

Counting Circulant Graphs of Prime-Power Order by Decomposing into Orbit Enumeration Problems

Valery Liskovets* and Reinhard Pöschel*

Institut für Algebra

Technische Universität Dresden

D-01062 Dresden, Germany[†]

[liskov, poeschel]@math.tu-dresden.de

August 2, 1997

Abstract

The set of circulant graphs with p^k vertices ($k \geq 1$, p an odd prime) is decomposed into a collection of well-specified subsets. The number of these subsets is equal to the k -th Catalan number, and they are in one-to-one correspondence with the monotone underdiagonal walks on the plane integer $(k+1) \times (k+1)$ lattice. The count of non-isomorphic circulant graphs in each of the subsets is presented as an orbit enumeration problem of Pólya type with respect to a certain Abelian group of multipliers. The descriptions are given in terms of equalities and congruences between multipliers in accordance with an isomorphism theorem for such circulant graphs. In this way, explicit uniform counting formulae have been obtained for various types of circulant graphs with p^2 vertices.

Keywords: circulant graph, cyclic graph, enumeration under group action, graph isomorphism, multiplier, monotone walk, plane integer lattice, Catalan number

Mathematics Subject Classifications (1991): 05C25, 05C30.

1 Introduction

A circulant graph (or briefly a circulant) is a (di)graph which is invariant with respect to a complete cyclic permutation of the vertices. ¿From the earliest days of their study,

*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.

[†]Current address of the first author: Institute of Mathematics, National Academy of Sciences, 220072, Minsk, BELARUS, liskov@im.bas-net.by

it became clear that properties of circulants heavily depend on the multiplicative nature of their order (the order of a graph means the number of its vertices). For a prime order p , the structure and description of circulants are well-known and rather simple. In particular, there is a simple one-multiplier isomorphism theorem for circulants of order p (Theorem 2.6 below). This criterion provides an easy way to count non-isomorphic circulants by applying the ordinary Pólya method with the transitive cyclic group of degree $p - 1$ (or $\frac{p-1}{2}$ for undirected circulant graphs). Almost all diverse enumerative results that have been obtained so far for various types of circulants are based upon this theorem and concern only prime orders (see, by chronology, [12, 33, 2, 6, 13, 8, 3, 11, 34, 31, 4]). Moreover, due to a recent progress in the algebraic theory of circulants (cf. [27]), a similar approach can be, in principle, extended to the square-free orders (although counting formulae for them will be, evidently, less pleasant, see [26]; cf. also [9] and [7]).

For the other orders (excepting several small values), the above-mentioned one-multiplier isomorphism theorem is not valid [29]. So that, the count of circulants of such orders is a more difficult task. Recently, M. Klin with the present authors have succeeded in counting circulants of order p^2 [21]. In particular, we have obtained Pólya type formulae for them (see Sec. 4 below) relying upon the corresponding two-multipliers isomorphism theorem proved in [22] (cf. [5]).

In this paper we generalize the same approach to orders p^k with arbitrary k and odd prime p by using the corresponding k -multipliers isomorphism theorem obtained in [23] (recently, it has also been reproved and strengthened in [28]). Due to combinatorial and number-theoretic features of the conditions in this theorem, the problem is decomposed into a certain collection of well-specified orbit enumeration subproblems. Each of them concerns a subgroup of the direct product of k cyclic groups which act by multiplication on certain sets of numbers. Every subproblem is of Pólya type, i.e. it deals with the induced element-wise action of a permutation group on the subsets. In principle, all these enumeration problems can be resolved by the ordinary Pólya technique. But their diversity and setting complexity grow quickly (in fact, exponentially) with k : they prove to be in a one-to-one correspondence with the monotone walks on the plane integer $(k+1) \times (k+1)$ lattice. Accordingly, the overall number of these subproblems is equal to the k -th Catalan number $\text{Cat}(k) = \frac{1}{k+1} \binom{2k}{k}$, so that we obtain 1, 2, 5, 14, 42, ... subproblems for $k = 1, 2, 3, 4, 5, \dots$, respectively. In these terms, the combinatorics of the problems that arose is described effectively. In particular, we describe a reduced collection of equalities and congruences between the multipliers which specifies the corresponding group.

For $k \geq 3$, finding an explicit formula for the number of non-isomorphic circulant p^k -graphs (and, moreover, finding a general solution of the above subproblems as an explicit function of the specifying lattice walk) still remains an open question.

2 Preliminaries. Isomorphism Theorems

2.1. As usual, $\mathbb{Z}$ stands for the ring of integers. Let n be a positive integer, $\mathbb{Z}_n := \{0, 1, 2, \dots, n-1\}$ 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 .

In the sequel, all arithmetic operations are regarded *modulo* n unless otherwise stated.

$\mathbb{Z}_n$ 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.

2.2. A *graph* will mean a finite *directed* graph without loops and multiple edges. If Γ is a graph, we write $\Gamma = \Gamma(V, E)$ where $V = V(\Gamma)$ and $E = E(\Gamma)$ are the sets of its vertices and (directed) edges, respectively. An *n-graph* means a graph of order n . Usually, for definiteness, the set of vertices is taken to be $\mathbb{Z}_n$.

For other graph-theoretic notions we refer to [18].

A *circulant graph* of order n , or simply a *circulant* (or an *n-circulant*) means an *n-graph* Γ on $\mathbb{Z}_n$ which is invariant with respect to the cyclic permutation $(0, 1, \dots, n-1)$, i.e. we have

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

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. Of course, up to isomorphism, both definitions are equivalent.

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,

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

Accordingly, we write $\Gamma = \Gamma(\mathbb{Z}_n, X)$, or, in short, $\Gamma = \Gamma(X)$. Obviously, $\Gamma(X)$ is a regular graph of valency $|X|$.

