ELSEVIER

Discrete Mathematics 256 (2002) 527–539

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Enumeration of Cayley graphs and digraphs

Brian Alspach[a,1], Marni Mishna[b,*,2]

[a] *Department of Mathematics and Statistics, University of Regina,
Regina, Saskatchewan, Canada S4S 0A2*

[b] *Department of Mathematics and Statistics, Simon Fraser University, Burnaby, B. C. Canada V5A 1S6*

Received 10 October 2000; received in revised form 2 February 2001; accepted 31 March 2001

Abstract

This paper deals with the enumeration of various families of Cayley graphs and digraphs. Both the directed and undirected cases of the following three families are studied: Cayley graphs on cyclic groups, known as circulant graphs, of square-free order, circulant graphs of arbitrary order n whose connection sets are subsets of the group of units of $\mathbb{Z}_n$, and Cayley graphs on elementary abelian groups.

Resumé

Cet article traite du dénombrement de quelques familles de graphes de Cayley, simples ou orientés. On considère les deux cas, simple et orientés, des trois familles suivantes: la famille des graphes de Cayley sur les groupes cyclique, appelés graphes circulants, dont l'ordre est un entier sans carré, la famille des graphes circulants d'ordre n quelconque dont l'ensemble des connecteurs est un sous-ensemble du groupe des unités de $\mathbb{Z}_n$, ainsi que la famille des graphes de Cayley sur les groupes abéliens élémentaires.

Keywords: Cayley graphs; Cycle index series; Enumeration

---

1. Introduction

The first author's initial foray into the topic of graphs and groups was reading Turner's elegant 1967 paper [19] in which he enumerated the vertex-transitive graphs

---

[*] Corresponding author.

E-mail address: alspach@math.uregina.ca (B. Alspach), mishna@math.uqam.ca (M. Mishna).

[1] This work was partially supported by the Natural Sciences and Engineering Research Council of Canada under grant A-4792.

[2] Current address: LaCIM, Université du Québec à Montréal, C. P. 8888, Succursale Centre-ville, Montréal, QC, Canada H3C 3P8.

PII: S0012-365X(02)00319-9

of prime order. It is not hard to see, in fact, that every vertex-transitive graph of prime order is a Cayley graph on a cyclic group, thus suggesting the possibility of extending his results to other families of Cayley graphs. Moreover, although not explicitly discussed in [19], it is easy to verify the techniques apply equally well to Cayley digraphs on cyclic groups of prime order which suggests a further extension to Cayley digraphs. The subject of this paper is the extension of Turner's results to other families of Cayley graphs and digraphs. The vast majority of the results in this paper form a portion of the second author's M.Sc. thesis [13].

To make certain we are all on the same page, we now define a few terms.

Definition 1.1. Let S be a subset of a finite group G satisfying $1 \notin S$, where 1 denotes the identity of G. A subset S satisfying the above condition is called a *Cayley subset*. The *Cayley digraph* $\vec{X}(G;S)$ is defined to be the digraph whose vertices correspond to the elements of G with an arc from g to h if and only if $h = gs$ for some $s \in S$. The set S is called the *connection set* and $\vec{X}(G;S)$ is called a *Cayley digraph on the group* G. If, in addition, $S = S^{-1}$, that is, $s \in S$ implies that $s^{-1} \in S$, then we define the *Cayley graph* $X(G;S)$ by letting its vertices be the elements of G with an edge between g and h if and only $h = gs$ for some $s \in S$. The set S is again called the connection set.

Definition 1.2. We let $\mathscr{C}(G)$ denote the set of Cayley graphs on the group G, and let $\vec{\mathscr{C}}(G)$ denote the set of Cayley digraphs on G.

Definition 1.3. If G is a cyclic group, the elements of $\mathscr{C}(G)$ are called *circulant* graphs. Likewise, Cayley digraphs on cyclic groups are called *circulant* digraphs. In the case of circulant graphs and digraphs on the cyclic group of order n, we shall use the notation $X(n;S)$ and $\vec{X}(n;S)$, respectively.

We let $\mathbb{Z}_n$ denote the ring of integers modulo n. We shall use $\mathbb{Z}_n^*$ to denote the multiplicative group of units in $\mathbb{Z}_n$. Frequently, we are interested only in the additive group structure of $\mathbb{Z}_n$ and in order to avoid confusion, we shall use the notation $(\mathbb{Z}_n, +)$ in these situations. In fact, we always view circulant graphs and circulant digraphs as Cayley graphs on $(\mathbb{Z}_n, +)$.

Two groups are said to be *isomorphic* if and only if there is an adjacency preserving bijection between their respective vertex sets. What Turner did in [19] was to prove that two circulant graphs $X(p;S_1)$ and $X(p;S_2)$ of prime order p are isomorphic if and only there exists an $a \in \mathbb{Z}_p^*$ such that $aS_1 = S_2$, where aS_1 denotes the set $\{as\colon s \in S_1\}$ and as denotes the product of a and s in $\mathbb{Z}_p$. Therefore, the isomorphism classes are equivalence classes under the multiplicative relation just defined. Furthermore, the multiplicative relation can be viewed as the action of a group acting on the set of connection sets. The equivalence classes are nothing more than the orbits of the group. The latter fact enabled Turner to employ Pólya's Enumeration Theorem [3] to completely solve the problem.

