Als Manuskript gedruckt

Technische Universität Dresden
Herausgeber: Der Rektor

On the Enumeration of Circulant Graphs of Prime-Power and Square-Free Orders[*]

Valery Liskovets and Reinhard Pöschel

MATH–AL–8–1996

October 1996

[*] 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.

Abstract

The aim of this work is twofold:

to unify, systematize and extend the known results of the analytical (i.e. formula-wise) counting of directed and undirected circulant graphs with a prime or, more generally, square-free number of vertices;

to develop a general combinatorial framework for the counting of non-isomorphic circulant graphs with p^k vertices, p odd prime, $k \geq 2$.

The general problem of counting circulant graphs of order p^k is decomposed into $\mathrm{Cat}(k)$ well-specified enumerative Pólya type subproblems with respect to certain Abelian groups where $\mathrm{Cat}(k)$ denotes the k-th Catalan number. These subproblems are parametrized by the monotone underdiagonal walks on the plane integer $(k+1) \times (k+1)$ lattice. The descriptions are given in terms of equalities and congruences between multipliers acting on sets of numbers in accordance with an isomorphism theorem for such circulant graphs. Tables contain new numerical results.

Contents

Introduction

A graph is called a circulant graph (or simply a circulant) if it possesses an automorphism which cyclically permutes all the vertices. Circulants are vertex-transitive graphs with interesting and attractive properties.

From the earliest days of the study of circulants it became clear that their properties depend heavily on the multiplicative nature of its order (a graph is said to be of order n if n is the number of its vertices). The structural theory is simple for prime orders $n = p$ (though the divisors of $p - 1$ should also be taken into account). Accordingly, it is a simple matter to count non-isomorphic p-circulants and this has been done by several researchers for various types of directed and undirected graphs. But every wider class of orders required a great amount of efforts. A considerable progress has been achieved in studying circulants for prime-power and (more recently) square-free orders. Here we are concerned with both these cases.

If some combinatorial objects are natural and interesting for study, their enumeration (in various senses: constructive, analytical and asymptotic) is also a natural and interesting task. This is the case for circulants. As typical for enumerative combinatorics in general, only a certain small but highly rigorous part of structural and algebraic properties of objects is significant for counting. In principle, the isomorphism theorems that have been previously obtained for the above-mentioned orders n are sufficient to count circulants analytically. However the real picture is somewhat more vague.

First of all, by their nature, circulants are not only combinatorial but algebraic and number-theoretic objects as well. Therefore they are described in terms slightly inconvenient for enumerative combinatorics. On the other hand, the base group "up to which" circulants are counted looks very simple: it is a cyclic group or a direct product of cyclic groups. This facilitates the counting indeed and provides a systematic way for enumerating circulants of square-free orders. However, for the case of prime-power orders, another difficult problem arises instead (as we shall see later): a subtle and awkwardly structured set on which this group acts. Thus, there is a gap between the effective main algebraic isomorphism theorem for circulants of order p^k and enumerative consequences from it. Do "closed, explicit" formulae exist? In Section 5 we give an answer *affirmative* in the following sense: the problem is decomposed into a certain set of ordinary well-specified subproblems of group orbit counting. Each one concerns a subgroup of the direct product of k cyclic groups that acts multiplicatively on certain subsets of numbers. Every subproblem can be resolved by the ordinary Pólya method. But their diversity and setting compexity grow exponentially quickly with k: the subproblems prove to be in one-to-one correspondence with the monotone underdiagonal walks on the plane $(k+1) \times (k+1)$ lattice, in which terms their combinatorics is described effectively. Accordingly, the overall number of the subproblems is equal to the k-th Catalan number $\mathrm{Cat}(k) = \dfrac{1}{k+1}\dbinom{2k}{k}$ (i.e. we have $1, 2, 5, 14, 42, \ldots$ subproblems for $k = 1, 2, 3, 4, 5, \ldots$, respectively). For $k \geq 3$, finding a general uniform solution of them as a function of the specifying walks remains an open question.

Recently, M. Klin with the present authors have succeeded in counting circulants of order p^2 [KliLP9x] by resolving both arising subproblems. This was the first enumarative result for the case when the so-called Ádám (single-multiplier) isomorphism condition does not hold (see 2.8). As a matter of fact, this condition corresponds to one (and the simplest!) of the subproblems for any k. The above-mentioned paper develops also a quite another "structural" approach to the count of circulants, which well supplements the present one. In few words, the structural approach uses a detailed information on the lattice of the automorphism groups of circulant graphs relying upon the fact that in certain cases all necessary information can be obtained by algebraic methods of S-rings.

As for counting circulant graphs of square-free orders, we solve this problem completely up to calculating explicitly the corresponding cycle indices. Moreover, we obtain uniform formulae for various well-known classes of circulant graphs: directed, undirected, self-complementary and tournaments. This form of results looks new even for prime orders.

The paper is concerned only with the enumeration. It is basically self-contained though it is assumed the knowledge of common enumerative methods (generating functions, Pólya's theory, etc.; see for example [KliPR88, Ch. 2] and [Ker91, Ch. 1 and 2]) as well as of elementary (multiplicative) number theory, (permutation) group theory and graph theory.

In order to serve partially as a state-of-the-art survey, the paper contains the complete (as far as we know) bibliography of analytical circulant graph enumeration. It comprises also references to some related publications, including ones devoted to constructive enumeration.

1 Basic definitions

1.1. 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* $\mathbf{S}_n$, $n=|U|$, is implicit. (G,U) is a permutation group if and only if this action is faithful.

$Z(n)$ denotes a *regular cyclic* permutation group of order (and degree) n, i.e. generated by an n-cycle. Usually we take $(0,1,2,\ldots,n-1)$ 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.

1.2. Sum, product and join of groups. Given two groups G and H acting on disjoint sets U and V, we define their *direct sum* $(G,U)\oplus(H,V):=(G\times H,U\dot{\cup}V)$ and *direct product* $(G,U)\otimes(H,V):=(G\times H,U\times V)$. In both cases this is the direct product of two groups which acts on the (disjoint) union and on the direct product of two sets respectively. These two actions are defined by the following rule: for any $(g,h)\in G\otimes H$, $u\in U$ and $v\in V$,

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

for $(G,U)\oplus(H,V)$ and

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

for $(G,U)\otimes(H,V)$, respectively.

Given a group G and two its actions (G,U) and (G,W) on disjoint sets U and W, their *join* $(G,U)\dot{\vee}(G,W):=(G,U\dot{\cup}W)$ means the same group and its combined actions defined by the following rule: for any $g\in G$ and $v\in U\dot{\cup}W$,

$$v^g:=\begin{cases}u^g & \text{for}\quad v=u\in U\\ w^g & \text{for}\quad v=w\in W\end{cases}.$$

$(G,U)\dot{\vee}(G,W)$ is the "diagonal" subgroup of the direct sum $(G,U)\oplus(G,W)$. This natural operation (going back to Burnside) is typical for combinatorial enumeration though we could not find an explicit description of it in the literature.

1.3. Cycle index. The polynomial

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

of degree $n=|U|$ in the variables $x_1,x_2,\ldots,x_n$ denotes the *cycle index* of a group

G 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.

Working with cycle indices of groups which act on sets of heterogeneous objects it is convenient to use variables of several different types. In particular, we shall sometimes 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 $x_1, x_2, \ldots, x_n$ (resp., $y_1, y_2, \ldots, y_n$) of variables and $\mathbf{xy}$ denotes all pairwise products $x_1y_1, x_2y_2, \ldots, x_ny_n$.

1.4. Faithful action. Let (G, U) be a group with an action and $(\overline{G}, U)$ the corresponding *faithful* permutation group, i.e. the quotient group $\overline{G} = G/K$ where $K = \{k \in G \mid \forall u \in U : u^k = u\}$ and the action of $\overline{G}$ is induced from that of G on U via $u^{\overline{g}} = u^g$ for $\overline{g} = Kg$. Then the following simple and useful property holds:

1.5. Lemma. $I_{(G,U)} = I_{(\overline{G},U)}$.

PROOF.

$$\begin{aligned} I_{(G,U)} &= \tfrac{1}{|G|} \sum_{g\in G} \prod_{i\geq 1} x_i^{a_i(g)} = \tfrac{1}{|G|} \sum_{k\in K} \sum_{\overline{g}\in\overline{G}} \prod_{i\geq 1} x_i^{a_i(k\overline{g})} \\ &= \tfrac{1}{|G|} \sum_{\overline{g}\in\overline{G}} \sum_{k\in K} \prod_{i\geq 1} x_i^{a_i(\overline{g})} = \tfrac{1}{|G|} \sum_{\overline{g}\in\overline{G}} |K| \prod_{i\geq 1} x_i^{a_i(\overline{g})} = I_{(\overline{G},U)}. \end{aligned}$$

□

Thus, both polynomials coincide, in spite of the fact that the numbers of their members are different by definition. Therefore the conversion to the faithful action provides *no* analytical and computational advantages. This implicitly well-known property will be henceforth referred to as the *Indifference* lemma.

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

$$I_{Z(n)} = \frac{1}{n} \sum_{i=1}^{n} x_{[i,n]/i}^{(i,n)} \tag{1.6.1}$$

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

$$I_{Z(n)} = \frac{1}{n} \sum_{r|n} \phi(r) x_r^{n/r} \tag{1.6.2}$$

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

Denote for brevity

$$\mathcal{I}_n(\mathbf{x}) := I_{Z(n)}(\mathbf{x}). \tag{1.6.3}$$

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

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 Indifference lemma 1.5,

$$I_{Z(n,s)} = I_{Z(s)}, \quad s|n. \tag{1.6.4}$$

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

$$I_{D(n)} = \tfrac{1}{2}(I_{Z(n)} + x_1 x_2^{(n-1)/2}). \tag{1.6.5}$$

For our aims, only actions of cyclic groups and groups built from them by means of the operations defined in 1.2 are necessary. The corresponding cycle indices are built by the following lemma.