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

$$mX := \{mv \mid v \in X\}. \tag{2.1}$$

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 $mv - mu = m(v - u) \in mX = X'$. Hence $\Gamma(mX) \cong \Gamma(X)$. $\square$

Note that the equality (M₁) just describes the induced element-wise action of the multiplicative group $\mathbb{Z}_n^*$ on connection sets, i.e. on subsets of $\mathbb{Z}'_n$.

2.4. 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).

The relation (M_1) is often referred to as *Ádám's condition* in view that A. Ádám in [1] conjectured the converse assertion. Namely,

2.5. Ádám's conjecture $A(n)$. *The connection sets of isomorphic circulant n -graphs are equivalent.*

2.6. Isomorphism theorem for p -circulants (cf. [33, 15, 16]). *The conjecture $A(n)$ is valid for all prime $n = p$.*

However, as we pointed out in the Introduction, Ádám's conjecture is false in general. So that, for non-square-free n , a subtler isomorphism criterion is needed. And such a criterion has been obtained for $n = p^k$.

2.7. Layers. For composite orders n , 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 $m \in \mathbb{Z}_n^*$.

Thus, for $n = p^k$ (p prime), k layers arise in accordance with the divisibility of the elements of X by powers of p :

$$X = X_{(0)} \dot{\cup} X_{(1)} \dot{\cup} \cdots \dot{\cup} X_{(k-1)} \quad (2.2)$$

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

2.8. Isomorphism theorem for p^k -circulants [23, Theorem 2.3] (cf. also [28]). *Let $n = p^k$ (p an odd prime) and let 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.*

$$X'_{(i)} = m_i X_{(i)}, \quad i = 0, 1, \dots, k-1, \quad (M_k)$$

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

$$(1 + p^{k-i-j-1})X_{(i)} \neq X_{(i)}, \quad (R_{ij})$$

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

$$\left. \begin{array}{lcl} m_{i+1} & \equiv & m_i \pmod{p^{k-i-j-1}} \\ m_{i+2} & \equiv & m_{i+1} \pmod{p^{k-i-j-2}} \\ & \dots & \\ m_{k-j-1} & \equiv & m_{k-j-2} \pmod{p} \end{array} \right\} \quad (E_{ij})$$

It is clear that, in principle, this crucial theorem is sufficient to split the count of p^k -circulants into a number of Pólya type problems. But in order to achieve this aim rigorously, we need to examine thoroughly the restrictions of the theorem and their interactions. At first, we introduce some additional definitions (for other combinatorial notions concerning groups with actions we refer to [20]).

2.9. 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 $\mathbf{S}(U)$ is implicit. (G, U) is a permutation group if and only if this action is faithful.

The action of $g \in G$ on $u \in U$ is written as u^g .

Given two groups G and H acting on disjoint sets U and V , we define their *direct sum* $(G, U) \oplus (H, V) := (G \times H, U \dot{\cup} V)$. This is the direct product $G \times H$ (as abstract groups) acting on the (disjoint) union $U \dot{\cup} V$ by the following rule:

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

for any $u \in U$, $v \in V$ and $(g, h) \in G \times H$.

Given a group G with two of its actions (G, U) and (G, V) on disjoint sets U and V , their *join* $(G, U) \dot{\vee} (G, V) := (G, U \dot{\cup} V)$ means the same group combining the two actions:

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

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

$(G, U) \dot{\vee} (G, V)$ is the “diagonal” subgroup of the direct sum $(G, U) \oplus (G, V)$. This natural operation is characteristic for combinatorial enumeration.

2.10. We need some multiplicative properties of integer numbers.

For $n = p^k$, as is 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 $W = W(p)$ which is a primitive root (i.e. a generator of $\mathbb{Z}_{p^k}^*$) for all k and is such that $1 < W < p^2$ (necessarily $p^W \equiv 1 \pmod{p^2}$). Instead, following H. Hasse [19, 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 in fact is 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 W is a primitive root modulo p^k , then one can simply take $w = W^{p^{k-1}}$. Therefore every element $m \in \mathbb{Z}_{p^k}^*$ has a unique representation

$$m = w^i(1+p)^j \pmod{p^k} \tag{2.3}$$

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

$$1+p^i \equiv (1+p)^{p^{i-1}} \pmod{p^k}. \tag{2.4}$$

2.11. The following elementary property is convenient for manipulating congruences modulo different p -power bases.

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

$$x \equiv h \pmod{p^\ell} \tag{2.5}$$

has a unique solution $x \bmod p^i$. It is simply h considered, coarser, modulo p^i . In other words, we may replace congruence (2.5) with 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 the greater values of i .

3 Decomposition

3.1. Henceforth, it will be convenient to interchangeably write pairs of parameters briefly as ij or in parentheses separated by commas, so that, for example, $(R_{(i,j)})$ denotes the same as (R_{ij}) .

The conditions in Theorem 2.8 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 “partially diagonal” subgroups of the direct sum $\mathbb{Z}_{p^k}^* \oplus \cdots \oplus \mathbb{Z}_{p^k}^*$ (in fact, of $\mathbb{Z}_{p^k}^* \oplus \mathbb{Z}_{p^{k-1}}^* \oplus \cdots \oplus \mathbb{Z}_p^*$) specified by combinations of the congruence sets (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, in fact, significant: due to congruence (2.4), the implication

$$(R_{ij}) \implies (R_{ij'}) \tag{3.1}$$

holds whenever $j' \geq j$. Hence 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 $f : [0, k-2] \rightarrow [0, k-2]$ 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

$$R_f = \{(R_{ij}) \mid i = 0, 1, \dots, k-2; j = f(i), j < k-1-i\} \tag{3.2}$$

and the set of the corresponding congruences

$$E_f = \{(E_{ij}) \mid i = 0, 1, \dots, k-2; j = f(i), j < k-1-i\}. \tag{3.3}$$

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

$$(1 + p^{k-i-j-1})X_{(i)} = X_{(i)} \tag{3.4} \quad (\neg R_{ij})$$

that do not contradict R_f by implication (3.1). For each i it suffices to take $(\neg R_{ij})$ with the maximal possible value of j , i.e. Q_f is specified by the set of the additional conditions

$$T_f = \{(\neg R_{(i,j-1)}) \mid i = 0, 1, \dots, k-2; j = f(i) > 0\}. \quad (3.4)$$

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

3.2. Now the problem Q_f can be formulated as follows:

count the orbits of the group

$$\mathcal{G}_f = (\mathbb{Z}_{p^k}^* \oplus \mathbb{Z}_{p^{k-1}}^* \oplus \dots \oplus \mathbb{Z}_p^*) \backslash E_f$$

acting multiplicatively component-wise on the set C_f (see below) of connection sets satisfying the restrictions $R_f \cup T_f$ as defined by (3.2) and (3.4).