The key to extending Turner's enumeration results is the observation that multiplication by $a \in \mathbb{Z}_p^*$ is a group automorphism of $(\mathbb{Z}_p, +)$. So in these terms what Turner proved is that two circulant graphs of prime order are isomorphic if and only if there is some automorphism of the underlying cyclic group which simultaneously acts as an isomorphism between the two graphs. This leads to the following definitions.

Definition 1.4. Let $X(G;S_1)$ be a Cayley graph on a finite group G. We say that $X(G;S_1)$ is a CI-*graph* provided that $X(G;S_1)$ is isomorphic to $X(G;S_2)$ if and only if there is a group automorphism $\alpha \in \mathrm{Aut}(G)$ satisfying $\alpha(S_1) = S_2$. Similarly, a Cayley digraph $\vec{X}(G;S_1)$ on G is said to be a DCI-*digraph* provided that $\vec{X}(G;S_1)$ is isomorphic to $\vec{X}(G;S_2)$ if and only if there is a group automorphism $\alpha \in \mathrm{Aut}(G)$ satisfying $\alpha(S_1) = S_2$.

Definition 1.5. If every Cayley graph on a finite group G is a CI-graph, then G is said to be a CI-*group*. Similarly, if every Cayley digraph on G is a DCI-digraph, then G is said to be a DCI-*group*.

In this terminology, Turner proved every cyclic group of prime order is a CI-group. If G is a DCI-group, then the orbits of $\mathrm{Aut}(G)$ acting on the Cayley subsets of G correspond to the isomorphism classes of the Cayley digraphs on G. The situation for Cayley graphs is almost the same except that in order for a Cayley graph to be defined, the Cayley subset S must satisfy $S = S^{-1}$. (We shall call such Cayley subsets *inverse-closed* Cayley subsets.) Thus, we consider the action of $\mathrm{Aut}(G)$ on the inverse-closed Cayley subsets in the case of Cayley graphs.

The strategy for extending his enumeration results is now clear. For every group G which is a CI-group or DCI-group, we examine the action of $\mathrm{Aut}(G)$ on the inverse-closed Cayley subsets or Cayley subsets of G. We want to determine the number of orbits in both cases. We complete the introduction by indicating how Pólya's Enumeration Theorem becomes involved.

For simplicity we discuss Cayley digraphs and make the obvious connection with Cayley graphs at the end. Suppose G is a DCI-group. The group $\mathrm{Aut}(G)$ acts in an obvious way on the Cayley subsets of G. We want to determine the number N of orbits of that action. To do so using Pólya's Theorem we first compute the *cycle index* (defined below) of $\mathrm{Aut}(G)$ acting on $G-1$, where $G-1$ denotes the non-identity elements of G. We can think of each Cayley digraph as being determined by its connection set and, in turn, we can think of the connection set as being defined by its characteristic function. So we can think of the Cayley digraphs as corresponding to functions from $G-1$ to $\{0,1\}$. Pólya's Theorem tells us that the number N equals the cycle index evaluated with each indeterminate set to the cardinality of the range of the functions which, in this case, is 2.

The cycle index of a permutation group G acting on a finite set Ω, denoted $\mathscr{Z}(G,\Omega)$, is defined in the following way. For any $g \in G$, look at the disjoint cycle decomposition of g. Suppose there are $e(i)$ cycles of length i in the decomposition. Then form the monomial

$$z(g) = x_1^{e(1)} x_2^{e(2)} x_3^{e(3)} \cdots$$

which terminates because Ω is finite. The cycle index is then defined by

$$\mathscr{Z}(G,\Omega)=\frac{1}{|G|}\sum_{g\in G}z(g). \tag{1}$$

The following theorem is the tool we use to count the number of non-isomorphic Cayley graphs and digraphs for families of CI-groups and DCI-groups. It is a standard setting for Pólya's Theorem and was used in essence in [19]. There are many similar results in [3].

Theorem 1.6. *If G is a finite DCI-group and Ω denotes the Cayley subsets of G, then the number of non-isomorphic Cayley digraphs on G is obtained by evaluating $\mathscr{Z}(\mathrm{Aut}(G),\Omega)$ with every indeterminate set to 2. Similarly, if G is a finite CI-group and Ω denotes the inverse-closed Cayley subsets of G, then the number of non-isomorphic Cayley graphs on G is obtained by evaluating $\mathscr{Z}(\mathrm{Aut}(G),\Omega)$ with every indeterminate set to 2.*

2. Circulant graphs and digraphs

Turner's result applies to Cayley graphs on cyclic groups of prime order. A natural extension of this is an attempt to remove the restriction on the group having prime order. In fact, Ádám [1] conjectured that every finite cyclic group is a CI-group. It appeared about 4 months earlier than Turner's paper, but the latter apparently did not know about Ádám's conjecture at the time. Ádám's conjecture generated considerable activity. A counterexample to the conjecture came quickly [6], but the final resolution of which cyclic groups are CI-groups was completed only recently by Muzychuk [15].

Theorem 2.1 (Muzychuk [15]). *The cyclic group $\mathbb{Z}_n$ is a CI-group if and only if $n=8, 9, 18$ or $n=2^e m$, where $e\in\{0,1,2\}$ and m is odd and square free.*

His result also includes the digraph case which we state separately for clarity.

