Séminaire Lotharingien de Combinatoire B36d (36pp.)

Analytical Enumeration of Circulant Graphs with Prime-Squared Number of Vertices*

Mikhail Klin,
Department of Mathematics & Computer Science
Ben-Gurion University of the Negev
84105 Beer-Sheva, Israel
klin@indigo.cs.bgu.ac.il

Valery Liskovets and **Reinhard Pöschel**
Institut für Algebra
Technische Universität Dresden
D-01062 Dresden, Germany
[liskov, poeschel]@math.tu-dresden.de

31.7.96

Abstract

A method for the analytical enumeration of circulant graphs with p^2 vertices, p a prime, is proposed and described in detail. It is based on the use of S-rings and Pólya's enumeration technique. Two different approaches, "structural" and "multiplier", are developed and compared. As a result we get counting formulae and generating functions (by valency) for non-isomorphic p^2-vertex directed and undirected circulant graphs as well as for some natural subclasses of them such as tournaments and self-complementary graphs. These are the first general enumerative results for circulant graphs for which the so-called Ádám (single-multiplier) isomorphism condition does not hold. Some numerical data and interrelations between formulae are also obtained. The first expository part of the paper may serve as a self-contained introduction to the use of Schur rings for enumeration.

1 Introduction

1.1. Circulant (cyclic) graphs, or, briefly, circulants, are Cayley graphs over a cyclic group, that is graphs which are invariant with respect to the action of a regular cyclic group on the vertices. During recent years, interest to circulant graphs has been growing dramatically, in particular, due to their applications in theoretical computer science, extremal graph theory, design of experiments, etc. In this paper we are interested in the enumeration of circulants.

Following I. A. Faradžev (cf. [Far78]) we distinguish two modes of exact enumeration: constructive and analytical. *Constructive enumeration* means getting a transversal of the set of isomorphism classes of combinatorial objects under consideration. *Analytical enumeration* is nowadays a rather traditional part of mathematics, see, e.g. [HarP73]. Of course, analytical enumeration might be viewed as an easy consequence of constructive enumeration. Usually, however, the two approaches are rather independent and supplement each other. The most "respectable" methods of analytical enumeration are based on the use of generating functions,

*This research was supported by the Grant No. I-0333-263.06/93 from the G.I.F., the German-Israeli Foundation for Scientific Research and Development.

aimed at getting (whenever possible) "closed" counting formulae and they are preferably oriented on infinite classes of graphs (e.g. parametrized by the number of vertices). On the contrary, the most significant results of constructive enumeration are achieved with the aid of computers based on the exhaustion of only a finite number of objects.

It is worthwhile to stress that enumerative combinatorics is one of the oldest and in some sense classical parts of combinatorics. Enumeration of elementary combinatorial objects such as permutations, combinations, arrangements, etc. is now commonly regarded as an obligatory part of mathematical education already at the sophomore-junior level, see, e.g. [Gri94]. Wider frames of modern enumerative combinatorics can be traced out, e.g. from [Sta86]. Here, however, we restricted ourselves only to the enumeration of such combinatorial objects as graphs, both directed and undirected.

1.2. If some combinatorial objects are natural and interesting for study, their enumeration is also a natural and interesting task for a better understanding of their intrinsic essence and how to master them. This is just the case for circulants. Numerous papers devoted to the analytical enumeration of circulants have been published over the last three decades. In the references, the reader will find a sufficiently representative (though not exhaustive) list of publications.

Practically all published papers rely on the use of the (one-multiplier) equivalence of circulant graphs: two circulant graphs Γ_1 and Γ_2 are called equivalent if there exists an automorphism of the cyclic group $\mathbb{Z}_n$ which transforms Γ_1 to Γ_2 ($\mathbb{Z}_n$ serves as the set of vertices for both graphs). Equivalent circulant graphs are certainly isomorphic. It was A. Ádám who conjectured (see [Ádá67]) that the converse claim is also valid. In spite of numerous counter-examples, Ádám's conjecture played a very stimulating role in the investigation of circulants, in particular stressing the essential features of that language which is convenient for describing isomorphism conditions of circulant graphs.

1.3. Our approach to the enumeration of circulants is based on necessary and sufficient conditions for two circulant graphs to be isomorphic. Such conditions were developed in the framework of S-ring theory.

The notion of S-ring goes back to a classical paper of I. Schur [Sch33]. Explicitly, this notion was pointed out by H. Wielandt. During several decades S-rings were regarded as a rather sophisticated tool for purely group-theoretical purposes, known and used only by a very restricted number of experts. However, starting with the paper [KliP78], promising applications of S-rings in combinatorics were elaborated. Nowadays S-rings have been recognized as an important part of Algebraic Combinatorics. One of the prominent results on circulant graphs – the description of all values n for which Adám's conjecture is true – has been recently obtained by M. Muzychuk on the base of S-ring theory, see [Muz95] and [Muz9x]. However, a wider use of S-rings in graph theory and enumerative combinatorics is still restricted by the absence of friendly introductional papers on this subject.

1.4. One more general methodological background of our paper is the approach to the enumeration of combinatorial objects ("patterns") with a prescribed automorphism group which is based on the use of the so-called Burnside marks. This approach was used, evidently for the first time, in [Kli70]. Its modern frames were outlined in [FarKM94], see also [Ker91]. Here we use this approach in a very simplified manner due to special features of the lattice of automorphism groups of circulant graphs.

1.5. Our paper may be considered as a part of new activities in the theory of circulant graphs, cf. [KliMW9x], [KliP9x] and [LisP9x]. Our goal in this series of papers is to deliver a unified approach to the investigation of symmetry properties of circulant graphs based on a systematically developed S-ring theory.

In particular, the present paper is designed as a self-contained introduction to the analytical enumeration of circulants. This is why the reader will find in the text a rather detailed account of the whole terminology and a large number of concrete examples and methodological explanations which follow each step in our exposition.

1.6. The paper consists of eight sections. In *Section* 2 we deliver a brief glossary of all necessary notions related to permutation groups, circulant graphs, Ádám's conjecture, S-rings, etc.

Sections 3 and 4 play the role of an expository part of the presentation. In *Section* 3 we describe the "structural" approach to the enumeration of n-vertex circulant graphs which is based on the knowledge of the lattice of all S-rings over the cyclic group $\mathbb{Z}_n$.

On the basis of this approach we describe in *Section* 4:

- the main features of the enumeration procedure of p-vertex circulant graphs, p a prime;
- a brief outline of the enumeration of p^2-vertex circulants;
- the main ideas of an alternative multiplier approach to the enumeration of circulant graphs.

Roughly speaking, the structural approach allows one to find the number of circulants with every possible automorphism group and, thus, requires rather redundant structural information about S-rings and permutation groups. The multiplier approach is based exclusively on the direct use of the isomorphism criterion, while the information about S-rings is in the end ignored.

The constructive enumeration of circulants is also briefly discussed in Section 4.

New results related to the enumeration of p^2-vertex circulant graphs are presented in Sections 5–7: this part is written on a more rigorous level assuming a knowledge of common enumerative methods (generating functions, Pólya's theorem, etc.). In *Section* 5 we deliver all necessary information about cycle indices. *Section* 6 deals with the Pólya enumeration technique applied to circulant graphs in the framework of S-rings. Our main results about the count of p^2-vertex circulants are formulated and proved in *Section* 7. Here we count, simultaneously and uniformly, circulants of several natural subclasses such as tournaments and self-complementary graphs. From the formulae obtained we derive some interesting interrelations between the numbers of circulants of various types.

Finally, in *Section* 8 we discuss further possibilities for the new enumerative methodology presented in the current paper. Generalizations of our methods and wider applications are postponed to subsequent publications. Our first goal will be the enumeration of p^m-vertex circulants, p a prime, $m \geq 3$.

2 Basic definitions and preliminary results

2.1. Groups and group actions. As usual, $\mathbb{Z}$ stands for the ring of integers. Let n be a positive integer, $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$ and $\mathbb{Z}'_n := \mathbb{Z}_n \setminus \{0\}$. We denote by $\mathbb{Z}^*_n$ the set of numbers in $\mathbb{Z}_n$ relatively prime to n, so that $|\mathbb{Z}^*_n| = \phi(n)$ where $\phi(n)$ is the Euler totient function.

In the sequel, all arithmetic operations are regarded *modulo* n unless otherwise stated. It is often convenient to represent a residue class modulo n by an appropriate member, not necessarily the least one. Elements of $\mathbb{Z}_n$ are also meant as the corresponding residue classes rather than simply integers.

$\mathbb{Z}_n$ forms a ring with respect to addition and multiplication. In particular, $\mathbb{Z}_n$ is an *additive cyclic* group of order n and $\mathbb{Z}_n^*$ is a *multiplicative* abelian group, which is referred to as the *prime residue class group* (modulo n).

Given a group G and an action of it on a set U, we denote this as (G, U) where the action, i.e. the corresponding homomorphism from G to the *symmetric group* $S(U)$ is implicit. (G, U) is a permutation group if and only if this action is faithful. Sometimes, in order to emphasize the difference between G as an abstract group and as a group with an action, we denote the former as $\mathbf{G}$ and the latter as $G = (\mathbf{G}, U)$. Usually, however, when the sense is clear from the context and no ambiguity arises, we shall not make a difference in the designations.

$Z(n)$ denotes a *regular cyclic* permutation group of order (and degree) n, i.e. generated by an n-cycle. Usually we take $(0, 1, 2, \dots, n-1)$ as such a cycle. Up to similarity of permutation groups, this is the regular presentation of $\mathbb{Z}_n$, i.e. $Z(n) \cong (\mathbb{Z}_n, \mathbb{Z}_n)$.

$D(n)$ denotes the transitive *dihedral* permutation group of degree n and order $2n$.

The action of $g \in G$ on $u \in U$ will be denoted as u^g.

(G, U) is called *semi-regular* if no non-identity element of G fixes an element of U.

2.2. Cycle index. The polynomial of degree $n = |U|$

$$I_G = I_{(G,U)} = I_G(\mathbf{x}) = I_G(n; x_1, x_2, \dots, x_n) := \frac{1}{|G|} \sum_{g \in G} \prod_{i \geq 1} x_i^{a_i(g)}$$

in the variables $x_1, x_2, \dots, x_n$ denotes the *cycle index* of a group $G = (\mathbf{G}, U)$ with an action on a finite set U where $a_i(g) = a_i(g, U)$ stands for the number of disjoint cycles of length i in g. This is one of the main enumerative tools.

2.3. Direct sum and join of groups. Given two groups G and H acting on disjoint sets U and V, we define their *direct sum* $G \oplus H$ acting on the (disjoint) union $U \dot\cup V$. As an abstract group, it is the direct product $G \times H$. An element $(g, h) \in G \oplus H$ acts by the following rule:

$$u^{(g,h)} := u^g, \quad v^{(g,h)} := v^h$$

for any $u \in U$ and $v \in V$.

Given two groups with actions $G_1 = (\mathbf{G}, U)$ and $G_2 = (\mathbf{G}, V)$ with *the same* abstract group $\mathbf{G}$ and disjoint sets U and V, the *join*

$$\check{G} = G_1 \dot\vee G_2 = (\mathbf{G}, U \dot\cup V)$$

means the group action combining these two actions of $\mathbf{G}$:

$$w^g := \begin{cases} u^g & \text{for } \ w = u \in U, \\ v^g & \text{for } \ w = v \in V \end{cases}$$

for any $w \in U \dot\cup V$ and $g \in G$.

$\check{G}$ is the "diagonal" subgroup of the direct sum $G_1 \oplus G_2$. This natural operation (going back to Burnside) is characteristic for combinatorial enumeration though we could not find an explicit description of it in literature (cf., however, [Dre71, p. 2]).

2.4. Semi-direct and wreath products. The semi-direct product of the group $\mathbb{Z}_n$ with some subgroup $H \leq \mathbb{Z}_n^*$ will be denoted by $\mathbb{Z}_n \rtimes H$; it consists of all permutations of the form $\mathbb{Z}_n \to \mathbb{Z}_n : z \mapsto az + b$ for $b \in \mathbb{Z}_n$ and $a \in H$.

Given two permutation groups G and H acting on sets U and V respectively, their *wreath product* $G \wr H$ is the permutation group of order $|G| \cdot |H|^{|U|}$ which acts on $U \times V$ and is defined as follows: $G \wr H$ consists of all permutations, symbolized by $f = [g, h(u)]$ (where $g \in G$ and $h(u) \in H$ for every $u \in U$), acting on the pairs $(u, v) \in U \times V$ by the rule

$$(u, v)^f = (u^g, v^{h(u)}).$$

2.5. Graphs. Throughout, we shall use the terms *graph* and *undirected graph*, so that by graph it is understood that we referring to one that is directed. In any case all graphs (directed or undirected) are without loops and multiple edges. Accordingly, we speak about edges (i.e. ordered pairs of vertices) and undirected edges (unordered pairs). We recall some graph theoretical notions and notations.

If Γ is a graph, we write $\Gamma = \Gamma(V, E)$ where $V = V(\Gamma)$ and $E = E(\Gamma) \subseteq V \times V$ are the sets of its vertices and edges, respectively.

Graphs Γ and Γ' are called *isomorphic* (denoted by $\Gamma \cong \Gamma'$) if there is a bijection g between $V(\Gamma)$ and $V(\Gamma')$ which induces a bijection between $E(\Gamma)$ and $E(\Gamma')$. In case $\Gamma = \Gamma'$, the permutation g is called an *automorphism* of Γ, and Γ is called *invariant* with respect to g. All such g form the *automorphism group* $\mathrm{Aut}(\Gamma)$. By definition, it is considered as a permutation group on $V(\Gamma)$. In particular, $Z(n)$ is the automorphism group of a complete directed n-cycle and $D(n)$ is the automorphism group of an undirected n-cycle.

An n-graph means a graph of order n, i.e. having n vertices. Usually, for definiteness, the set of vertices of an n-graph is taken to be $\mathbb{Z}_n$.

As usual, an edge (u, v) is depicted by an arrow from the vertex u (its beginning) to the vertex v (its end). This edge is said to be *out-incident* (or simply *incident*) to u and *in-incident* to v. Accordingly, v is called *(out-)adjacent* to u. An undirected edge (u, v) [1] of an undirected graph is depicted by a line segment between vertices u and v. It is incident to u and v.

The *out-valency* (or simply *valency*) of a vertex means the number of edges out-incident to it. The *in-valency* is defined analogously.

A *regular* graph (of valency r) is a graph with coinciding out- and in-valencies (equal to r) for all vertices.

The *complete* n-graph is the graph containing all possible edges between its vertices. It is the only regular graph of valency $n - 1$. It is symmetric and can thus be regarded as an undirected graph. The *null* graph is the n-graph with no edges.

2.6. Circulants. A circulant graph, or simply a *circulant*, means a graph Γ on $\mathbb{Z}_n$ which is invariant with respect to the cyclic permutation $(0, 1, 2, \ldots, n-1)$, i.e.

$$(u, v) \in E(\Gamma) \Longrightarrow (u + 1, v + 1) \in E(\Gamma).$$

Sometimes it is useful to mean by a circulant graph, instead, an n-graph which is invariant with respect to an *arbitrary* complete n-cyclic permutation. But up to isomorphism, both definitions are equivalent. In the literature, circulants are sometimes called *cyclic* or *rotation(al)* graphs.

The *connection set* of a circulant Γ is the set

$$X = X(\Gamma) := \{v \in \mathbb{Z}_n' \mid (0, v) \in E(\Gamma)\}$$

of all vertices adjacent to the vertex 0.

[1] To be precise, one should take the set $\{(u, v), (v, u)\}$ as definition of an undirected edge.

A circulant Γ is completely specified by its connection set X. In fact,

$$E(\Gamma) = \{(u,v) \,|\, u,v \in \mathbb{Z}_n,\ v-u \in X(\Gamma)\}.$$

Accordingly, we write $\Gamma = \Gamma(\mathbb{Z}_n, X)$, in short, $\Gamma = \Gamma(X)$. Obviously, $\Gamma(X)$ is a regular graph of valency $|X|$. In algebraic terms, $\Gamma(X)$ is simply the *Cayley graph* of the cyclic group $\mathbb{Z}_n$ with respect to X. The sets $X = \emptyset$ and $X = \mathbb{Z}'_n$ represent the null and the complete graphs, respectively.

2.7. Undirected circulants. Suppose $v \in X(\Gamma)$, i.e. $(0,v)$ is an edge of the circulant Γ. Applying the permutation $(0,1,2,\dots,n-1)^{n-v}$, we see that Γ contains also the edge $(n-v,0)$. Therefore the connection set X of an undirected circulant n-graph Γ is *symmetric*, which means $v \in X$ if and only if $n-v \in X$ for any $v \in \mathbb{Z}'_n$, or simply $-X = X$ where $-X := \{-v \,|\, v \in X\}$.

Given a connection set X of a circulant graph, $X^{\text{sym}} := X \cup (-X)$ denotes its *symmetrized* connection set of the corresponding undirected circulant graph.

On the the other hand, let X be a symmetric connection set. Then $X^{\text{red}} = X \cap \mathbb{Z}'_{\frac{n-1}{2}}$ for odd n and $X^{\text{red}} = X \cap \mathbb{Z}'_{\frac{n}{2}}$ for even n will denote the *reduced* ("halved") connection set. It is clear that an undirected circulant n-graph $\Gamma(X)$ is completely defined by X^{red}, and different undirected circulant graphs possess different reduced connection sets.

The following simple result plays the key role in the theory of circulants.

2.8. Lemma. *For an arbitrary n, let X and X' be two connection sets such that*

$$mX = X'.\,[2] \tag{$\mathbf{M}_1$}$$

for some integer m prime to n. Then the n-circulants $\Gamma(X)$ and $\Gamma(X')$ are isomorphic.

Proof. In fact, the mapping $\alpha_m : v \mapsto mv$, $\forall\, v \in \mathbb{Z}_n$, is an isomorphism. It is a bijection from $\mathbb{Z}_n$ onto itself since $m \in \mathbb{Z}^*_n$ is invertible. Let (u,v) be an edge of $\Gamma(X)$, then, by definition, $v-u \in X$. Now $(u,v)^{\alpha_m} = (mu,mv)$ is an edge of $\Gamma(X')$ since $mv - mu = m(v-u) \in mX = X'$. Thus, $\Gamma(mX) \cong \Gamma(X)$. □

Note that the equality $(\mathbf{M}_1)$ just describes the induced action of the multiplicative group $\mathbb{Z}^*_n$ on connection sets, i.e. on subsets of $\mathbb{Z}'_n$.