1.7. Lemma. *Let $(G,U),(G,W)$ and (H,V) be groups with actions where the set U is disjoint with W and V. Then*

$$I_{(G,U)\oplus(H,V)} = I_{(G,U)} \cdot I_{(H,V)}, \tag{1.7.1}$$

$$I_{(G,U)\otimes(H,V)} = \frac{1}{|G||H|} \sum_{g,h} \prod_{i,j} x_{[i,j]}^{(i,j)a_i(g)a_j(h)} \tag{1.7.2}$$

and

$$I_{(G,U)\dot\vee(G,W)}(\mathbf{x},\mathbf{y}) = I_{(G,U)}(\mathbf{x}) \ \dot\vee \ I_{(G,W)}(\mathbf{y}) \tag{1.7.3}$$

where

$$I_{(G,U)}(\mathbf{x}) \ \dot\vee \ I_{(G,W)}(\mathbf{y}) := \frac{1}{|G|} \sum_{g\in G} \prod_{i\geq 1} x_i^{a_i(g,U)} y_i^{a_i(g,W)}. \tag{1.7.4}$$

Proof. The first two formulae are well known, see [Ker91, p. 74]. Formula (1.7.3) is evident by definition. □

1.8. Remarks. 1. The operation "$\dot\vee$" for cycle indices as defined by (1.7.4) depends *not only* on the polynomials by themselves but also on the underlying group G, namely on the correspondence of terms in both cycle indices to the same element $g \in G$. For cyclic groups, the result can be obtained in almost straightforward fasion based on formula (1.6.1). 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 (1.6.4), we obtain

$$I_{Z(ps,s)}(\mathbf{x})\dot{\vee}I_{Z(ps)}(\mathbf{y}) = \frac{1}{ps}\Big(\sum_{r|s}(p-1)\phi(r)x_r^{s/r}y_{pr}^{s/r} + \sum_{r|s}\phi(r)x_r^{s/r}y_r^{ps/r}\Big). \qquad (1.8.1)$$

2. For checking calculations with cycle indices it is useful to take into account the following evident identity valid for an arbitrary group acting on an n-element set:

$$I_G(\mathbf{x})|_{\{x_r:=t^r\}_{r=1,2,\dots}} = t^n. \qquad (1.8.2)$$

In particular,

$$I_G(n;1,1,\dots,1) = 1.$$

1.9. Residue generators of $\mathbb{Z}^*_{p^k}$. We shall use some multiplicative properties of integer numbers.

For $n = p^k$, as well-known, $\mathbb{Z}^*_n$ is a multiplicative *cyclic* group of order $p^{k-1}(p-1)$. Moreover, it is possible to find an integer $\omega = \omega(p)$ which is a primitive root (i.e. a generator of $\mathbb{Z}^*_{p^k}$) for *all* k and is such that $1 < \omega < p^2$ (necessarily $p^\omega \equiv 1 \pmod{p^2}$). Instead, following H. Hasse [Has64, p. 80] we shall make use of representing this cyclic group as the direct product of two cyclic groups of orders p^{k-1} and $p-1$, respectively. The first group is generated by the number $1+p$ (which is really of order p^{k-1} modulo p^k). The second group is generated by an element $w = w(p,k)$ such that w is a primitive root modulo p (i.e. $\langle w\rangle = \mathbb{Z}^*_p \pmod{p}$) and satisfies the congruence $w^{p-1} \equiv 1 \pmod{p^k}$. In other words, w is of order $p-1$ both modulo p and p^{k-1}. Such an element w does exist: if ω is a primitive root modulo p^k, then one can simply take $w = \omega^{p^{k-1}}$. Thus, every element $m \in \mathbb{Z}^*_{p^k}$ has a unique representation

$$m = w^i(1+p)^j \pmod{p^k} \qquad (1.9.1)$$

for some $i \in \{0,1,\dots,p-2\}$ and $j \in \{0,1,\dots,p^{k-1}-1\}$.

Moreover, the multiplier $1+p^i,\ i>0$, is of order p^{k-i} modulo p^k since

$$1+p^i \equiv (1+p)^{p^{i-1}}. \qquad (1.9.2)$$

1.10. Congruences versus equalities. The following elementary property is convenient for manipulating congruences modulo different p-power bases.

Let i, j and l be positive integers such that $i \le j,\ i \le l$, and let h be a number considered modulo p^j. Then the equation

$$x \equiv h \pmod{p^l} \qquad (1.10.1)$$

has a unique solution $x \bmod p^i$. It is simply h considered, coarser, modulo p^i. In other words, we may replace congruence (1.10.1) by the equality

$$x = h$$

(and in this form, x just as h is considered modulo p^j). Of course this assertion is not valid for greater values of i.

1.11. Graphs. Throughout we shall use the terms *graph* and *undirected graph*, so that a graph means a directed graph. Accordingly, we speak about edges (i.e. ordered pairs of vertices) and undirected edges (unordered pairs of vertices). Undirected graphs are identified with symmetric graphs, i.e. undirected edges are identified with the corresponding pairs of edges directed oppositely. All graphs (directed or undirected) are without loops and multiple edges. 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 the 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 $\mathbb{Z}_n$.

An edge (u, v) 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) is called 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.

1.12. 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. we have

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

Sometimes it is useful to mean by a circulant graph, instead, an n-graph which is invariant with respect to an *arbitrary* n-cyclic permutation. Up to isomorphism, both definitions are equivalent. Sometimes, however, in order to make a difference between the definitions, in the second case we speak of *freely* circulant graph.

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.

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.

Sometimes in the literature, circulants are called cyclic or rotation(al) graphs and their connection sets are called symbols.

1.13. Undirected circulants. Suppose $v \in X(\Gamma)$, i.e. $(0, v)$ is an edge of the circulant Γ. Applying the permutation $(0, 1, 2, \ldots, n-1)^{n-v}$, 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.

1.14. Circulant 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 exists 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 are also of valency $r = (n-1)/2$ and, thus, exist only for odd n. 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.

1.15. Remark. As has been recently established (cf. [BroH95] and [Als9y]), undirected self-complementary n-graphs exist if and only if $4|(p-1)$ for *any* prime p dividing n.

1.16. Notations for the numbers of circulants. 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]).

2 Background results

As a trivial consequence of the notion of the connection set, we can count all circulants, *"labelled"* as they are called in enumerative combinatorics, i.e. such that two circulants are counted as different unless they coincide. In other words, labelled graphs are defined on the same set of vertices and (non-trivial) isomorphisms between them play no role.

2.1. Lemma. *For an arbitrary n, there exist exactly:*

- 2^{n-1} *n-circulants and* $\binom{n-1}{r}$ *r-regular n-circulants;*
- $2^{\lfloor n/2 \rfloor}$ *undirected n-circulants and* $\binom{\lfloor n/2 \rfloor}{r}$ *r-regular undirected n-circulants;*
- $2^{(n-1)/2}$ *n-tournaments, n odd.*

Here $\lfloor x \rfloor$ denotes the integer part of x.

PROOF. 2^{n-1} is simply the number of subsets and $\binom{n-1}{r}$ the number of r-subsets of $\mathbb{Z}'_n$, each of which can serve as a connection set of a circulant. In the undirected case, one may choose only from $\mathbb{Z}'_{\lfloor n/2 \rfloor}$ (see 1.13). Finally, for tournaments we are to make $(n-1)/2$ arbitrary pairwise choices from 1 and $n-1$, 2 and $n-2$,…, $\frac{n-1}{2}$ and $\frac{n+1}{2}$. □

As a matter of fact, we aim at counting *"unlabelled"* circulants, that is up to isomorphism. As usual, the labelled enumeration serves as an intermediate subsidiary step to that end.

In the labelled case we must distinguish circulant and freely circulant graphs as they are defined in 1.12: the underlying cyclic automorphism is now essential.

2.2. Corollary. *Suppose $n = p$ is prime and $0 < r < p-1$. The number of labelled r-regular freely circulant p-graphs of each of the following types: (directed) graphs, undirected graphs and tournaments – is equal to $(p-2)!$ multiplied by the corresponding number given in Lemma 2.1.*

PROOF. In the case of prime $n = p$, a freely circulant n-graph cannot be invariant with respect to two different complete cycles unless it is the complete or null graph or these cyclic permutations are powers of each other. This assertion follows easily from the well-known structure of the group $\mathrm{Aut}(\Gamma)$ for prime p (see [ChaW73], [DreKM92], [FarKM94] and references in the latter work). Namely, we need only to know that $\mathrm{Aut}(\Gamma)$ turns out to be a cyclic p-group or a Frobenius group, that is a nonregular transitive group with no non-identity element fixing more than one point. Therefore in any case, $|\mathrm{Aut}(\Gamma)| = |A_0| + |A_1| + 1$ where A_i denotes the subset of elements having exactly i fixed points. On the other hand, by Burnside's formula for the number of orbits (see below), we obtain $1 = \frac{1}{|\mathrm{Aut}(\Gamma)|}(p + |A_1|)$. Hence from these two formulae, $|A_0| = p-1$. But this is just the number of different non-identity powers of a p-cycle.

Thus, the set of freely circulant graphs Γ is partitioned in accordance with the regular cyclic subgroups of $\mathrm{Aut}(\Gamma)$. There are $(p-1)!/(p-1) = (p-2)!$ such groups, and the number of circulants corresponding to each of them, in the three cases, is equal to the one pointed out in Lemma 2.1. □

The paper [ChaW83] contains some other more detailed enumerative results for labelled freely circulant p-graphs. The approach of its authors is based upon known properties of the automorphism groups and simple reduction to the unlabelled enumeration. No results are known for composite n.

Now we pass to unlabelled circulants and isomorphisms between them. The following simple result plays a key role in the theory of circulants.

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

$$mX = X' \tag{M$_1$}$$

for some integer m prime to n where

$$mX := \{mv \mid v \in X\}. \tag{2.3.1}$$

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, $\Gamma(mX) \cong \Gamma(X)$. □

2.4. Remark. For undirected circulant graphs, Lemma 2.3 is clearly also valid in terms of their *reduced* connection sets. Note that Lemma 2.3 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.

2.5. Corollary. *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 (M$_1$) of Lemma 2.3. □

2.6. Layers. In view of Lemma 2.3 it is natural to partition the elements of $X = X(\Gamma)$ into layers according to their greatest divisors common to n: such a divisor remains invariable with respect to multiplying by any number $m \in \mathbb{Z}_n^*$. For any $l|n$ we denote

$$X^{(l)} := \{v \mid v \in X,\ (v, n) = l\} \tag{2.6.1}$$

and call $X^{(l)}$ the *l-layer* of $\Gamma(X)$.

2.7. One-multiplier equivalence. Two connection sets X and X' satisfying the condition (M_1) are called *equivalent* (more exactly, *one-multiplier equivalent* with respect to the multiplier m).

2.8. Ádám's conjecture. Sometimes, (M_1) is also referred to as *Ádám's condition* (though Lemma 2.3 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.*

In principle, of course, directed and undirected circulants should be considered separately. But, usually, the choice is meant only implicitly.

In such a general setting this conjecture is false even for the class of undirected circulants. Therefore two natural questions arose long ago and have been actively discussed since then: to detect the values of n for which the conjecture $\mathbf{A}(n)$ is valid and to find appropriate generalizations of it to other values. These questions are not the subject of the present paper. But we shall discuss them in the course of the whole paper because our approach to the count of circulant graphs heavily relies upon isomorphism criteria.

The following theorem is well known.

2.9. Isomorphism theorem for p-circulants. *The conjecture $\mathbf{A}(n)$ is valid for prime $n = p$.*

This is not a difficult assertion and several its proofs were published since the first one given in [Tur67]. An efficient proof suitable for various generalizations can be obtained in the framework of S-ring theory (see [KliLP9x]).

2.10. Historical remark. In fact (see, for example, [HJP93]), the origin of this direction of researches should be attributed to the thirties, when S. Bays and P. Lambossy proved similar assertions for various classes of combinatorial objects which are defined on p points and possess a (cyclic) automorphism of order p.

Lemma 2.3 and the validity of Ádám's conjecture imply important consequences for enumeration.

2.11. 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 circulant graphs under consideration is equal to the number of orbits of the group $\mathbb{Z}_n^*$ in its induced multiplicative action on the connection sets.* □

This assertion makes it possible to apply Pólya's enumeration theory to the count of circulants.