Theorem 2.2 (Muzychuk [15]). *The cyclic group $\mathbb{Z}_n$ is a DCI-group if and only if $n=2^e m$, where $e\in\{0,1,2\}$ and m is odd and square free.*

We shall consider the digraph case first. Let $n=p_1p_2\cdots p_t$, where $p_2,p_3,\ldots,p_t$ are distinct odd primes. If n is odd, then p_1 is a distinct odd prime as well. If n is even, then $p_1=2$ or 4. We want to determine the cycle index of $\mathrm{Aut}(\mathbb{Z}_n)$ acting on $\mathbb{Z}_n-0$ (we use 0 for the identity in the case of circulant graphs and digraphs because we think of them as Cayley graphs and digraphs on the additive group $(\mathbb{Z}_n,+)$). This action is simply multiplication by elements of $\mathbb{Z}_n^*$ carried out in $\mathbb{Z}_n$. The most convenient way to look at $\mathrm{Aut}(\mathbb{Z}_n)$ is via the Chinese Remainder Theorem. Using this famous theorem, we have a very nice one-to-one correspondence between the elements of $\mathbb{Z}_n$ and the set $\mathscr{T}$ of t-tuples $\{(x_1,x_2,\dots,x_t): 0 \leqq x_i \leqq p_i - 1, i=1,2,\dots,t\}$. Going from $y \in \mathbb{Z}_n$ to an element of $\mathscr{T}$, we use the residue of y modulo p_i in coordinate i. The Chinese Remainder Theorem tells us the reverse procedure gives us a unique element in $\mathbb{Z}_n$ for each element of $\mathscr{T}$. When n is odd, an element of $\mathscr{T}$ corresponds to an element of $\mathbb{Z}_n^*$ if and only if each coordinate is non-zero. When n is even, the first coordinate must be odd.

Multiplication of two elements of $\mathscr{T}$ is obtained by multiplying coordinate by coordinate. This allows us to determine the cycle structure of the action of an element in $\mathbb{Z}_n^*$ rather easily. Let $\alpha = (a_1,a_2,\dots,a_t) \in \mathbb{Z}_n^*$. The *order-type* of α is the t-tuple $(d_1,d_2,\dots,d_t)$, where d_i is the order of a_i in $\mathbb{Z}_{p_i}^*$. Let $R \subseteq \{1,2,\dots,t\}$. Let $\mathscr{T}_R = \{(x_1,x_2,\dots,x_t) \in \mathscr{T}: x_i \in \mathbb{Z}_{p_i}^*$ if and only if $i \in R\}$. Thus, the elements of $\mathscr{T}_R$ are zero in any coordinate $i \notin R$ corresponding to an odd prime, and when n is even and $1 \notin R$, then the first coordinate is even. When $R=\emptyset$, $\mathscr{T}_R = \{(0,0,\dots,0)\}$ unless $p_1 = 4$ in which case $\mathscr{T}_R = \{(0,0,\dots,0),(2,0,0,\dots,0)\}$.

Note that $|\mathscr{T}_R| = \prod_{i\in R} |\mathbb{Z}_{p_i}^*|$ except when $p_1=4$ and $1 \notin R$. In the latter case, $|\mathscr{T}_R| = 2\prod_{i\in R} |\mathbb{Z}_{p_i}^*|$ because both 0 and 2 will occur in the first coordinate. Multiplication by α fixes $\mathscr{T}_R$ setwise. A typical cycle on $\mathscr{T}_R$ has the form $x, \alpha(x), \alpha^2(x), \dots$ and closes off with length equal to the order of α restricted to the coordinates corresponding to R. The latter order is nothing more than the least common multiple of the orders in the order-type of α restricted to the same set of coordinates. This observation allows us a straightforward generalization of Turner's Theorem in that we can sum over all the possible order-types. The number of elements of $\mathbb{Z}_n^*$ with order-type $(d_1,d_2,\dots,d_t)$ is $\prod_{i=1}^t \phi(p_i)$, where ϕ denotes the Euler totient function. This completes the proof of the following theorem.

Theorem 2.3. *Let* $n = p_1 p_2 \cdots p_t$, *where either* $p_1,p_2,\dots,p_t$ *are distinct primes, or* $p_1=4$ *and* $p_2,p_3,\dots,p_t$ *are distinct odd primes. The cycle index* $\mathscr{Z}(\mathrm{Aut}(\mathbb{Z}_n), \mathbb{Z}_n - 0)$ *is given by*

$$\frac{1}{\phi(n)} \sum_{(d_1,d_2,\dots,d_t)} \phi(d_1)\phi(d_2)\cdots\phi(d_t) \prod_R x_{\mathrm{lcm}(R)}^{|\mathscr{T}_R|/\mathrm{lcm}(R)}, \tag{2}$$

where the sum is taken over all possible order types of $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$, *the product is taken over all non-empty subsets* R *of* $\{1,2,\dots,t\}$ *unless* $p_1=4$ *in which case* $R=\emptyset$ *is included and* $\mathscr{T}_\emptyset = \{(2,0,0,\dots,0)\}$, *and* $\mathrm{lcm}(R)$ *denotes the least common multiple of the* d_i *terms in the coordinates corresponding to the elements of* R.