2.9. Remark. For undirected circulant graphs, Lemma 2.8 is clearly also valid in terms of their *reduced* connection sets. Note that Lemma 2.8 may be formulated in a more general context, namely, for any *Cayley object* of $\mathbb{Z}_n$ ([Bab77], [Pál87]), i.e. for a relational structure on the set $\mathbb{Z}_n$ such that all (right) translations are automorphisms of the structure.

2.10. One-multiplier equivalence. Two connection sets X and X' satisfying the condition $(\mathbf{M}_1)$ are called *equivalent* (more exactly, *one-multiplier equivalent* with respect to the multiplier m).

2.11. Ádám's Conjecture. Sometimes, $(\mathbf{M}_1)$ is also referred to as *Ádám's condition* (though Lemma 2.8 was known long ago). A. Ádám in [Ádá67] conjectured the opposite assertion, namely,

$\mathbf{A}(n)$: *The connection sets of isomorphic circulant n-graphs are equivalent.*

[2] $mX := \{mv \,|\, v \in X\}$.

In such a general setting this conjecture is false even for the class of undirected circulants. As we shall see in Section 4, the conjecture $\mathbf{A}(n)$ is valid for prime $n = p$ and is false for $n = p^2$ (except for $n = 4$ and for undirected circulants with $n = 9$). In general, according to [Muz95] and [Muz9y], $\mathbf{A}(n)$ is true for $n = \varepsilon p_1 p_2 \cdots p_k$ where $p_1, p_2, \cdots, p_k$ are pairwise distinct odd prime numbers and $\varepsilon \in \{1, 2, 4\}$), and it is false for all other numbers greater 18 [Pál87].

2.12. Layers. In view of Lemma 2.8 it is natural to partition the elements of $X = X(\Gamma)$ according to their divisors common to n: the layers so obtained are invariant with respect to the (multiplicative) action of $\mathbb{Z}_n^*$.

For $n = p^2$, two layers arise in accordance with the divisibility of the elements of X by p:

$$X = X_{(0)} \dot{\cup} X_{(1)}. \tag{2.12.1}$$

Here the 0-*layer* $X_{(0)}$ is a subset of $\mathbb{Z}_{p^2}^*$ and the 1-layer $X_{(1)}$ is a subset of $p\mathbb{Z}_p^*$. Such a partition can be naturally generalized to $n = p^k$ for any k.

2.13. Residue generators of $\mathbb{Z}_{p^2}^*$. The investigation of p^2-circulants and their isomorphisms is based also on several number-theoretic properties of the prime residue class group.

Let p be an odd prime. As well known, $\mathbb{Z}_{p^2}^*$ is a (multiplicative) cyclic group of order $\phi(p^2) = p(p-1)$. Following [Has64, p. 80], we shall make use of representing this cyclic group in the form of the direct product of two cyclic groups of orders p and $p-1$, respectively (these considerations can be generalized to p^k as well). The first group is generated by the element $1+p$ (which is of order p modulo p^2). The second group is generated by an element $w = w(p,2)$ where w is a primitive root modulo p (i.e. $\langle w \rangle = \mathbb{Z}_p^* \pmod p$) satisfying the congruence $w^{p-1} \equiv 1 \pmod{p^2}$. Such an element w exists: if W is a primitive root modulo p^2, then one can simply take $w = W^p$. Thus, the following assertion is valid.

2.14. Lemma. *Given w as defined in* 2.13, *every element $m \in \mathbb{Z}_{p^2}^*$ has a unique representation*

$$m = m_{i,j} := w^i (1+p)^j \pmod{p^2} \tag{2.14.1}$$

for some $i \in \{0, 1, \ldots, p-2\}$ and $j \in \{0, 1, \ldots, p-1\}$. In other words, all different elements of $\mathbb{Z}_{p^2}^*$ fit in the $(p-1) \times (p)$ matrix $M(p, 2, w) := (m_{i,j})$. □

The choice of $w = w(p,2)$ is immaterial for the sequel; let some value be selected.

2.15. Group ring $\mathbb{Z}[\mathbb{Z}_n]$. In the following we introduce and explain some basic definitions and facts about S-rings over the additive cyclic group $\mathbb{Z}_n$ (for a more general exposition we refer to, e.g., [Wie64]).

The group ring[3] $\langle \mathbb{Z}[\mathbb{Z}_n]; +, \cdot \rangle$ of $\mathbb{Z}_n$ over $\mathbb{Z}$ consists of all formal sums $\sum_{h \in \mathbb{Z}_n} \alpha_h \underline{h}$ with $\alpha_h \in \mathbb{Z}$, $h \in \mathbb{Z}_n$, together with addition

$$\sum_{h \in \mathbb{Z}_n} \alpha_h \underline{h} + \sum_{h \in \mathbb{Z}_n} \beta_h \underline{h} := \sum_{h \in \mathbb{Z}_n} (\alpha_h + \beta_h) \underline{h} \tag{2.15.1}$$

and formal multiplication

$$\Big(\sum_{h \in \mathbb{Z}_n} \alpha_h \underline{h}\Big) \cdot \Big(\sum_{k \in \mathbb{Z}_n} \beta_k k\Big) := \sum_{h,k \in \mathbb{Z}_n} (\alpha_h \beta_k) \underline{(h+k)} = \sum_{h \in \mathbb{Z}_n} \Big(\sum_{k \in \mathbb{Z}_n} \alpha_{h-k} \beta_k\Big) \underline{h}. \tag{2.15.2}$$

$\mathbb{Z}[\mathbb{Z}_n]$ is also a $\mathbb{Z}$-module with scalar multiplication

$$\alpha\Big(\sum_{h \in \mathbb{Z}_n} \alpha_h \underline{h}\Big) := \sum_{h \in \mathbb{Z}_n} (\alpha \alpha_h) \underline{h} \tag{2.15.3}$$

[3] Instead of $\mathbb{Z}$, other rings or fields can be used, e.g. real or complex numbers.

for $\alpha \in \mathbb{Z}$.

The $\mathbb{Z}$-submodule of $\mathbb{Z}[\mathbb{Z}_n]$ generated by elements $\eta_1, \ldots, \eta_r \in \mathbb{Z}[\mathbb{Z}_n]$ will be denoted by

$$\langle \eta_1, \ldots, \eta_r \rangle_{\mathbf{Z}} \text{ or simply } \langle \eta_1, \ldots, \eta_r \rangle \ .$$

Elements of the form

$$\underline{T} := \sum_{h \in T} \underline{h}$$

for $T \subseteq \mathbb{Z}_n$ are called *simple quantities* in $\mathbb{Z}[\mathbb{Z}_n]$ (i.e. $\underline{T} = \sum_{h \in \mathbf{Z}_n} \alpha_h \underline{h}$ with $\alpha_h = 1$ iff $h \in T$, and $\alpha_h = 0$ otherwise). For $T = \{t_1, \ldots, t_q\}$ we write

$$\underline{t_1, \ldots, t_q}$$

instead of $\underline{\{t_1, \ldots, t_q\}}$.

An element h (resp., a subset $U \subseteq \mathbb{Z}_n$) is said to *belong* to (resp., to be *contained* in) $\sum_{h \in \mathbf{Z}_n} \alpha_h \underline{h} \in \mathbb{Z}[\mathbb{Z}_n]$, if $\alpha_h \neq 0$ (resp., $\forall h \in U : \alpha_h \neq 0$).

We introduce further operations. The *Schur-Hadamard product* $\circ$ of elements of $\mathbb{Z}[\mathbb{Z}_n]$ is defined by

$$\Big(\sum_{h \in \mathbf{Z}_n} \alpha_h \underline{h}\Big) \circ \Big(\sum_{h \in \mathbf{Z}_n} \beta_h \underline{h}\Big) := \sum (\alpha_h \beta_h) \underline{h}. \tag{2.15.4}$$

Note, e.g., that $\underline{T} \circ \underline{T'} = \underline{T \cap T'}$ for $T, T' \subseteq \mathbb{Z}_n$, while $\underline{T} \cdot \underline{T'} = \sum_{h \in \mathbf{Z}_n} \alpha_h \underline{h}$ where $\alpha_h = |\{k \in T' \,|\, h - k \in T\}|$. The *transposed* element of $\eta = \sum_{h \in \mathbf{Z}_n} \alpha_h \underline{h} \in \mathbb{Z}[\mathbb{Z}_n]$ is given by

$$\eta^{\top} := \sum_{h \in \mathbf{Z}_n} \alpha_h (\underline{-h}) \ . \tag{2.15.5}$$

2.16. S-rings and automorphisms. An *S-ring*[4] $\mathfrak{S}$ over the group $\mathbb{Z}_n$ *of rank* r is a subring of the group ring $\mathbb{Z}[\mathbb{Z}_n]$ which is generated as $\mathbb{Z}$-module by simple quantities

$$\mathfrak{S} = \langle \underline{T_0}, \underline{T_1}, \ldots, \underline{T_{r-1}} \rangle_{\mathbf{Z}} \tag{2.16.1}$$

where $T_0 = \{0\}$, $\{T_0, T_1, \ldots, T_{r-1}\}$ is a partition of $\mathbb{Z}_n$ (thus, $\sum_{i=0}^{r-1} \underline{T_i} = \underline{\mathbb{Z}_n}$) and $\forall\, i \,\exists\, j : (-T_i) = T_j$ (thus, $\underline{T_i}^{\top} = \underline{T_j}$).

The simple quantities $\underline{T_i}$ are called *basis elements of* $\mathfrak{S}$ and their corresponding sets T_i will be called *basis sets* of $\mathfrak{S}$. A *sub-S-ring* $\mathfrak{S}'$ of an S-ring $\mathfrak{S}$ over $\mathbb{Z}_n$ is an S-ring for which every basis element is a sum of basis elements of $\mathfrak{S}$.

Every $x \in \mathbb{Z}_n$ belongs to a unique basis set, which sometimes will be denoted by $T_{(x)}$ or $T_{(x)}^{\mathfrak{S}}$. Due to (2.16.1), every element of an S-ring $\mathfrak{S}$ is the sum of basis elements. In particular, the S-ring multiplication $\cdot$ is completely given by the *structure constants* ("intersection numbers") $p_{ij}^k \in \mathbb{Z}$ defined by

$$\underline{T_i} \cdot \underline{T_j} = \sum_{k=1}^{r} p_{ij}^k \, \underline{T_k} \, . \tag{2.16.2}$$

Note that for a given partition $\{T_0, T_1, \ldots, T_{r-1}\}$, the property of (2.16.1) being a subring can be checked by the validity of (2.16.2) for suitable p_{ij}^k.

[4] S stands for I. Schur.

The structure constants p_{ij}^k of an S-ring $\mathfrak{S}$ have a natural graph theoretical interpretation for the circulants $\Gamma_i := \Gamma(\mathbb{Z}_n, T_i)$. In fact, for $(u,v) \in E(\Gamma_k)$,

$$p_{ij}^k = |\{w \,|\, (u,w) \in E(\Gamma_i) \wedge (w,v) \in E(\Gamma_j)\}|$$

is the number of paths $u \to w \to v$ of length 2 connecting the ends of a fixed edge $(u,v) \in E(\Gamma_k)$ along an edge (u,w) of $E(\Gamma_i)$ and an edge $(w,v) \in E(\Gamma_j)$. It turns out (via S-ring properties) that this number is independent of the concrete choice of $(u,v) \in E(\Gamma_k)$.

A permutation $g : \mathbb{Z}_n \to \mathbb{Z}_n$ is called an *automorphism* of an S-ring $\mathfrak{S}$ if it is an automorphism of every graph Γ_i.

$$\operatorname{Aut} \mathfrak{S} := \bigcap_{i=0}^{r-1} \operatorname{Aut} \Gamma_i \tag{2.16.3}$$

is the *automorphism group* of $\mathfrak{S}$. Equivalently, $g \in \operatorname{Aut} \mathfrak{S}$ iff $u - v \in T$ implies $u^g - v^g \in T$ for every basis set T of $\mathfrak{S}$.

The *S-ring generated by* a circulant graph $\Gamma(\mathbb{Z}_n, X)$ is the smallest S-ring $\mathfrak{S}$ over $\mathbb{Z}_n$ such that $\underline{X}$ belongs to $\mathfrak{S}$.

2.17. Transitivity modules of groups. Let $(G, \mathbb{Z}_n)$ be a permutation group containing the cyclic group $(\mathbb{Z}_n, \mathbb{Z}_n)$. Consider the stabilizer G_0 and its orbits 1-$Orb(G_0, \mathbb{Z}_n) = \{T_0, \ldots, T_{r-1}\}$ where again we put $T_0 := \{0\}$. Then

$$\mathfrak{S}(G, \mathbb{Z}_n) := \langle \underline{T_0}, \ldots, \underline{T_{r-1}} \rangle_{\mathbf{Z}}$$

is called the *transitivity module* of $(G, \mathbb{Z}_n)$. A celebrated result of I. Schur [Sch33] shows that $\mathfrak{S}(G, \mathbb{Z}_n)$ is an S-ring. Moreover, $\mathfrak{S}(G, \mathbb{Z}_n)$ is closed with respect to the Schur-Hadamard product (2.15.4).

An S-ring $\mathfrak{S}$ is called *Schurian* [Pös74] if it is the transitivity module of some overgroup $(G, \mathbb{Z}_n)$ of $(\mathbb{Z}_n, \mathbb{Z}_n)$. By the well-known properties of Galois correspondence (cf. e.g. [Aig79]) we have

$$\operatorname{Aut}(\mathfrak{S}(\operatorname{Aut} \mathfrak{S}, \mathbb{Z}_n)) = \operatorname{Aut} \mathfrak{S} \quad \text{and} \quad \mathfrak{S}(\operatorname{Aut}(\mathfrak{S}(G, \mathbb{Z}_n)) = \mathfrak{S}(G, \mathbb{Z}_n).$$

A permutation group (G, U) is called 2-*closed* if it is the automorphism group of a coloured graph (that means a set of graphs), i.e. if it is of the form as the right side of (2.16.3). Then we have

$$\mathfrak{S}(\operatorname{Aut} \mathfrak{S}, \mathbb{Z}_n) = \mathfrak{S} \quad \text{and} \quad \operatorname{Aut} \mathfrak{S}(G, \mathbb{Z}_n) = G$$

for every Schurian S-ring $\mathfrak{S}$ and every 2-closed permutation group G containing $\mathbb{Z}_n$.

3 Enumeration of circulants: structural approach based on S-rings

3.1. Conditions. We start with a general scheme of a constructive and analytical enumeration of n-vertex circulant graphs. This will work in any case where we can obtain a complete description of the lattice $\mathcal{L}(n)$ of all S-rings over $\mathbb{Z}_n$. (How to succeed at this will be discussed later.) Moreover, we suppose the following conditions to be satisfied:

- Condition (**S**) for n:
  each S-ring from $\mathcal{L}(n)$ is Schurian (cf. 2.17), i.e. it is a transitivity module of a suitable overgroup $(G, \mathbb{Z}_n)$ of the regular group $(\mathbb{Z}_n, \mathbb{Z}_n)$;
- Condition (**U**) for n:
  all S-rings from $\mathcal{L}(n)$ are pairwise non-isomorphic.

It turns out that condition (**U**) is satisfied for all values of n. This crucial property of S-rings over $\mathbb{Z}_n$ was proved by M. Muzychuk in [Muz94].

Condition (**S**) also seems to be valid for all values n. In particular, it is true for $n = p^m$, $m \geq 1$, p a prime (this follows from the fact that a p-group is Schurian (i.e. satisfies (**S**)) if and only if it is cyclic [Pös74]), and in the case of square-free n, see [Muz9y]. We believe that the validity of condition (**S**) will be proved rather soon on the basis of recent significant progress in understanding the structure of S-rings over $\mathbb{Z}_n$.

3.2. Scheme. With the above assumptions, the following enumeration scheme may be used (see [Kli70] and [FarKM94] for details).

Let us write the set $\mathcal{L}$ of all S-rings as a sequence $\mathcal{L} = (\mathfrak{S}_1, \mathfrak{S}_2, \ldots, \mathfrak{S}_s)$ in such an order that $\mathfrak{S}_j \subseteq \mathfrak{S}_i$ implies $j \leq i$ (if we use other indices, this means that $\mathfrak{S}_j$ appears to the left of $\mathfrak{S}_i$ in the ordered sequence $\mathcal{L}$). Let

$$\widetilde{d}_{ir} := |\{T_{(x)} \in \mathfrak{S}_i \mid x \neq 0 \text{ and } |T_{(x)}| = r\}|$$

be the number of r-element basis sets of the S-ring $\mathfrak{S}_i$ different from the basis set $T_0 = \{0\}$. Further, let

$$d_{ir} := |\{T^{\mathrm{sym}}_{(x)} \mid x \neq 0 \text{ and } |T^{\mathrm{sym}}_{(x)}| = r\}|$$

be the number of r-element symmetrized basis sets of $\mathfrak{S}_i$ (cf. 2.7) different from T_0.

Let us define the generating functions

$$\widetilde{f}_i(t) := \textstyle\sum_{r=0}^{n-1} \widetilde{f}_{ir} t^r := \displaystyle\prod_{r=1}^{n-1} (1+t^r)^{\widetilde{d}_{ir}} \ ,$$

$$f_i(t) := \textstyle\sum_{r=0}^{n-1} f_{ir} t^r := \displaystyle\prod_{r=1}^{n-1} (1+t^r)^{d_{ir}} \ .$$

Note that the graph which corresponds to $T \in \mathfrak{S}_i$ is of valency r if T has r elements. Symmetrized sets correspond to undirected circulant graphs. One can show without difficulty that $f_i(t)$ and $\widetilde{f}_i(t)$ enumerate (with respect to valencies) all *labelled* undirected and directed circulant graphs, respectively, which belong to the S-ring $\mathfrak{S}_i$. In particular, $\widetilde{f}_i(1)$ is the number of all labelled circulant graphs in $\mathfrak{S}_i$.

3.3. Lemma. *Let $G_i = \mathrm{Aut}(\mathfrak{S}_i)$, let $N(G_i) = N_{S_n}(G_i)$ be the normalizer of the group G_i in S_n, and let Γ be a circulant graph belonging to $\mathfrak{S}_i$. Then*

(a) $\mathrm{Aut}(\Gamma) = G_i \iff \Gamma$ *generates* $\mathfrak{S}_i$.

(b) *If* $\mathrm{Aut}(\Gamma) = G_i$ *then there are exactly* $[N(G_i) : G_i]$ *distinct circulant graphs which are isomorphic to* Γ.

