclic subspaces, one each of orders $\mathrm{ord}(a)$ and $\mathrm{ord}(b)$. Thus, the elements in each of these respective subspaces are organized in cycles of lengths $\mathrm{ord}(a)$ and $\mathrm{ord}(b)$, respectively. The size of both subspaces is p. The remaining $(p - 1)^2$ elements in the subspace are in cycles of length $lcm(\mathrm{ord}(a), \mathrm{ord}(b))$. This is also a consequence of Theorem 5.9. There are $\Phi(a)$ elements of order a and $\Phi(b)$ elements of order b. However, we do not include the case when $a = b$ since they are special and are covered in (5.4). This gives us (5.5).

$\star$

5.15 COROLLARY. *The number of non-isomorphic Cayley digraphs on $\mathbb{Z}_p \times \mathbb{Z}_p$ for p prime* *is*

$$\begin{aligned} & \frac{1}{(p^2-p)(p^2-1)} \sum_{d|p-1} \Phi(d) 2^{\frac{p-1}{2d}} (p^2 - 1 + 2^{\frac{(p-1)^2}{d}}) \\ + & \frac{1}{p^2-1} \sum_{\substack{d|(p^2-1) \\ p \not\equiv 1 \pmod d}} \Phi(d) 2^{(p^2-p)/d-1} \\ + & \frac{1}{(p-1)^2} \sum_{d|(p-1)} \sum_{\substack{e|(p-1) \\ e \leq d}} \Phi'(d,e) 2^{(p-1)(p-1+\frac{d+e}{gcd(d,e)})/lcm(d,e)} \end{aligned}$$

with Φ' defined in Theorem 5.14.

EXAMPLE. The cycle index for $GL(2,3)$ acting on $\mathbb{Z}_3 \times \mathbb{Z}_3 \setminus (0,0)$ is

$$\frac{1}{48}(12x_2^3x_1^2 + 12x_8 + 6x_4^2 + 8x_6x_2 + 8x_3^2x_1^2 + x_2^4 + x_1^8).$$

Hence the number of non-isomorphic Cayley digraphs on $\mathbb{Z}_3 \times \mathbb{Z}_3$ is

$$\frac{1}{48}(12 \cdot 2^3 \cdot 2^2 + 12 \cdot 2 + 6 \cdot 2^2 + 8 \cdot 2 \cdot 2 + 8 \cdot 2^2 \cdot 2^2 + 2^4 + 2^8) = 18.$$

The generating function for valency is

$$1 + u + 2u^2 + 2u^3 + 4u^4 + 3u^5 + 2u^2 + u^7 + u^8.$$

To determine the analogous result for ordinary graphs requires a modification of the action of $GL(2,p)$ on $\mathbb{Z}_p \times \mathbb{Z}_p$. As in the circulant case we are looking at the group of automorphisms acting on the quotient group, in this case $(\mathbb{Z}_p \times \mathbb{Z}_p \setminus (0,0))/\{(1,1),(-1,-1)\}$, which we shall denote **Z**. In the circulant case it simplified matters to pare down the automorphism group. In this case, it is simpler to use $GL(2,p)$.

We have already determined the nature and size of the conjugacy classes. However, the cycle structure of a transformation is different when we identify x and $-x$ in $\mathbb{Z}_p^2$.

5.16 LEMMA. *Consider monic, irreducible, $\phi \in \mathbb{F}_p[x]$ with $k = \operatorname{ord}(\phi)$. Let k' be the smallest integer such that $\phi(x)$ divides $x^{k'} + 1$, if it exists. Then $k' = k/2$ if k is even and does not exists if k is odd.*

PROOF: If $k = 2d$, then $\phi(x)$ divides $x^{2d} - 1 = (x^d - 1)(x^d + 1)$. By the definition of order, ϕ must divide $x^d + 1$. Thus $k' \leq d = k/2$. If $k' < d$, then $\phi(x)$ divides $(x^{k'} + 1)(x^{k'} - 1) = x^{2k'} - 1$, contradicting the order of ϕ.

If k is odd, then as in the previous case certainly if k' existed it could be no less than $k/2$, no more than k and must divide k. Thus, it does not exist.