Example 2.4. Consider the case of $n = 20 = 4\times 5$. The possible order-types are (1,1), (1,2), (1,4), (2,1), (2,2) and (2,4). For example, there are two automorphisms of order-type (1,4). Since $p_1=4$, the term corresponding to $R=\emptyset$ appears in the product, but this element, which is $(2,0) = 10 \in \mathbb{Z}_{20}$, is fixed by every automorphism thereby contributing x_1 to the product. The action on the terms corresponding to $R=\{1\}$ is the identity contributing x_1^2. The action on the terms corresponding to $R=\{2\}$ has order 4. This contributes x_4^2. Similarly, the action on the terms corresponding to $R=\{1,2\}$

contributes x_4^2. So the monomial we obtain for an automorphism of order type (1,4) is $x_1^3x_4^4$. Doing this over all possible order types yields a cycle index of

$$\tfrac{1}{8}\,(x_1^{19}+x_1^3x_2^8+2x_1^3x_4^4+x_1^9x_2^5+x_1x_2^9+2x_1x_2x_4^4).$$

Substitution of 2 for each variable gives 68,016 non-isomorphic circulant digraphs of order 20.

We now move to the undirected case. Some additional work is required because of the fact that Cayley graphs require the connection sets to be inverse-closed. In other words, if we choose to put y in the connection set, then we must also include $-y$. Thus, instead of considering the action of $\mathrm{Aut}(\mathbb{Z}_n)$ on $\mathbb{Z}_n-0$, we consider the action on the set of pairs $\{y,-y\}$ chosen from $\mathbb{Z}_n-0$. We shall call them the set of *inverse pairs*. In the digraph case we could have calculated the cycle index using the product formula [9,17] and the cycle indices for $Z(\mathrm{Aut}(\mathbb{Z}_{p_i}),\mathbb{Z}_{p_i})$. However, because of the inverse pairs, it is not a suitable approach in the undirected case.

There are three exceptional values in Theorem 2.1 and we handle them separately. These values are $n=8,9$ and 18. The cycle index of $\mathrm{Aut}(\mathbb{Z}_8)$ acting on the inverse pairs for $\mathbb{Z}_8-0$ is $\frac{1}{2}(x_1^4+x_1^2x_2)$, the cycle index of $\mathrm{Aut}(\mathbb{Z}_9)$ acting on the inverse pairs for $\mathbb{Z}_9-0$ is $\frac{1}{3}(x_1^4+2x_1x_3)$, and the cycle index of $\mathrm{Aut}(\mathbb{Z}_{18})$ acting on the inverse pairs for $\mathbb{Z}_{18}-0$ is $\frac{1}{3}(x_1^9+2x_1^3x_3^2)$.

For the remaining appropriate values of n, we have already described the action of $\mathrm{Aut}(\mathbb{Z}_n)$ on $\mathbb{Z}_n-0$. We translate this into the action on the inverse pairs by essentially identifying y and $-y$. There are two possibilities. If y and $-y$ lie in the same cycle, then the cycle must have length $2m$ for some m, and $\alpha^m(y)=-y$ must hold. Therefore, this cycle collapses to a single cycle of length m for the corresponding action on inverse pairs. If y and $-y$ lie in different cycles, then the two cycles have the same length m and the entries of one cycle are simply the negatives of the entries of the other cycle. Hence, these two cycles of length m collapse to a single cycle of length m for the corresponding action on inverse pairs.

As above let $\alpha=(a_1,a_2,\dots,a_t)\in\mathbb{Z}_n^*$. How can we recognize when y and $-y$ lie in the same cycle of the action of α on $\mathbb{Z}_n-0$? Suppose $y\in\mathscr{T}_R$ for some $R\subseteq\{1,2,\dots,t\}$, that is, $y=(y_1,y_2,\dots,y_t)$, where $y_i\in\mathbb{Z}_{p_i}^*$ if and only if $i\in R$. Then $\alpha(y)=(a_1y_1,a_2y_2,\dots,a_ty_t)$ and so on for $\alpha^2(y),\alpha^3(y),\dots$. Thus, if $\alpha^m(y)=-y$ for some positive integer m, where m is the smallest such positive integer, then $a_i^m=-1$ for each $i\in R$. This implies that d_i, the order of $a_i\in\mathbb{Z}_{p_i}$, is even. Further, if $d_i=2^eb$, where b is odd, then m must be an odd multiple of $2^{e-1}b$. But this must hold for each $i\in R$ so that every d_i, $i\in R$, has 2^e as the largest power of 2 which divides d_i. Therefore, for $y\in\mathscr{T}_R$, y and $-y$ lie in the same cycle of the action of $\alpha=(a_1,a_2,\dots,a_t)$ on $\mathbb{Z}_n-0$ precisely when the orders of all $a_i, i\in R$, are even and the same power of 2 times an odd number.

The preceding discussion allows us to give the undirected analog of Theorem 2.3 as soon as we introduce some new notation in the next definition.

Definition 2.5. Let $(d_1, d_2, \ldots, d_t)$ be the order type of some $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$, and let $R \subseteq \{1, 2, \ldots, t\}$. If each d_i, $i \in R$, has the form $d_i = 2^e b$, where $e \geqq 1$ and b is odd, then let $\mathrm{lcm}^*(R) = \mathrm{lcm}(R)/2$. In all other cases, let $\mathrm{lcm}^*(R) = \mathrm{lcm}(R)$.