The PROOF easily follows from the definitions and conditions (**S**) and (**U**). □

3.4. Definition. Let

$$g_i(t) = \sum_{r=0}^{n-1} g_{ir} t^r \quad \text{and} \quad \widetilde{g}_i(t) = \sum_{r=0}^{n-1} \widetilde{g}_{ir} t^r$$

be the generating functions for the number of pairwise non-isomorphic undirected and directed circulant graphs, respectively, with automorphism group G_i. Let

$$g(t) = g(n,t) \quad \text{and} \quad \widetilde{g}(t) = \widetilde{g}(n,t)$$

be the generating functions for the number of all pairwise non-isomorphic undirected and directed circulant graphs, respectively, with n vertices. We emphasize that here all generating functions are specified by valencies. Note moreover that $g(1)$ and $\widetilde{g}(1)$ are just the numbers of all non-isomorphic undirected and directed circulant graphs, respectively, with n vertices.

3.5. Theorem.

$$
\begin{aligned}
g_i(t) &= \frac{|G_i|}{|N(G_i)|}\left(f_i(t) - \sum_{\mathfrak{S}_j \subseteq \mathfrak{S}_i} \frac{|N(G_j)|}{|G_j|} g_j(t)\right), \\
\widetilde{g}_i(t) &= \frac{|G_i|}{|N(G_i)|}\left(\widetilde{f}_i(t) - \sum_{\mathfrak{S}_j \subseteq \mathfrak{S}_i} \frac{|N(G_j)|}{|G_j|} \widetilde{g}_j(t)\right), \\
g(t) &= \sum_{i=1}^{s} g_i(t), \qquad \widetilde{g}(t) = \sum_{i=1}^{s} \widetilde{g}_i(t).
\end{aligned}
$$

Proof. Let us prove, for example, the formula for $g_i(t)$. At first we fix r and consider all undirected circulant graphs invariant with respect to G_i and having valency r. There are f_{ir} such graphs. These graphs have automorphism groups $G_j \geq G_i$ (dually, this corresponds to the inclusion $\mathfrak{S}_j \subseteq \mathfrak{S}_i$). According to Lemma 3.3, there exist exactly $\frac{|N(G_j)|}{|G_j|} g_{jr}$ labelled undirected circulant graphs with automorphism group G_j. Subtracting from f_{ir} the obtained quantity for each group G_j such that $G_j \geq G_i$, we get the number of labelled undirected graphs with the group G_i. Then again Lemma 3.3 is used. This reasoning is valid for all r, $0 \leq r \leq n-1$. Therefore the formula for $g_i(t)$ is proved. The proof for $\widetilde{g}_i(t)$ is similar. The formulae for $g(t)$ and $\widetilde{g}(t)$ are evident. □

3.6. Remark. The above proof is in fact based on the use of the classical principle of inclusion and exclusion. In a more advanced version of this principle (see [Kli70] and [FarKM94]) so-called Burnside marks are used. However, because of conditions (**S**) and (**U**) of 3.1 we can reasonably simplify the approach, moreover we have to take into account only 2-closed permutation groups.

3.7. Example. Let $n = 6$. We start with the list $\mathcal{L} = (\mathfrak{S}_1, \ldots, \mathfrak{S}_6)$ of all S-rings over $\mathbb{Z}_6$:

$$
\begin{aligned}
\mathfrak{S}_1 &= \langle \underline{0}, \underline{1,2,3,4,5} \rangle, \\
\mathfrak{S}_2 &= \langle \underline{0}, \underline{1,2,4,5}, \underline{3} \rangle, \\
\mathfrak{S}_3 &= \langle \underline{0}, \underline{1,3,5}, \underline{2,4} \rangle, \\
\mathfrak{S}_4 &= \langle \underline{0}, \underline{1,5}, \underline{2,4}, \underline{3} \rangle, \\
\mathfrak{S}_5 &= \langle \underline{0}, \underline{1,3,5}, \underline{2}, \underline{4} \rangle, \\
\mathfrak{S}_6 &= \langle \underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5} \rangle.
\end{aligned}
$$

According to 3.2 we get

$$
\begin{aligned}
f_1(t) &= & \widetilde{f}_1(t) &= 1 + t^5, \\
f_2(t) &= & \widetilde{f}_2(t) &= (1+t)(1+t^4), \\
f_3(t) &= & \widetilde{f}_3(t) &= (1+t^2)(1+t^3), \\
f_4(t) &= & \widetilde{f}_4(t) &= (1+t)(1+t^2)^2, \\
f_5(t) &= (1+t^2)(1+t^3), & \widetilde{f}_5(t) &= (1+t)^2(1+t^3), \\
f_6(t) &= (1+t)(1+t^2)^2, & \widetilde{f}_6(t) &= (1+t)^5.
\end{aligned}
$$

According to Theorem 3.5 we need some information about the groups and their respective normalizers. We have

$$
\begin{aligned}
G_1 &= S_6, & N(G_1) &= G_1, \\
G_2 &= S_3 \wr S_2, & N(G_2) &= G_2, \\
G_3 &= S_2 \wr S_3, & N(G_3) &= G_3, \\
G_4 &= D_6, & N(G_4) &= G_4, \\
G_5 &= S_2 \wr \mathbb{Z}_3, & [N(G_5) : G_5] &= 2, \\
G_6 &= \mathbb{Z}_6, & [N(G_6) : G_6] &= 2.
\end{aligned}
$$

Now we can apply Theorem 3.5 to get

$$
\begin{aligned}
g_1(t) &= f_1(t) && = 1 + t^5, \\
g_2(t) &= f_2(t) - g_1(t) && = t + t^4, \\
g_3(t) &= f_3(t) - g_1(t) && = t^2 + t^3, \\
g_4(t) &= f_4(t) - f_1(t) - f_2(t) - f_3(t) && = t^2 + t^3, \\
g_5(t) &= \tfrac{1}{2}(f_5(t) - g_1(t) - g_3(t)) && = 0, \\
g_6(t) &= \tfrac{1}{2}(f_6(t) - g_1(t) - g_2(t) - g_3(t) - g_4(t) - 2g_5(t)) && = 0, \\
g(t) &= 1 + t + 2t^2 + 2t^3 + t^4 + t^5.
\end{aligned}
$$

In a similar manner, one obtains the functions $\widetilde{g}_i(t)$ and $\widetilde{g}(t)$. In particular,

$$\widetilde{g}(t) = 1 + 3t + 6t^2 + 6t^3 + 3t^4 + t^5.$$

3.8. Example. Let $n = 8$. We start with the list $\mathcal{L} = (\mathfrak{S}_1, \ldots, \mathfrak{S}_{10})$ of all S-rings over $\mathbb{Z}_8$.

$$
\begin{aligned}
\mathfrak{S}_1 &= \langle \underline{0}, \underline{1, 2, 3, 4, 5, 6, 7} \rangle, \\
\mathfrak{S}_2 &= \langle \underline{0}, \underline{1, 2, 3, 5, 6, 7}, \underline{4} \rangle, \\
\mathfrak{S}_3 &= \langle \underline{0}, \underline{1, 3, 5, 7}, \underline{2, 6, 4} \rangle, \\
\mathfrak{S}_4 &= \langle \underline{0}, \underline{1, 3, 5, 7}, \underline{2, 6}, \underline{4} \rangle, \\
\mathfrak{S}_5 &= \langle \underline{0}, \underline{1, 3, 5, 7}, \underline{2}, \underline{6}, \underline{4} \rangle, \\
\mathfrak{S}_6 &= \langle \underline{0}, \underline{1, 5}, \underline{3, 7}, \underline{2, 6}, \underline{4} \rangle, \\
\mathfrak{S}_7 &= \langle \underline{0}, \underline{1, 5}, \underline{3, 7}, \underline{2}, \underline{6}, \underline{4} \rangle, \\
\mathfrak{S}_8 &= \langle \underline{0}, \underline{1, 3}, \underline{5, 7}, \underline{2, 6}, \underline{4} \rangle, \\
\mathfrak{S}_9 &= \langle \underline{0}, \underline{1, 7}, \underline{3, 5}, \underline{2, 6}, \underline{4} \rangle, \\
\mathfrak{S}_{10} &= \langle \underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \underline{6}, \underline{7} \rangle.
\end{aligned}
$$

According to 3.2 we get

$$
\begin{aligned}
f_1(t) &= & \widetilde{f}_1(t) &= (1 + t^7), \\
f_2(t) &= & \widetilde{f}_2(t) &= (1 + t)(1 + t^6), \\
f_3(t) &= & \widetilde{f}_3(t) &= (1 + t^3)(1 + t^4), \\
f_4(t) &= & \widetilde{f}_4(t) &= (1 + t)(1 + t^2)(1 + t^4), \\
f_5(t) &= (1 + t)(1 + t^2)(1 + t^4), & \widetilde{f}_5(t) &= (1 + t)^3(1 + t^4), \\
f_6(t) &= (1 + t)(1 + t^2)(1 + t^4), & \widetilde{f}_6(t) &= (1 + t)(1 + t^2)^3, \\
f_7(t) &= (1 + t)(1 + t^2)(1 + t^4), & \widetilde{f}_7(t) &= (1 + t)^3(1 + t^2)^2, \\
f_8(t) &= (1 + t)(1 + t^2)(1 + t^4), & \widetilde{f}_8(t) &= (1 + t)(1 + t^2)^3, \\
f_9(t) &= & \widetilde{f}_9(t) &= (1 + t)(1 + t^2)^3, \\
f_{10}(t) &= (1 + t)(1 + t^2)^3, & \widetilde{f}_{10}(t) &= (1 + t)^7.
\end{aligned}
$$

In order to apply Theorem 3.5 we need some information about the orders of the automorphism groups and their normalizers (we shall not go into details here and therefore will not present the groups themselves):

$$\begin{array}{rlcrl}
|G_1| &= 8! & , & [N(G_1):G_1] &= 1, \\
|G_2| &= 4!\cdot 2^4, & & [N(G_2):G_2] &= 1, \\
|G_3| &= 2(4!)^2, & & [N(G_3):G_3] &= 1, \\
|G_4| &= 2\cdot 8^2 & , & [N(G_4):G_4] &= 1, \\
|G_5| &= 2\cdot 4^2 & , & [N(G_5):G_5] &= 2, \\
|G_6| &= 4\cdot 2^4 & , & [N(G_6):G_6] &= 2, \\
|G_7| &= 16 & , & [N(G_7):G_7] &= 4, \\
|G_8| &= 16 & , & [N(G_8):G_8] &= 2, \\
|G_9| &= 16 & , & [N(G_9):G_9] &= 2, \\
|G_{10}| &= 8 & , & [N(G_{10}):G_{10}] &= 4.
\end{array}$$

From Theorem 3.5 we now conclude

$$\begin{aligned}
g_1(t) &= f_1(t) = 1 + t^7, \\
g_2(t) &= 1\cdot(f_2(t) - 1\cdot g_1(t)) = t + t^6, \\
&\vdots \\
g_7(t) &= \tfrac{1}{4}(f_7(t) - g_1(t) - g_2(t) - g_3(t) - g_4(t) - 2g_5(t) - 2g_6(t)), \\
&\vdots \\
g(t) &= g_1(t) + g_2(t) + \ldots + g_{10}(t).
\end{aligned}$$

In order to avoid long computations with polynomials we shall compute here only the numbers $g_i(1)$, $\widetilde{g}_i(1)$ of all graphs with automorphism group G_i. To start, we have

$$\begin{array}{rlrl}
f_1(1) = & & \widetilde{f}_1(1) = & 2, \\
f_2(1) = & & \widetilde{f}_2(1) = & 4, \\
f_3(1) = & & \widetilde{f}_3(1) = & 4, \\
f_4(1) = & & \widetilde{f}_4(1) = & 8, \\
f_5(1) = & 8, & \widetilde{f}_5(1) = & 16, \\
f_6(1) = & 8, & \widetilde{f}_6(1) = & 16, \\
f_7(1) = & 8, & \widetilde{f}_7(1) = & 32, \\
f_8(1) = & 8, & \widetilde{f}_8(1) = & 16, \\
f_9(1) = & & \widetilde{f}_9(1) = & 16, \\
f_{10}(1) = & 16, & \widetilde{f}_{10}(1) = & 128,
\end{array}$$

Now we proceed according to Theorem 3.5:

$$\begin{array}{llll}
g_1(1) = & = 2, & \widetilde{g}_1(1) = & = 2, \\
g_2(1) = 4-2 & = 2, & \widetilde{g}_2(1) = & = 2, \\
g_3(1) = 4-2 & = 2, & \widetilde{g}_3(1) = & = 2, \\
g_4(1) = 8-2-2-2 & = 2, & \widetilde{g}_4(1) = & = 2, \\
g_5(1) = \frac{1}{2}(8-2-2-2-2) & = 0, & \widetilde{g}_5(1) = \frac{1}{2}(16-2-2-2-2) & = 4, \\
g_6(1) = \frac{1}{2}(8-2-2-2-2) & = 0, & \widetilde{g}_6(1) = \frac{1}{2}(16-2-2-2-2) & = 4, \\
g_7(1) = \frac{1}{4}(8-2-2-2-2) & = 0, & \widetilde{g}_7(1) = \frac{1}{4}(32-2-2-2-2-8-8) & = 2, \\
g_8(1) = \frac{1}{2}(8-2-2-2-2) & = 0, & \widetilde{g}_8(1) = \frac{1}{2}(16-2-2-2-2) & = 4, \\
g_9(1) = \frac{1}{2}(16-2-2-2-2) & = 4, & \widetilde{g}_9(1) = & = 4, \\
g_{10}(1) = \frac{1}{4}(16-8-2-2-2-2) & = 0, & \widetilde{g}_{10}(1) = \frac{1}{4}(128-2-2-2-2 & \\
 & & \qquad -8-8-8-8-4) & = 21, \\
g(1) = g(8,1) & = 12, & \widetilde{g}(1) = \widetilde{g}(8,1) & = 47.
\end{array}$$

3.9. Remark. In what follows, the above outlined approach for the enumeration of circulants will be called the *structural* approach. This means that the global information about the number of all circulants is collected from the detailed information about the number of circulants with a prescribed group, where the input of each possible group is separately encountered. The advantage of this structural approach is that for each concrete value of n, certain information about S-rings and their automorphism groups is sufficient for completing the enumeration. An alternative *multiplier* approach will be developed in Sections 5–7 below. Here our goal will be to get formulae for the count of non-isomorphic circulants without direct use of the lattice $\mathcal{L}_n$ as well as without explicit computation of the functions $g_i(t)$ and $\widetilde{g}_i(t)$. Instead, the multiplier approach is based on isomorphism theorems.

4 Enumeration for concrete cases with known S-ring structure

We now apply the structural approach to some cases where all neccessary information about S-rings is completely known in advance.

(A) Enumeration for $n = p$

4.1. List of S-rings. For $n = p$, p a prime number, the S-rings and their automorphism groups can be described explicitly. Let $H = H_d$ be the subgroup of order d of the multiplicative group $\mathbb{Z}_p^*$. Let $H, y_2H, \ldots, y_lH$, $l = \frac{p-1}{d}$, be the set of distinct cosets of subgroup H in $\mathbb{Z}_p^*$. It is easy to see that $\mathfrak{S}_d = \langle \underline{0}, \underline{H}, \ldots, \underline{y_lH} \rangle$ is an S-ring over $\mathbb{Z}_p$: this is the transitivity module of the stabilizer of 0 in $\mathbb{Z}_p \rtimes H_d$. It turns out that each S-ring over Z_p coincides with $\mathfrak{S}_d$ for a suitable $d|(p-1)$. This fact appeared in literature, explicitly or implicitly, many times; see [PösK79], [FarIK90] and [DreKM92] for more details. We have the following theorem (given here without proof):

4.2. Theorem.

(i) *Each S-ring over* $\mathbb{Z}_p$ *coincides with some* $\mathfrak{S}_d$ $(d|(p-1))$.

(ii) $\mathrm{Aut}(\mathfrak{S}_d) = \begin{cases} \mathbb{Z}_p \rtimes H_d & \textit{if} \quad d < p-1 \\ S_p & \textit{if} \quad d = p-1 \end{cases}.$

(iii) $N(\mathrm{Aut}(\mathfrak{S}_d)) = \begin{cases} \mathbb{Z}_p \rtimes \mathbb{Z}_p^* & \textit{if} \quad d < p-1 \\ S_p & \textit{if} \quad d = p-1 \end{cases}.$

(iv) $[N(\mathrm{Aut}(\mathfrak{S}_d)) : \mathrm{Aut}(\mathfrak{S}_d)] = \dfrac{p-1}{d}.$

4.3. Corollary. *Adam's conjecture* $\mathbf{A}(n)$ *is valid for all prime numbers* $n = p$.

Proof. It easily follows from Theorem 4.2 that conditions $(\mathbf{S})$ and $(\mathbf{U})$ of 3.1 are satisfied for $n = p$. This implies that if two circulant graphs $\Gamma = \Gamma(\mathbb{Z}_p, X)$ and $\Gamma' = \Gamma(\mathbb{Z}_p, X')$ are isomorphic then $\underline{X}$ and $\underline{X'}$ generate the same S-ring $\mathfrak{S} = \mathfrak{S}_d$ for some $d|(p-1)$. Thus, using Lemma 3.3, we get that $X' = X^g$ for some $g \in N(\mathrm{Aut}(\mathfrak{S}))$. Now we take into account that, according to 4.2(ii) and 4.2(iii), for each $g \in N(\mathrm{Aut}(\mathfrak{S}))$ there exists an $m \in \mathbb{Z}_p^*$ such that $X^g = mX$. $\square$

4.4. Example. Let $n = 13$. With notations from 4.1, the list of all S-rings over $\mathbb{Z}_p$ is

$$\mathcal{L} = (\mathfrak{S}_{12}, \mathfrak{S}_6, \mathfrak{S}_4, \mathfrak{S}_3, \mathfrak{S}_2, \mathfrak{S}_1).$$ [5]

Let us count the numbers $g(13, 1)$ and $\widetilde{g}(13, 1)$ of all pairwise non-isomorphic 13-vertex undirected and directed circulants. We get

$$\begin{array}{ll}
f_{12}(1) = & \widetilde{f}_{12}(1) = 2^1, \\
f_6(1) = & \widetilde{f}_6(1) = 2^2, \\
f_4(1) = & \widetilde{f}_4(1) = 2^3, \\
f_3(1) = 2^2, & \widetilde{f}_3(1) = 2^4, \\
f_2(1) = & \widetilde{f}_2(1) = 2^6, \\
f_1(1) = 2^6, & \widetilde{f}_1(1) = 2^{12}.
\end{array}$$

Now

$$\begin{array}{llll}
g_{12}(1) = \frac{1}{1} \cdot 2 & = 2, & \widetilde{g}_{12}(1) = & = 2, \\
g_6(1) = \frac{1}{2}(2^2 - 2) & = 1, & \widetilde{g}_6(1) = & = 1, \\
g_4(1) = \frac{1}{3}(2^3 - 2) & = 2, & \widetilde{g}_4(1) = & = 2, \\
g_3(1) = \frac{1}{4}(2^2 - 2 - 2) & = 0, & \widetilde{g}_3(1) = \frac{1}{4}(2^4 - 2 - 2) & = 3, \\
g_2(1) = \frac{1}{6}(2^6 - 2 - 2 - 6) & = 9, & \widetilde{g}_2(1) = & = 9, \\
g_1(1) = \frac{1}{12}(2^6 - 2 - 2 - 6 - 0 - 54) & = 0, & \widetilde{g}_1(1) = \frac{1}{12}(2^{12} - 2 - 2 - 6 - 12 - 54) & = 335, \\
 & & & \\
g(1) = g(13, 1) & = 14, & \widetilde{g}(1) = \widetilde{g}(13, 1) & = 352.
\end{array}$$

(B) Enumeration for $n = p^2$

The case $n = p^2$ (for prime p) is the simplest case in which Adam's conjecture $\mathbf{A}(n)$ is not generally valid. We follow the general scheme as described in 3.1–3.5 and start with a description of all S-rings over $\mathbb{Z}_n$.