$\star$

This k' serves as a new form of order. If V is an n–dimensional subspace cyclic with respect to $A \in GL(n,p)$, then the length of a cycle of A acting on an element of V where x and $-x$ are identified is $k = ord(A)$ if k is even and $k/2$ if k is odd. We capture this action with the notation

$$H(x) = \begin{cases} x & x \text{ is odd} \\ x/2 & \text{otherwise.} \end{cases}$$

5.17 THEOREM. *The cycle index of $GL(n,p)$ acting on $\mathbf{Z}$ is*

$$\mathcal{Z}(GL(2,p),\mathbf{Z}) \tag{5.6}$$

$$= \frac{1}{(p^2-p)(p^2-1)} \sum_{d|(p-1)} \Phi(d) x_{H(d)}^{\frac{p^2-1}{2H(d)}} \tag{5.7}$$

$$+ \frac{1}{2(p^2-1)} \sum_{\substack{d|p^2-1 \\ p\not\equiv 1 \pmod d}} \Phi(d) x_{H(d)}^{\frac{p^2-1}{2H(d)}} \tag{5.8}$$

$$+ \frac{1}{p^2-p} \sum_{d|p-1} \Phi(d) x_{H(d)}^{\frac{p-1}{H(d)}} x_{pH(d)}^{\frac{p-1}{H(d)}} \tag{5.9}$$

$$+ \frac{1}{(p-1)^2} \sum_{d|p-1} \sum_{\substack{e|p-1 \\ e\leq d}} \Phi'(d,e) x_{H(d)}^{\frac{p-1}{H(d)}} x_{H(e)}^{\frac{p-1}{H(e)}} x_{L(d,e)}^{\frac{(p-1)^2}{L(d,e)}} \tag{5.10}$$

where Φ' is as defined in Theorem 5.14, and

$$L(d,e) = \begin{cases} lcm(d,e)/2 & \textit{Both d and e are even and are divisble by the same powers of two} \\ lcm(d,e) & \textit{otherwise.} \end{cases}$$

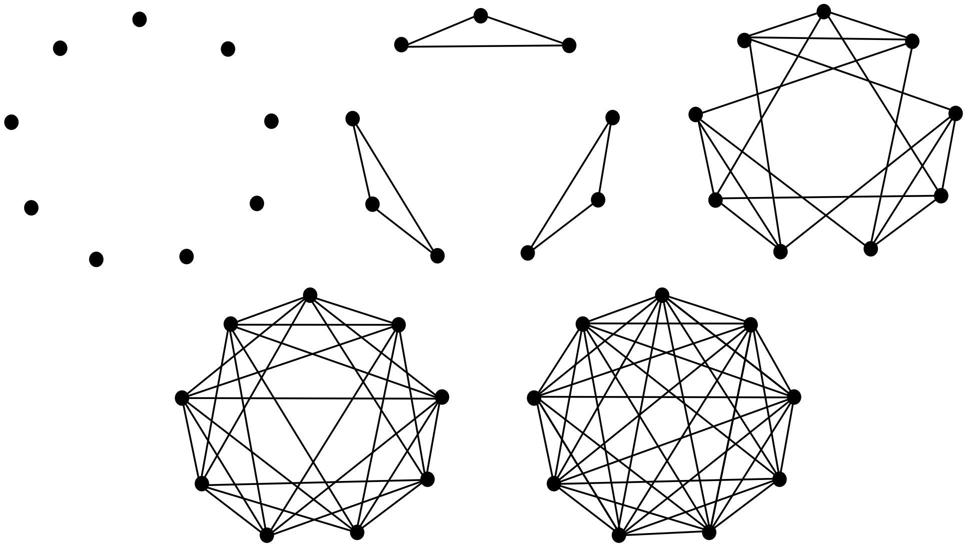

Figure 5.1: THE FIVE ISOMORPHISM CLASSES OF $X(\mathbb{Z}_3 \times \mathbb{Z}_3, S)$

5.18 COROLLARY. *The number of non-isomorphic Cayley graphs on $\mathbb{Z}_p \times \mathbb{Z}_p$ for $p > 2$ prime is*

$$\begin{aligned}
& \mathcal{Z}(GL(2,p), \mathbf{Z}) && (5.11)\\
= \quad & \frac{1}{(p^2-p)(p^2-1)} \sum_{d|(p-1)} \Phi(d) 2^{\frac{p^2-1}{2H(d)}} && (5.12)\\
+ \quad & \frac{1}{2(p^2-1)} \sum_{\substack{d|p^2-1 \\ p \not\equiv 1 \pmod{d}}} \Phi(d) 2^{\frac{p^2-1}{2H(d)}} && (5.13)\\
+ \quad & \frac{1}{p^2-p} \sum_{d|p-1} \Phi(d) 2^{\frac{p-1}{H(d)}} 2^{\frac{p-1}{H(d)}} && (5.14)\\
+ \quad & \frac{1}{(p-1)^2} \sum_{d|p-1} \sum_{\substack{e|p-1 \\ e \le d}} \Phi'(d,e) 2^{\frac{p-1}{H(d)}} 2^{\frac{p-1}{H(e)}} 2^{\frac{(p-1)^2}{L(d,e)}} && (5.15)
\end{aligned}$$