Here $\backslash E_f$ denotes *taking the subgroup* of all multiplier tuples that meet the congruences in E_f (see (3.3)). $\mathcal{G}_f$ is considered in its induced setwise action as defined by formula (2.1).

C_f is the disjoint union

$$C_f = C_{(0,f(0))} \dot{\cup} C_{(1,f(1))} \dot{\cup} \dots \dot{\cup} C_{(k-2,f(k-2))} \dot{\cup} C_{k-1} \quad (3.5)$$

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

3.3. The reduction 3.1 is a straightforward consequence of Theorem 2.8. 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 implication between the congruences

$$(E_{ij}) \implies (E_{i'j}) \quad (3.6)$$

whenever $i' \geq i$; this is immediate from the definition of (E_{ij}) . Therefore, if two primary subproblems Q_f and $Q_{f'}$ differ only in index pairs that are connected by implications (3.6), then $E_f = E_{f'}$ and $\mathcal{G}_f = \mathcal{G}_{f'}$. Thus, instead of orbits of two groups with actions $(\mathcal{G}_f, C_f)$ and $(\mathcal{G}_{f'}, C_{f'})$, we may count orbits of their join, i.e. we may replace the problems Q_f and $Q_{f'}$ by one new combined problem.

As a result, we arrive at the following collection of enlarged enumerative problems $P_{\mathbf{B}}$ which are specified by $\mathcal{G}_{\mathbf{B}}$ and $C_{\mathbf{B}}$ and will be denoted by $P_{\mathbf{B}} = [\mathcal{G}_{\mathbf{B}}, C_{\mathbf{B}}]$. Here $\mathbf{B}$ is an arbitrary (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

$$ij \leq i'j' \iff i \leq i' \text{ \& } j \leq j'.$$

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:

$$\mathbf{B} := \{i_s j_s \mid s = 1, 2, \dots\} = \{i_1 j_1, i_2 j_2, \dots \mid i_1 < i_2 < \dots; j_1 > j_2 > \dots\}. \quad (3.7)$$

Let also

$$\mathbf{B}^1 := \{i_1, i_2, \dots\}$$

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

$$\mathcal{G}_{\mathbf{B}} = (\mathbb{Z}_{p^k}^* \oplus \mathbb{Z}_{p^{k-1}}^* \oplus \cdots \oplus \mathbb{Z}_p^*) \setminus E_{\mathbf{B}} \quad (3.8)$$

where

$$E_{\mathbf{B}} = \{(E_{i_s j_s}) \mid i_s j_s \in \mathbf{B}\}$$

and $\setminus E_{\mathbf{B}}$ denotes, as above, taking the subgroup of all multiplier tuples that meet the congruences in $E_{\mathbf{B}}$.

3.4. To specify $\mathbf{C}_{\mathbf{B}}$, it is convenient to represent index pairs ij by points of the plane *integer lattice*. More exactly, we consider the triangular region Δ_k of points with integer coordinates ij satisfying the inequalities $0 \leq i$, $0 \leq j$ and $i + j \leq k$. Δ_k contains the main diagonal $\{ij \mid i + j = k, i, j \geq 0\}$ and the *subdiagonal* $\{ij \mid i + j = k - 1, i, j \geq 0\}$ while, by definition, the points $i_s j_s$ of $\mathbf{B}$ lie strictly below them. The points in $\mathbf{B}$ are called the *base points* (of order k), 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 $i \geq i_s$ and $j \geq j_s$ for some $i_s j_s \in \mathbf{B}$.

In these terms, the problem $\mathbf{P}_{\mathbf{B}}$ combines the primary subproblems $\mathbf{Q}_f$ 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 $i_s \in \mathbf{B}^1$ where $i_s j_s \in \mathbf{B}$.

More explicitly, $U_{\mathbf{B}}$ is specified by the set $V_{\mathbf{B}}$ 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: $\overline{U_{\mathbf{B}}} = U_{\mathbf{B}} \cup \{ij \mid i + j = k, i, j \geq 0\}$. 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 $V_{\mathbf{B}}$. We adjoin all such points to $V_{\mathbf{B}}$ 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 $\mathbf{B}$. See Fig. 1 illustrating these constructions.

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).
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 $V_{\mathbf{B}}$ in order to obtain $W_{\mathbf{B}}$.