4.5. Definition. An S-ring $\mathfrak{S} = \langle \underline{T_0}, \underline{T_1}, \dots, \underline{T_l} \rangle$ over $\mathbb{Z}_n$ is called *wreath decomposable* if there exists a non-trivial proper subgroup $K \leq \mathbb{Z}_n$ such that for every basic element T_i, either $T_i \subseteq K$ or T_i is a union of suitable cosets of $\mathbb{Z}_n/K$ (i.e. $T_i = \bigcup_{x \in T_i}(K + x)$). In particular we have $\underline{K} \in \mathfrak{S}$. The S-ring $\mathfrak{S}$ is called *wreath indecomposable* if it is not wreath decomposable.

4.6. Example and Definition. Let $n = p^2$, $K = \mathbb{Z}_p$. Let

$$\mathfrak{S}_1 = \langle \underline{Q_0}, \underline{Q_1}, \dots, \underline{Q_d} \rangle \text{ and } \mathfrak{S}_2 = \langle \underline{R_0}, \underline{R_1}, \dots, \underline{R_k} \rangle$$

be S-rings over $\mathbb{Z}_p$. Let

$$\begin{aligned}
T_{1,i} &:= \{px_2 \mid x_2 \in R_i\}, \qquad 0 \leq i \leq k, \\
T_{2,i} &:= \{x_1 + px_2 \mid x_1 \in Q_j, \quad x_2 \in \mathbb{Z}_p\}, \qquad 1 \leq j \leq d.
\end{aligned}$$

These sets are basis sets of an S-ring $\mathfrak{S}$ over $\mathbb{Z}_{p^2}$,

$$\mathfrak{S} := \langle \underline{T_{1,0}}, \underline{T_{1,1}}, \dots, \underline{T_{1,k}}, \underline{T_{2,1}}, \dots, \underline{T_{2,d}} \rangle,$$

which is called the *wreath composition* of $\mathfrak{S}_1$ and $\mathfrak{S}_2$ and is denoted by $\mathfrak{S} = \mathfrak{S}_1[\mathfrak{S}_2]$. The S-ring property of $\mathfrak{S}$ can be easily seen by direct computations using the fact that $\mathfrak{S}_1$ and $\mathfrak{S}_2$ are S-rings. Moreover, by definition 4.5, $\mathfrak{S}$ is a wreath decomposable S-ring (take $K = p\mathbb{Z}_p$).

[5] Note here the different numeration – because of 4.1 – of the S-rings (indices do not increase). Nevertheless, this $\mathcal{L}$ satisfies the property described in 3.2 because $\mathfrak{S}_d \subseteq \mathfrak{S}_{d'} \iff d' | d$.

4.7. Remark. The definition of wreath composition and of wreath decomposable S-rings can be given for arbitrary values of n and, moreover, over arbitrary groups. The construction of the wreath composition of S-rings is a special case of a wreath product construction for cellular rings (algebras) (see [Wei76]). In a different context it was discussed in [KalK76], [KliP78] and [PösK79], see also [KliMW9x] and [KliP9x]. It turns out that each wreath decomposable S-ring over a group H can be represented as a wreath composition of suitable S-rings $\mathfrak{S}_1$ and $\mathfrak{S}_2$ over groups of smaller order (sometimes iterated wreath composition appears). The notion is motivated by the fact that the automorphism group $\mathrm{Aut}(\mathfrak{S}_1[\mathfrak{S}_2])$ is the wreath product of the automorphism groups of the S-rings $\mathfrak{S}_1$ and $\mathfrak{S}_2$. In what follows we shall use these facts for the special case $n = p^2$.

4.8. Theorem ([Pös74], [KliP78], [PösK79]). *Let $\mathfrak{S}$ be a non-trivial S-ring over $\mathbb{Z}_{p^2}$. Then we have*

(a) *Either*

(i) *$\mathfrak{S}$ is a wreath composition $\mathfrak{S} = \mathfrak{S}_1[\mathfrak{S}_2]$ of S-rings $\mathfrak{S}_1$, $\mathfrak{S}_2$ over $\mathbb{Z}_p$,*

or

(ii) $\mathfrak{S} = \langle \underline{0}, \underline{H}, \underline{y_1 H}, \ldots, \underline{y_l H} \rangle$, *where $H \le \mathbb{Z}_{p^2}^*$, $(1+p) \notin H$, $y_i \in \mathbb{Z}_p^*$ for $1 \le i \le l$;*

(b) $$\mathrm{Aut}(\mathfrak{S}) = \begin{cases} \mathrm{Aut}(\mathfrak{S}_1) \wr \mathrm{Aut}(\mathfrak{S}_2) & \textit{in case } \text{(i)[6]} \\ \mathbb{Z}_{p^2} \rtimes H & \textit{in case } \text{(ii)} \end{cases};$$

(c) $$[N(\mathrm{Aut}(\mathfrak{S})) : \mathrm{Aut}(\mathfrak{S})] = \begin{cases} \displaystyle\prod_{i=1}^{2} [N(\mathrm{Aut}(\mathfrak{S}_i)) : \mathrm{Aut}(\mathfrak{S}_i)] & \textit{in case } \text{(i)} \\ \dfrac{(p-1)p}{|H|} & \textit{in case } \text{(ii)} \end{cases}.$$

4.9. Example. Let $n = 9$. The list of all S-rings over $\mathbb{Z}_9$ is $\mathcal{L} = (\mathfrak{S}_1, \ldots, \mathfrak{S}_7)$ where

$$\begin{aligned}
\mathfrak{S}_1 &= \langle \underline{0}, \underline{1,2,3,4,5,6,7,8} \rangle, \\
\mathfrak{S}_2 &= \langle \underline{0}, \underline{1,2,4,5,7,8}, \underline{3,6} \rangle, \\
\mathfrak{S}_3 &= \langle \underline{0}, \underline{1,4,7}, \underline{2,5,8}, \underline{3,6} \rangle, \\
\mathfrak{S}_4 &= \langle \underline{0}, \underline{1,2,4,5,7,8}, \underline{3}, \underline{6} \rangle, \\
\mathfrak{S}_5 &= \langle \underline{0}, \underline{1,4,7}, \underline{2,5,8}, \underline{3}, \underline{6} \rangle, \\
\mathfrak{S}_6 &= \langle \underline{0}, \underline{1,8}, \underline{2,7}, \underline{3,6}, \underline{4,5} \rangle, \\
\mathfrak{S}_7 &= \langle \underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \underline{6}, \underline{7}, \underline{8} \rangle.
\end{aligned}$$

We again give only the briefest necessary information about the automorphism groups of all S-rings in $\mathcal{L}$:

$$\begin{aligned}
G_1 &= S_9, & [N(G_1) : G_1] &= 1, \\
G_2 &= S_3 \wr S_3, & [N(G_2) : G_2] &= 1, \\
G_3 &= \mathbb{Z}_3 \wr S_3, & [N(G_3) : G_3] &= 2, \\
G_4 &= S_3 \wr \mathbb{Z}_3, & [N(G_4) : G_4] &= 2, \\
G_5 &= \mathbb{Z}_3 \wr \mathbb{Z}_3, & [N(G_5) : G_5] &= 4, \\
G_6 &= D_9, & [N(G_6) : G_6] &= 3, \\
G_7 &= \mathbb{Z}_9, & [N(G_7) : G_7] &= 6.
\end{aligned}$$

[6] Here the wreath product acts on $\mathbb{Z}_{p^2}$ via its action on $\mathbb{Z}_p \times \mathbb{Z}_p$ (cf. 2.4) and the canonical isomorphism induced by the bijection $\mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_{p^2} : (x, y) \mapsto x + yp$.

Now we are able to use the structural approach (3.2 and 3.5) in order to count the number of undirected and directed circulants.

$$\begin{aligned}
f_1(1) &= & \widetilde{f}_1(1) &= 2,\\
f_2(1) &= & \widetilde{f}_2(1) &= 2^2,\\
f_3(1) &= 2^2, & \widetilde{f}_3(1) &= 2^3,\\
f_4(1) &= 2^2, & \widetilde{f}_4(1) &= 2^3,\\
f_5(1) &= 2^2, & \widetilde{f}_5(1) &= 2^4,\\
f_6(1) &= & \widetilde{f}_6(1) &= 2^4,\\
f_7(1) &= 2^4, & \widetilde{f}_7(1) &= 2^8.
\end{aligned}$$

Therefore

$$\begin{aligned}
g_1(1) &= & &= 2, & \widetilde{g}_1(1) &= & &= 2,\\
g_2(1) &= 2^2-2 & &= 2, & \widetilde{g}_2(1) &= & &= 2,\\
g_3(1) &= \tfrac{1}{2}(2^2-2-2) & &= 0, & \widetilde{g}_3(1) &= \tfrac{1}{2}(2^3-2-2) & &= 2,\\
g_4(1) &= \tfrac{1}{2}(2^2-2-2) & &= 0, & \widetilde{g}_4(1) &= \tfrac{1}{2}(2^3-2-2) & &= 2,\\
g_5(1) &= \tfrac{1}{4}(2^2-2-2) & &= 0, & \widetilde{g}_5(1) &= \tfrac{1}{4}(2^4-2-2-4-4) & &= 1,\\
g_6(1) &= \tfrac{1}{3}(2^4-2-2) & &= 4, & \widetilde{g}_6(1) &= & &= 4,\\
g_7(1) &= \tfrac{1}{6}(2^4-2-2-3\cdot 4) & &= 0, & \widetilde{g}_7(1) &= \tfrac{1}{6}(2^8-2-2-4-4-4-12) & &= 38,\\
\\
g(1) &= g(9,1) & &= 8, & \widetilde{g}(1) &= \widetilde{g}(9,1) & &= 51.
\end{aligned}$$

4.10. Remark. The reader can easily see that the conjecture $\mathbf{A}(9)$ is valid in the class of undirected graphs; however, it is not valid in the class of directed circulants. The only S-ring which is "responsible" for the non-validity of $\mathbf{A}(9)$ is the S-ring $\mathfrak{S}_5$. Namely, e.g., the circulant graphs $\Gamma = \Gamma(\mathbb{Z}_9, X)$ and $\Gamma' = \Gamma(\mathbb{Z}_9, X')$ with $X = \{1,3,4,7\}$ and $X' = \{1,6,4,7\}$ are not one-multiplier isomorphic because, evidently, no multiplier transforms X into X'. Nevertheless, Γ and Γ' are isomorphic under the isomorphism $(0)(1)(2)(3,6)(4,7)(5,8)$. These graphs are depicted in Figure 1 where the arrow $\Longrightarrow$ indicates the complete set of edges connecting all vertices of the two 3-vertex sets in the specified direction (in other words, here $\Longrightarrow$ denotes 9 usual edges).

For $p \geq 5$ one can construct analogous examples of undirected graphs on $n = p^2$ vertices for which the conjecture $\mathbf{A}(n)$ is not valid. E.g. the circulant graphs $\Gamma(\mathbb{Z}_{25}, Y)$ and $\Gamma(\mathbb{Z}_{25}, Y')$ on 25 vertices with the connection sets $Y = \{1,4,6,9,11,14,16,19,21,24,5,20\}$ and $Y' = \{1,4,6,9,11,14,16,19,21,24,10,15\}$ yield such an example.

4.11. Constructive enumeration. In this and the previous section we have outlined the methodology of the analytical enumeration of circulant graphs based on the systematical use of the lattice $\mathcal{L}$ of all S-rings over $\mathbb{Z}_n$. This can be naturally extended to the description of a constructive enumeration procedure for circulants: for each S-ring $\mathfrak{S}$ from $\mathcal{L}$ we describe the set $C(\mathfrak{S})$ of all circulants $\Gamma(\mathbb{Z}_n, X)$ such that $\underline{X}$ generates $\mathfrak{S}$. Then we find the orbits of the action of $N(\mathrm{Aut}(\mathfrak{S}))/\mathrm{Aut}(\mathfrak{S})$ on $C(\mathfrak{S})$. Each transversal $\mathcal{T}(\mathfrak{S})$ of this set of orbits represents (up to isomorphism) all circulants with automorphism group $\mathrm{Aut}(\mathfrak{S})$. The union $\mathcal{T} = \bigcup_{\mathfrak{S}\in\mathcal{L}} \mathcal{T}(\mathfrak{S})$ gives a constructive representation of all n-vertex circulants. Sometimes it is rather natural to consider the canonical transversal $\mathcal{T}_{\mathrm{can}}$ which consists of all minimal (maximal) representatives of the orbits with respect to a certain lexicographical ordering of the connection sets. Let us illustrate this scheme on a simple example. In more detail, this scheme will be presented in [FieK9x].

4.12. Example. Let $n = 9$. We want to enumerate constructively all circulants of valency 2. We have altogether $\binom{8}{2} = 28$ 2-element connection sets. We list ${}_2C(\mathfrak{S}_i)$ and ${}_2\mathcal{T}_{\mathrm{can}}(\mathfrak{S}_i)$ (the

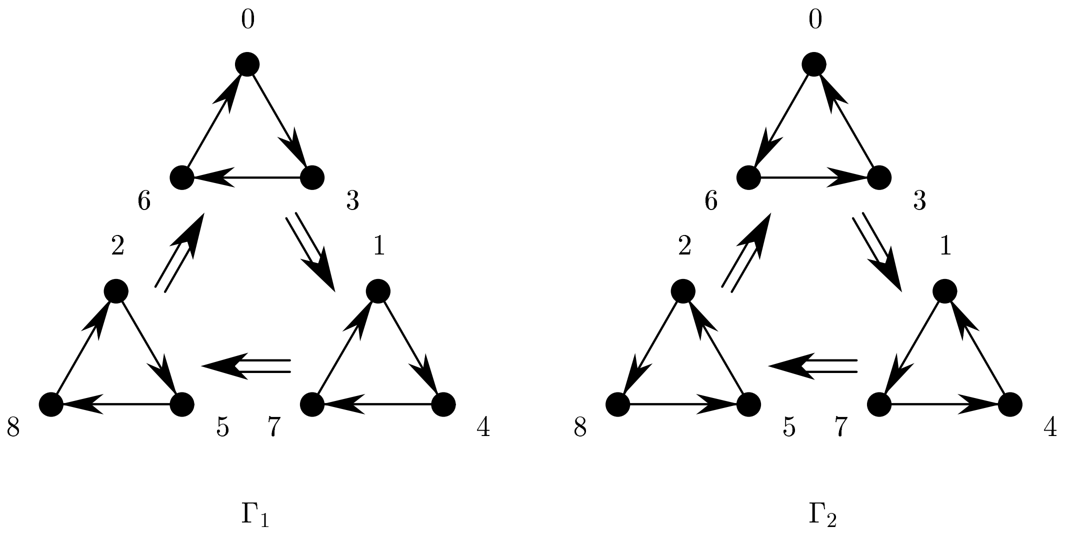


Figure 1: Isomorphic but not one-multiplier isomorphic circulants

left subscript represents the valency under consideration, the numeration of S-rings is the same as in Example 4.9).

$$\begin{array}{llll}
{}_2C(\mathfrak{S}_1) = \emptyset, & & & \\
{}_2C(\mathfrak{S}_2) = \{\{3,6\}\}, & & {}_2\mathcal{T}\mathrm{can}(\mathfrak{S}_2) = \{\{3,6\}\}, & \\
{}_2C(\mathfrak{S}_3) = \emptyset, & & & \\
{}_2C(\mathfrak{S}_4) = \emptyset, & & & \\
{}_2C(\mathfrak{S}_6) = \{\{1,8\},\{2,7\},\{3,6\}\}, & & {}_2\mathcal{T}\mathrm{can}(\mathfrak{S}_6) = \{\{1,8\}\}, &
\end{array}$$

${}_2C(\mathfrak{S}_7)$ consists of 24 representatives, on which the cyclic group $\mathbb{Z}_9^*$ of order 6 acts semiregularly. Therefore we easily get that

$${}_2\mathcal{T}\mathrm{can}(\mathfrak{S}_6) = \{\{1,2\},\{1,3\},\{1,4\},\{1,6\}\}.$$

Finally, we get a canonical transversal ${}_2\mathcal{T}\mathrm{can}(\mathbb{Z}_9)$ of all circulants of valency 2:

$${}_2\mathcal{T}\mathrm{can}(\mathbb{Z}_9) = {}_2\mathcal{T}\mathrm{can}(\mathfrak{S}_2) \cup {}_2\mathcal{T}\mathrm{can}(\mathfrak{S}_6) \cup {}_2\mathcal{T}\mathrm{can}(\mathfrak{S}_7).$$

(C) From structural to multiplier approach

We would now like to outline the multiplier approach (which will be given in more detail and greater rigour in the three subsequent sections). Our goal will be to obtain the generating functions $g(n,x)$ and $\widetilde{g}(n,x)$ without direct use of the lattice $\mathcal{L}_n$ as well as without explicit computation of the functions $g_i(x)$ and $\widetilde{g}_i(x)$ for all elements $\mathfrak{S}_i \in \mathcal{L}_n$. It turns out that the complexity of such an approach will heavily depend on the "multiplicative complexity" of n: for example, the simplest description will be available for prime numbers.