2.12. Enumeration schemes. Let A be an arbitrary class of combinatorial objects defined on an n-set V of points. Then counting non-isomorphic objects in A in the framework of Pólya–Redfield's enumeration theory can be described, in a rather general form, to consist of the following principal tasks:

- to find a group G acting on A in such a way that two objects $a_1, a_2 \in A$ are isomorphic if and only if $a_1^g = a_2$ for some $g \in G$ (usually $G \subseteq \mathbf{S}_n$ and the action of elements of G on A is induced naturally by relabelling points);
- to count, for any given $g \in G$, the number of objects in A which are invariant with respect to g, i.e. the number $|\{a \in A \mid a^g = a\}|$;
- to apply the well-known orbit enumeration formula which is usually called Burnside's (or the Cauchy–Frobenius–Burnside) lemma.

Sometimes, the last two steps can be replaced by more efficient steps based upon Pólya's theorem of counting (cf. [KliPR88, 2.2], [Ker91, p. 71] or [PalR84]). To that end, one needs:

- to find an intermediate class B of objects defined on the same points such that $A = 2^B$,[1] i.e. the objects under consideration are interpreted as *all possible subsets* of B ("configurations" of "figures", in the terminology of G. Pólya');
- to describe carefully the induced action of the group G on B and to construct its cycle index;
- to make an appropriate substitution of variables in the cycle index (usually such as $x_r := 1 + t^r$, $r = 1, 2, \ldots$) and, whenever possible, to simplify the result.

For example, if A is the class of graphs then we may take $G = \mathbf{S}_n$ and $B = \{(u, v) \mid u, v \in V\}$.

There are also various modifications and generalizations of the second scheme, and later we shall use some of them giving only necessary references and brief explanations.

Now, from the foregoing results it is clear that both schemes are well applicable to circulant graphs, provided the conjecture $\mathbf{A}(n)$ is valid for a given n. In fact, all enumerative results published so far have been obtained just in this way. In terms of these schemes we have:

- $G = \mathbb{Z}_n^*$, the structure of this Abelian group being well known and rather simple for any n;

[1] Or, more generally, $A = d^B$, the set of all functions from B into a d-element set, $d \geq 2$.

- $B = \mathbb{Z}'_n$, that is the set of (the connection sets of) circulant graphs can be identified with $2^{\mathbb{Z}'_n}$ (and the multiplicative group $\mathbb{Z}^*_n$ acts on the subsets of $\mathbb{Z}'_n$ by formula (2.3.1)).

So that we need to describe the action of the group $\mathbb{Z}^*_n$ on $\mathbb{Z}'_n$, i.e. to describe $(\mathbb{Z}^*_n, \mathbb{Z}'_n)$ and to find its cycle index. After that we need to find, if any, the appropriate substitutions of variables for various types of circulant graphs. And for some types, as we shall see later, certain ad hoc reasons should be used.

2.13. Remark. As we mentioned in the Introduction, there exists also an alternative "structural" approach to the enumeration of circulant graphs developed in [KliLP9x]. Instead of isomorphism criterions in terms of multipliers, it uses the lattice of the automorphism groups of circulants. For certain orders n (such as p, p^2 and other) this lattice can be described effectively. This approach is completely based upon the technique of S-rings (cf. [Pös74]) unlike the present paper, where we use only one type of result of this theory: isomorphism theorems. The structural approach is closer to the constructive enumeration and results in quite different counting formulae even for the circulant graphs of order p.

3 Counting circulant graphs of prime orders

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

3.1. Application of the general scheme. Theorem 2.9 enables us to apply the general enumerative schemes 2.12. But in the case of prime $n = p$, the enumeration is simplified considerably (in comparison with the general case) by the fact that $\mathbb{Z}^*_p = \mathbb{Z}'_p$. This means that we need to consider simply the regular action of $\mathbb{Z}^*_p$ on itself, i.e. the permutation group $(\mathbb{Z}^*_p, \mathbb{Z}'_p) = Z_{p-1}$. Thus, its cycle index is defined by formula (1.6.2). Now it remains only to find appropriate substitutions of variables.

For directed circulant graphs, all subsets of $\mathbb{Z}'_p$ without restrictions can serve as their connection sets. This is just the case covered by Pólya's theorem. Therefore the counting polynomial in t is expressed as $\mathcal{I}_n(\mathbf{x})|_{\{x_r:=1+t^r\}_{r=1,2,\dots}}$ where r denotes the valency. The overall number of nonequivalent 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. This yields the desired result for $C_{\mathrm{d}}(p, r), c_{\mathrm{d}}(p, t)$ and $C_{\mathrm{d}}(p)$.

Remarkably that the other two quantities of directed circulant graphs under consideration 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 1.14, 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. It is well known in general (see [PalR84] or [Ker91, p. 73]) that 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, much 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 terms possess only a half degree of freedom. In other words, we put $x_{2i} := 0$ and $x^2_{2i-1} := 2$ (i.e. $x_{2i-1} := \sqrt{2}$) for all i.

Undirected circulant graphs can be counted with the help of a different permutation group than one used for directed circulants. This is the dihedral group (cf. formula (1.6.5) for the corresponding cycle index). But undirected circulant graphs can be also encoded by reduced connection sets as described in 1.13 (cf. also Remark 2.4). Therefore there is 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 $\mathcal{I}_{\frac{p-1}{2}}(\mathbf{x})$.

The 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 into the valency (and the valency of $\Gamma(X)$ is equal to $2|X^{\mathrm{red}}|$ where $X^{\mathrm{red}} \subseteq \mathbb{Z}'_{\frac{p-1}{2}}$).

Thus, we have proved the following theorem.

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

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

□

These formulae cover numerous counting results published earlier in [Dav65], [Tur67], [Als70], [Ast72], [Dav72], [Als73], [ChaW73], [ChiL86], [Zha90], [Ray91] and [Als9x].

3.3. 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 $p = 3, 7, 19, 31$ with corresponding $q = 5, 13, 37, 61$.)

PROOF. Indeed, substitute $q = 2p-1$ instead of p in the second and last formulae of Theorem 3.2. □

3.4. Example. Let $p = 13$. We have here

$$\mathcal{I}_{12}(\mathbf{x}) = \frac{1}{12}(x_1^{12} + x_2^6 + 2x_3^4 + 2x_4^3 + 2x_6^2 + 4x_{12})$$

whence

$$C_{\mathrm{d}}(13) = \frac{1}{12}(2^{12} + 2^6 + 2\cdot 2^4 + 2\cdot 2^3 + 2\cdot 2^2 + 4\cdot 2) = 352.$$

Now,

$$C_{\mathrm{t}}(13) = \frac{1}{12}(2^6 + 2\cdot 2^2) = 6$$

and

$$C_{\mathrm{sd}}(13) = \frac{1}{12}(2^6 + 2\cdot 2^3 + 2\cdot 2^2 + 4\cdot 2) = 8.$$

Similarly

$$\mathcal{I}_6(\mathbf{x}) = \frac{1}{6}(x_1^6 + x_2^3 + 2x_3^2 + 2x_6),$$

$$C_{\mathrm{u}}(13) = \frac{1}{6}(2^6 + 2^3 + 2\cdot 2^3 + 2\cdot 2) = 14$$

and

$$C_{\mathrm{su}}(13) = \frac{1}{6}(2^3 + 2\cdot 2) = 2.$$

4 Circulant graphs of square-free orders

4.1. Isomorphism theorem for circulants of square-free orders [Muz95]. *The conjecture* $\mathbf{A}(n)$ *is valid if* n *is square-free.*

This assertion has been conjectured and actively discussed in the literature long ago. Numerous partial results had been obtained, in particular for $n = pq$ (see [KliP78], [AlsP79], [God83] and [Pál87]). As we mentioned above, M. Muzychuk proved this theorem by using a strong algebraic technique of S-rings.

4.2. Remark. In general, according to [Muz95] and [Muz9x], the conjecture $\mathbf{A}(n)$ (both for directed and undirected graphs) is true for $n = ep_1p_2\cdots p_k$ where $p_1, p_2, \cdots, p_k$ are pairwise distinct odd prime numbers and $e \in \{1, 2, 4\}$), and it is false for all other numbers greater 18 (cf. [Pál87]). See Section 7 for some additional details. Besides, the same isomorphism theorem is known to be valid for certain particular subclasses of circulant graphs of an arbitrary order, for example, undirected graphs of valency 4 (cf. [Sun88] and [Li95]) or those for which X consists only of numbers prime to n, i.e. $X = X^{(1)} \subseteq \mathbb{Z}_n^*$ (cf. [Cha90]). In any of these cases we could apply the same technique to count the corresponding circulants.

Now we are in the position to count circulant graphs of square-free orders. This will be done mostly as in the preceeding section.

4.3. The group $\mathbb{Z}_n^*$ and its actions. The structure of $\mathbb{Z}_n^*$, as an abstract group, is well known from number theory. For square-free n, $\mathbb{Z}_n^* = \prod_{p|n} \mathbb{Z}_{p-1}$ where $\prod$ denotes the direct product (if n is even, $p = 2$ may be, of course, excluded from the product).

As a permutation group, $\mathbb{Z}_n^*$ is also the direct product of regular cyclic groups $Z(p-1)$ *when* it is considered as acting multiplicatively on itself. Thus, its cycle index is expressed by formula (1.7.2) in terms of the cycle indices of the factors. But we need to consider the action of $\mathbb{Z}_n^*$ *on the whole* $\mathbb{Z}_n'$. For brevity, let this group action be denoted by $[\mathbb{Z}_n^*]$ (that is, $[\mathbb{Z}_n^*] = (\mathbb{Z}_n^*, \mathbb{Z}_n')$). It is a (multiple) join as defined in 1.2. Therefore the cycle index of the direct product should be modified appropriately according to formula (1.7.3): new factors appear in each summand. It is a straightforward though somewhat awkward technical matter: the action on a layer $\mathbb{Z}_n^{(l)}$, $l|n$, is calculated by formulae (1.6.1) and (1.6.4) (see formula (1.8.1); cf. also [WeX93]). Discussing these questions goes beyond the framework of our research. It is only worth recalling that $I_{[\mathbb{Z}_n^*]}$ is described in terms of the multiplicative orders of its elements rather than in terms of the very multipliers; these orders are divisors of $\phi(n)$.

Likewise, as explained in 1.13, for undirected circulants we need, instead, to consider the action of $\mathbb{Z}_n^*$ on the set $\mathbb{Z}'_{\frac{n-1}{2}}$. Let the resulting group action be denoted by $[[\mathbb{Z}_n^*]]$.

As a matter of fact, the cycle index of $[[\mathbb{Z}_n^*]]$ could be expressed through that of $[\mathbb{Z}_n^*]$ by some tricky change of variables. We need not to do this and shall consider both polynomials separately.

4.4. Substitutions. Provided that the cyclic index of the required group action has been constructed, it remains only to find the appropriate substitutions of variables.