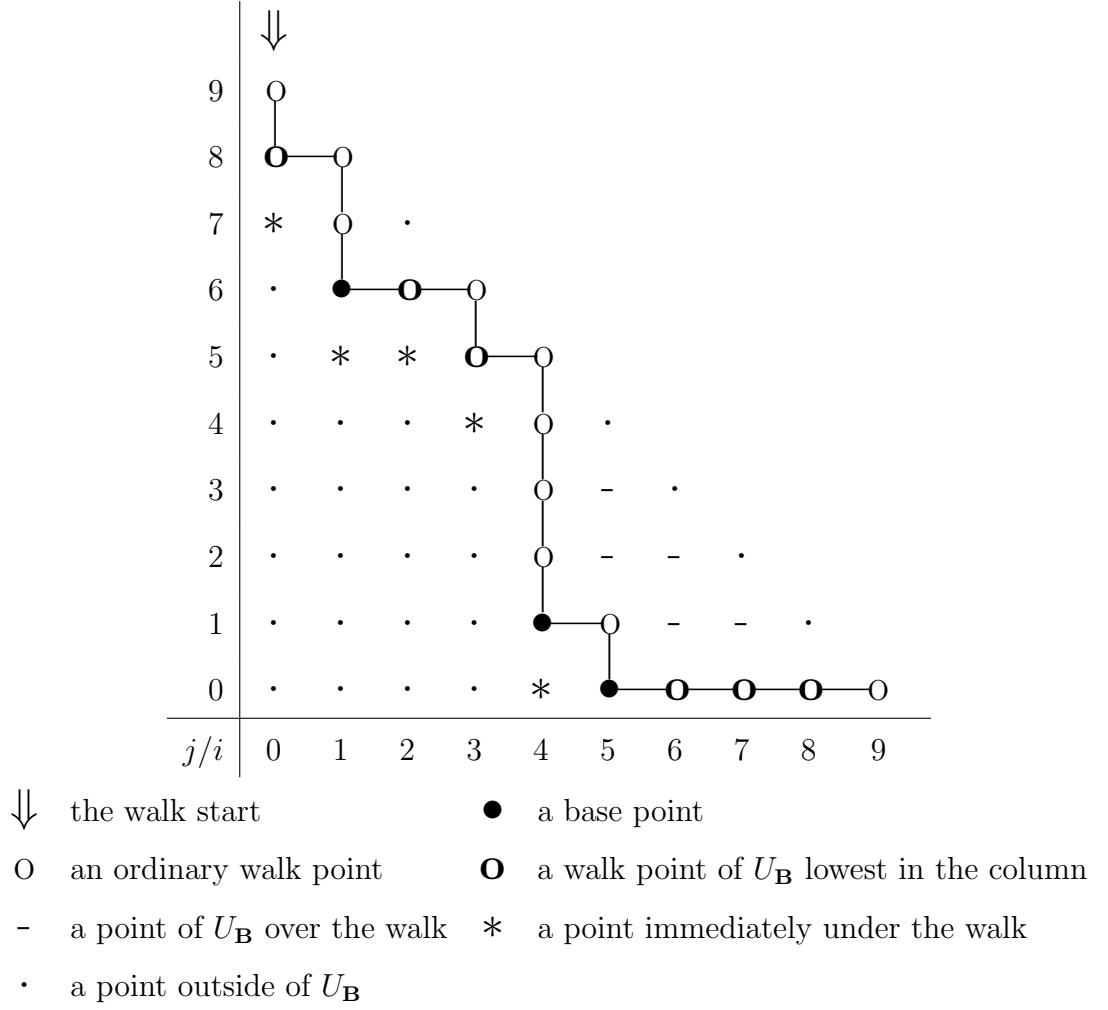


Figure 1: A 9-walk and its base point set $\mathbf{B} = \{16, 41, 50\}$

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 $\text{Cat}(k) = \frac{1}{k+1} \binom{2k}{k}$ (cf., for example, [32, Ch.5] and [14]).

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 $j = \lambda_{\mathbf{B}}(i)$ are emphasized. In general, $\lambda_{\mathbf{B}}(i)$ is a monotone decreasing (“ladder”) function that can easily be 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 $\mathbf{C}_{\mathbf{B}}$ combines the connection sets $\mathbf{C}_f$ 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 imposed, while we have the following set of the non-invariance conditions

$$R_{\mathbf{B}} = \{(R_{i_s j_s}) \mid i_s j_s \in \mathbf{B}; s = 1, 2, \dots\} \quad (3.9)$$

and the following set of the invariance conditions

$$T_{\mathbf{B}} = \{(\neg R_{(i, \lambda_{\mathbf{B}}(i)-1)}) \mid i = 0, 1, \dots, k-2; \lambda_{\mathbf{B}}(i) > 0\}. \quad (3.10)$$

In Fig. 1, the corresponding points $(i, \lambda_{\mathbf{B}}(i) - 1)$, i.e. ones lying directly under the walk, are depicted as “*”.

In general, these are much simpler restrictions as compared with C_f (formula (3.5)) especially when the set $\mathbf{B}$ consists of points $i_s j_s$ with small coordinates. The most dramatic reduction takes place for $\mathbf{B} = \{00\}$: the problem $P_{\{00\}}$ covers $(k-1)!$ primary subproblems Q_f , and its connection sets are restricted by the single condition (R_{00}) .

Speaking formally, we obtain here the disjoint union

$$C_{\mathbf{B}} = \overline{C}_{(0, \lambda_{\mathbf{B}}(0))} \dot{\cup} \overline{C}_{(1, \lambda_{\mathbf{B}}(1))} \dot{\cup} \dots \dot{\cup} \overline{C}_{(k-2, \lambda_{\mathbf{B}}(k-2))} \dot{\cup} C_{k-1} \quad (3.11)$$

where $\overline{C}_{(i, \lambda_{\mathbf{B}}(i))} = C_{(i, \lambda_{\mathbf{B}}(i))}$ (cf. (3.5)) if $i = i_s \in \mathbf{B}^1$ for some s (i.e. $(i, \lambda_{\mathbf{B}}(i)) \in \mathbf{B}$) and, otherwise, $\overline{C}_{(i, \lambda_{\mathbf{B}}(i))}$ consists of all subsets of $p^i \mathbb{Z}_{p^{k-i}}^*$ satisfying the single condition $(\neg R_{(i, \lambda_{\mathbf{B}}(i)-1)})$, which is interpreted to be empty if $\lambda_{\mathbf{B}}(i) = 0$.