where Φ' is as defined in Theorem 5.14, and L is as defined in Theorem 5.17

EXAMPLE. The cycle index for $GL(2,3)$ acting on $\mathbb{Z}_3 \times \mathbb{Z}_3 \setminus (0,0)/\{1,-1\}$ is

$$\frac{1}{48}(12x_2x_1^2 + 12x_4 + 6x_2^2 + 16x_3x_1 + 2x_1^4)$$

hence the number of non-isomorphic Cayley graphs on $\mathbb{Z}_3 \times \mathbb{Z}_3$ is

$$\frac{1}{48}(12 \cdot 2 \cdot 2^2 + 12 \cdot 2 + 6 \cdot 2^2 + 16 \cdot 2 \cdot 2 + 2 \cdot 2^4) = 5,$$

as illustrated in Figure 5.3. The valency generating function is $1 + u^2 + u^4 + u^6 + u^8$, also as expected.

5.4 $\mathbb{Z}_p^3$ and Beyond

The methods we have developed so far this chapter have been sufficiently general that they can be used to count Cayley graphs over $\mathbb{Z}_p^3$ and any other CI-Group of the form $\mathbb{Z}_p^n$. However, a a better notation is essential. The following notation was derived by H. Fripertinger [3] for the cycle index of $GL(n, p)$ acting on $\mathbb{Z}_p^n$. It encapsulates much of the work and removes the intuition, but allows one to calculate and so it is included.

5.5 The Cycle Index of $GL(n, p)$

To facilitate the description of the cycle index we introduce a product notation. Let A and B be polynomials in indeterminates $x_1, x_2, \ldots$ such that

$$\begin{aligned} A(x_1, \ldots, x_n) &= \sum_{(j)} a_{(j)} \prod_{i=1}^{n} x_i^{j_i} \\ B(x_1, \ldots, x_m) &= \sum_{(k)} b_{(k)} \prod_{i=1}^{m} x_i^{k_i}. \end{aligned}$$

Define the operator $\diamond$ on A and B as follows

$$A(x_1, \ldots, x_n) \diamond B(x_1, \ldots, x_m) = \sum_{(j)} \sum_{(k)} a_{(j)} b_{(k)} \prod_{i=1}^{n} \prod_{l=1}^{m} x_i^{j_i} \diamond x_l^{k_l}$$

where

$$x_i^{j_i} \diamond x_l^{k_l} = x_{\mathrm{lcm}(i,l)}^{j_i k_l \gcd(i,l)}.$$

We will denote the k^{th} power of this operator by $A(x_1, \ldots, x_n)^{\diamond k}$.

We have already determined the cycle structure and size of a conjugacy class. The last task for determining the cycle index of $GL(n,p)$ is to determine all possible normal forms.

Let μ be the Möbius function. There are

$$N_p(d) = \frac{1}{d}\sum_{t|d} \mu(t)p^{d/t}$$

monic, irreducible polynomials of degree d over $\mathbb{Z}_p$. Each monic, irreducible polynomial of degree at most n with the exception of $\phi(x) = x$ can occur as a divisor of the characteristic polynomial of a matrix $A \in GL(n,p)$. Label these $t_n = \sum_{i=1}^{n} N_p(i) - 1$ polynomials as $\phi_1(x), \phi_2(x), \ldots, \phi_{t_n}(x)$, with the degree of $\phi_i(x)$ as d_i. We need to find all solutions $\gamma = (\gamma_1, \ldots, \gamma_{t_n})$, to

$$\sum_{i=1}^{t_n} \gamma_i d_i = n \tag{5.16}$$

where γ_i is a non-negative integer. For each solution γ one must determine the possible cycle types, that is, the partitions $\lambda^{(i)}$ of γ_i. Call this set $CT(\gamma_i)$. The representative of the conjugacy class of matrices A with characteristic polynomial

$$\phi(x) = \prod_{i=1}^{t_n} \phi_i(x)^{\gamma_i}$$

is

$$\bar{A} = diag(D(\phi_1, \lambda^{(1)}), \ldots, D(\phi_{t_n}, \lambda^{(t_n)})).$$

We now have our cycle index for $GL(n,p)$.