For odd n there are no distinctions in comparison with the particular case of prime n. We can only add that the corresponding substitution for tournaments could be applied separately to the factors $I_{Z(p-1)}$ before using them for constructing $I_{[\mathbf{Z}_n^*]}$ since the number $[i, j]$ is even if and only if at least one of i and j is even: see formula (1.7.2). Due to this, many summands vanish (a similar reduction is possible for the class of self-complementary circulants); cf. the papers [Ast72] and [Ray91] for details concerning the particular cases $n = p$ or $n = pq$.

Consider now the case of even orders, that is, circulants with $2n$ vertices, n odd square-free. Here, instead of working with $I_{[\mathbf{Z}_{2n}^*]}$ and $I_{[[\mathbf{Z}_{2n}^*]]}$, there is a possibility to make use of $I_{[\mathbf{Z}_n^*]}$ and $I_{[[\mathbf{Z}_n^*]]}$ but only slightly modifying them for calculating $c_d(2n, t)$ and $c_u(2n, t)$.

Namely, as can be easily seen, to calculate $c_d(2n, t)$ and $c_u(2n, t)$ we may do the following:

- take $I_{[\mathbf{Z}_n^*]}$ and $I_{[[\mathbf{Z}_n^*]]}$ respectively;
- raise all their members to power 2 (because we have now the cycle of order $2n$ instead of n);
- multiply finally the result by an additional variable $\tilde{x}_1$ in both cases.

The latter factor corresponds to a possible contribution from the pecular set of symmetric edges ("spokes") connecting the opposite vertices $(0, n)$, $(1, n + 1), \ldots$, $(n, 0), \ldots$, $(2n - 1, n - 1)$. In terms of connection sets, these edges correspond to the case when $n \in X$. But instead of the above modification, we can use directly the same polynomials $I_{[\mathbf{Z}_n^*]}$ and $I_{[[\mathbf{Z}_n^*]]}$ with the modified substitutions $x_r := (1 + t^r)^2$ and $x_r := (1 + t^{2r})^2$ respectively; moreover, $\tilde{x}_1 := 1 + t$.

Finally, as we know, for even n, tournaments and self-complementary graphs do not exist.

The above considerations are summarized in the following theorem.

4.5. Theorem. *Let n be an odd square-free positive integer, then*

$$\begin{aligned}
c_{\rm d}(n,t) &= I_{[\mathsf{Z}_n^*]}(\mathbf{x})|_{\{x_r:=1+t^r\}_{r=1,2,\ldots}}\\
c_{\rm u}(n,t) &= I_{[[\mathsf{Z}_n^*]]}(\mathbf{x})|_{\{x_r:=1+t^{2r}\}_{r=1,2,\ldots}}\\
C_{\rm t}(n) &= I_{[\mathsf{Z}_n^*]}(\mathbf{x})|_{\{x_r:=0\}_{r\ \rm even},\ \{x_r^2:=2\}_{r\ \rm odd}}\\
C_{\rm sd}(n) &= I_{[\mathsf{Z}_n^*]}(\mathbf{x})|_{\{x_r:=0\}_{r\ \rm odd},\ \{x_r:=2\}_{r\ \rm even}}\\
C_{\rm su}(n) &= I_{[[\mathsf{Z}_n^*]]}(\mathbf{x})|_{\{x_r:=0\}_{r\ \rm odd},\ \{x_r:=2\}_{r\ \rm even}}\\
c_{\rm d}(2n,t) &= (1+t)I_{[\mathsf{Z}_n^*]}(\mathbf{x})|_{\{x_r:=(1+t^r)^2\}_{r=1,2,\ldots}}\\
c_{\rm u}(2n,t) &= (1+t)I_{[[\mathsf{Z}_n^*]]}(\mathbf{x})|_{\{x_r:=(1+t^{2r})^2\}_{r=1,2,\ldots}}.
\end{aligned}$$

□

4.6. Examples. We illustrate Theorem 3.2 and the preceeding considerations for the values $n = 15$ and 21. For a better understanding, in the cycle indices we shall use separate variables reflecting the actions on the different layers (namely, in these examples, on the 1-, 3-, 5- and 7-layers).

We have $\mathbb{Z}_{15}^* = \mathbb{Z}_4 \times \mathbb{Z}_2$ as an abstract group. Applying formulae (1.74) and (1.8.1) after some efforts we obtain

$$I_{[\mathsf{Z}_{15}^*]} = \frac{1}{8}(x_1^8y_1^4z_1^2 + x_2^4y_1^4z_2 + x_2^4y_2^2z_1^2 + x_2^4y_2^2z_2 + 2x_4^2y_4z_1^2 + 2x_4^2y_4z_2).$$

Then substituting $x_r = y_r = z_r := 1 + t^r,\ r = 1, 2, \ldots$, we calculate

$$\begin{aligned}
c_{\rm d}(15,t) = {}&1 + 3t + 15t^2 + 50t^3 + 137t^4 + 263t^5 + 395t^6 + 444t^7\\
&+ 395t^8 + 263t^9 + 137t^{10} + 50t^{11} + 15t^{12} + 3t^{13} + t^{14}.
\end{aligned}$$

Now we find $C_{\rm t}(15) = 16,\ C_{\rm sd}(15) = 20$ and $C_{\rm d}(30) = 67195520$. Likewise

$$I_{[[\mathsf{Z}_{15}^*]]} = \frac{z_1}{4}(x_1^4y_1^2 + x_2^2y_1^2 + 2x_4y_2)$$

and by the corresponding substitutions we calculate

$$c_{\rm u}(15,t) = 1 + 3t^2 + 7t^4 + 11t^6 + 11t^8 + 7t^{10} + 3t^{12} + t^{14},$$

$C_{\rm su}(15) = 0$ (cf. Remark 1.15) and

$$\begin{aligned}
c_{\rm u}(30,t) = {}&1 + t + 6t^2 + 6t^3 + 29t^4 + 29t^5 + 104t^6 + 104t^7 + 273t^8\\
&+ 273t^9 + 534t^{10} + 534t^{11} + 793t^{12} + 793t^{13} + 904t^{14}\\
&+ 904t^{15} + 793t^{16} + 793t^{17} + 534t^{18} + 534t^{19} + 273t^{20}\\
&+ 273t^{21} + 104t^{22} + 104t^{23} + 29t^{24} + 29t^{25} + 6t^{26} + 6t^{27} + t^{28} + t^{29}.
\end{aligned}$$

Likewise

$$\begin{aligned}
I_{[\mathsf{Z}_{21}^*]} = {}&\tfrac{1}{12}(x_1^{12}y_1^6z_1^2 + x_2^6y_1^6z_2 + x_2^6y_2^3z_1^2 + x_2^6y_2^3z_2 + 2x_3^4y_3^2z_1^2 + 2x_6^2y_3^2z_2\\
&+ 2x_6^2y_6z_1^2 + 2x_6^2y_62z_2)
\end{aligned}$$

whence $C_{\mathrm{d}}(21) = 88376$ and $C_{\mathrm{t}}(21) = C_{\mathrm{sd}}(21) = 88$. Finally

$$I_{[[\mathbf{Z}^*_{21}]]} = \frac{z_1}{6}(x_1^6 y_1^3 + x_2^3 y_1^3 + 2x_3^2 y_3 + 2x_6 y_3),$$

whence $c_{\mathrm{u}}(21,t) = 1+3t^2+9t^4+24t^6+40t^8+46t^{10}+40t^{12}+24t^{14}+9t^{16}+3t^{18}+t^{20}$ and $C_{\mathrm{u}}(42) = 355200$.

5 Circulant graphs of order p^k

Prime-powers represent another generalization of primes, and our results for circulant graphs of such orders considerably differ from the previous ones. Here we only reduce the enumeration to a certain number of well-specified problems of Pólya's type.

5.1. p^i-Layers. For $n = p^k$ (p prime), we partition any connection set X into k layers according to the divisibility of the elements of X by powers of p:

$$X = X_{(0)} \mathbin{\dot\cup} X_{(1)} \mathbin{\dot\cup} \cdots \mathbin{\dot\cup} X_{(k-1)} \tag{5.1.2}$$

where the *i-layer* is $X_{(i)} = X \cap p^i Z^*_{p^{k-i}}$ (the set $p^{-i}X_{(i)}$ can be regarded modulo p^{k-i}). In designations of 2.6, $X_{(i)} = X^{(p^i)}$.

The following theorem plays the crucial role in the subsequent considerations.

5.2. Isomorphism theorem for p^k-circulants [KliP80, Theorem 2.3]**.** *Let $n = p^k$ (p an odd prime) and Γ and Γ' be two p^k-circulants with the connection sets $X = X(\Gamma)$ and $X' = X(\Gamma')$, respectively. Then Γ and Γ' are isomorphic if and only if their respective layers are multiplicatively equivalent, i.e.*

$$X'_{(i)} = m_i X_{(i)}, \quad i = 0, 1, \ldots, k-1, \tag{M$_k$}$$

for an arbitrary set of multipliers $m_0, m_1, \ldots, m_{k-1}$ which satisfy the following constraints: whenever the layer $X_{(i)}$ satisfies the non-invariance condition

$$(1 + p^{k-i-j-1})X_{(i)} \neq X_{(i)}, \tag{R$_{ij}$}$$

for some $i \in \{0, 1, \ldots, k-2\}$ and $j \in \{0, 1, \ldots, k-2-i\}$, then the successive multipliers $m_i, \ldots, m_{k-j-1}$ must meet the congruences

$$\left.\begin{array}{lll} m_{i+1} & \equiv m_i & (\mathrm{mod}\ p^{k-i-j-1}) \\ m_{i+2} & \equiv m_{i+1} & (\mathrm{mod}\ p^{k-i-j-2}) \\ & \cdots & \\ m_{k-j-1} & \equiv m_{k-j-2} & (\mathrm{mod}\ p) \end{array}\right\} \tag{E$_{ij}$}$$

A similar isomorphism theorem is valid for $p = 2$ as well [GolNP85] but with minor pecularities. Therefore we exclude this case from the further consideration.

It is clear that, in principle, this theorem is sufficient to split the count of p^k-circulants into a number of Pólya type problems (cf. 2.12). But in order to achieve this aim rigorously, we need to examine thoroughly the restrictions of the theorem and their interactions.

Henceforth, to facilitate comprehension, we shall write pairs of parameters briefly as ij or in parentheses separated by commas, so that, for example, $(\mathrm{R}_{(i,j)})$ denotes the same as (R_{ij}).

5.3. Decomposition. The conditions in Theorem 5.2 imply a number of properties important for enumeration. Instead of a single multiplier acting on the connection sets by (M_1), we have k multipliers acting on the layers by (M_k). These multipliers form certain "near-diagonal" subgroups of the direct sum $Z^*_{p^k} \oplus \cdots \oplus Z^*_{p^k}$ (in fact, of $Z^*_{p^k} \oplus Z^*_{p^{k-1}} \oplus \cdots \oplus Z^*_p$) specified by the combinations of congruences (E_{ij}). And, moreover, the (induced setwise) action of such a restricted subgroup is defined exactly on the connection sets that meet the corresponding non-invariance conditions (R_{ij}).