The multiplier approach is based on the use of necessary and sufficient conditions for the isomorphism of two circulant graphs. These conditions are formulated in terms of the action of multiplier groups on the connection sets of circulants. The action $(\mathbf{M}_1)$ defined in Lemma 2.8, and justified by Corollary 4.3, is the simplest (and most well-known) case in which the multiplier approach is most efficient.

4.13. Example. Let $n = 13$ (cf. Example 4.4). We know that for $n = 13$ the conjecture $\mathbf{A}(13)$ is valid, i.e. we are able to use the (single-)multiplier approach. This means that the number of non-isomorphic circulants is equal to the number of orbits of the action of $\mathbb{Z}_{13}^*$ on the set of all connection sets. Hence it is enough to find the cycle index $I_{\mathbb{Z}_{13}^*}(\mathbf{x})$ of the group $\mathbb{Z}_{13}^*$ in its regular action and then to apply the ordinary Pólya enumeration theorem. Thus we get

$$I_{\mathbb{Z}_{13}^*}(\mathbf{x}) = \frac{1}{12}(x_1^{12} + x_2^6 + 2x_3^4 + 2x_4^3 + 2x_6^2 + 4x_{12})$$

and therefore

$$\widetilde{g}(13,1) = I_{\mathbb{Z}_{13}^*}(2) = \frac{1}{12}(2^{12} + 2^6 + 2 \cdot 2^4 + 2 \cdot 2^3 + 2 \cdot 2^2 + 4 \cdot 2) = 352.$$

In the same manner we use

$$I_{\mathbb{Z}_6^*}(\mathbf{x}) = \frac{1}{6}(x_1^6 + x_2^3 + 2x_3^2 + 2x_6)$$

and obtain

$$g(13,1) = \frac{1}{6}(2^6 + 2^3 + 2 \cdot 2^2 + 2 \cdot 2) = 14.$$

We strongly encourage the reader to compare the results of the structural and multiplier approach (cf. Example 4.4).

4.14. Explanation. We may distinguish two different manners of substantiation for the multiplier approach in the case $n = p$, p a prime.

The first manner is directly based on Corollary 4.3. In our exposition we derived it as a consequence of S-ring theory. But, in principle, one could give another proof which is absolutely independent of S-ring theory, see, e.g., [Djo70].

The other manner may be called *"explanation"*. Namely, based on S-ring theory, we get a complete list of the automorphism groups of circulant graphs with p vertices. The lattice of all these groups is isomorphic to the lattice of all subgroups in the group $\mathbb{Z}_p^*$. For each group G in the former lattice, its index in the normalizer $N_{S_p}(G)$ coincides with the index of the corresponding normalizer in the latter lattice. Thus, according to Theorem 3.5, the enumeration of circulant graphs with p vertices will correspond to the enumeration of subsets of $\mathbb{Z}_n^*$ with respect to the group action $(\mathbb{Z}_n^*, \mathbb{Z}_n^*)$. In this case, the procedure described in Theorem 3.5 is equivalent to the method of Möbius inversion applied to the group $(\mathbb{Z}_n^*, \mathbb{Z}_n^*)$. Thus, the structural approach here serves as a tool for "explaining" the multiplier approach.

However, in the general case in which $\mathbf{A}(n)$ is true (see 2.11), we are still not able to deliver a similar simple structural "explanation" of the multiplier approach – even in spite of the fact that all S-rings over $\mathbb{Z}_n$, where n is a square-free number, are completely classified (see [Muz9x]).

For $n = p^2$, as shown above, $\mathbf{A}(n)$ is no longer valid. However, we shall see in this case that the main idea of the multiplier approach will again have an unambiguous advantage over the structural approach. On the other hand, the multiplier approach is based on the corresponding isomorphism theorem, which, in turn, can be obtained by S-ring theory as was done above in the case $n = p$ (see 4.3).

The result we need is the following:

4.15. Isomorphism Theorem for p^2-circulants. *Two circulant graphs $\Gamma = \Gamma(X)$ and $\Gamma' = \Gamma(X')$ with $n = p^2$ vertices are isomorphic if and only if their respective layers (as defined in* 2.12*) are multiplicatively equivalent, i.e.*

$$X'_{(0)} = m_0 X_{(0)}, \quad X'_{(1)} = m_1 X_{(1)}, \tag{$\mathbf{M}_2$}$$

for a pair of multipliers $m_0, m_1 \in Z^*_{p^2}$. Moreover, in the above, one must have

$$m_0 = m_1, \tag{$\mathbf{E}$}$$

whenever

$$(1+p)X_{(0)} \neq X_{(0)}. \tag{$\mathbf{R}$}$$

This theorem was obtained for the first time in [KliP78] in a slightly more detailed form that specifies additional exceptional cases when both multipliers can be chosen to be equal (a sufficient condition) independent of the relation ($\mathbf{R}$). But for the purpose of enumeration, these cases need not be considered separately.

4.16. Remark. In ($\mathbf{M}_2$) above we may assume $m_0 \in \mathbb{Z}^*_p$. The multiplier $1+p$ leaves fixed any multiple of p because $(1+p)pr \equiv pr \pmod{p^2}$ for any r. Hence the 1-layer $X_{(1)}$ of any p^2-circulant is $(1+p)$-invariant (i.e. invariant under the multiplicative action of $(1+p)$).

4.17. Examples. The following two simple examples of pairs of p^2-vertex circulants for $p = 3$ illustrate the sufficiency and necessity of the Isomorphism Theorem 4.15.

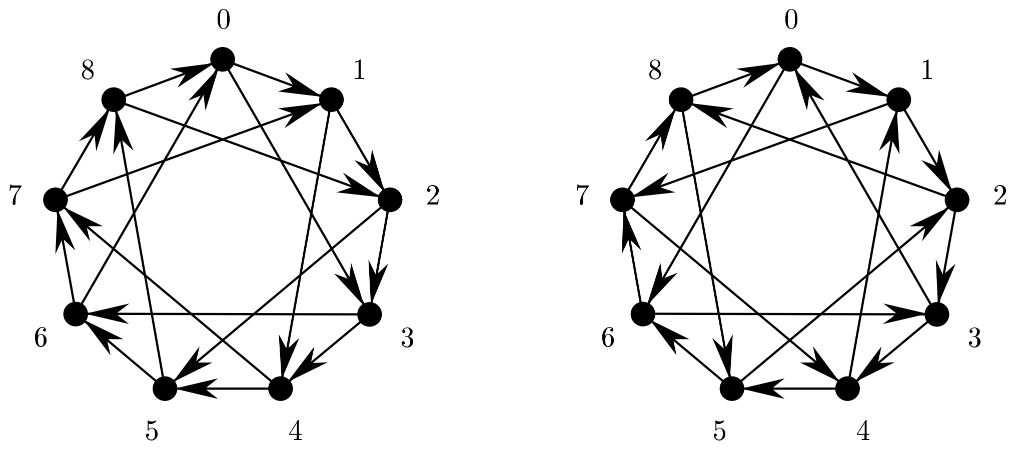
Take, e.g., the circulants of order 9 from Fig. 1 with the connection sets $X = \{1,3,4,7\}$ and $X' = \{1,6,4,7\}$. As mentioned in 4.10, no multiplier transforms X into X'. Here we have $X_{(0)} = \{1,4,7\} = X'_{(0)}$, $X_{(1)} = \{3\}$ and $X'_{(1)} = \{6\}$. Condition ($\mathbf{R}$) does *not* hold since $(1+3)X_{(0)} = X_{(0)}$. So by Theorem 4.15 we may use two arbitrary multipliers in ($\mathbf{M}_2$). In fact, the pair $m_0 = 1$ and $m_1 = 2$ yields the required equivalence of the layers, so that $\Gamma(X') \cong \Gamma(X)$, in agreement with 4.10.

On the other hand, let $n = 9$, $X = \{1,3\}$ and $X' = \{1,6\}$. Here again the pair $m_0 = 1$ and $m_1 = 2$ yield a multiplicative layer-wise equivalence. But this pair violates the requirement of Theorem 4.15 because $(1+3)X_{(0)} \neq X_{(0)}$. For no m does the equality $mX' = X$ hold; thus, the circulants $\Gamma' = \Gamma(X')$ and $\Gamma = \Gamma(X)$ are *not* isomorphic. This can be seen directly because, e.g., Γ' contains directed 4-cycles, for example, $(0,1,2,3)$ (see Fig. 2) but Γ possesses no such cycle. (Indeed, observe the latter claim "visually" or try to find a solution of equation $x_1 + x_2 + x_3 + x_4 = 0$ in $\mathbb{Z}_9$ where $x_i \in \{1,3\}$.)

4.18. 9-Circulants. Finally, let us try to outline, only for the concrete case $n = 9$, the multiplier approach in terms of our previous knowledge (in more general frames, the example will be reconsidered in Section 7).

The multiplicative group $(\mathbb{Z}^*_9, \mathbb{Z}_9)$ is generated by permutation $h_0 = (0)(1,2,4,8,7,5)(3,6)$. This group acts intransitively on the set $\Omega = \mathbb{Z}'_9$ with two orbits $\Omega_0 = \{1,2,4,5,7,8\}$ and $\Omega_1 = \{3,6\}$. Counting orbits of the induced action of $(\mathbb{Z}^*_9, \mathbb{Z}'_9)$ on the set 2^Ω of all subsets of Ω we get the number of one-multiplier equivalent directed circulants. This number may be obtained by the application of Pólya's method to the cyclic index $\mathcal{A} = I_{(\mathbb{Z}^*_9, \Omega)}$.

However, we know that the result of enumeration will include more than the desired number of isomorphism classes. Therefore let us subtract from this result the number of all classes which correspond to the "abnormal" (cf. 4.10) S-ring $\mathfrak{S}_5$. These classes are exactly those which are invariant with respect to the cyclic group $H = \langle h \rangle$ generated by the permutation $h = h_0^2 = (1,4,7)(2,8,5)(3)(6)$. Finally, on these classes we have to consider the action



Γ Γ'

Figure 2: Non-isomorphic circulant 9-graphs of valency 2

of the more "strong" (non-faithful) group $\mathbb{Z}_9^* \times \mathbb{Z}_9^*$ where each copy of $\mathbb{Z}_9^*$ acts *independently* on the sets Ω_0 and Ω_1 (a two-multiplier action).

The number of classes being "subtracted" can be obtained via the cycle index $\mathcal{B} = I_{(\mathbf{Z}_2, \mathcal{O})}$ where $\mathbb{Z}_2$ acts semi-regularly on the four-element set $\mathcal{O}$ of orbits of H. The final "addition" of the number of classes can be obtained via the cyclic index $\mathcal{D} = I_{(\mathbf{Z}_2 \times \mathbf{Z}_2, \mathcal{O})}$ where $\mathbb{Z}_2 \times \mathbb{Z}_2$ acts intransitively on the same set $\mathcal{O}$.

Hence we get

$$\begin{aligned}
\mathcal{A} &= \frac{1}{6}(x_1^8 + x_2^4 + 2x_1^2x_3^2 + 2x_2x_5), \\
\mathcal{B} &= \frac{1}{2}(x_1^4 + x_2^2), \\
\mathcal{D} &= \frac{1}{4}(x_1^4 + 2x_1^2x_2 + x_2^2).
\end{aligned}$$

Therefore

$$\begin{aligned}
\widetilde{g}(9,1) &= \mathcal{A}|_{\{x_i:=2\}_{i=1,2,\ldots}} - \mathcal{B}|_{\{x_i:=2\}_{i=1,2,\ldots}} + \mathcal{D}|_{\{x_i:=2\}_{i=1,2,\ldots}} \\
&= \frac{1}{6}(2^8 + 2^4 + 2 \cdot 2^4 + 2 \cdot 2^2) - \frac{1}{2}(2^4 + 2^2) + \frac{1}{4}(2^4 + 2 \cdot 2^3 + 2^2) \\
&= 52 - 10 + 9 = 51.
\end{aligned}$$

So, we obtain the same number as in Example 4.9.

We would like to stress that this example shows only the main features of the multiplier approach. Numerous technical difficulties related to its complete realization will be overcome in Section 7 where, in particular, we will return once more to the same case $n = 9$.

5 The multiplier approach: additional definitions

The multiplier approach for counting circulant graphs is based on the isomorphism theorems (see 4.3 and 4.15) and on the ordinary Pólya enumeration technique (see, e.g. [KliPR88, Ch. 2] and [Ker91, Ch. 1 and 2]). It results in closed formulae expressed in terms of cycle indices of the appropriate group actions. Due to the use of multivariable polynomials, these counting formulae can be presented in technically different forms and can be obtained simultaneously and uniformly (with only a few additional efforts) for several natural classes of circulant graphs. For this reason, it is convenient to introduce new unified notations different from ones used in the preceding sections.

The formulae obtained will enable us to reveal some interesting interrelations between the numbers of circulants of various types. In particular, we shall analyse the behaviour of the difference between the actual number of non-isomorphic undirected p^2-circulants and the number of them considered up to the equivalence under the action of the regular cyclic group (i.e. the number obtained under the Ádám condition). This difference turns out to vanish for the majority of vertex valencies.

5.1. Faithful action. Let $G = (\mathbf{G}, U)$ be a group with an action, and $\overline{G} = (\overline{\mathbf{G}}, U)$ the corresponding faithful permutation group: i.e. $\overline{\mathbf{G}} = \mathbf{G}/\mathbf{K}$ where $\mathbf{K} = \{k \in \mathbf{G} \mid \forall u \in U : u^k = u\}$ and the action of $\overline{G}$ on U is induced from that of $\mathbf{G}$ on U via $u^{\overline{g}} = u^g$ for $\overline{g} = \mathbf{K}g$. Then we have:

5.2. Lemma. $I_G = I_{\overline{G}}$.

PROOF. $I_G = \frac{1}{|G|} \sum\limits_{g \in G} \prod\limits_{i \geq 1} x_i^{a_i(g)} = \frac{1}{|G|} \sum\limits_{k \in K} \sum\limits_{\overline{g} \in \overline{G}} \prod\limits_{i \geq 1} x_i^{a_i(k\overline{g})}$
$= \frac{1}{|G|} \sum\limits_{\overline{g} \in \overline{G}} \sum\limits_{k \in K} \prod\limits_{i \geq 1} x_i^{a_i(\overline{g})} = \frac{1}{|G|} \sum\limits_{\overline{g} \in \overline{G}} |K| \prod\limits_{i \geq 1} x_i^{a_i(\overline{g})} = I_{\overline{G}}$. □

Thus, in spite of the perceived differences in the numbers of terms by definition, both polynomials in fact coincide. Therefore the conversion to the faithful action provides *no* analytical and computational advantages. This implicitly well-known and useful property will be sometimes referred to as the *Indifference Lemma*.

5.3. Cycle indices of cyclic groups. For the regular cyclic group $Z(n) = (\mathbb{Z}_n, \mathbb{Z}_n)$ it is easy to see that

$$I_{Z(n)} = \frac{1}{n} \sum_{i=1}^{n} x_{[i,n]/i}^{(i,n)} \tag{5.3.1}$$

where (i, n) and $[i, n]$ denote the g.c.d. and l.c.m., respectively. It follows (cf. [Ker91, p. 72]) that

$$I_{Z(n)} = \frac{1}{n} \sum_{r|n} \phi(r) x_r^{n/r} \tag{5.3.2}$$

since $\phi(r)$ enumerates the exponents $i,\ i \leq n$, with $(i, n) = n/r$.

Denote for brevity

$$\mathcal{I}_n(\mathbf{x}) := I_{Z(n)}(\mathbf{x}). \tag{5.3.3}$$

In particular for $n = p$ prime, $I_{\mathbf{Z}_p^*} = \mathcal{I}_{p-1}(\mathbf{x}) = \frac{1}{p-1} \sum\limits_{r|p-1} \phi(r) x_r^{(p-1)/r}$.

Given $s|n$, the cyclic group $\mathbb{Z}_s$ is a subgroup of $\mathbb{Z}_n$ and we may consider $\mathbb{Z}_n$ as acting (additively mod s) on $\mathbb{Z}_s$. Let $Z(n, s)$ denote this group action. In particular, $Z(n, n) = Z(n)$.

Then by the Indifference Lemma 5.2,

$$I_{Z(n,s)} = I_{Z(s)}, \quad s|n. \tag{5.3.4}$$

For the dihedral permutation group $D(n)$ with odd n we have (see [Ker91, p. 72]):

$$I_{D(n)} = \tfrac{1}{2}(I_{Z(n)} + x_1 x_2^{(n-1)/2}). \tag{5.3.5}$$

5.4. Operations with cycle indices. Working with cycle indices of groups acting on sets of complicated objects it is sometimes very convenient to use variables of several different types (cf. [Rob81]). In particular, we shall use cycle indices not only in variables $\mathbf{x}$ but also in $\mathbf{y}$ and even in $\mathbf{xy}$ where $\mathbf{x}$ (resp., $\mathbf{y}$) is the generic notation for the sequences of variables $x_1, x_2, \ldots, x_n$ (resp., $y_1, y_2, \ldots, y_n$) and $\mathbf{xy}$ denotes all pairwise products $x_1y_1, x_2y_2, \ldots, x_ny_n$.

For our aims, only actions of cyclic groups and groups built from them by means of the operations defined in 2.3 are necessary. The corresponding cycle indices are built according to the following lemma.