5.19 THEOREM. *The cycle index of $GL(n,p)$ acting on $Z_p^n \setminus \bar{0}$ is*

$$\frac{1}{[\,p\,]_n}\sum_{\gamma}\sum_{\lambda}\frac{[\,p\,]_n}{\prod_{i=1}^{s} b(d_i, \lambda^{(i)})}\prod_{i=1}^{t_n}\prod_{j=1}^{\gamma_i}\left(\prod_{k=1}^{j} x_{e_{ik}}^{a_{ik}}\right)^{\diamond\lambda_j^{(i)}},$$

where $e_{ik} = ord(\phi_i(x)^k)$. Furthermore $a_{ik} = \frac{p^{kd_i} - p^{(k-1)d_i}}{e_{ik}}$, $[\,p\,]_n$ is the order of $GL(n,p)$, and $b(d_i, \lambda^{(i)})$ is the size of the centralizer of $D(\phi_i, \lambda^{(i)})$ as computed in 5.4. The first sum *runs over all solutions $\gamma = (\gamma_1, \ldots, \gamma_{t_n})$ of 5.16 and the second runs over all t_n-tuples $\lambda = (\lambda^{(1)}, \ldots, \lambda^{(t_n)}) \in \prod_{i=1}^{t_n} CT(\gamma_i)$.*

The formula from Theorem 5.19 can be used directly to enumerate digraphs in a manner similar to every other family of Cayley digraphs we have encountered so far. With some additional notation as one could also develop a formula for Cayley graphs. Lemma 5.16 gives how to modify this cycle index to get the cycle index of $GL(n, p)$ acting on $\mathbb{Z}_p^n/(1_n, -1_n)$.

5.6 Final Thoughts

Cayley graphs and digraphs are a very elegant family of graphs. By demanding a specific relationship between the automorphisms of the group and the isomorphisms of Cayley graphs on the group, we have been able to develop a nice way to enumerate the non-isomorphic Cayley graphs of a given order for certain CI-groups. As more groups are identified as CI-groups, this method can be revisited as a method of enumeration. Since currently most energy in the CI-group problem is directed at products of cyclic groups, a better form for $\mathcal{Z}(GL(n,p), \mathbb{Z}_p^n)$ would produce more satisfying enumeration results. For every case that Pólya's Enumeration Theorem is used, it may be worthwhile to investigate other uses of the cycle index apart from straight enumeration. For example, one could count the number of distinct edge colourings using k colours by substituting $k + 1$ for each x_i in the cycle index. A different, though likely interesting, epilogue to these results here would be the computation of asymptotics. Of particular interest may be to determine the percentage of circulants which are unit circulants.

Bibliography

[1] E. Beckenbach, editor. *Applied Combinatorial Mathematics*. John Wiley and Sons, New York, 1964.

[2] E. Dobson. Isomorphism problem for Cayley graphs of $\mathbb{Z}_p^3$. *Discrete Math*, 147:87–94, 1995.

[3] H. Fripertinger. Cycle indices of linear, affine and projective groups. *Lin. Alg. Apps.*, 263:133–156, 1997.

[4] C. D. Godsil. On Cayley graph isomorphisms. *Ars Combin.*, 15:231–246, 1983.

[5] I. N. Herstein. *Topics in Algebra*. Xerox College Publishing, Lexington, Massachusetts, 1975.

[6] J. P. S. Kung. The cycle structure of a linear transformation over a finite field. *Lin. Alg. Apps.*, 36:141–155, 1981.

[7] R. Lidl and H. Niederreiter. *Finite Fields*. Addison-Wesley, London, 1983.

[8] J. Morris. *Isomorphisms of Cayley Graphs*. PhD thesis, Simon Fraser University, 1999.

[9] M. Muzychuk. Ádám's conjecture is true in the square-free case. *J. Combin. Theory Ser. A*, 72:118–134, 1995.

[10] L. Nowitz. A non-Cayley-invariant Cayley Graph of the elementary abelian group of order 64. *Discrete Math*, 110:223–228, 1992.

[11] G. Pólya. Kombinatorische anzahlbestimmungen fúr gruppen, graphen, und chemische verbindungen. *Acta Math.*, 68:145–254, 1937.

[12] R.C. Read. *Combinatorial Enumeration for Groups, Graphs and Chemical Compounds*. Springer-Verlag, New York, 1987.

[13] D. J. S. Robinson. *A Course in the Theory of Groups*. Springer-Verlag, New York, 1995.

[14] K. I. M. Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag, New York, 1983.

[15] S. Toida. A note on Ádám's conjecture. *J. Combin. Theory Ser. B*, 23:239–246, 1977.

[16] J. Turner. Point-symmetric graphs with a prime number of points. *J. Combin Theory*, 3:136–145, 1967.

[17] M.-Y. Xu. On isomorphism of Cayley digraphs and graphs of groups of order p^3. *Adv. in Math (China)*, 17:427–428, 1988.