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

3.5. Theorem. *The number of non-isomorphic circulant p^k -graphs equals the sum of the solutions of $\text{Cat}(k)$ of orbit enumeration problems $P_{\mathbf{B}} = [\mathcal{G}_{\mathbf{B}}, C_{\mathbf{B}}]$ parametrized by the base point sets $\mathbf{B}$ of order k , where the group $\mathcal{G}_{\mathbf{B}}$ of multipliers is defined by expression (3.8) and $C_{\mathbf{B}}$ is the set of all connection sets satisfying the restrictions $R_{\mathbf{B}} \cup T_{\mathbf{B}}$ as specified by (3.9) and (3.10). $\square$*

Each $P_{\mathbf{B}}$ is a “routine”, though possibly tedious, Pólya type problem. Indeed, due to representation (2.3) of numbers, $P_{\mathbf{B}}$ can be described as dealing with the count of all (minimal) invariant subsets of a certain set with respect to the induced action of the corresponding group.

Of course, the same decomposition takes place for various natural subclasses of circulant graphs with p^k vertices such as undirected graphs or tournaments, etc.

3.6. The description of the group $\mathcal{G}_{\mathbf{B}}$ can be simplified further due to the following idea. The non-invariance condition (R_{ij}) can be rewritten in terms of the set $p^{-i} X_{(i)} \subseteq \mathbb{Z}_{p^{k-i}}^*$. Accordingly, the 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 2.11, 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 $m_{k-1} = m_{k-2} = \dots = m_{i+1} = m_i$. In particular, the non-invariance relation (R_{00}) implies that *all* multipliers $m_0, m_1, \dots, m_{k-1}$ 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 $E_{\mathbf{B}} = \{(E_{i_s j_s})_{i_s j_s \in \mathbf{B}}\}$ are redundant and which ones can be replaced by equalities?

If $(-R_{ij}) \in T_{\mathbf{B}}$, 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} . Therefore we may now consider m_i modulo $p^{k-i-j-1}$, a fortiori narrowing the domain of m_i and the group $\mathcal{G}_{\mathbf{B}}$. Generally speaking, this is unessential for the count of orbits (cf. Lemma 4.3 below) 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 $E_{\mathbf{B}}$ 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 the description of $E_{\mathbf{B}}$ 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 an 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 an 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

$$m_{i+1} \equiv m_i \pmod{p^{k-\lambda_{\mathbf{B}}(i)-i-1}}, \quad i = 0, 1, \dots, k-2, \quad (3.12)$$

which, in fact, represent a non-trivial condition if and only if $\lambda_{\mathbf{B}}(i) < k - i - 1$.

On the other hand, according to the set of conditions $T_{\mathbf{B}}$ (see (3.10)) 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} , hence m_i , $i = 0, 1, \dots, k-2$, are defined mod $p^{k-\lambda_{\mathbf{B}}(i)-i}$ regardless of whether $\lambda_{\mathbf{B}}(i) = 0$ or not.

Now, according to Subsection 2.11, congruence (3.12) for some index i may be replaced by the corresponding equality if and only if either $k - \lambda_{\mathbf{B}}(i) - i \leq k - \lambda_{\mathbf{B}}(i) - i - 1$, which 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 Subsection 3.4, this is valid if and only if $i+1 \notin \mathbf{B}^1$. Thus, we arrive at the following statement.

3.7. Theorem. *The reduced group $\mathcal{G}'_{\mathbf{B}}$ of the problem $P_{\mathbf{B}}$ is specified by the following set of equalities and congruences*

$$\left. \begin{array}{ll} m_i = m_{i-1} & \text{if } i \notin \mathbf{B}^1 \\ m_i \equiv m_{i-1} \pmod{p^{k-\lambda_{\mathbf{B}}(i-1)-i}} & \text{otherwise} \end{array} \right\} \quad (\mathbf{F}_{\mathbf{B}})$$

which are defined for all $i = 1, 2, \dots, k-1$ satisfying the inequality

$$\lambda_{\mathbf{B}}(i-1) < k-i. \quad \square$$

Consider a simple illustrating example for $k = 4$ and the subproblem specified by two base points 01 and 10, see Fig. 2. The connection sets satisfy the restrictions (R_{01}) , (R_{10}) and $(\neg R_{00})$. By Theorem 2.8 we have four congruences:

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

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 congruence into an equality. The invariance condition $(\neg R_{00})$ implies only that m_0 is defined modulo p^3 . The multiplier m_1 has the same domain. Hence no other reductions are possible, and the final restrictions are $m_3 = m_2 = m_1$ and $m_1 \equiv m_0 \pmod{p^2}$. In other words, denoting $m_1 := m$ and $m_0 := m + \ell p^2$ where m is modulo p^2 and ℓ is modulo p , we obtain the group of all multiplier quadruples of the form $(m + \ell p^2, m, m, m)$ with the element-wise multiplication.

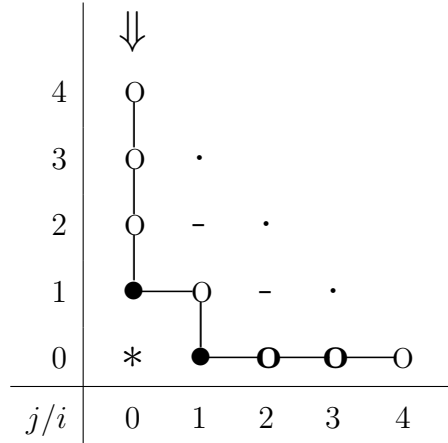


Figure 2: The 4-walk with $\mathbf{B} = \{01, 10\}$

Note (though 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 Theorem 3.7, we obtain:

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

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

3.8. Corollary. *All reduced groups $\mathcal{G}'_{\mathbf{B}}$ (and problems $\mathbf{P}_{\mathbf{B}}$, respectively) are pairwise different. In all but one of the cases, the set of equalities $m_i = m_{i-1}$ in the system $(\mathbf{F}_{\mathbf{B}})$ specifying $\mathcal{G}'_{\mathbf{B}}$ is not empty (i.e. $\varrho(\mathbf{B}) < k$) and in all but one of the 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 $\mathcal{G}'_{\mathbf{B}}$ is equal to the number of all (proper or improper) counterclockwise zigzag points of the walk $W_{\mathbf{B}}$. $\square$*

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

As can be easily seen (cf. [14]), there are $\frac{1}{k} \binom{k}{r} \binom{k}{r-1}$ monotone k -walks having r counterclockwise zigzag points, $r = 1, 2, \dots, k$ (these are the well-known Narayana numbers, see [32, Ch.5]). Due to the last statement of the Corollary, this is the number of problems $\mathbf{P}_{\mathbf{B}}$ with the reduced groups $\mathcal{G}'_{\mathbf{B}}$ of rank r .