5.5. Lemma. *Let groups G, H, G_1 and G_2 be as considered in* 2.3, *then*

$$I_{G\oplus H} = I_G \cdot I_H \tag{5.5.1}$$

and

$$I_{G_1 \dot\vee G_2}(\mathbf{x}, \mathbf{y}) = I_{G_1}(\mathbf{x}) \dot\vee I_{G_2}(\mathbf{y}) \tag{5.5.2}$$

where

$$I_{G_1}(\mathbf{x}) \dot\vee I_{G_2}(\mathbf{y}) := \frac{1}{|G|} \sum_{g\in G} \prod_{i\geq 1} x_i^{a_i(g,U)} y_i^{a_i(g,V)}. \tag{5.5.3}$$

PROOF. The first formula is well known, see [Ker91, p. 74]. Formula (5.5.2) is evident by definition. □

5.6. Remark. The operation "$\dot\vee$" for cycle indices as defined by (5.5.3) depends *not only* on the polynomials by themselves but also on the underlying group $\mathbf{G}$ (cf. 2.3), namely on the correspondence of terms in both cycle indices to the same element $g \in \mathbf{G}$. For cyclic groups the result can be obtained in almost straightforward fasion based on (5.3.1). In general, the cycle index of an action of an arbitrary cyclic group is calculated by the cyclic structure of the generating permutation, though the formula can look combersome. Here is a particular case, used subsequently. Let $n = ps$, p prime, $(p, s) = 1$. Then taking into account (5.3.4) we get

$$I_{Z(ps,s)}(\mathbf{x}) \dot\vee I_{Z(ps)}(\mathbf{y}) = \frac{1}{ps}\Big(\sum_{r|s}(p-1)\phi(r) x_r^{s/r} y_{pr}^{s/r} + \sum_{r|s} \phi(r) x_r^{s/r} y_r^{ps/r}\Big). \tag{5.6.1}$$

5.7. Tournaments and self-complementary graphs. A *tournament* means a complete anti-symmetric graph, i.e. a directed graph in which for any pair of different vertices u, v there is exactly one edge connecting them: (u, v) or (v, u).

Two graphs on the same set of vertices are called *complements* of each other if they contain no edge in common but every possible edge belongs to one of them. In particular, the complete and null graphs are complements of one another.

The *converse* of a graph Γ means the graph defined on the same set of vertices and consisting of edges (v, u) such that $(u, v) \in E(\Gamma)$.

A *self-complementary* graph means a graph isomorphic to its complement.

A *self-converse* graph means a graph isomorphic to its converse. In particular, all undirected graphs are examples of self-converse graphs (with respect to the identity isomorphism). For tournaments this notion coincides with that of self-complementary tournament.

Self-complementary and self-converse graphs possess additional symmetries and are therefore interesting for consideration and enumeration (cf. [Sri70], [Rob81] and [PalR84]).

The connection set X of any circulant n-tournament satisfies the conditions $X \cap (-X) = \emptyset$ and $X \cup (-X) = \mathbb{Z}'_n$. Conversely, any X that meets these two conditions represents a circulant n-tournament.

The complement of a circulant $\Gamma(X)$ is the circulant $\Gamma(\mathbb{Z}'_n \setminus X)$, and its converse is the circulant $\Gamma(-X)$.

It is clear that a circulant n-tournament can exist only for odd n, in which case it is a regular anti-symmetric graph of valency $r = |X| = (n-1)/2$. Self-complementary graphs also exist only for odd n and are of valency $r = (n-1)/2$. Moreover, undirected self-complementary n-graphs can exist only if $4|(n-1)$ since they contain $n(n-1)/4$ edges. Note, finally, that an undirected regular graph of valency r contains $rn/2$ edges, so that r and n cannot be odd simultaneously.

5.8. Proposition. *Any circulant graph is self-converse. In particular, any circulant tournament is self-complementary.*

PROOF. This is simply the case $m = -1$ in the condition $(\mathbf{M}_1)$ of Lemma 2.8. □

5.9. Numbers of circulants: new notations. We are interested in counting several types of circulant graphs. For convenience, the type will be designated in the subscript. Henceforth:

$C_{\mathrm{d}}(n)$ denotes the number of non-isomorphic (**d**irected) circulant n-graphs;

$C_{\mathrm{u}}(n)$ denotes the number of non-isomorphic **u**ndirected circulant n-graphs;

$C_{\mathrm{t}}(n)$ denotes the number of non-isomorphic circulant n-**t**ournaments;

$C_{\mathrm{sd}}(n)$ and $C_{\mathrm{su}}(n)$ denote the numbers of non-isomorphic **s**elf-complementary **d**irected and **u**ndirected circulant graphs respectively;

$C_{\mathrm{d}}(n,r)$ and $C_{\mathrm{u}}(n,r)$ denote the corresponding numbers of (regular) circulants of valency r and $c_{\mathrm{d}}(n,t)$ and $c_{\mathrm{u}}(n,t)$ are their ordinary generating functions (polynomials in the variable t):

$$c_{\mathrm{d}}(n,t) := \sum_{r \geq 0} C_{\mathrm{d}}(n,r)t^r \quad \text{and} \quad c_{\mathrm{u}}(n,t) := \sum_{r \geq 0} C_{\mathrm{u}}(n,r)t^r.$$

Clearly $C_{\mathrm{d}}(n) = c_{\mathrm{d}}(n,1)$ and $C_{\mathrm{u}}(n) = c_{\mathrm{u}}(n,1)$. The functions c_{d} and c_{u} can also be extended to multigraphs (cf. [Zha90]).

6 Enumeration based on isomorphism theorems

As a preliminary step we provide here enumerative formulae for all the classes of circulant graphs of prime order. These results are not new but seem to have never been presented in such a unified and simplified manner.

Lemma 2.8 and the validity of Ádám's conjecture for this case imply important consequences for our enumeration.

6.1. Corollary. *If the conjecture* $\mathbf{A}(n)$ *is valid for a given order* n *and a given set of* n*-circulants, then the number of non-isomorphic circulants under consideration is equal to the number of orbits of the group* $\mathbb{Z}^*_n$ *in its induced multiplicative action on the connection sets.* □

6.2. Orbit enumeration. Counting orbits under group actions in the framework of Pólya's theory consists of two principal tasks:

- to describe carefully the group and its action on the objects and to construct its cycle index;
- to find an appropriate substitution of variables, to execute it and to simplify the result as much as possible.

In general, the structure of the multiplicative group $\mathbb{Z}_n^*$ is well known and rather simple. So, it remains only to induce its action on the connection sets and to apply, whenever possible, ordinary Pólya's theorem of counting. All enumerative results for circulants that have been published so far obtained in exactly this way.

We shall not apply here the above corollary in such general form (in principle, this could be done for all square-free orders) restricting ourselves to the simplest case of prime $n = p$.

6.3. Count of p-circulants. Once the cycle index I_G of a group action on a set has been constructed, it is a simple matter to count the non-isomorphic subsets with respect to the induced element-wise action on them. This is just our case for directed circulant graphs according to Corollary 6.1. By Pólya's theorem (cf. [KliPR88, 2.2], [Ker91, p. 71] or [PalR84]), the counting polynomial in t is expressed as $I_G|_{\{x_r:=1+t^r\}_{r=1,2,\ldots}}$ where r denotes the valency. The overall number of non-isomorphic sets is obtained by substituting $t := 1$ or, in other words, $x_r := 2$ for all r. In the latter case we could, instead, reason equally well in terms of Burnside's lemma (also called the lemma of Cauchy–Frobenius–Burnside [KliPR88, 2.1]; see also [Ker91, p. 11]). For the problem under consideration, this means to count the connection sets invariant with respect to a multiplier of a given order r.

Applied to the polynomial $\mathcal{I}_{p-1}(\mathbf{x})$ as defined in (5.3.3), this yields the desired result for $C_{\mathrm{d}}(p,r), c_{\mathrm{d}}(p,t)$ and $C_{\mathrm{d}}(p)$. Note that the size $r = |X|$ equals the valency of $\Gamma(X)$.

Other desired numbers of directed circulant graphs can be obtained from *the same* cycle index through appropriate substitutions. Again, the conventional enumerative technique is applicable to this end. As we know from 5.7, the self-complementary circulants are described by the self-complementary connection sets, i.e., by those X for which $mX = \mathbb{Z}_n' \setminus X$ for some m. As is well known in general (see [PalR84] or [Ker91, p. 73]), the number of such self-complementary sets is obtained by substituting $x_{2i} := 2$ and $x_{2i-1} := 0$ for all i (or, in other words, $t := -1$ in the above substitution). In our case this means that we simply exclude the monomials containing variables with *odd* indices. This approach yields, evidently, simpler explicit expressions than ones appeared in [ChaW82] and [ChiL86].

No tournament possesses an automorphism of *even* order. This follows from consideration of edges between the opposite vertices of a cycle c of even order: any c-invariant graph must contain either all of these in both directions or none. This contradicts the definition of tournaments. Thus, contrary to the previous case, we must exclude the *even*-index variables. Besides, the other members possess only a half degree of freedom. In other words, we put $x_{2i} := 0$ and $x_{2i-1}^2 := 2$ (i.e. $x_{2i-1} := \sqrt{2}$) for all i. Due to this, many summands vanish; cf. [Ast72] and [Ray91] for details.

Undirected circulant graphs can be counted with the help of a different permutation group than one used for directed circulants (though, in principle, we could use the same group). This is the dihedral group (cf. formula (5.3.5) for the corresponding cycle index). But undirected circulant graphs can be encoded by reduced connection sets as described in 2.7 (cf. also Remark 2.9). Therefore there is also another more customary way to use the modified *"halved"* permutation group, i.e. the subgroup of index 2 in $(\mathbb{Z}_p^*, \mathbb{Z}_p^*) = Z(p-1)$. It is simply $Z(\frac{p-1}{2})$ (cf. [Tur67]) with the cycle index $\mathcal{I}_{\frac{p-1}{2}}(\mathbf{x})$.

Ordinary Pólya substitutions $x_r := 1 + t^{2r}$ for all r applied to $\mathcal{I}_{\frac{p-1}{2}}(\mathbf{x})$ give rise to $c_{\mathrm{u}}(p,t)$ while the substitutions $x_{2i} := 2$ and $x_{2i-1} := 0$ (or, equivalently, the subsequent substitution $t^2 := -1$ after Pólya's one) give rise to $C_{\mathrm{su}}(p)$ as above. Here $2r$ in the exponent of t reflects the fact that any undirected edge consists of two edges and contributes 2 to the valency (and the valency of $\Gamma(X)$ equals $2|X^{\mathrm{red}}|$ where $X^{\mathrm{red}} \subseteq \mathbb{Z}'_{\frac{p-1}{2}}$).

Thus, we have proved the following

6.4. Theorem. *For $n = p$ an odd prime,*

$$\begin{aligned}
c_{\mathrm{d}}(p,t) &= \mathcal{I}_{p-1}(\mathbf{x})|_{\{x_r:=1+t^r\}_{r=1,2,\dots}}\\
c_{\mathrm{u}}(p,t) &= \mathcal{I}_{\frac{p-1}{2}}(\mathbf{x})|_{\{x_r:=1+t^{2r}\}_{r=1,2,\dots}}\\
C_{\mathrm{t}}(p) &= \mathcal{I}_{p-1}(\mathbf{x})|_{\{x_r:=0\}_{r\ \mathrm{even}},\ \{x_r^2:=2\}_{r\ \mathrm{odd}}}\\
C_{\mathrm{sd}}(p) &= \mathcal{I}_{p-1}(\mathbf{x})|_{\{x_r:=0\}_{r\ \mathrm{odd}},\ \{x_r:=2\}_{r\ \mathrm{even}}}\\
C_{\mathrm{su}}(p) &= \mathcal{I}_{\frac{p-1}{2}}(\mathbf{x})|_{\{x_r:=0\}_{r\ \mathrm{odd}},\ \{x_r:=2\}_{r\ \mathrm{even}}}.
\end{aligned}$$

These formulae cover numerous counting results published in [Dav65], [Tur67], [Als70], [Ast72], [Dav72], [Als73], [ChaW73], [ChiL86], [Zha90] and [Ray91].

6.5. Corollary. *If p is a prime number such that $q = 2p - 1$ is also prime, then*

$$c_{\mathrm{u}}(2p-1,t) = c_{\mathrm{d}}(p,t^2)$$

and

$$C_{\mathrm{su}}(2p-1) = C_{\mathrm{sd}}(p).$$

(The first four such primes are $p = 3, 7, 19, 31, \dots$ with corresponding $q = 5, 13, 37, 61, \dots$)

Proof. Indeed, substitute $q = 2p - 1$ instead of p in the second and last formulae above. □

7 Count of p^2-circulants

7.1. Outline. By Isomorphism Theorem 4.15, p^2-circulants can be counted in the following way. Count first their connection sets up to single-multiplier actions. Let $A(p^2)$ denote the corresponding number. According to the condition (**R**) (cf. also Remark 4.16), this count does not accurately reflect the true number of $(1+p)$-invariant connection sets. Let their number, thus calculated, be equal to $B(p^2)$. Instead, here we must use the group $\mathbb{Z}^*_{p^2} \oplus \mathbb{Z}^*_{p^2}$ with the induced layer-wise action on such connection sets. Let $D(p^2)$ denote the number of its orbits. Let, finally, $C(p^2)$ be the required number of non-isomorphic circulants; these are *generic* designations of all types of circulants under consideration. Then $C(p^2) = A(p^2) - B(p^2) + D(p^2)$ or, specifically,

$$C_{\mathrm{h}}(p^2) = A_{\mathrm{h}}(p^2) - B_{\mathrm{h}}(p^2) + D_{\mathrm{h}}(p^2) \qquad (7.1.1)$$

where $\mathrm{h} \in \{\mathrm{d}, \mathrm{t}, \mathrm{u}, \mathrm{sd}, \mathrm{su}\}$ (cf. 5.9) and $c_{\mathrm{h}}(p^2,t) = a_{\mathrm{h}}(p^2,t) - b_{\mathrm{h}}(p^2,t) + d_{\mathrm{h}}(p^2,t)$ where $\mathrm{h} \in \{\mathrm{d}, \mathrm{u}\}$, $A_{\mathrm{d}}(p^2) = a_{\mathrm{d}}(p^2,t)|_{t=1}$, etc.

$A_{\mathrm{d}}(p^2)$ and $a_{\mathrm{d}}(p^2,t)$ can be found in the same way as described in 6.2: the corresponding group action is the join of two actions of the cyclic group $\mathbb{Z}^*_{p^2}$:

$$(\mathbb{Z}^*_{p^2}, \mathbb{Z}'_{p^2}) = (\mathbb{Z}^*_{p^2}, \mathbb{Z}^*_p)\dot{\vee}(\mathbb{Z}^*_{p^2}, \mathbb{Z}^*_{p^2}).$$

According to formula (5.6.1) (with $s = p - 1$), we introduce

$$\mathcal{A}_1(p^2;\mathbf{x},\mathbf{y}) := \frac{1}{p}\sum_{r|p-1}\phi(r)(x_r y_{pr})^{\frac{p-1}{r}} + \frac{1}{p(p-1)}\sum_{r|p-1}\phi(r)(x_r y_r^p)^{\frac{p-1}{r}} \tag{7.1.2}$$

and via this, $a_{\mathrm{d}}(p^2,t)$ is expressed by the "standard" Pólya substitutions:

$$x_r := 1+t^r,\ y_r := 1+t^r.$$

7.2. Remark. As for the numbers $B(p^2)$ and $D(p^2)$, there is a general approach proposed by N. G. de Bruijn (cf. [Rob81]) to enumerate the group orbits on elements invariant with respect to a normal subgroup. On the other hand, the following specific property of cyclic groups can be taken into account in the case of $B(p^2)$. We need to count circulants invariant with respect to the group $\langle 1+p, m\rangle$ generated by $1+p$ and m, for each multiplier m. But in our case it is again a certain *cyclic* group generated, say, by m'. This means that $B(p^2)$ is the sum of certain summands of $A(p^2)$, which we could simply try to distinguish and eliminate from (7.1.2). (By Lemma 2.14, if $m = w^i(1+p)^j$, then we may take $m' = w^i(1+p)$.) However, we need not use these possibilities; so that we shall proceed in a more direct way.

7.3. Enumerative formulae. According to Remark 4.16, any set of p-fold numbers is $(1+p)$-invariant. On the other hand, the rows of the matrix $M(p,2,w)$ in Lemma 2.14 represent minimal $(1+p)$-invariant sets (orbits) of numbers prime to p. As we have seen in 2.13, these rows are in a natural one-to-one correspondence with the numbers $1,2,\ldots,p-1$. Thus, in the corresponding join, the member $(\mathbb{Z}^*_{p^2},\mathbb{Z}^*_{p^2})$ should be replaced by one additional $(\mathbb{Z}^*_{p^2},\mathbb{Z}^*_{p})$. The only distinction is that each row of the matrix $M(p,2,w)$ now contributes p edges instead of 1. (This explains why we used separated variables $\{x_r\}$ and $\{y_r\}$; so that in the case of $c_{\mathrm{d}}(n,t)$, the substitutions $x_r := 1+t^r$ and $y_r := 1+t^{pr}$ for all r, $r|(p-1)$, are carried out.) Thus, for expressing $B(p^2)$ we get the cycle index $\mathcal{B}(p^2;\mathbf{x},\mathbf{y}) = I_{(\mathbf{Z}^*_{p^2},\mathbf{Z}^*_p)}(\mathbf{x})\dot{\vee} I_{(\mathbf{Z}^*_{p^2},\mathbf{Z}^*_p)}(\mathbf{y})$ so that

$$\mathcal{B}(p^2;\mathbf{x},\mathbf{y}) := \frac{1}{p-1}\sum_{r|p-1}\phi(r)x_r^{(p-1)/r}y_r^{(p-1)/r} = \mathcal{I}_{p-1}(\mathbf{xy}) \tag{7.3.1}$$

where $\mathbf{xy} = \{x_1y_1, x_2y_2, \ldots\}$ and $\mathcal{I}_{p-1}(\mathbf{x})$ is defined by (5.3.3).

The same considerations are valid for calculating $D(p^2)$ with the direct sum $\oplus$ instead of the join $\dot{\vee}$. According to formula (5.5.1), the corresponding cycle index $\mathcal{D}(p^2;\mathbf{x},\mathbf{y})$ is $I_{(\mathbf{Z}^*_{p^2},\mathbf{Z}^*_p)}(\mathbf{x}) \cdot I_{(\mathbf{Z}^*_{p^2},\mathbf{Z}^*_p)}(\mathbf{y})$ so that

$$\mathcal{D}(p^2;\mathbf{x},\mathbf{y}) = \mathcal{I}_{p-1}(\mathbf{x})\mathcal{I}_{p-1}(\mathbf{y}). \tag{7.3.2}$$

Finally, in order to unify the substitutions of variables, let us transform the polynomial $\mathcal{A}_1(p^2;\mathbf{x},\mathbf{y})$ as follows: in formula (7.1.2), replace all variables y_{pr} by y_r in the first sum and all y_r by x_r in the second sum. The polynomial thus obtained will be denoted by $\mathcal{A}(p^2;\mathbf{x},\mathbf{y})$. Then

$$\mathcal{A}(p^2;\mathbf{x},\mathbf{y}) = \tfrac{1}{p}\mathcal{I}_{p-1}(\mathbf{x}^{p+1}) + \tfrac{p-1}{p}\mathcal{I}_{p-1}(\mathbf{xy}), \tag{7.3.3}$$

and the polynomial $a_{\mathrm{d}}(p^2,t)$ is obtained from $\mathcal{A}(p^2;\mathbf{x},\mathbf{y})$ by our usual substitutions $x_r := 1+t^r$ and $y_r := 1+t^{pr}$, etc.