Theorem 2.6. *Let* $n = p_1 p_2 \cdots p_t$, *where either* $p_1, p_2, \ldots, p_t$ *are distinct primes, or* $p_1 = 4$ *and* $p_2, p_3, \ldots, p_t$ *are distinct odd primes, and let* Ω *denote the set of inverse pairs of* $\mathbb{Z}_n - 0$. *The cycle index* $\mathscr{Z}(\mathrm{Aut}(\mathbb{Z}_n), \Omega)$ *is given by*

$$\frac{1}{\phi(n)} \sum_{(d_1, d_2, \ldots, d_t)} \phi(d_1)\phi(d_2)\cdots\phi(d_t) \prod_R x_{\mathrm{lcm}^*(R)}^{|\mathscr{T}_R|/2\mathrm{lcm}^*(R)}, \tag{3}$$

where the sum is taken over all possible order types of $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$, *and the product is taken over all non-empty subsets* R *of* $\{1, 2, \ldots, t\}$ *unless* $p_1 = 4$ *in which case* $R = \emptyset$ *is included and* $|\mathscr{T}_\emptyset|$ *is taken to be* 2.

We complete this section with an example of the preceding theorem. We again use $n = 20$.

Example 2.7. Consider the case of $n = 20 = 4 \times 5$. The possible order-types are (1,1), (1,2), (1,4), (2,1), (2,2) and (2,4). For example, there are two automorphisms of order-type (1,4). Since $p_1 = 4$, the term corresponding to $R = \emptyset$ appears in the product, and the contribution is x_1 since we consider $\mathrm{lcm}^*(\emptyset) = 1$ and $|\mathscr{T}_\emptyset| = 2$. For $R = \{1\}$, we have $\mathrm{lcm}^*(R) = 1$ and $|\mathscr{T}_R| = 2$. This gives us a contribution of x_1. For $R = \{2\}$, we have $\mathrm{lcm}^*(R) = 2$ and $|\mathscr{T}_R| = 8$. This contributes x_2^2. Finally, when $R = \{1, 2\}$, we have $\mathrm{lcm}^*(R) = 4$ and $|\mathscr{T}_R| = 8$. The contribution is x_4. So the monomial we obtain for an automorphism of order type (1,4) is $x_1^2 x_2^2 x_4$. Doing this over all possible order types yields a cycle index of

$$\tfrac{1}{4}(x_1^{10} + x_1^6 x_2^2 + 2x_1^2 x_2^2 x_4).$$

Substitution of 2 for each variable gives 336 non-isomorphic circulant graphs of order 20.

3. Unit circulant graphs and digraphs

Even though the group $\mathbb{Z}_n$ is neither a CI-group nor a DCI-group in general, there is a subclass of the circulant graphs and digraphs which is nicely behaved in this regard for all n.

Definition 3.1. If $S \subseteq \mathbb{Z}_n^*$, then the circulant digraph $\vec{X}(n, S)$ is called a unit *circulant digraph*. Similarly, if $S \subseteq \mathbb{Z}_n^*$ is inverse-closed, then the circulant graph $X(n, S)$ is called a unit *circulant graph*.

Toida [18] conjectured that every unit circulant graph is a CI-graph. The conjecture has been proved recently by Klin et al. [10] and independently by Dobson and

Morris [5]. The proof includes the directed case as well so we include that in the following statement.

Theorem 3.2. *Unit circulant digraphs and unit circulant graphs are DCI-digraphs and CI-graphs, respectively.*

The preceding theorem allows us to enumerate the unit circulant graphs and digraphs of order n. The notation is the same as that used in Section 2. We examine the directed case first. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, where $p_1, p_2, \ldots, p_t$ are distinct primes and $e_i \geqq 1$ for $i = 1, 2, \ldots, t$. Every automorphism of $(\mathbb{Z}_n, +)$ arises from multiplication by an element α of $\mathbb{Z}_n^*$. We can write $\alpha = (a_1, a_2, \ldots, a_t)$, where $a_i \in \mathbb{Z}_{p_i^{e_i}}$ for $i = 1, 2, \ldots, t$. Of course, multiplication of a unit in $\mathbb{Z}_n$ by a unit produces a unit so that $\mathbb{Z}_n^*$ is fixed setwise by α. We want the cycle index of $\mathrm{Aut}(\mathbb{Z}_n)$ acting on $\mathbb{Z}_n^*$. The situation is the same as for the proof of Theorem 2.3 with $R = \{1, 2, \ldots, t\}$ because $\mathscr{T}_R = \mathbb{Z}_n^*$ in this case. The next result now follows from the proof of Theorem 2.3.

Theorem 3.3. *The cycle index* $\mathscr{Z}(\mathrm{Aut}(\mathbb{Z}_n), \mathbb{Z}_n^*)$ *is given by*

$$\frac{1}{\phi(n)} \sum_{(d_1, d_2, \ldots, d_t)} \phi(d_1)\phi(d_2)\cdots\phi(d_t) x_{\mathrm{lcm}(d_1, d_2, \ldots, d_t)}^{\phi(n)/\mathrm{lcm}(d_1, d_2, \ldots, d_t)}, \tag{4}$$

where the sum is over all order-types of elements in $\mathrm{Aut}(\mathbb{Z}_n)$.

Example 3.4. We shall enumerate the unit circulant digraphs of order 20. The value of $\phi(20)$ is 8. As in the previous examples, the order-types are (1,1), (1,2), (1,4), (2,1), (2,2), (2,4). There are two elements with order-type (2,4), and $\mathrm{lcm}(2,4) = 4$ so that the contribution to the cycle index is $2x_4^2$. Performing a similar calculation over all order-types gives a cycle index of

$$\tfrac{1}{8}(x_1^8 + 3x_2^4 + 4x_4^2).$$

Substitution of 2 for all the variables gives 40 unit circulant digraphs of order 20.