The set of congruences in $\mathbf{F}_{\mathbf{B}}$ specifying $\mathbf{P}_{\mathbf{B}}$ 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

3.9. Corollary. *There exist exactly 2^{k-1} subproblems each of which is specified by a system of “diagonal” equalities $m_i = m_{i-1}$ solely, without congruences. $\square$*

Let $H_{\mathbf{B}}$ denote the number of primary problems $\mathbf{Q}_f$ covered by the problem $\mathbf{P}_{\mathbf{B}}$. This number can be easily calculated via $\lambda_{\mathbf{B}}(i)$:

$$H_{\mathbf{B}} = \prod_{i \notin \mathbf{B}^1} \left(k - \lambda_{\mathbf{B}}(i) - i \right).$$

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

3.10. Remarks. 1. Monotone lattice walks are often depicted 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 an appropriate change of variables in Theorem 2.8. But in the coordinates we use, some expressions obtained look more convenient.

2. In practice, evidently, it is more suitable 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 principle. In the next Section we shall see this for $n = p^2$.

4 p^2 -Circulants

We describe briefly how the above approach can be applied to the case $k = 2$. This is the first successful “global” enumeration when Ádám’s condition (M_1) does not hold. The proofs and other details can be found in [21].

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

k	$\mathbf{B} = \{ij\}$	$T_{\mathbf{B}}$ (indices)	$H_{\mathbf{B}}$	$\varrho(\mathbf{B})$	$(F_{\mathbf{B}})$	
					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	$m_2 = m_1$	$m_1 \equiv m_0 \pmod{p}$
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	$m_3 = m_2 = m_1$	$m_1 \equiv m_0 \pmod{p^2}$
	01,20	00,10	2	2	$m_3 = m_2, m_1 = m_0$	$m_2 \equiv m_1 \pmod{p}$
	02,10	01	2	2	$m_3 = m_2 = m_1$	$m_1 \equiv m_0 \pmod{p}$
	02,11	01,10,20	1	3	$m_2 = m_1$	$m_1 \equiv m_0 \pmod{p}$
	02,20	01,11	1	2	$m_3 = m_2, m_1 = m_0$	-
	11,20	02,10	1	3	$m_3 = m_2$	$m_2 \equiv m_1 \pmod{p}$
	02,11,20	01,10	1	3	$m_3 = m_2$	$m_2 \equiv m_1 \pmod{p},$ $m_1 \equiv m_0 \pmod{p}$

4.1. By isomorphism Theorem 2.8, p^2 -circulants can be counted 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 $A(p^2)$ denote the corresponding number. 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 $B(p^2)$. Instead, as we know, in the case when

$$(1+p)X_{(0)} = X_{(0)} \quad (\neg R_{00})$$

is valid, multipliers m_0 and m_1 are allowed to be independent, i.e. we have here the group $\mathbb{Z}_{p^2}^* \oplus \mathbb{Z}_{p^2}^*$ and its induced layer-wise action on such connection sets. Let $D(p^2)$ denote the number of its orbits, i.e. the number which is to be correctly contributed instead of $B(p^2)$. Let, finally, $C(p^2)$ denote the required number of non-isomorphic circulants (in generic designations). Then

$$C(p^2) = A(p^2) - B(p^2) + D(p^2). \quad (4.1)$$

The right-hand terms can be found by Pólya's method (cf., for example, [20] or [24]) applied to the appropriate groups of multipliers. $A(p^2)$ corresponds to the join

$$(\mathbb{Z}_{p^2}^*, \mathbb{Z}_{p^2}') = (\mathbb{Z}_{p^2}^*, \mathbb{Z}_p^*) \dot{\vee} (\mathbb{Z}_{p^2}^*, \mathbb{Z}_{p^2}^*), \quad (4.2)$$

$B(p^2)$ corresponds to the join

$$(\mathbb{Z}_{p^2}^*, \mathbb{Z}_p^*) \dot{\vee} (\mathbb{Z}_{p^2}^*, \mathbb{Z}_p^*), \quad (4.3)$$

while $D(p^2)$ corresponds to the direct sum

$$(\mathbb{Z}_{p^2}^*, \mathbb{Z}_p^*) \oplus (\mathbb{Z}_{p^2}^*, \mathbb{Z}_p^*). \quad (4.4)$$

Notice also that in order to make these operations correct formally as they are defined in Subsection 2.9, we must use two disjoint copies of the set $\mathbb{Z}_p^*$ on which the multiplicative group $\mathbb{Z}_{p^2}^*$ acts.

4.2. Given a group G with an action on a finite set U , we denote by $I_{(G,U)} = I_{(G,U)}(\mathbf{x}) = I_{(G,U)}(n; x_1, x_2, \dots, x_n)$ its *cycle index*, which is a polynomial of degree $n = |U|$ in the variables $x_1, x_2, \dots, x_n$. Working with cycle indices of groups acting on sets of heterogeneous objects it is sometimes convenient to use variables of several different types. In particular, we shall use cycle indices not only in variables $\mathbf{x}$ but also in $\mathbf{y}$ and even in $\mathbf{xy}$ where $\mathbf{x}$ (resp., $\mathbf{y}$) is the generic notation for the sequences $x_1, x_2, \dots, x_n$ (resp., $y_1, y_2, \dots, y_n$) of variables and $\mathbf{xy}$ denotes all pairwise products $x_1y_1, x_2y_2, \dots, x_ny_n$.