In accordance with (7.1.1), we introduce

$$\mathcal{C}(p^2;\mathbf{x},\mathbf{y}) := \mathcal{A}(p^2;\mathbf{x},\mathbf{y}) - \mathcal{B}(p^2;\mathbf{x},\mathbf{y}) + \mathcal{D}(p^2;\mathbf{x},\mathbf{y}).$$

Then by formulae (7.3.1) – (7.3.3) we obtain after elementary transformations,

$$\mathcal{C}(p^2;\mathbf{x},\mathbf{y}) = \tfrac{1}{p}\mathcal{I}_{p-1}(\mathbf{x}^{p+1}) - \tfrac{1}{p}\mathcal{I}_{p-1}(\mathbf{xy}) + \mathcal{I}_{p-1}(\mathbf{x})\mathcal{I}_{p-1}(\mathbf{y}). \tag{7.3.4}$$

It is easy to see that this, and previous polynomials, are also suitable for the two remaining classes of directed circulants.

For undirected circulants we need simply to replace $\mathcal{I}_{p-1}$ by $\mathcal{I}_{\frac{p-1}{2}}$, i.e. to take

$$\mathcal{C}^*(p^2;\mathbf{x},\mathbf{y}) := \tfrac{1}{p}\mathcal{I}_{\frac{p-1}{2}}(\mathbf{x}^{p+1}) - \tfrac{1}{p}\mathcal{I}_{\frac{p-1}{2}}(\mathbf{xy}) + \mathcal{I}_{\frac{p-1}{2}}(\mathbf{x})\mathcal{I}_{\frac{p-1}{2}}(\mathbf{y}). \tag{7.3.5}$$

It is sometimes useful to count A, B and D separately. For undirected circulants, this requires the same modifications applied to $\mathcal{A}, \mathcal{B}$ and $\mathcal{D}$, that is, we introduce

$$\mathcal{A}^*(p^2;\mathbf{x},\mathbf{y}) := \tfrac{1}{p}\mathcal{I}_{\frac{p-1}{2}}(\mathbf{x}^{p+1}) + \tfrac{p-1}{p}\mathcal{I}_{\frac{p-1}{2}}(\mathbf{xy}),$$

$$\mathcal{B}^*(p^2;\mathbf{x},\mathbf{y}) := \mathcal{I}_{\frac{p-1}{2}}(\mathbf{xy}),$$

and

$$\mathcal{D}^*(p^2;\mathbf{x},\mathbf{y}) := \mathcal{I}_{\frac{p-1}{2}}(\mathbf{x})\mathcal{I}_{\frac{p-1}{2}}(\mathbf{y}).$$

The appropriate substitutions of variables in all the cases are clear from the above reasoning and from the proof of Proposition 6.4. This completes the proof of the following main result:

7.4. Theorem.

$$\begin{aligned}
c_{\mathrm{d}}(p^2,t) &= \mathcal{C}(p^2;\mathbf{x},\mathbf{y})|_{\{x_r:=1+t^r,\ y_r:=1+t^{pr}\}_{r=1,2,\ldots}}\\
c_{\mathrm{u}}(p^2,t) &= \mathcal{C}^*(p^2;\mathbf{x},\mathbf{y})|_{\{x_r:=1+t^{2r},\ y_r:=1+t^{2pr}\}_{r=1,2,\ldots}}\\
C_{\mathrm{t}}(p^2) &= \mathcal{C}(p^2;\mathbf{x},\mathbf{y})|_{\{x_r:=0,\ y_r:=0\}_{r\ \mathrm{even}},\ \{x_r^2:=2,\ y_r^2:=2\}_{r\ \mathrm{odd}}}\\
C_{\mathrm{sd}}(p^2) &= \mathcal{C}(p^2;\mathbf{x},\mathbf{y})|_{\{x_r:=0,\ y_r:=0\}_{r\ \mathrm{odd}},\ \{x_r:=2,\ y_r:=2\}_{r\ \mathrm{even}}}\\
C_{\mathrm{su}}(p^2) &= \mathcal{C}^*(p^2;\mathbf{x},\mathbf{y})|_{\{x_r:=0,\ y_r:=0\}_{r\ \mathrm{odd}},\ \{x_r:=2,\ y_r:=2\}_{r\ \mathrm{even}}}
\end{aligned}$$

where polynomials $\mathcal{C}(p^2;\mathbf{x},\mathbf{y})$ and $\mathcal{C}^*(p^2;\mathbf{x},\mathbf{y})$ are defined by (7.3.4), (7.3.5) *and* (5.3.3). □

As we pointed out above, instead of these formulae, it is possible to make the corresponding substitutions into $\mathcal{A}, \mathcal{B}$ and $\mathcal{D}$ (or $\mathcal{A}^*, \mathcal{B}^*$ and $\mathcal{D}^*$ for undirected circulants) and then to use expression (7.1.1).

In fact, we need to make a distinction between x_r and y_r only in the first two formulae. Accordingly, the last three formulae can be simplified further (see below). Besides, we could reduce all expressions to include only the variables x_r by replacing $\{y_r := x_{pr}\}_{r=1,2,\ldots}$ and so on. However, for the sake of possible generalizations we prefer to use separate variables.

Note also that a p^2-vertex circulant graph is disconnected if and only if its leading layer $X_{(0)}$ is empty. This layer does not meet the condition (**R**). This enables one to count easily *disconnected* (and, thus, connected as well) undirected and directed p^2-circulants, e.g., by some clear modification of the first two formulae of the Theorem.

When counting only by the number of vertices, it is possible to represent these results via an *explicit uniform* formula without using cycle indices.

7.5. Corollary. *Let* $\mathrm{h} \in \{\mathrm{d},\mathrm{t},\mathrm{u},\mathrm{sd},\mathrm{su}\}$. *Then*

$$C_{\mathrm{h}}(p^2) = \frac{\alpha_{\mathrm{h}}}{p(p-1)}\sum_{F_{\mathrm{h}}}\phi(r)\Big(2^{(p+1)\frac{p-1}{\beta_{\mathrm{h}}r}} - 2^{2\frac{p-1}{\beta_{\mathrm{h}}r}}\Big) + \Big(\frac{\alpha_{\mathrm{h}}}{p-1}\sum_{F_{\mathrm{h}}}\phi(r)2^{\frac{p-1}{\beta_{\mathrm{h}}r}}\Big)^2$$

where $\alpha_{\mathrm{d}} = \alpha_{\mathrm{t}} = \alpha_{\mathrm{sd}} = 1$, $\alpha_{\mathrm{u}} = \alpha_{\mathrm{su}} = 2$, $\beta_{\mathrm{d}} = \beta_{\mathrm{sd}} = 1$, $\beta_{\mathrm{t}} = \beta_{\mathrm{u}} = \beta_{\mathrm{su}} = 2$ *and the summation is taken over* r, $r|(p-1)$, *satisfying the restriction* F_{h} *defined as follows:*

F_{d} : r arbitrary;
F_{t} : r odd;
F_{sd} : r even;
F_{u} : $\frac{p-1}{r}$ even;
F_{su} : r and $\frac{p-1}{r}$ even. □

Here evidently $F_{\mathrm{d}} = F_{\mathrm{t}} \vee F_{\mathrm{sd}},\ F_{\mathrm{u}} = F_{\mathrm{t}} \vee F_{\mathrm{su}}$.

7.6. Corollary.

1. *If* $4 \not| \ (p-1)$, *then*

$$\begin{aligned} C_{\mathrm{su}}(p^2) &= 0, \\ C_{\mathrm{t}}(p^2) &= C_{\mathrm{sd}}(p^2), \\ A_{\mathrm{u}}(p^2) &= 2A_{\mathrm{sd}}(p^2), \\ B_{\mathrm{u}}(p^2) &= 2B_{\mathrm{sd}}(p^2), \\ D_{\mathrm{u}}(p^2) &= 4D_{\mathrm{sd}}(p^2). \end{aligned}$$

2. *For any prime* p

$$\begin{aligned} D_{\mathrm{d}}(p^2) &= C_{\mathrm{d}}(p)^2, \\ D_{\mathrm{t}}(p^2) &= C_{\mathrm{t}}(p)^2, \\ D_{\mathrm{sd}}(p^2) &= C_{\mathrm{sd}}(p)^2, \\ D_{\mathrm{su}}(p^2) &= C_{\mathrm{su}}(p)^2. \end{aligned}$$

3. *If* p *and* $2p-1$ *are both prime (cf. Corollary* 6.5*), then*

$$\begin{aligned} b_{\mathrm{u}}((2p-1)^2, t) &= b_{\mathrm{d}}(p^2, t^2), \\ d_{\mathrm{u}}((2p-1)^2, t) &= d_{\mathrm{d}}(p^2, t^2), \\ B_{\mathrm{su}}((2p-1)^2) &= B_{\mathrm{sd}}(p^2), \\ D_{\mathrm{su}}((2p-1)^2) &= D_{\mathrm{sd}}(p^2). \end{aligned}$$

PROOF. Straightforward by Theorem 7.4 and Proposition 6.4. □

7.7. Examples. 1) $n = 9$.

$$\mathcal{I}_2(\mathbf{x}) = \frac{1}{2}(x_1^2 + x_2)$$

so that

$$\begin{aligned} \mathcal{C}(9; \mathbf{x}, \mathbf{y}) &= \tfrac{1}{3}\mathcal{I}_2(\mathbf{x}^4) - \tfrac{1}{3}\mathcal{I}_2(\mathbf{xy}) + \mathcal{I}_2(\mathbf{x})\mathcal{I}_2(\mathbf{y}) \\ &= \tfrac{1}{6}(x_1^8 + x_2^4) - \tfrac{1}{6}(x_1^2 y_1^2 + x_2 y_2) + \tfrac{1}{4}(x_1^2 + x_2)(y_1^2 + y_2) \end{aligned}$$

whence

$$c_{\mathrm{d}}(9, t) = 1 + 2t + 6t^2 + 10t^3 + 13t^4 + 10t^5 + 6t^6 + 2t^7 + t^8.$$

Likewise

$$\mathcal{C}^*(9; \mathbf{x}, \mathbf{y}) = \frac{1}{3}x_1^4 + \frac{2}{3}x_1 y_1$$

and

$$c_{\mathrm{u}}(9, t) = 1 + 2t^2 + 2t^4 + 2t^6 + t^8.$$

2) $n = 25$. We get

$$\begin{aligned} \mathcal{C}(25; \mathbf{x}, \mathbf{y}) &= \tfrac{1}{20}(x_1^{24} + x_2^{12} + 2x_4^6) - \tfrac{1}{20}(x_1^4 y_1^4 + x_2^2 y_2^2 + 2x_4 y_4) \\ &\quad + \tfrac{1}{16}(x_1^4 + x_2^2 + 2x_4)(y_1^4 + y_2^2 + 2y_4). \end{aligned}$$

Then

$$\begin{aligned} c_{\mathrm{d}}(25,t) &= 1 + 2t + 16t^2 + 102t^3 + 536t^4 + 2126t^5 + 6741t^6 + 17306t^7 \\ &\quad + 36800t^8 + 65376t^9 + 98104t^{10} + 124808t^{11} + 135258t^{12} \\ &\quad + 124808t^{13} + 98104t^{14} + 65376t^{15} + 36800t^{16} + 17306t^{17} \\ &\quad + 6741t^{18} + 2126t^{19} + 536t^{20} + 102t^{21} + 16t^{22} + 2t^{23} + t^{24}. \end{aligned}$$

$$\mathcal{C}^*(25;\mathbf{x},\mathbf{y}) = \frac{1}{10}(x_1^{12} + x_2^6) - \frac{1}{10}(x_1^2y_1^2 + x_2y_2) + \frac{1}{4}(x_1^2 + x_2)(y_1^2 + y_2)$$

and

$$\begin{aligned} c_{\mathrm{u}}(25,t) &= 1 + 2t^2 + 8t^4 + 22t^6 + 51t^8 + 80t^{10} + 95t^{12} \\ &\quad + 80t^{14} + 51t^{16} + 22t^{18} + 8t^{20} + 2t^{22} + t^{24}. \end{aligned}$$

7.8. Table. Values contributed by the separate terms of formula (7.1.1) and the resulting numbers of p^2-circulants are provided in Table 1 (cf. Corollary 7.6). The relative magnitudes of these values show spectacularly that, in comformity with Theorem 4.15, $-B + D$ is only a slight correction term to the main contribution A. Missing entries are too large to be included in the table.

According to Table 1, $B_{\mathrm{u}}(9) = D_{\mathrm{u}}(9)$. This confirms once more that 9 is an exceptional values of n for which the conjecture $\mathbf{A}(n)$ holds for *undirected* circulants (though it does not hold for all circulants). Also, entries of the table confirm the repetitions predicted by Corollary 7.6.

	p						
Funct.	3	5	7	11	13	17	19
$C_{\mathrm{d}}(p^2)$	51	839094	6701785562464	-	-	-	-
$A_{\mathrm{d}}(p^2)$	52	839128	6701785562968	-	-	-	-
$B_{\mathrm{d}}(p^2)$	10	70	700	104968	1398500	-	-
$D_{\mathrm{d}}(p^2)$	9	36	196	11664	123904	-	-
$C_{\mathrm{u}}(p^2)$	8	423	798952	-	-	-	-
$A_{\mathrm{u}}(p^2)$	8	424	798960	-	-	-	-
$B_{\mathrm{u}}(p^2)$	4	10	24	208	700	8230	29144
$D_{\mathrm{u}}(p^2)$	4	9	16	64	196	1296	3600
$C_{\mathrm{su}}(p^2)$	0	7	0	0	56385212104	-	0
$A_{\mathrm{su}}(p^2)$	0	8	0	0	56385212112	-	0
$B_{\mathrm{su}}(p^2)$	0	2	0	0	12	38	0
$D_{\mathrm{su}}(p^2)$	0	1	0	0	4	16	0
$C_{\mathrm{sd}}(p^2)$	3	214	399472	-	-	-	-
$A_{\mathrm{sd}}(p^2)$	4	216	399480	-	-	-	-
$B_{\mathrm{sd}}(p^2)$	2	6	12	104	356	4134	14572
$D_{\mathrm{sd}}(p^2)$	1	4	4	16	64	441	900
$C_{\mathrm{t}}(p^2)$	3	205	399472	-	-	-	-
$A_{\mathrm{t}}(p^2)$	4	208	399480	-	-	-	-
$B_{\mathrm{t}}(p^2)$	2	4	12	104	344	4096	14572
$D_{\mathrm{t}}(p^2)$	1	1	4	16	36	256	900

Table 1: Numbers of circulant p^2-graphs and contributing terms, p prime

7.9. CI-valencies. Let us return to the questions mentioned in 2.10. There are somewhat unexpected qualitative implications of Theorem 7.4 that concern circulants specified by valencies.

In the well-known terminology introduced by L. Babai [Bab77], the falsity of conjecture $\mathbf{A}(n)$ for certain n means that the cyclic group $\mathbb{Z}_n$ is not generally a $\mathcal{G}$-CI-group and not a $\widetilde{\mathcal{G}}$-CI-group where CI stands for Cayley isomorphism and $\mathcal{G}$ (resp., $\widetilde{\mathcal{G}}$) denotes the set of all undirected (resp., directed) graphs.

Therefore it is reasonable to narrow the set of graphs and to consider the restricted analogue:

Conjecture $\mathbf{A}_P(n)$. *Given n and a property P of graphs, isomorphic circulant n-graphs possessing the property P are equivalent.*

Let us denote the sets of undirected and directed graphs possessing property P by $\mathcal{G}_P$ and $\widetilde{\mathcal{G}}_P$, respectively.

Now the general question becomes: For which "interesting" properties P is conjecture $\mathbf{A}_P(n)$ valid?

If the answer is affirmative, we call such P a CI-*property* of circulant n-graphs. In other words, P is a CI-property of undirected (resp., directed) circulant n-graphs if and only if $\mathbb{Z}_n$ is a $\mathcal{G}_P$-CI-group (resp., $\widetilde{\mathcal{G}}_P$-CI-group).

Let (r) and $[r]$ $(r \geq 1)$ denote the properties of being a regular undirected or directed graph of valency r, respectively.

For $n = p^2$, the answer to the above question for properties (r) and $[r]$ can be presented in terms of the *lacunarity* for the difference of polynomials considered above (cf. formula (7.1.1)), namely:

> *Conjecture $\mathbf{A}_{(r)}(p^2)$ (resp., $\mathbf{A}_{[r]}(p^2)$) is valid if and only if the coefficient of t^r in the polynomial $b_{\mathrm{u}}(p^2,t) - d_{\mathrm{u}}(p^2,t)$ (resp., in the polynomial $b_{\mathrm{d}}(p^2,t) - d_{\mathrm{d}}(p^2,t)$) vanishes.*

Thus, Theorem 7.4 contains implicit answers in both cases. As for an explicit description of such valencies r, we restrict ourselves to partial observations. The problem for undirected graphs is little more tractable (moreover, for the primes stipulated in Corollary 7.6(3) directed graphs are reduced to undirected ones), so it is this problem that will be considered. In other words, we ask:

Which valencies of undirected p^2-circulants are responsible for "non-Ádám" behaviour?

The exponents r with zero coefficients in $b_{\mathrm{u}}(p^2,t) - d_{\mathrm{u}}(p^2,t)$ will be called p^2-*vanishing* (for undirected circulant graphs), or simply *vanishing*. Due to the above criterion, these are just CI-valencies, i.e. valencies r for which (r) is a CI-property of undirected circulant p^2-graphs.

We distinguish simpler cases when coefficients of t^r are equal to 0 in *both* b_u and d_u. Such vanishing exponents r will be called *trivial*.

According to 7.3,

$$b_{\mathrm{u}}(p^2,t) = \mathcal{I}_{\frac{p-1}{2}}(\mathbf{xy})\big|_{\{x_r:=1+t^{2r},\ y_r:=1+t^{2pr}\}_{r=1,2,\dots}}$$
$$d_{\mathrm{u}}(p^2,t) = \mathcal{I}_{\frac{p-1}{2}}(\mathbf{x})\mathcal{I}_{\frac{p-1}{2}}(\mathbf{y})\big|_{\{x_r:=1+t^{2r},\ y_r:=1+t^{2pr}\}_{r=1,2,\dots}}$$

Note that $b_{\mathrm{u}}, d_{\mathrm{u}}$ and $b_{\mathrm{u}} - d_{\mathrm{u}}$ are polynomials with non-negative coefficients.