There are $\binom{k}{2}$ non-invariance conditions (R_{ij}), and all their combinations together with the remaining invariance conditions must be considered as separate action constraints. But not all of such combinations are significant: due to congruence (1.9.2), the implication

$$(\mathrm{R}_{ij}) \Longrightarrow (\mathrm{R}_{ij'}) \tag{5.3.1}$$

holds whenever $j' \geq j$. Thus, for each i, no more than one condition (R_{ij}) should be selected and placed into a combination of constraints on connection sets.

This means that we can split (additively) the count of p^k-circulants into $k!$ *"primary"* subproblems Q_f. Every Q_f is parametrized by an integer-valued function $f:\ [0,k-2] \to [0,k-2]$ satisfying the restriction $i+f(i) \leq k-1$ for all i. The problem Q_f is specified exactly by the set of the non-invariance conditions

$$\mathrm{R}_f = \{(\mathrm{R}_{ij}) \mid i = 0,1,\ldots,k-2;\ j = f(i),\ j < k-1-i\} \tag{5.3.2}$$

and the set of the corresponding congruences

$$\mathrm{E}_f = \{(\mathrm{E}_{ij}) \mid i = 0,1,\ldots,k-2;\ j = f(i),\ j < k-1-i\}. \tag{5.3.3}$$

For uniformity we put $j = f(i) := k-1-i$ whenever for some i, no condition (R_{ij}) is presented in R_f.

The exact choice of the set R_f means that it should be complemented by the set of all *invariance* conditions

$$(1+p^{k-i-j-1})X_{(i)} = X_{(i)} \qquad \neg(\mathrm{R}_{ij})$$

that do not contradict R_f by implication (5.3.1). For each i it suffices to take $\neg(\mathrm{R}_{ij})$ with the maximal possible value of j, i.e. Q_f is specified by the set of the additional conditions

$$\mathrm{T}_f = \{\neg(\mathrm{R}_{(i,j-1)}) \mid i = 0, 1, \ldots, k-2;\ j = f(i) > 0\}. \qquad (5.3.4)$$

They are valid for the case when $f(i) = k - 1 - i$ as well.

5.4. Subproblem specification. Now the problem Q_f can be formulated as follows:

> *count the orbits of the group*
>
> $$\mathcal{G}_f = (Z^*_{p^k} \oplus Z^*_{p^{k-1}} \oplus \cdots \oplus Z^*_p)/\mathrm{E}_f$$
>
> *acting multiplicatively component-wise on the set* C_f *(see below) of connection sets satisfying the restrictions* $\mathrm{R}_f \cup \mathrm{T}_f$ *as defined by* (5.3.2) *and* (5.3.4).

Here $/\mathrm{E}_f$ denotes taking the subgroup of multipliers that meet all congruences in E_f. $\mathcal{G}_f$ is considered in its induced setwise action as defined by formula (2.3.1).

C_f is the disjoint union

$$\mathsf{C}_f = \mathrm{C}_{(0,f(0))} \mathbin{\dot{\bigcup}} \mathrm{C}_{(1,f(1))} \mathbin{\dot{\bigcup}} \cdots \mathbin{\dot{\bigcup}} \mathrm{C}_{(k-2,f(k-2))} \mathbin{\dot{\bigcup}} \mathrm{C}_{k-1} \qquad (5.4.1)$$

where the set $\mathrm{C}_{(i,f(i))}$ consists of all subsets of $p^i Z^*_{p^{k-i}}$ satisfying the condition $(\mathrm{R}_{(i,f(i))})$ if $f(i) < k - 1 - i$ and, moreover, satisfying the condition $\neg(\mathrm{R}_{(i,f(i)-1)})$ if $f(i) > 0$. C_{k-1} is the set of all subsets of $p^{k-1}Z^*_p$ with no restrictions.

5.5. Base points. The reduction 5.3 is a straightforward consequence of Theorem 5.2. But there is a possibility to reduce the collection of subproblems by joining some of them and, what is more important, simplifying their settings at the same time.

The idea is to make use of the similar implication between the congruences

$$(\mathrm{E}_{ij}) \Longrightarrow (\mathrm{E}_{i'j}) \qquad (5.5.1)$$

whenever $i' \geq i$. It is immediate from the definition of (E_{ij}). Therefore, if two primary subproblems Q_f and $\mathsf{Q}_{f'}$ differ only in index pairs that are connected by implications (5.5.1), then $\mathrm{E}_f = \mathrm{E}_{f'}$ and $\mathcal{G}_f = \mathcal{G}_{f'}$. Thus, instead of orbits of two groups with actions $(\mathcal{G}_f, \mathsf{C}_f)$ and $(\mathcal{G}_{f'}, \mathsf{C}_{f'})$, we can count orbits of their join, i.e. we may replace the problems Q_f and $\mathsf{Q}_{f'}$ by one new combined problem.

As a result, we arrive at the following collection of enlarged enumerative problems $\mathsf{P}_{\mathbf{b}}$ which are specified by $\mathcal{G}_{\mathbf{b}}$ and $\mathsf{C}_{\mathbf{b}}$ and will be denoted by $\mathsf{P}_{\mathbf{b}} = [\mathcal{G}_{\mathbf{b}}, \mathsf{C}_{\mathbf{b}}]$. Here $\mathbf{b}$ is any (possibly, empty) set of pairs ij which satisfy the inequalities $i, j \geq 0$ and $i + j \leq k - 2$ and are mutually *incompatible* in the partial order

$$ij \leq i'j' \iff i \leq i' \ \&\ j \leq j'.$$

In other words, for no different pairs ij and $i'j'$ in $\mathbf{b}$, the inequalities $i \leq i'$ and $j \leq j'$ hold simultaneously. Therefore we can present $\mathbf{b}$ as the following ordered sequence of pairs:

$$\mathbf{b} := \{i_s j_s \mid s = 1, 2, \ldots\} = \{i_1 j_1, i_2 j_2, \ldots \mid i_1 < i_2 < \ldots;\ j_1 > j_2 > \ldots\}. \quad (5.5.2)$$

Let also

$$\mathbf{b}^{(1)} := \{i_1, i_2, \ldots\}$$

denote the sequence of i-indices of the pairs in $\mathbf{b}$ in ascending order. Now

$$\mathcal{G}_{\mathbf{b}} = (Z^*_{p^k} \oplus Z^*_{p^{k-1}} \oplus \cdots \oplus Z^*_p)/\mathrm{E}_{\mathbf{b}} \quad (5.5.3)$$

where $\mathrm{E}_{\mathbf{b}} = \{(\mathrm{E}_{i_s j_s}) \mid i_s j_s \in \mathbf{b}\}$ and $/\mathrm{E}_{\mathbf{b}}$ denotes, as above, taking the subgroup of multipliers that meet all congruences in $\mathrm{E}_{\mathbf{b}}$.

5.6. Lattice walks. To specify $\mathsf{C}_{\mathbf{b}}$, it is convenient to represent pairs ij by points of the plane *integer lattice*. More exactly, we consider the triangle Δ_k of points with integer coordinates ij satisfying the inequalities $0 \le i,\ 0 \le j$ and $i + j \le k$. Δ_k contains the main diagonal $\{ij \mid i + j = k,\ i, j \ge 0\}$ and the *subdiagonal* $\{ij \mid i + j = k - 1,\ i, j \ge 0\}$ while, by definition, the points $i_s j_s$ of $\mathbf{b}$ lie strictly below them. The points from $\mathbf{b}$ are called the *base* points, all points below the subdiagonal are called *proper* and the points on the main diagonal and subdiagonal are called *improper*.

Consider the region $U_{\mathbf{b}}$ in Δ_k consisting of the subdiagonal and all proper points ij such that $i \ge i_s$ and $j \ge j_s$ for some $i_s j_s \in \mathbf{b}$.

In these terms, the problem $\mathsf{P}_{\mathbf{b}}$ combines the primary subproblems Q_f with arbitrary functions f whose graphs lie in $U_{\mathbf{b}}$ and pass through all the base points, i.e. $(i, f(i)) \in U_{\mathbf{b}}$ for any i and $f(i_s) = j_s$ for any $i_s \in \mathbf{b}^{(1)}$ and $i_s j_s \in \mathbf{b}$.

More explicitly, $U_{\mathbf{b}}$ is specified by the set $w_{\mathbf{b}}$ of all its lowest points in the columns together with all its extreme left points in the rows. Let us augment the region $U_{\mathbf{b}}$ by the main diagonal: $\overline{U_{\mathbf{b}}} = U_{\mathbf{b}} \cup \{ij \mid i + j = k,\ i, j \ge 0\}$. Now take every point $ij \in \Delta_k$ such that both neighbouring points below and to the left of it (i.e. the points $(i, j - 1)$ and $(i - 1, j)$, respectively) belong to $w_{\mathbf{b}}$. We adjoin all such points to $w_{\mathbf{b}}$ and denote the extended set, thus obtained, by $W_{\mathbf{b}}$. Then, clearly, $W_{\mathbf{b}}$ forms a *monotone*, right- and downwards, *k-walk* going from the point $0k$ to $k0$ and possessing the property that $\mathbf{b}$ is the set of all *proper* zigzag points on $W_{\mathbf{b}}$ turning it counterclockwise (i.e. its proper south-west corners). Vice versa, for any monotone k-walk, the set of all its points together with the points lying over them up to the main diagonal forms the region $\overline{U_{\mathbf{b}}}$ for some $\mathbf{b}$.

An example is depicted in Fig. 1 where the solid circles "•" present the base points while the hollow circles "∘" present the other points on the walk. The points lying over the walk and belonging to $U_{\mathbf{b}}$ are emphasized.

It is evident that for any $\mathbf{b}$, there exists a unique monotone walk $W_{\mathbf{b}}$ and it can be constructed according to the following rules:

(1) Start with $0k$ and move down (to the south).

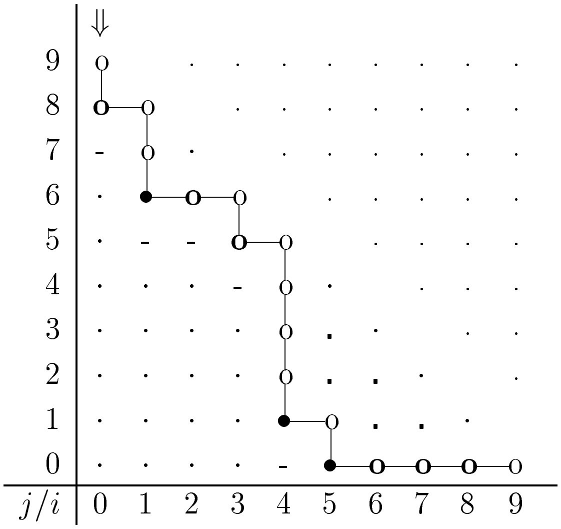

Figure 1: A 9-walk and its base point set $\mathbf{b} = \{16, 41, 50\}$

(2) Any time after turning to the east (counterclockwise) proceed to move horizontally until reaching the nearest point situated over a base point or on the main diagonal. There turn down (clockwise).

(3) Any time moving down (including the start) go until reaching the base point, if any in the column, or otherwise one step only (to the corresponding subdiagonal point). Here again turn to the east and go on in the same manner until reaching the point $k0$.