When we move to unit circulant graphs, the same considerations come into play as for the move from circulant digraphs to circulant graphs in the preceding section. The proof of the following theorem is immediate from the discussions above.

Theorem 3.5. *If* Ω *denotes the inverse pairs of* $\mathbb{Z}_n$, *then* $\mathscr{Z}(\mathrm{Aut}(\mathbb{Z}_n), \Omega)$ *is given by*

$$\frac{1}{\phi(n)} \sum_{(d_1, d_2, \ldots, d_t)} \phi(d_1)\phi(d_2)\cdots\phi(d_t) x_{\mathrm{lcm}^*(d_1, d_2, \ldots, d_t)}^{\phi(n)/2\mathrm{lcm}^*(d_1, d_2, \ldots, d_t)}, \tag{5}$$

where the sum is over all order-types of elements in $\mathrm{Aut}(\mathbb{Z}_n)$.

Example 3.6. Returning to the same example of $n = 20$, we get a cycle index of

$$\tfrac{1}{4}(x_1^4 + x_2^2 + 2x_4)$$

for $\mathrm{Aut}(\mathbb{Z}_{20})$ acting on the inverse pairs of $\mathbb{Z}_{20}^*$. This gives 6 unit circulant graphs of order 20.

4. Elementary abelian groups

Another family of abelian groups which has garnered some attention for these isomorphism questions is the family of elementary abelian groups. We use $\mathbb{Z}_p^t$, p a prime, to denote the direct product of $\mathbb{Z}_p$ with itself t times. Of course, Turner's original paper proved that $\mathbb{Z}_p$ is a CI-group. Babai and Frankl [2] asked whether or not all groups of the form $\mathbb{Z}_p^t$ are CI-groups. Godsil [8] proved that $\mathbb{Z}_p^2$ is a CI-group. The first published proof that $\mathbb{Z}_p^3$ is a CI-group was by Dobson [4]. Morris [14] has proved that $\mathbb{Z}_p^4$ is a CI-group. However, Nowitz [16] has proved that $\mathbb{Z}_2^6$ is not a CI-group so that not all elementary abelian groups are CI-groups.

The preceding results allow the Cayley digraphs and Cayley graphs on the groups $\mathbb{Z}_p^t$, $t \in \{2,3,4\}$, to be enumerated using the same method employed earlier. To do so requires the cycle indices of $\mathrm{Aut}(\mathbb{Z}_p^t,+)$ acting on $\mathbb{Z}_p^t - 0$ and the inverse pairs of $\mathbb{Z}_p^t - 0$, respectively. Now $\mathrm{Aut}(\mathbb{Z}_p^t,+)$ is the general linear group $\mathrm{GL}(t,p)$ of invertible $t \times t$ matrices over $\mathbb{Z}_p$.

Viewing $(\mathbb{Z}_p^t,+)$ as a t-dimensional vector space over $\mathbb{Z}_p$, an element of $\mathrm{GL}(t,p)$ acts as a permutation of $(\mathbb{Z}_p^t,+)$ fixing the 0-vector. Hence, it makes sense to view an element of $\mathrm{GL}(t,p)$ as a permutation on $\mathbb{Z}_p^t - 0$. Since conjugate elements (group conjugacy) of $\mathrm{GL}(t,p)$ have the same cycle structure as permutations, one should use convenient representatives of the conjugacy classes. This is the approach taken by Fripertinger [7], using some results of Kung [11], to obtain a general expression for the cycle index of $\mathrm{GL}(t,q)$, q a prime power, acting on several sets. For the particular cases in which we are interested, it is easier to go ahead and work directly with convenient representatives of the conjugacy classes. Following is a detailed examination of the case $t = 2$. Similar considerations work for $t = 3$ and 4, but we omit the details because of space considerations. The following table contains information about the conjugacy classes for $\mathrm{GL}(2,p)$.

The conjugacy classes corresponding to linear minimal polynomials correspond to the elements of the center of $\mathrm{GL}(2,p)$. Thus, each such conjugacy class is a singleton and the matrix is a scalar multiple of the identity matrix. If the scalar multiple is aI, then it is clear that the action of aI on $\mathbb{Z}_p^2 - 0$ as a permutation is a product of $(p^2-1)/|a|$ cycles of length $|a|$, where $|a|$ denotes the order of a in $\mathbb{Z}_p^*$.

The action of aI on the inverse pairs of $\mathbb{Z}_p^2 - 0$ is a little more complicated. If $|a|$ is odd, then (x,y) and $(-x,-y)$ are in different cycles for the action on $\mathbb{Z}_p^2 - 0$. Thus, for the action on the inverse pairs, two cycles of length $|a|$ collapse to a single cycle of length $|a|$. Hence, we obtain $(p^2-1)/2|a|$ cycles of length $|a|$. On the other hand, if $|a|$ is even, then (x,y) and $(-x,-y)$ are in the same cycle for the action on $\mathbb{Z}_p^2 - 0$.

Hence, this single cycle collapses to a single cycle with length $|a|/2$ for the action on the inverse pairs of $\mathbb{Z}_p^2 - 0$.