Now some numerical results:

(1) $p=7$. $\mathcal{I}_{\frac{p-1}{2}}(\mathbf{x})=\frac{1}{3}(x_1^3+2x_3)$, whence

$$\begin{aligned} b_{\mathrm{u}}(7^2,t) &= 1+t^2+t^4+t^6+t^{14}+3t^{16}+3t^{18}+t^{20}\\ &\quad +t^{28}+3t^{30}+3t^{32}+t^{34}+t^{42}+t^{44}+t^{46}+t^{48};\\ d_{\mathrm{u}}(7^2,t) &= 1+t^2+t^4+t^6+t^{14}+t^{16}+t^{18}+t^{20}\\ &\quad +t^{28}+t^{30}+t^{32}+t^{34}+t^{42}+t^{44}+t^{46}+t^{48} \end{aligned}$$

and

$$b_{\mathrm{u}}(7^2,t)-d_{\mathrm{u}}(7^2,t)=2t^{16}+2t^{18}+2t^{30}+2t^{32}.$$

Lacunary intervals: $[0,14]$, $[20,28]$, $[34,48]$.

Non-trivial vanishing exponents below 24: $0,2,4,6,14,20$.

(2) $p=11$. We get similarly

$$\begin{aligned} b_{\mathrm{u}}(11^2,t)-d_{\mathrm{u}}(11^2,t) &= 4t^{24}+8t^{26}+8t^{28}+4t^{30}\\ &\quad +8t^{46}+16t^{48}+16t^{50}+8t^{52}+\dots \end{aligned}$$

(we drop the symmetrical members with exponents greater than 60).

Lacunary intervals: $[0,22]$, $[32,44]$, $[54,64],\dots$.

Non-trivial vanishing exponents below 60: $0,2,4,6,8,10,22,32,44,54$.

(3) $p=13$.

$$\begin{aligned} b_{\mathrm{u}}(13^2,t)-d_{\mathrm{u}}(13^2,t) &= 5t^{28}+12t^{30}+16t^{32}+12t^{34}\\ &\quad +5t^{36}+12t^{54}+30t^{56}+38t^{58}+30t^{60}\\ &\quad +12t^{62}+16t^{80}+38t^{82}+52t^{84}+\dots \end{aligned}$$

(Again, the coefficients for greater exponents are determined by symmetry.)

Lacunary intervals: $[0,26]$, $[38,52]$, $[64,78],\dots$.

Non-trivial vanishing exponents below 84: $0,2,4,6,8,10,12,26,38,52,64,78$.

Note also that $b_{\mathrm{u}}(13^2,t)-d_{\mathrm{u}}(13^2,t)=b_{\mathrm{d}}(7^2,t^2)-d_{\mathrm{d}}(7^2,t^2)$ in this case.

Evidently, the first non-zero member in $b_{\mathrm{u}}(p^2,t)-d_{\mathrm{u}}(p^2,t)$ equals $\frac{p-3}{2}t^{2(p+1)}$. This exponent is much greater than the known general lower bound 6 of non-CI-valencies valid for all n (see [Sun88] and [Li95]) and shows that for various sets of graph orders, one can expect much better bounds.

Studying the polynomials $b_{\mathrm{u}}(p^2,t)$ leads easily to the following

7.10. Triviality test. *$2r$ is a trivial p^2-vanishing exponent for undirected circulants if and only if r is not representable in the form $r=i+pj$ where i and j are non-negative integer not exceeding $\frac{p-1}{2}$.*

Note that the non-trivial vanishing exponents between $p-1$ and p^2-p are, evidently, $2ip$ and $(2i-1)p-1$, $i=1,2,\dots,\frac{p-1}{2}$. We may conclude in general that the majority of valencies are CI-valencies of undirected circulant graphs of order p^2.

8 Discussion

8.1. One of the main purposes of this paper is to introduce and compare two different approaches for the enumeration of circulant graphs. In general, capabilities of the structural approach are strongly limited by the exponential growth of the number of S-rings over $\mathbb{Z}_n$ for many values of n. In spite of this limitation we are sure that this approach will create a nice background for understanding the essence of the problem and developing effective strategies for its solution. Moreover, it also serves as a bridge between techniques of S-rings and Pólya's enumeration theory.

8.2. The information required for the structural approach consists of the list of all S-rings over $\mathbb{Z}_n$, their automorphism groups, and the normalizers in S_n of these automorphism groups. In many cases such information is available at the theoretical level, e.g., for $n = p, pq, p^2$.

Another possibility is created by the use of computers, especially by the use of the package COCO for computations on coherent configurations. In our case of circulant graphs, the only necessary input in the "main technological chain" of this package consists of the permutation $(1, 2, \ldots, n-1)$, which generates the standard regular representation of $\mathbb{Z}_n$ (for details see [FarK91] and [FarKM94]). Many interesting experimental results obtained with the help of COCO and its predecessors (cf. [FieK9x]) still are await a convenient theoretical generalization.

8.3. For composite n of a rather high "multiplicative complexity," the multiplier approach is of course the only possible way to elaborate the enumeration of circulant graphs. A striking example arises in the case of square-free n, that is $n = p_1 \cdots p_s$ where $p_1, p_2, \ldots, p_s$ are pairwise different primes. As follows from [Gol85] and [Muz94], in this case the problem of the enumeration of so-called rational S-rings over $\mathbb{Z}_n$ is equivalent to the enumeration of finite topologies with s points. The latter problem is regarded as one of the most difficult problems in modern enumerative combinatorics, see, e.g., [Sta86]. Thus, the realization of the structural approach for the square-free case looks rather hopeless (even in spite of the recent classification of all S-rings over $\mathbb{Z}_n$, n square-free, achieved in [Muz9y]). At the same time for square-free n, the conjecture $\mathbf{A}(n)$ is valid. Therefore the enumeration via the one-multiplier approach definitely will be successful (though with certain purely technical difficulties, and probably in a rather cumbersome form).

8.4. The case $n = p^m$, p a prime, can be considered as a promising subject for combining both approaches. In [KliP80], two of the present authors proved a general Isomorphism Theorem for p^m-circulants. It is worthwhile to mention that the proof was based only on certain general properties of S-rings over $\mathbb{Z}_{p^m}$ and not on the detailed structure of their automorphism groups and the respective normalizers. (In fact, for many years, only limited knowledge of the structure of these groups has been achieved. This is remedied in the forthcoming paper [KliP9x].)

In principle, the aforementioned Isomorphism Theorem is sufficient for developing a similar multiplier enumeration approach as elaborated in Section 7 for $n = p^2$. But the constraints imposed by this theorem on multipliers are rather subtle and their complexity grows quickly with m.

It turns out that the count of p^m-circulants can be reduced to a certain number (namely, $\mathrm{Cat}(m)$, the Catalan number) of well specified independent Pólya-type counting problems with respect to some subgroups of the direct product of m cyclic groups. Thus, in this case, one may really speak of a joint use of the two methodologies: each Pólya-type problem may be solved via the multiplier approach while the general reduction of the initial problem is the subject of the structural approach. First "reductive" results related to the general case $n = p^m,\ m \geq 3$, will be published elsewhere [LisP9x].

In a more general setting, the enumeration of circulants still remains a challenging problem on the boundary between algebraic and enumerative combinatorics. We believe that a more deep use of S-rings will help in the future to achieve significant progress in this problem.

Acknowledgements

We are much grateful to Frank Fiedler for his help in the preparation of the manuscript of this paper. Our thanks are also due to Brendan McKay for useful discussions of numerical results and questions concerning CI-valencies. Finally, we are very glad to express our deep gratitude to Andy Woldar for his numerous valuable corrections of the text.

References

[Ádá67] A. Ádám, Research problem 2–10. *J. Combin. Th.*, **2** (1967), No 3, 393.

[Aig79] M. Aigner, Combinatorial Theory. Springer-Verlag, Berlin, 1979.

[Als70] B. Alspach, On point-symmetric tournaments. *Canad. Math. Bull.*, **13** (1970), No 3, 317–323.

[Als73] B. Alspach, Point-symmetric graphs and digraphs of prime order and transitive permutation groups of prime degree. *J. Combin. Th.*, **B15** (1973), No 1, 12–17.

[AlsP79] B. Alspach and T. D. Parsons, Isomorphism of circulant graphs and digraphs. *Discr. Math.*, **25** (1979), No 1, 97–108.

[Ast72] A. Astie, Groupes d'automorphismes des tournois sommet-symmétriques d'ordre premier et dénombrement de ces tournois. *C. r. Acad. Sci. Paris* (A), **275** (1972), No 3, 167–169.

[Bab77] L. Babai, Isomorphism problem for a class of point-symmetric structures. *Acta Math. Acad. Sci. Hungar.*, **29** (1977), No 3–4, 329–336.

[Cha71] C. Y. Chao, On the classification of symmetric graphs with a prime number of vertices. *Trans. Amer. Math. Soc.*, **158** (1971), No 1, 247–256.

[Cha90] C. Y. Chao, On digraphs with circulant adjacency matrices. *Archiv Math.*, **54** (1990), No 1, 93–104.

[ChaW73] C. Y. Chao and J. G. Wells, A class of vertex-transitive digraphs. *J. Combin. Th.*, **B14** (1973), No 3, 246–255.

[ChaW82] C. Y. Chao and J. G. Wells, A class of vertex-transitive digraphs, II. *J. Combin. Th.*, **B32** (1982), No 3, 336–346.

[ChaW83] C. Y. Chao and J. G. Wells, On labeled vertex-transitive digraphs with a prime number of vertices. *Discr. Math.*, **46** (1983), No 3, 311–315.

[ChiL86] G. L. Chia and C. K. Lim, A class of self-complementary vertex-transitive digraphs. *J. Graph Th.*, **10** (1986), No 2, 241–249.

[Dav65] H. A. David, Enumeration of cyclic paired-comparison designs. *Amer. Math. Monthly*, **72** (1965), No 3, 241–248.

[Dav72] H. A. David, Enumeration of cyclic graphs and cyclic designs. *J. Combin. Th.*, **B13** (1972), No 3, 303–308.

[Djo70] D. Ž. Djoković, Isomorphism problem for a special class of graphs. *Acta Math. Acad. Sci. Hung.*, **21** (1970), No 3–4, 267–270.

[Dre71] A. W. M. Dress, Notes on the theory of representations of finite groups. Part I. The Burnside ring of a finite group and some AGN-applications. *Lecture Notes*, Bielefeld, 1971.

[DreKM92] A. W. M. Dress, M. H. Klin and M. E. Muzichuk, On p-configurations with few slopes in the affine plane over $\mathbf{F}_p$ and a theorem of W.Burnside's. *Bayreuther Math. Schr.*, No 40 (1992), 7–19.

[ElsT70] B. Elspas and J. Turner, Graphs with circulant adjacency matrices. *J. Combin. Th.*, **9** (1970), No 3, 297–307.

[Far78] I.A. Faradjev, Constructive enumeration of combinatorial objects. *Colloque Intern. du Centre National de la Recherche Sci.*, Paris, **260** (1978), 131–135.

[FarK91] I. A. Faradžev and M. H. Klin, Computer package for computations with coherent configurations. *Proc. ISAAC'91*, Bonn, 1991, 219–223.

[FarIK90] I. A. Faradžev, A. A. Ivanov and M. H. Klin, Galois correspondence between permutation groups and cellular rings (association schemes). *Graphs & Combin.*, **6** (1990), No 3, 303–332.

[FarKM94] I. A. Faradžev, M. H. Klin and M. E. Muzichuk. Cellular rings and groups of automorphisms of graphs, In: I. A. Faradžev, A. A. Ivanov, M. H. Klin and A. J. Woldar (eds.). *Investigations in Algebraic Theory of Combinatorial Objects*, Kluwer (Mathematics and Its Applications, Soviet Series, **84**), Dordrecht, 1994, 1–152.

[FieK9x] F. Fiedler and M. Klin, Constructive enumeration of S-rings and Cayley graphs over the groups of small order. *Manuscript in preperation.*

[God83] C. D. Godsil, On Cayley graph isomorphism. *Ars Combin.*, **15** (1983), 231–246.

[Gol85] J. J. Gol'fand, A description of subrings in $V(Sp_1 \times Sp_2 \times \cdots Sp_m)$. In: *Investigations in Algebraic Theory of Combinatorial Objects*, Moscow, VNIISI, 1985, 65–76 (in Russian). English translation in: I. A. Faradžev, A. A. Ivanov, M. H. Klin and A. J. Woldar (eds.). *Investigations in Algebraic Theory of Combinatorial Objects*, Kluwer (Mathematics and Its Applications, Soviet Series, **84**), Dordrecht, 1994, 209–223.

[GolNP85] J. J. Gol'fand, N. L. Najmark and R. Pöschel, The structure of S-rings over Z_{2^m}. *Preprint* P-MATH-01/85, AdWDDR, ZIMM, Berlin, 1985, 30 pp.

[Gri94] R. P. Grimaldi, *Discrete and Combinatorial Mathematics. An Applied Introduction.* Third edition. Reading, Addison-Wesley, MA, 1994.

[HarP73] F. Harary and E. M. Palmer, *Graphical Enumeration.* Acad. Press, New York, 1973.

[Has64] H. Hasse, *Vorlesungen über Zahlentheorie.* 2 Auflage. Springer–Verlag, Berlin, 1964.

[KalK76] L. A. Kalužnin and M. H. Klin, On certain numerical invariants of permutation groups. *Latv. Mat. Ežegodnik*, **18** (1976), 81–99 (in Russian).

[Ker91] A. Kerber, *Algebraic Combinatorics via Finite Group Actions.* BI-Wissenschaftsverlag, Mannheim, 1991.

[Kli70] M. H. Klin, On the number of graphs for which a given permutation group is the automorphism group. *Kibernetika* (Kiev), No 6 (1970), 131–137 (in Russian). Engl. translation: *Kibernetika*, **5** (1973), 862–870.

[KliMW9x] M. Klin, M. Muzychuk and A. J. Woldar, Circulant graphs via Schur rings theory, I. *Manuscript in preperation.*

[KliP78] M. H. Klin and R. Pöschel, The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings. *Preprint* AdWDDR, ZIMM, Berlin (1978), 43 pp. A shortened version in: *Colloq. Math. Soc. J. Bolyai*, **25**. *Algebr. Methods in Graph Theory, Szeged, 1978*, p. 2. North-Holland, Amsterdam, 1981, 405–434.

[KliP80] M. Ch. Klin and R. Pöschel, The isomorphism problem for circulant digraphs with p^n vertices. *Preprint* P34/80, AdWDDR, ZIMM, Berlin, 1980, 40 pp.

[KliP9x] M. Klin and R. Pöschel, Automorphism groups of p^m-vertex circulant graphs, p – an odd prime. *Manuscript in preperation.*

[KliPR88] M. Ch. Klin, R. Pöschel and K. Rosenbaum, *Angewandte Algebra für Mathematiker und Informatiker. Einführung in gruppentheoretisch-kombinatorische Methoden.* Friedr. Vieweg & Sohn, Braunschweig/Wiesbaden, 1988.

[Li95] C. H. Li, Isomorphisms and classification of Cayley graphs of small valencies on finite Abelian groups. *Australas. J. Combin.*, **12** (1995), No 1, 3–14.

[LisP9x] V. Liskovets and R. Pöschel, On the enumeration of circulant graphs of prime-power and square-free orders. *Manuscript in preperation.*

[Muz94] M. E. Muzychuk, On the structure of basic sets of Schur rings over cyclic groups. *J. Algebra*, **169** (1994), No 2, 665–678.

[Muz95] M. Muzychuk, Ádám's conjecture is true in the square-free case. *J. Combin. Th.*, **A72** (1995), No 1, 118–134.

[Muz9x] M. Muzychuk, On Ádám's conjecture for circulant graphs. *Discr. Math.* (to appear).

[Muz9y] M. Muzychuk, The structure of Schur rings over cyclic groups of square-free order. *Acta Applic. Math.* (to appear).

[Pál87] P. P. Pálfy, Isomorphism problem for relational structures with a cyclic automorphism. *Europ. J. Combin.*, **8** (1987), No 1, 35–43.

[PalR84] E. M. Palmer and R. W. Robinson, Enumeration of self-dual configurations. *Pacif. J. Math.*, **110** (1984), No 1, 203–221.

[Pös74] R. Pöschel, Untersuchungen von S-Ringen, insbesondere im Gruppenring von p-Gruppen. *Math. Nachr.*, **60** (1974), 1–27.

[PösK79] R. Pöschel and L. A. Kalužnin, *Funktionen- und Relationenalgebren.* Berlin, 1979.

[Ray91] V. J. Rayward-Smith, The discovery and enumeration of representative symbols for circulant tournaments. *Int. J. Math. Educ. Sci. Technol.*, **22** (1991), No 1, 23–33.

[Rob81] R. W. Robinson, Counting graphs with a duality property. In: *Proc. 8-th Brit. Combin. Conf.* (H. N. V. Temperley ed.), London Math. Soc. Lect. Note Ser., **52**, 1981, 156–186.

[Sch33] I. Schur, Über einfach transitive Permutationsgruppen. *Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalisch-Mathematische Klasse*, 1933, 598–623. Reprinted in: I. Schur, *Gesammelte Abhandlungen.* Volume 3. Berlin, 1973.

[Sri70] M. R. Sridharan, Self-complementary and self-converse oriented graphs. *Indag. Math.*, **32** (1970), No 5, 441–447.

[Sta86] R. Stanley, *Enumerative Combinatorics.* Volume 1. Wadsworth & Brooks/Cole, Monterey, 1986.

[Sun88] L. Sun, Isomorphism of undirected circulant graphs. *Chinese Ann. Math., Ser.* A, **9** (1988), No 5, 567–574.

[Tur67] J. Turner, Point-symmetric graphs with a prime number of points. *J. Combin. Th.*, **3** (1967), No 2, 136–145.

[Wei76] B. Weisfeiler (ed.), *On Construction and Identification of Graphs.* Lect. Notes Math., **558**, Springer–Verlag, 1976.

[Wie64] H. Wielandt, *Finite Permutation Groups.* Acad. Press, New York and London, 1964.

[Zha90] H. Zhang, Point-color-symmetric graphs with a prime number of vertices. *Graphs & Combin.*, **6** (1990), No 3, 297–302.