Let (G, U) be a group with an action and $(\overline{G}, U)$ the corresponding *faithful* permutation group. Here $\overline{G} = G/K$ is the quotient group by $K = \{k \in G \mid \forall u \in U : u^k = u\}$, 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:

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

PROOF.

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

where $a_i(g) = a_i(g, U)$ stands for the number of disjoint cycles of length i in g . $\square$

Thus, both polynomials coincide, in spite of the fact that the numbers of their terms are different by definition. Hence the reduction to the faithful action provides no analytical or computational advantages.

4.4. Lemma. Let (G, U) , (G, V) and (H, V) be groups with actions as considered in Subsection 2.9, then

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

and

$$I_{(G,U) \dot{\vee} (G,V)}(\mathbf{x}, \mathbf{y}) = I_{(G,U)}(\mathbf{x}) \dot{\vee} I_{(G,V)}(\mathbf{y}) \quad (4.5)$$

where

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

PROOF. The first formula is well known, see [20, p. 74]. Formula (4.5) is evident by definition. $\square$

4.5. For the regular cyclic permutation group $Z(n) \cong (\mathbb{Z}_n, \mathbb{Z}_n)$ denote $\mathcal{J}_n(\mathbf{x}) := I_{Z(n)}(\mathbf{x})$. In particular for prime $n = p$, we have

$$I_{(\mathbb{Z}_p^*, \mathbb{Z}_p^*)} = \mathcal{J}_{p-1}(\mathbf{x}) = \frac{1}{p-1} \sum_{r|p-1} \phi(r) x_r^{(p-1)/r} \quad (4.6)$$

where $\phi(n)$ is the Euler totient function.

Now we can easily find cycle indices of the groups with actions (4.2), (4.3) and (4.4). After a few elementary transformations we arrive at the polynomial

$$\mathcal{C}(p^2; \mathbf{x}, \mathbf{y}) := \frac{1}{p} \mathcal{J}_{p-1}(\mathbf{x}^{p+1}) - \frac{1}{p} \mathcal{J}_{p-1}(\mathbf{x}\mathbf{y}) + \mathcal{J}_{p-1}(\mathbf{x}) \mathcal{J}_{p-1}(\mathbf{y}) \quad (4.7)$$

for directed circulants and the polynomial

$$\mathcal{C}^*(p^2; \mathbf{x}, \mathbf{y}) := \frac{1}{p} \mathcal{J}_{\frac{p-1}{2}}(\mathbf{x}^{p+1}) - \frac{1}{p} \mathcal{J}_{\frac{p-1}{2}}(\mathbf{x}\mathbf{y}) + \mathcal{J}_{\frac{p-1}{2}}(\mathbf{x}) \mathcal{J}_{\frac{p-1}{2}}(\mathbf{y}) \quad (4.8)$$

for undirected circulants. In fact, they are also suitable to count several different types of circulant graphs simultaneously. Namely, we consider the following quantities:

$C_d(n)$ the number of non-isomorphic directed circulant n -graphs;

$C_u(n)$ the number of non-isomorphic undirected circulant n -graphs;

$C_t(n)$ the number of non-isomorphic circulant n -tournaments;

$C_{sd}(n)$ and $C_{su}(n)$ the numbers of non-isomorphic self-complementary directed and undirected circulant graphs, respectively.

Let also $C_d(n, r)$ and $C_u(n, r)$ denote the corresponding numbers of regular circulant graphs of valency r and $c_d(n, t)$ and $c_u(n, t)$ denote their ordinary generating functions (polynomials in the variable t):

$$c_d(n, t) := \sum_{r \geq 0} C_d(n, r) t^r \quad \text{and} \quad c_u(n, t) := \sum_{r \geq 0} C_u(n, r) t^r.$$

Clearly $C_d(n) = c_d(n, 1)$ and $C_u(n) = c_u(n, 1)$.

4.6. Theorem [21].

$$\begin{aligned} c_d(p^2, t) &= \mathcal{C}(p^2; \mathbf{x}, \mathbf{y})|_{\{x_r := 1+t^r, y_r := 1+t^{pr}\}_{r=1,2,\dots}}, \\ c_u(p^2, t) &= \mathcal{C}^*(p^2; \mathbf{x}, \mathbf{y})|_{\{x_r := 1+t^{2r}, y_r := 1+t^{2pr}\}_{r=1,2,\dots}}, \\ C_t(p^2) &= \mathcal{C}(p^2; \mathbf{x}, \mathbf{y})|_{\{x_r := 0, y_r := 0\}_{r \text{ even}}, \{x_r^2 := 2, y_r^2 := 2\}_{r \text{ odd}}}, \\ C_{sd}(p^2) &= \mathcal{C}(p^2; \mathbf{x}, \mathbf{y})|_{\{x_r := 0, y_r := 0\}_{r \text{ odd}}, \{x_r := 2, y_r := 2\}_{r \text{ even}}}, \\ C_{su}(p^2) &= \mathcal{C}^*(p^2; \mathbf{x}, \mathbf{y})|_{\{x_r := 0, y_r := 0\}_{r \text{ odd}}, \{x_r := 2, y_r := 2\}_{r \text{ even}}}. \end{aligned}$$

There are some interesting interrelations and consequences of the above formulae, for which, together with numerical data, we refer to the paper [21].

5 Concluding remarks

1. There exists also an alternative “structural” approach to the enumeration of circulant graphs. It has been developed in [21]. Instead of isomorphism criteria in terms of layers and 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. [30]) unlike the present paper, where we use only one result of this theory, Theorem 2.8. The structural approach is closer to the constructive enumeration and results in different formulae even for the circulant graphs of order p .