Note also that clockwise turns are just the points we have added to $w_{\mathbf{b}}$ in order to obtain $W_{\mathbf{b}}$.

In this way we have established a one-to-one correspondence between arbitrary base point sets and monotone k-walks. The cardinality of the latter is known to be equal to the k-th *Catalan* number $\mathrm{Cat}(k) = \dfrac{1}{k+1}\dbinom{2k}{k}$ (cf., for example, [HilP91], [Sta9x] and [DerZ80]).

Let $\lambda_{\mathbf{b}}(i)$ denote the row number of the lowest point of the set $U_{\mathbf{b}}$ (and $W_{\mathbf{b}}$, by definition) in the i-th column, $0 \leq i \leq k-1$. In particular, $\lambda_{\mathbf{b}}(i_s) = j_s$ if $i_s j_s \in \mathbf{b}$. In Fig. 1, the other corresponding points $ij \in W_{\mathbf{b}}$ with $j = \lambda_{\mathbf{b}}(i)$ (hole circles) are emphasized. In general, $\lambda_{\mathbf{b}}(i)$ is a monotone decreasing ("ladder") function that can be easily calculated: if i is such that $i_s \leq i < i_{s+1}$ for some $s \geq 1$ (or i is greater than or equal to the greatest $i_s \in \mathbf{b}^{(1)}$) and $i + j_s < k$, then $\lambda_{\mathbf{b}}(i) = j_s$, otherwise (including the case $i < i_1$ when $i_1 > 0$) $\lambda_{\mathbf{b}}(i) = k - i - 1$ (the corresponding subdiagonal point).

In these terms, the set $\mathsf{C}_{\mathbf{b}}$ combines the connection sets C_f with all possible functions $j = f(i)$ taking values $j \in [\lambda_{\mathbf{b}}(i), k-1-i]$ for any $i \notin \mathbf{b}^{(1)}$. This means that for such i, no restriction (R_{ij}) is endowed while we have the following set of the non-invariance conditions

$$\mathrm{R}_{\mathbf{b}} = \{(\mathrm{R}_{i_s j_s}) \mid i_s j_s \in \mathbf{b};\ s = 1, 2, \ldots\} \tag{5.6.1}$$

and the following set of the invariance conditions

$$\mathrm{T}_{\mathbf{b}} = \{\neg(\mathrm{R}_{(i,\lambda_{\mathbf{b}}(i)-1)}) \mid i = 0, 1, \ldots, k-2;\ \lambda_{\mathbf{b}}(i) > 0\}. \tag{5.6.2}$$

In Fig. 1, the points with coordinates $(i, \lambda_{\mathbf{b}}(i) - 1)$, i.e. lying directly below the walk, are marked as "–".

In general, these are much simpler restrictions in comparison with C_f (formula (5.4.1)) especially when the set $\mathbf{b}$ consists of points $i_s j_s$ with small coordinates. The most dramatic reduction takes place for $\mathbf{b} = \{00\}$: $\mathsf{P}_{\{00\}}$ covers $(k-1)!$ primary subproblems Q_f and its connection sets are restricted by the only condition (R_{00}).

Speaking formally, we obtain here the disjoint union

$$\mathsf{C}_{\mathbf{b}} = \overline{\mathrm{C}}_{(0,\lambda_{\mathbf{b}}(0))} \mathbin{\dot{\bigcup}} \overline{\mathrm{C}}_{(1,\lambda_{\mathbf{b}}(1))} \mathbin{\dot{\bigcup}} \cdots \mathbin{\dot{\bigcup}} \overline{\mathrm{C}}_{(k-2,\lambda_{\mathbf{b}}(k-2))} \mathbin{\dot{\bigcup}} \mathrm{C}_{k-1} \tag{5.6.3}$$

where $\overline{\mathrm{C}}_{(i,\lambda_{\mathbf{b}}(i))} = \mathrm{C}_{(i,\lambda_{\mathbf{b}}(i))}$ (cf. (5.4.1)) if $i = i_s \in \mathbf{b}^{(1)}$ for some s (i.e. $(i, \lambda_{\mathbf{b}}(i)) \in \mathbf{b}$) and, otherwise, $\overline{\mathrm{C}}_{(i,\lambda_{\mathbf{b}}(i))}$ consists of all subsets of $p^i Z^*_{p^{k-i}}$ satisfying the single condition $\neg(\mathrm{R}_{(i,\lambda_{\mathbf{b}}(i)-1)})$, provided $\lambda_{\mathbf{b}}(i) > 0$ (the latter condition has no meaning if $\lambda_{\mathbf{b}}(i) = 0$).

Thus, we have obtained the main result of this paper.

5.7. Theorem. *The number of non-isomorphic circulant p^k-graphs equals the sum of the solutions of* $\mathrm{Cat}(k)$ *of orbit enumeration problems* $\mathsf{P}_{\mathbf{b}} = [\mathcal{G}_{\mathbf{b}}, \mathsf{C}_{\mathbf{b}}]$ *where the group $\mathcal{G}_{\mathbf{b}}$ of multipliers is defined by formula* (5.5.3) *and $\mathsf{C}_{\mathbf{b}}$ is the set of all connection sets satisfying the restrictions* $\mathrm{R}_{\mathbf{b}} \cup \mathrm{T}_{\mathbf{b}}$ *as specified by* (5.6.1) *and* (5.6.2). □

Each $\mathsf{P}_{\mathbf{b}}$ is a "routine", though possibly tedious, Pólya type problem. Really, due to representation (1.9.1) of numbers, $\mathsf{P}_{\mathbf{b}}$ can be described as dealing with the count of invariant subsets of a certain set with respect to the induced action of the corresponding group.

Of course the same decomposition takes place for all subclasses of circulant p^k-graphs considered above: undirected graphs, tournaments, etc.

Recall that asymptotically $\mathrm{Cat}(k)$ grows exponentially, namely, as $\pi^{-1/2}k^{-3/2}4^k$.

5.8. Equalities between multipliers. The description of $\mathcal{G}_{\mathbf{b}}$ can be simplified further due to the following idea. The non-invariance condition (R_{ij}) can be rewritten in terms of the set $p^{-i}X_{(i)} \subseteq Z^*_{p^{k-i}}$. Accordingly, multipliers m_i together with the numbers in this set can be considered modulo p^{k-i}. Let us consider the system of congruences (E_{i0}). In the first congruence $m_{i+1} \equiv m_i \pmod{p^{k-i-1}}$, the left-hand member m_{i+1} is defined modulo p^{k-i-1}. Therefore, according to 1.10, this congruence may be replaced by an equality. The same holds for the other congruences making it possible to rewrite all of them in the form of "diagonal" equalities $m_{k-1} = m_{k-2} = \ldots = m_{i+1} = m_i$. In particular, the non-invariance relation (R_{00}) implies that *all* multipliers $m_0, m_1, \ldots, m_{k-1}$ coincide. This is just Ádám's condition (M_1), the simplest case.

Now let us discuss such questions in general: given an arbitrary base point set $\mathbf{b}$, which congruences in $\mathrm{E}_{\mathbf{b}} = \{(\mathrm{E}_{i_s j_s}) \mid i_s j_s \in \mathbf{b}\}$ are redundant and which ones can be replaced by equalities?

If $\neg(\mathrm{R}_{ij}) \in \mathrm{T}_{\mathbf{b}}$, then m_i and the elements of $X_{(i)}$ are defined up to the factor $1 + p^{k-i-j-1}$ of order p^{i+j+1}. Thus, we may now consider m_i modulo $p^{k-i-j-1}$, a fortiori narrowing the domain of the multiplier m_i and the group $\mathcal{G}_{\mathbf{b}}$. Generally speaking, by Indifference lemma 1.5, this is unessential for the count of orbits and we may consider $\mathcal{G}_{\mathbf{b}}$ *up to* such possible refinements. But it enables us to transform some congruences into equalities. In this manner, the number of multipliers generating $\mathcal{G}_{\mathbf{b}}$ can be reduced. It is natural to reduce $\mathcal{G}_{\mathbf{b}}$ as much as possible. Let $\mathcal{G}'_{\mathbf{b}}$ denote the resulting *reduced* group. Then $\mathcal{G}'_{\mathbf{b}}$ is generated by $\varrho_{\mathbf{b}}$ independent multipliers (*"the multiplier rank"*) where $\varrho_{\mathbf{b}} = k - \varepsilon_{\mathbf{b}}$ and $\varepsilon_{\mathbf{b}}$ stands for the number of (independent) congruences in $\mathrm{E}_{\mathbf{b}}$ which are representable as equalities. In particular, $\varrho_{\mathbf{b}} = 1$ means that the group $\mathcal{G}'_{\mathbf{b}}$ corresponds to Ádám's condition, i.e. it is generated by a single multiplier.

Observe also that, given m_i, the congruence $m_{i+1} \equiv m_i \pmod{p^{k-i-j-1}}$, $j \geq 0$, provides p^j degrees of freedom for selecting a value of m_{i+1}. Then for any such value, the next congruence $m_{i+2} \equiv m_{i+1} \pmod{p^{k-i-j-2}}$ provides p^j degrees of freedom for selecting a value of m_{i+2} and so on.

Now, some simplifications in describing $\mathrm{E}_{\mathbf{b}}$ follow directly from the fact that the congruence $m_{i+1} \equiv m_i \pmod{p^v}$ implies $m_{i+1} \equiv m_i \pmod{p^u}$ if $u \leq v$.

A base point $i_s j_s$ defines $k - i_s - j_s - 1$ congruences $m_{i+1} \equiv m_i \pmod{p^{k-j_s-i-1}}$ for all $i \in [i_s,\ k - j_s - 2]$. These segments with growing ends can intersect. Given index i, consider all such segments which contain i. If i belongs to several segments, that is, if the congruences $m_{i+1} \equiv m_i$ appear several times, then all these congruences are absorbed by one of them modulo p^{k-j_s-i-1} with the minimal j_s, i.e. with the maximal index s. Now it is clear that this "absorbing" exponent j_s is equal to $\lambda_{\mathbf{b}}(i)$. If for some i no such congruence arises, for uniformity we may put formally such exponent to be equal to $\lambda_{\mathbf{b}}(i) = k - i - 1$: this value corresponds to the vacuous congruence $m_{i+1} \equiv m_i \pmod{p^0}$.

Thus, the reduced group $\mathcal{G}'_{\mathbf{b}}$ is specified by the system of congruences

$$m_{i+1} \equiv m_i \pmod{p^{k-\lambda_{\mathbf{b}}(i)-i-1}},\ i = 0, 1, \ldots, k-2, \tag{5.8.1}$$

which, in fact, have a sense if and only if $\lambda_{\mathbf{b}}(i) < k - i - 1$.

On the other hand, according to the set of conditions $\mathrm{T}_{\mathbf{b}}$ (see (5.6.2)) we know that the multiplier m_i is defined modulo $p^{k-\lambda_{\mathbf{b}}(i)-i}$ if $\lambda_{\mathbf{b}}(i) > 0$. But m_i is certainly defined modulo p^{k-i}, so that m_i, $i = 0, 1, \ldots, k-2$, is defined mod $p^{k-\lambda_{\mathbf{b}}(i)-i}$ regardless of whether $\lambda_{\mathbf{b}}(i) = 0$ or not.