GL(2, p)

Minimal polynomial	Representative	Number of classes	Elements in a class
$x-a$	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$p-1$	1
$(x-a)^2$	$\begin{pmatrix} a & 0 \\ 1 & a \end{pmatrix}$	$p-1$	p^2-1
$(x-a)(x-b)$	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$	$\begin{pmatrix} p-1 \\ 2 \end{pmatrix}$	p^2+p
x^2+ax+b	$\begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix}$	$\frac{p^2-p}{2}$	p^2-p

There are $p-1$ conjugacy classes corresponding to minimal polynomials of the form $(x-a)^2$, and each class contains p^2-1 elements. Let A_1 denote the representative shown in the table above. The action of A_1 on any pair of the form $(0,y)$ generates a cycle of length $|a|$. Thus, we get $(p-1)/|a|$ cycles of length $|a|$. The action on a pair of the form $(x,0)$ is a little more complicated. The first coordinate runs through the sequence $x, ax, a^2x, \ldots, a^{|a|-1}x, x, \ldots$ so that x is repeated at every multiple of $|a|$. The second coordinate runs through $0, x, 2ax, 3a^2x, \ldots, (p-1)a^{p-2}x, 0, \ldots$ so that 0 is repeated at every multiple of p. Since $|a|$ and p are relatively prime, and $(x,0), (ax,0), (a^2x,0), \ldots, (a^{|a|-1}x,0)$ lie in the same cycle, we obtain $(p-1)/|a|$ cycles of length $p|a|$. The total number of elements lying in both types of cycles is p^2-1 so everything is accounted for in the action of A on $\mathbb{Z}_p^2 - 0$.

The action of A_1 on the inverse pairs of $\mathbb{Z}_p^2$ depends on $|a|$. If $|a|$ is odd, then $(0,y)$ and $(0,-y)$ lie in different cycles so that we get $(p-1)/2|a|$ cycles of length $|a|$ on the inverse pairs with 0 in the first coordinate. Similarly, when $|a|$ is odd, we have $(p-1)/2|a|$ cycles of length $p|a|$ on the remaining inverse pairs. When $|a|$ is even, we have $(p-1)/|a|$ cycles of length $|a|/2$ on inverse pairs with 0 in the first coordinate, and $(p-1)/|a|$ cycles of length $p|a|/2$ on the remaining inverse pairs.

If the minimal polynomial has the form $(x-a)(x-b)$, where $a \neq b$, then there are $\binom{p-1}{2}$ conjugacy classes each of which has p^2+p elements. The representative we use is a diagonal matrix A_2 making the cycle decomposition easy to analyze. We get $(p-1)/|a|$ cycles of length $|a|$ from the action of A_2 on pairs of the form $(x,0)$. Similarly, the action of A_2 on pairs of the form $(0,y)$ produces $(p-1)/|b|$ cycles of length $|b|$. Finally, the action on the remaining pairs produces $(p-1)^2/\mathrm{lcm}(|a|,|b|)$ cycles of length $\mathrm{lcm}(|a|,|b|)$.

For the action of A_2 of inverse pairs, recall the definition of lcm^* in Definition 2.5. If $|a|$ is odd, then we get $(p-1)/2|a|$ cycles of length $|a|$ on inverse pairs with second coordinate 0. If $|a|$ is even, then we get $(p-1)/|a|$ cycles of length $|a|/2$ on inverse pairs with second coordinate 0. Similar statements hold for inverse pairs with first coordinate

0 with respect to $|b|$. On the remaining pairs, we get $(p-1)^2/2\mathrm{lcm}^*(|a|,|b|)$ cycles of length $\mathrm{lcm}^*(|a|,|b|)$.

The remaining type of representative corresponds to a minimal polynomial of the form x^2+ax+b which is irreducible over $\mathbb{Z}_p$. There are $(p^2-p)/2$ conjugacy classes [7] each of which has p^2-p elements. Let the matrix representative be denoted A_3. The *order* of A_3 is the smallest d such that $A_3^d=I$. It is known [12] that A_3 is a product of $(p^2-1)/d$ cycles of length d in its action on $\mathbb{Z}_p^2-0$. This means we need information on the orders of the matrices in conjugacy classes corresponding to irreducible polynomials of degree 2 over $\mathbb{Z}_p$. It is known [12] that the order d divides p^2-1, and for all divisors d of p^2-1 satisfying $p\not\equiv 1 \pmod d$, the number of conjugacy classes whose matrices have order d is $\phi(d)/2$. We now have all the information we need to get the cycle index of $\mathrm{GL}(2,p)$ acting on $\mathbb{Z}_p^2-0$. Doing the appropriate arithmetic produces the following theorem.

Theorem 4.1. *The cycle index* $\mathscr{Z}(\mathrm{GL}(2,p),\mathbb{Z}_p^2-0)$ *is*

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

$$+\frac{1}{(p^2-p)}\sum_{d|(p-1)}\phi(d)x_d^{(p-1)/d}x_{pd}^{(p-1)/d}$$

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

$$+\frac{1}{(p-1)^2}\sum_{\substack{d,e|(p-1)\\ e>d}}\phi(d)\phi(e)x_d^{(p-1)/d}x_e^{(p-1)/e}x_{\mathrm{lcm}(d,e)}^{(p-1)^2/\mathrm{lcm}(d,e)}$$

$$+\frac{1}{2(p^2-1)}\sum_{\substack{d|(p^2-1)\\ p\not\equiv 1 \,(\mathrm{mod}\, d)\\ d\neq 1}}\phi(d)x_d^{(p^2-1)/d}.$$

Note that there is one more summand appearing in Theorem 4.1 than the number of types of representatives under discussion. This is accounted for by breaking the conjugacy classes for minimal polynomials of the form $(x-a)(x-b)$ into those for which a and b have the same order—the third summand—and those for which a and b have different orders—the fourth summand. We do the same in the statement of Theorem 4.2.