2. Manipulating with lattice walks, we introduced several simple notions similar or equivalent to ones used actively in recent researches (cf., for example, [17, 25]). 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 an appropriate change of the coordinates, the empty set of south-east corners (turns) would define another off-diagonal lattice path from $0k$ to $k0$ having only one turn (in kk).

3. The considerations in Section 3 reflect an intrinsic splitting of the set of p^k -circulants into $\text{Cat}(k)$ subsets in conformity with the isomorphism theorem. The parametrization of these subsets by lattice walks will be, hopefully, useful in investigating other, non-enumerative, combinatorial and algebraic properties of p^k -circulants.

4. In [28], M. Muzychuk with one of the present authors obtained some necessary and also some sufficient conditions for two circulant graphs of an *arbitrary order* to be isomorphic. These conditions generalize and strengthen Theorem 2.8 for prime-power orders and the one-multiplier isomorphism criterion for the square-free orders proved in [27]. Presumably, these results can be applied to promote the enumeration of circulant graphs of other orders (first of all, of the form $p^k q^\ell$, p, q primes).

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 this paper has been started and partially fulfilled within the framework of the “Research in Pairs” program. We wish to thank a referee for helpful suggestions.

References

- [1] A. Ádám, Research problem 2–10, *J. Combin. Th.*, **2** (1967), No 3, 393.
- [2] B. Alspach, On point-symmetric tournaments, *Canad. Math. Bull.*, **13** (1970), No 3, 317–323.
- [3] 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.

- [4] B. Alspach, Isomorphism and Cayley graphs on abelian groups, in: *Graph Symmetry*, (Montréal, PQ, 1996), 1–22. NATO Adv. Sci. Inst. Ser. C, Math. Phys. Sci., 497, Kluwer Acad. Publ., Dordrecht, 1997.
- [5] B. Alspach and T.D. Parsons, Isomorphism of circulant graphs and digraphs, *Discr. Math.*, **25** (1979), No 1, 97–108.
- [6] A. Astie, Groupes d’automorphismes des tournois sommet-symétriques d’ordre premier et dénombrement de ces tournois, *C. r. Acad. Sci. Paris (A)*, **275** (1972), No 3, 167–169.
- [7] C.Y. Chao, On digraphs with circulant adjacency matrices, *Archiv Math.*, **54** (1990), No 1, 93–104.
- [8] C.Y. Chao and J.G. Wells, A class of vertex-transitive digraphs, *J. Combin. Th.*, **B14** (1973), No 3, 246–255.
- [9] C.Y. Chao and J.G. Wells, A class of vertex-transitive digraphs, II, *J. Combin. Th.*, **B32** (1982), No 3, 336–346.
- [10] 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.
- [11] G.L. Chia and C.K. Lim, A class of self-complementary vertex-transitive digraphs, *J. Graph Th.*, **10** (1986), No 2, 241–249.
- [12] H.A. David, Enumeration of cyclic paired-comparison designs, *Amer. Math. Monthly*, **72** (1965), No 3, 241–248.
- [13] H.A. David, Enumeration of cyclic graphs and cyclic designs, *J. Combin. Th.*, **B13** (1972), No 3, 303–308.
- [14] N. Dershowitz and S. Zaks, Enumeration of ordered trees, *Discr. Math.*, **31** (1980), No 1, 9–28.
- [15] B. Elspas and J. Turner, Graphs with circulant adjacency matrices, *J. Combin. Th.*, **9** (1970), No 3, 297–307.
- [16] 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.
- [17] I. Gessel, W. Goddard, W. Shur, H. S. Wilf and L. Yen, Counting pairs of lattice paths by intersections, *J. Combin. Th.*, **A74** (1996), No 2, 173–187.
- [18] F. Harary, *Graph Theory*, Addison-Wesley, Reading, MA, 1969.
- [19] H. Hasse, *Vorlesungen über Zahlentheorie*, 2 Auflage, Springer-Verlag, Berlin, 1964.
- [20] A. Kerber, *Algebraic Combinatorics via Finite Group Actions*, BI-Wissenschaftsverlag, Mannheim, 1991.
- [21] M. Klin, V. Liskovets and R. Pöschel, Analytical enumeration of circulant graphs with prime-squared number of vertices, *Sém. Lotharing. Combin.*, **36** (1996), B36d, 36 pp.
- [22] 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.

- [23] 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.
- [24] 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.
- [25] C. Krattenthaler and R. A. Sulanke, Counting pairs of nonintersecting lattice paths with respect to weighted turns, *Discr. Math.*, **153** (1996), No 1–3, 189–198.
- [26] V. Liskovets and R. Pöschel, On the enumeration of circulant graphs of prime-power and square-free orders. *Preprint* Math-AL-8-1996, TU-Dresden, 37 pp.
- [27] M. Muzychuk, *Ádám's conjecture is true in the square-free case*, *J. Combin. Th.*, **A72** (1995), No 1, 118–134.
- [28] M. Muzychuk and R. Pöschel, Isomorphism conditions for S-rings and circulant graphs, *in preparation*.
- [29] P. P. Pálffy, Isomorphism problem for relational structures with a cyclic automorphism, *Europ. J. Combin.*, **8** (1987), No 1, 35–43.
- [30] R. Pöschel, Untersuchungen von S-Ringen, insbesondere im Gruppenring von p -Gruppen, *Math. Nachr.*, **60** (1974), 1–27.
- [31] 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.
- [32] R. P. Stanley, *Enumerative Combinatorics*, v. 2, Cambridge Univ. Press, Cambridge (1999).
- [33] J. Turner, Point-symmetric graphs with a prime number of points, *J. Combin. Th.*, **3** (1967), No 2, 136–145.
- [34] H. Zhang, Point-color-symmetric graphs with a prime number of vertices, *Graphs & Combin.*, **6** (1990), No 3, 297–302.