Now, according to 1.10, congruence (5.8.1) for some index i may be replaced by the corresponding equality if and only if either $k-\lambda_{\mathbf{b}}(i)-i \leq k-\lambda_{\mathbf{b}}(i)-i-1$, what is impossible, or $k-\lambda_{\mathbf{b}}(i+1)-(i+1) \leq k-\lambda_{\mathbf{b}}(i)-i-1$, i.e. $\lambda_{\mathbf{b}}(i+1) \geq \lambda_{\mathbf{b}}(i)$. But $\lambda_{\mathbf{b}}(i)$ is a decreasing function, therefore the last inequality takes place if and only if $\lambda_{\mathbf{b}}(i+1) = \lambda_{\mathbf{b}}(i)$. In turn, by the description of the function $\lambda_{\mathbf{b}}(i)$ given in 5.6, this is valid if and only if $i+1 \notin \mathbf{b}^{(1)}$. Thus, we arrived at the following statement.

5.9. Proposition. *The reduced group $\mathcal{G}'_{\mathbf{b}}$ of the problem $\mathsf{P}_{\mathbf{b}}$ is specified by the equalities*

$$m_i = m_{i-1} \tag{5.9.1}$$

for all i, $i = 1, 2, \ldots, k-1$, such that

$$i \notin \mathbf{b}^{(1)} \text{ and } \lambda_{\mathbf{b}}(i-1) < k-i$$

and by the congruences

$$m_i \equiv m_{i-1} \pmod{p^{k-\lambda_{\mathbf{b}}(i-1)-i}}$$

for the remaining i such that $\lambda_{\mathbf{b}}(i-1) < k-i$. □

5.10. Examples. We consider a simple illustrating example for $k = 4$ and the subproblem specified by two base points 01 and 10, cf. Fig. 2. The connection sets satisfy the restrictions (R_{01}), (R_{10}) and $\neg(\mathrm{R}_{00})$. By Theorem 5.2 we have four congruences:

$$m_1 \equiv m_0 \pmod{p^2},\ m_2 \equiv m_1 \pmod{p},\ m_2 \equiv m_1 \pmod{p^2},\ m_3 \equiv m_2 \pmod{p}.$$

Now the third congruence implies the second one. The multiplier m_3 is defined modulo p, whence the last congruence may be turned into an equality. Likewise, m_2 modulo p^2 transforms the third congruences into an equality. The invariance condition $\neg(\mathrm{R}_{00})$ implies only that m_0 is defined modulo p^3. The multiplier m_1 has the same domain. Thus, no other reductions are possible and the final restrictions are

$$m_3 = m_2 = m_1 \text{ and } m_1 \equiv m_0 \pmod{p^2}.$$

In other words, denoting $m_1 := m$ and $m_0 := m + lp^2$ where m is modulo p^2 and l is modulo p, we obtain the group of all multiplier quadruples of the form $(m + lp^2, m, m, m)$ with the element-wise multiplication.

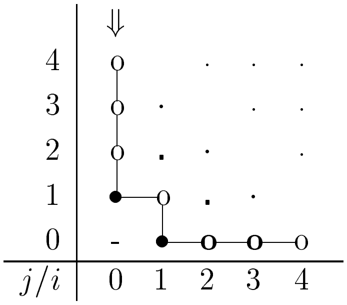

Figure 2: The 4-walk with $\mathbf{b} = \{01, 10\}$

Note also (though, as we know, this is nonessential for enumeration) that in this example the multipliers m_2 and m_3 are initially defined modulo p^2 and p respectively. But in spite of that, we need to consider their common value modulo p^3 since they are equal to m_1, which is defined modulo p^3.

Similarly, for the problem presented in Fig. 1, by Proposition 5.9, we obtain:

$$m_8 = m_7 = m_6 = m_5, \ m_2 = m_1 \ \text{ and } \ m_5 \equiv m_4 \pmod{p^3}.$$

Several useful properties follow directly from the above reasonings and some evident properties of the monotone walks.

5.11. Corollary. *All reduced groups $\mathcal{G}'_{\mathbf{b}}$ (and problems $\mathsf{P}_{\mathbf{b}}$, respectively) are pairwise different. In all but one cases the set of equalities* (5.9.1) *specifying $\mathcal{G}'_{\mathbf{b}}$ is not empty (i.e. $\varrho_{\mathbf{b}} < k$) and in all but one cases the number of these equalities is less than $k-1$ (i.e. $\varrho_{\mathbf{b}} > 1$). More exactly, the rank $\varrho_{\mathbf{b}}$ of $\mathcal{G}'_{\mathbf{b}}$ equals the number of all (proper or improper) counterclockwise zigzag points of the walk $W_{\mathbf{b}}$.* □

The two exceptional cases mentioned in this corollary correspond to $\mathbf{b} = \emptyset$ and $\mathbf{b} = \{00\}$, respectively.

As can be easily seen (cf. [DerZ80] and [MalW72]), there are $\frac{1}{k}\binom{k}{r}\binom{k}{r-1}$ monotone k-walks having r counterclockwise zigzag points, $r = 1, 2, \ldots, k$, (these are the so-called Narayana numbers). Due to the last statement of the Corollary, this is the number of problems $\mathsf{P}_{\mathbf{b}}$ with the reduced groups $\mathcal{G}'_{\mathbf{b}}$ of rank r.

The set of the remaining congruences specifying $\mathsf{P}_{\mathbf{b}}$ is empty if and only if the walk $W_{\mathbf{b}}$ is such that all its clockwise zigzag points lie on the main diagonal. Any combinations are possible and each of them defines $W_{\mathbf{b}}$. Therefore

5.12. Corollary. *There exist exactly 2^{k-1} subproblems which are specified by "diagonal" equalities* (5.9.1) *without congruences.* □

Let $H_\mathbf{b}$ denote the number of primary problems Q_f covered by the problem $\mathsf{P}_\mathbf{b}$. It can be easily calculated via $\lambda_\mathbf{b}(i)$:

$$H_\mathbf{b} = \prod_{i \notin \mathbf{b}^{(1)}} \Big(k - \lambda_\mathbf{b}(i) - i\Big).$$

The results of the case-by-case analysis of the subproblems for $k \le 4$ are presented in Table 1.

k	$\mathbf{b} =$	$\mathrm{T}_\mathbf{b}$:	$H_\mathbf{b}$	Group $\mathcal{G}'_\mathbf{b}$		
	$\{ij\}$	indices		$\varrho_\mathbf{b}$	Equalities	Congruences
1	$\emptyset$	$\emptyset$	1	1	-	-
2	$\emptyset$	00	1	2	-	-
	00	$\emptyset$	1	1	$m_1 = m_0$	-
3	$\emptyset$	01,10	1	3	-	-
	00	$\emptyset$	2	1	$m_2 = m_1 = m_0$	-
	01	00,10	1	2	$m_1 = m_0$	-
	10	01	1	2	$m_2 = m_1$	-
	01,10	00	1	2	$m_2 = m_1$	$m_1 \equiv m_0\ (p)$
4	$\emptyset$	02,11,20	1	4	-	-
	00	$\emptyset$	6	1	$m_3 = m_2 = m_1 = m_0$	-
	01	00,10,20	2	2	$m_2 = m_1 = m_0$	-
	02	01,11,20	1	3	$m_1 = m_0$	-
	10	02	2	2	$m_3 = m_2 = m_1$	-
	11	02,10,20	1	3	$m_2 = m_1$	-
	20	02,11	1	3	$m_3 = m_2$	-
	01,10	00	2	2	$m_3 = m_2 = m_1$	$m_1 \equiv m_0\ (p^2)$
	01,20	00,10	2	2	$m_3 = m_2,\ m_1 = m_0$	$m_2 \equiv m_1\ (p)$
	02,10	01	2	2	$m_3 = m_2 = m_1$	$m_1 \equiv m_0\ (p)$
	02,11	01,10,20	1	3	$m_2 = m_1$	$m_1 \equiv m_0\ (p)$
	02,20	01,11	1	2	$m_3 = m_2,\ m_1 = m_0$	-
	11,20	02,10	1	3	$m_3 = m_2$	$m_2 \equiv m_1\ (p)$
	02,11,20	01,10	1	3	$m_3 = m_2$	$m_2 \equiv m_1\ (p)$, $m_1 \equiv m_0\ (p)$

Table 1: The subproblem list for counting p^k-circulants, $k \le 4$

5.13. Concluding remarks. 1. Monotone lattice walks are usually considered to go from the origin 00 to kk in the positive directions over (or, sometimes, under) the diagonal $i = j$. Of course, we could "normalize" our descriptions by a suitable change of variables in Theorem 5.2. But in the coordinates we use, some expressions obtained look more convenient.

2. In practice, evidently, it is more convenient to count orbits under restrictions having the form of equalities (invariance conditions) rather than inequalities (such as (R_{ij})), subtracting then the result from the total number. Thus, the subproblems under consideration should be, in turn, separated into intermediate problems, which can be combined by the inclusion–exclusion method. This takes place even in the case of $n = p^2$ (see the next section).

3. It is noteworthy that there is another connection between p^k-circulants and the classical Catalan numbers which has been recently established in [KliP9x]. Namely, the number of certain "atomic sequences" important for constructing the automorphism groups of such circulants turned out to be equal to $\mathrm{Cat}(k-1)$.

4. Manipulating with lattice walks, we introduced several simple notions similar or equivalent to ones used actively in recent researches (cf., for example, [Kra95a], and [Kra95b]). One peculiarity is that we distinguish proper and improper points. In particular, the empty set $\mathbf{b}$ corresponds to the k-walk $W_\emptyset$ possessing k improper counterclockwise zigzag points. Instead, in terms of the mentioned papers up to the appropriate change of directions, the empty set of south-east turns would define another over-diagonal lattice path from $0k$ to $k0$ having only one turn (in kk).

5. The considerations in this section reflect an intrinsic splitting of the set of p^k-circulants into $\mathrm{Cat}(k)$ subsets in conformity with the isomorphism theorem. The parametrization of these subsets by lattice walks will be, hopefully, useful in investigating other combinatorial and algebraic properties of p^k-circulants. Is it possible to generalize these constructions (of course, together with the isomorphism theorem) to other orders such as $n = p^k q$ (or, more generally, $n = p^k q^l$) with odd primes p and q?

6 Formulae for circulant graphs of order p^2

For completeness, we describe briefly how the approach of the preceeding section can be applied to the case $k = 2$. The proofs and other details can be found in [KliLP9x].