All we are missing in order to get the cycle index of $\mathrm{GL}(2,p)$ acting on the inverse pairs of $\mathbb{Z}_p^2-0$ is what happens for A_3. If the latter matrix has even order d in its action on $\mathbb{Z}_p^2-0$, then x and $-x$ are in the same cycle [13, Lemma 5.16] so that we now get $(p^2-1)/d$ cycles of length $d/2$. Otherwise, x and $-x$ are in different cycles and we get $(p^2-1)/2d$ cycles of length d.

For purposes of stating the following theorem, it is convenient to use the following notation:

$$h(d)=\begin{cases} d & d \text{ is odd,}\\ \frac{d}{2} & \text{otherwise.}\end{cases}$$

Theorem 4.2. *If Ω denotes the inverse pairs of $\mathbb{Z}_p^2-0$, then the cycle index $\mathscr{Z}(\mathrm{GL}(2,p),\Omega)$ is given by*

$$\frac{1}{(p^2-1)(p^2-p)}\sum_{d\mid(p-1)}\phi(d)x_{h(d)}^{(p^2-1)/2h(d)}$$

$$+\frac{1}{(p^2-p)}\sum_{d\mid(p-1)}\phi(d)x_{h(d)}^{(p-1)/2h(d)}x_{ph(d)}^{(p-1)/2h(d)}$$

$$+\frac{1}{2(p-1)^2}\sum_{d\mid(p-1)}\phi(d)(\phi(d)-1)x_{h(d)}^{(p^2-1)/h(d)}$$

$$+\frac{1}{(p-1)^2}\sum_{\substack{d,e\mid(p-1)\\ e>d}}\phi(d)\phi(e)x_{h(d)}^{(p-1)/2h(d)}x_{h(e)}^{(p-1)/2h(e)}x_{\mathrm{lcm}^*(d,e)}^{(p-1)^2/2\mathrm{lcm}^*(d,e)}$$

$$+\frac{1}{2(p^2-1)}\sum_{\substack{d\mid(p^2-1)\\ p\not\equiv 1(\mathrm{mod}\, d)\\ d\neq 1}}\phi(d)x_{h(d)}^{(p^2-1)/2h(d)}.$$

Example 4.3. The cycle index of GL(2,3) acting on the inverse pairs of $\mathbb{Z}_3^2$ is

$$\tfrac{1}{48}(2x_1^4+12x_1^2x_2+16x_1x_3+6x_2^2+12x_4).$$

Hence, there are five non-isomorphic Cayley graphs on $\mathbb{Z}_3^2$.

References

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

[2] L. Babai, P. Frankl, Isomorphisms of Cayley graphs I, in: Colloquia Mathematica Societatis Janos Bolyai, Vol. 18, Combinatorics, Keszthely, 1976, North-Holland, Amsterdam, 1978, pp. 35–52.

[3] N.G. de Bruijn, Pólya's theory of counting, in: Applied Combinatorial Mathematics, Wiley, New York, 1964 (Chapter 5).

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

[5] E. Dobson, J. Morris, Toida's conjecture is true, Elec. J. Combin., submitted for publication.

[6] B. Elspas, J. Turner, Graphs with circulant adjacency matrices, J. Combin. Theory 9 (1970) 297–307.

[7] H. Fripertinger, Cycle indices of linear, affine and projective groups, Linear Algebra Appl. 263 (1997) 133–156.

[8] C.D. Godsil, On Cayley graph isomorphisms, Ars Combin. 15 (1983) 231–246.

[9] M.A. Harrison, R.G. High, On the cycle index of a product of permutation groups, J. Combin. Theory, 4 (1968) 277–299.

[10] M. Muzychuk, M. Klin, R. Pöschel, The isomorphism problem for circulant graphs via Schur ring theory, in: Codes and Association Schemes, DIMACS, Am. Math. Soc., Providence, RI, pp. 241–264.
[11] J.P.S. Kung, The cycle structure of a linear transformation over a finite field, Linear Algebra Appl. 36 (1981) 141–155.
[12] R. Lidl, H. Niederreiter, Finite Fields, Addison-Wesley, London, 1983.
[13] M. Mishna, Cayley graph enumeration, M.Sc. Thesis, Simon Fraser University, March, 2000.
[14] J. Morris, Isomorphisms of Cayley graphs, Ph.D. Thesis, Simon Fraser University, November, 1999.
[15] M. Muzychuk, On Ádám's conjecture for circulant graphs, Discrete Math. 167/168 (1997) 497–510.
[16] L. Nowitz, A non-Cayley-invariant Cayley graph of the elementary Abelian group of order 64, Discrete Math. 110 (1992) 223–228.
[17] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chermische Verbindungen, Acta Mathematica 68 (1937) 145–254.
[18] S. Toida, A note on Ádám's conjecture, J. Combin. Theory Ser. B 23 (1977) 239–246.
[19] J. Turner, Point-symmetric graphs with a prime number of points, J. Combin. Theory 3 (1967) 136–145.