6.1. For $n = p^2$ as we know, two enumerative subproblems arise, and they can be resolved in the following way. Here we have two layers and two possible multipliers m_0 and m_1. Count first the connection sets up to single-multiplier actions, i.e. assuming $m_1 = m_0$. Let $A_{\mathrm{i}}(p^2)$ denote the corresponding number where $\mathrm{i} \in \{\mathrm{d}, \mathrm{u}, \mathrm{t}, \mathrm{sd}, \mathrm{su}\}$. But this count does not accurately reflect the true contribution from the connection sets with $(1+p)$-invariant 0-layers. Let their number calculated in this way be equal to $B_{\mathrm{i}}(p^2)$. Instead, by isomorphism Theorem 5.2, in the case when

$$(1+p)X_{(0)} = X_{(0)} \qquad (\mathrm{R}_{00})$$

is valid, multipliers m_0 and m_1 are allowed to be independent, i.e. we have here the group $\mathbb{Z}^*_{p^2} \oplus \mathbb{Z}^*_{p^2}$. Let $D_{\mathrm{i}}(p^2)$ denote the number of its orbits, i.e. the number which is to be correctly contributed instead of $B_{\mathrm{i}}(p^2)$. Let, finally, $C_{\mathrm{i}}(p^2)$ be the required number of non-isomorphic circulants (in generic designations for $\mathrm{i} \in \{\mathrm{d}, \mathrm{u}, \mathrm{t}, \mathrm{sd}, \mathrm{su}\}$). Then

$$C_{\mathrm{i}}(p^2) = A_{\mathrm{i}}(p^2) - B_{\mathrm{i}}(p^2) + D_{\mathrm{i}}(p^2). \tag{6.1.1}$$

Now the right-hand terms can be found by Pólya's method applied to the appropriate groups of multipliers. Namely, $A_{\mathrm{i}}(p^2)$ corresponds to the join

$$(\mathbb{Z}^*_{p^2}, \mathbb{Z}'_{p^2}) = (\mathbb{Z}^*_{p^2}, \mathbb{Z}^*_p) \mathbin{\dot\vee} (\mathbb{Z}^*_{p^2}, \mathbb{Z}^*_{p^2}), \tag{6.1.2}$$

$B_{\mathrm{i}}(p^2)$ corresponds to the join

$$(\mathbb{Z}^*_{p^2}, \mathbb{Z}^*_p) \mathbin{\dot\vee} (\mathbb{Z}^*_{p^2}, \mathbb{Z}^*_p), \tag{6.1.3}$$

while $D_{\mathrm{i}}(p^2)$ corresponds to the direct sum

$$(\mathbb{Z}^*_{p^2}, \mathbb{Z}^*_p) \oplus (\mathbb{Z}^*_{p^2}, \mathbb{Z}^*_p). \tag{6.1.4}$$

Add also that in order to make these operations correct formally as they are defined in 1.2, we must use two disjoint copies of the set $\mathbb{Z}^*_p$ on which the group $\mathbb{Z}^*_{p^2}$ acts.

Now according to Lemma 1.7 we can easily find the cycle indices of the groups with actions (6.1.2), (6.1.3) and (6.1.4). After several elementary transformations we arrive at the polynomial

$$\mathcal{C}(p^2; \mathbf{x}, \mathbf{y}) := \tfrac{1}{p}\mathcal{I}_{p-1}(\mathbf{x}^{p+1}) - \tfrac{1}{p}\mathcal{I}_{p-1}(\mathbf{xy}) + \mathcal{I}_{p-1}(\mathbf{x})\mathcal{I}_{p-1}(\mathbf{y}) \tag{6.1.5}$$

for directed circulants and the polynomial

$$\mathcal{C}^*(p^2; \mathbf{x}, \mathbf{y}) := \tfrac{1}{p}\mathcal{I}_{\frac{p-1}{2}}(\mathbf{x}^{p+1}) - \tfrac{1}{p}\mathcal{I}_{\frac{p-1}{2}}(\mathbf{xy}) + \mathcal{I}_{\frac{p-1}{2}}(\mathbf{x})\mathcal{I}_{\frac{p-1}{2}}(\mathbf{y}) \tag{6.1.6}$$

for undirected circulants. Both polynomials are in two sets of variables $\{x_1, x_2, \ldots\}$ and $\{y_1, y_2, \ldots\}$ (cf. 1.3). Then for all five types of circulant graphs under consideration, the substitutions of variables similar to the ones used in Sections 3 and 4 yield the following result.

6.2. Theorem [KliLP9x]**.**

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

There are some interesting interrelations and consequences of the above formulae, for which we refer to the paper [KliLP9x].

7 Numerical results

Tables 2 and 3 contain new values obtained by the above formulae together with values taken from numerous previous publications (see [Dav65], [Tur67], [Als70], [ChaW73], [ChaW82], [ChiL86], [McKR90], [Ray91] and [FarKM94]).

n	$C_{\mathrm{d}}(n)$	$C_{\mathrm{u}}(n)$	$C_{\mathrm{su}}(n)$	$C_{\mathrm{sd}}(n)$	$C_{\mathrm{t}}(n)$	$C^0_{\mathrm{d}}(n)$
3	3	2	0	1	1	1
5	6	3	1	2	1	1
7	14	4	0	2	2	1
9	51	8	0	3	3	
11	108	8	0	4	4	3
13	352	14	2	8	6	5
15	2172	44	0	20	16	
17	4116	36	4	20	16	16
19	14602	60	0	30	30	28
21	88376	200	0	88	88	
23	190746	188	0	94	94	93
25	839094	423	7	214	205	
29	9587580	1182	10	596	586	585
31	35792568	2192	0	1096	1096	1091
...						
37	-	14602	30	7316	7286	7280
...						
41	-	52488	56	26272	26216	26214
...						
49	6701785562464	798952	0	399472	399472	

Table 2: Numbers of circulant n-graphs, n odd

Our calculations in both tables for undirected graphs were checked by the unpublished tables composed by B. D. McKay [McK95] for the values of $C_{\mathrm{u}}(n,N)$ and of the corresponding $A_{\mathrm{u}}(n,N)$ (see (6.1.1)).

$C^0_{\mathrm{d}}(n)$ in Table 2 denotes the number of n-circulants having no automorphism outside of $Z(n)$. Their values (which are known only for prime $n = p$ and are unexpectedly close to those of $C_{\mathrm{t}}(n)$) have been taken from [ChiL86]. Evidently, $C_{\mathrm{t}}(n) + C_{\mathrm{su}}(n) \leq C_{\mathrm{sd}}(n)$. But for $n = p$, this becomes *equality* as shown in [ChiL86]. In other words, any self-complementary circulant p-graph is a tournament unless it is symmetric. One can also observe that self-complementary graphs are very rare among undirected circulants. In fact, nonzero values of $C_{\mathrm{su}}(n)$ (cf. also Remark 1.15) grow approximately as $\frac{1}{n-1}2^{\frac{n+3}{4}}$, what is much slower than the growth of the other four quantities.

$2n$	$C_{\mathrm{d}}(2n)$	$C_{\mathrm{u}}(2n)$
2	2	2
6	20	8
10	140	20
14	1440	48
18		192
22	209936	416
26	2797000	1400
30	67195520	8768
34	536879180	16460
38	-	58288
42	-	355200
46	-	762608

Table 3: Numbers of circulant $2n$-graphs, n odd

The values 14, 30 and 14602 appear repeatedly in different columns of Table 2 in conformity with Corollary 3.3.

For $n = p^2$, separate contributions by formula (6.1.1) can be seen in Table 4 (it is reproduced here from [KliLP9x]). Missing entries in it are too large to be included. The value sizes show spectacularly that, in comformity with Theorem 5.2, $-B_{\mathrm{i}} + D_{\mathrm{i}}$ is only a slight correction term to the main contribution A_{i}.

According to Table 4, $B_{\mathrm{u}}(9) = D_{\mathrm{u}}(9)$. This agrees with the well-known fact [Pál87] that 9 is one of three exceptional values of n for which the conjecture $\mathbf{A}(n)$ holds for *undirected* circulants though does not hold for all circulants (the other two values are 8 and 18).

Acknowledgements

We are deeply grateful to Mikhail Klin for fruitful and stimulating discussions of the subject. Our thanks are also due to the Mathematisches Forschungsinstitut Oberwolfach where we started and partially fulfilled this paper within the framework of the "Research in Pairs" program.

	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 4: Numbers of circulant p^2-graphs and contributions, p prime

References

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

[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.

[Als9x] B. Alspach, Isomorphism and Cayley graphs, *Preprint* (1996), 11 pp.

[Als9y] B. Alspach, Lecture notes (1996), 34 pp (unpublished).

[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.

[BroH95] I. Broere and J. H. Hattingh, On the construction of self-complementary circulant graphs, *Graph Th., Combin. and Algorithms (Proc. 7-th Intern. Conf., Western Mich. Univ.)*, Vol. **1** (Y. Alavi and A. Schwenk eds.), *J. Wiley & Sons* (1995), 123–129.

[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.

[ChiL85] G. L. Chia and C. K. Lim, Counting 2-circulant graphs, *J. Austral. Math. Soc.* (A), **39** (1985), No 2, 270–281.

[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.

[DerZ80] N. Dershowitz and S. Zaks, Enumeration of ordered trees, *Discr. Math.*, **31** (1980), No 1, 9–28.

[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.

[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* (Mathematics and Its Applications, Soviet Series, **84**), Kluwer, Dordrecht (1994), 1–152.

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

[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.

[Har69] F.Harary, *Graph Theory*, Addison-Wesley, Reading, MA (1969).

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

[HilP91] P. Hilton and J. Pedersen, Catalan numbers, their generalization, and their uses, *Math. Intellig.*, **13** (1991), No 2, 64–75.

[HJP93] W. C. Huffman, V. Job and V. Pless. Multipliers and generalized multipliers of cyclic objects and cyclic codes. *J. Combin. Th.*, **A62** (1993), No 2, 183–215.

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

[KliLP9x] M. Klin, V. Liskovets and R. Pöschel, Analytical enumeration of circulant graphs with prime-squared number of vertices, *Sém. Lotharing. Combin.*, **36** (1996), submitted.

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

[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).

[Kra95a] C. Krattenthaler, The major counting of nonintersecting lattice paths and generating functions for tableaux, *Mem. Amer. Math. Soc*, **115** (1995), No 552, 109 pp.

[Kra95b] C. Krattenthaler, Counting nonintersecting lattice paths with turns, *Sém. Lotharing. Combin.*, **34** (1995), B34i, 17 pp.

[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.

[MalW72] C. L. Mallows and K. W. Wachter, Valency enumeration of rooted plane trees, *J. Austral. Math. Soc*, **13** (1972), No 3, 472–476.

[McK95] B. D. McKay, Personal communication (1995).

[McKR90] B. D. McKay and G. F. Royle, The transitive graphs with at most 26 vertices, *Ars Combin.*, **30** (1990), 161–176.

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

[Muz9y] M. Muzychuk, On Ádám's conjecture for circulant graphs. *Discr. 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.

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

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

[Sta9x] R. P. Stanley, Problems on Catalan and related numbers, *Preprint* (excerpted from *Enumerative Combinatorics*, vol. **2**), 1996, 35 pp.

[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.

[WeX93] W. D. Wei and J. Y. Xu. Cycle index of direct product of permutation groups and number of equivalence classes of subsets of Z_v. *Discr. Math.*, **123** (1993), No 1–3, 179–188.

[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.

Authors' address:

Valery Liskovets, Reinhard Pöschel
Technische Universität Dresden
Institut für Algebra
D – 01062 Dresden
Germany
e-mail: `[liskov,poeschel]@math.tu-dresden.de`