Séminaire Lotharingien de Combinatoire **51** (2005), Article B51h

THE NUMBER OF INDECOMPOSABLE SCHUR RINGS OVER A CYCLIC 2-GROUP

I. KOVÁCS*

Abstract. Indecomposable Schur rings over a cyclic group Z_n of order n are considered. In the case $n = p^m$, p an odd prime, the total number of such rings was described in terms of Catalan numbers by Liskovets and Pöschel [*Discr. Math.* **214** (2000), 173–191]. Here, a closed formula is shown for the total number of indecomposable Schur rings over Z_{2^m} using Catalan and Schröder numbers. The result is obtained after the initial problem is turned into a lattice path problem.

1. Introduction

Let H be a finite group with identity element e. Denote by $\mathbb{Z}[H]$ the *group ring* of all formal sums $\sum_{h\in H} a_h h$, $a_h \in \mathbb{Z}$, $h \in H$. For $T \subseteq H$, the group ring element $\sum_{h\in T} h$ will be denoted by $\underline{T}$. Such an element is also called a *simple quantity*. The *transpose* of $\alpha = \sum_{h\in H} a_h h$ is defined as $\alpha^\top = \sum_{h\in H} a_h(h^{-1})$. A subring $\mathfrak{S}$ of $\mathbb{Z}[H]$ is called a *Schur ring over H* (for short *S-ring*) if it is generated as a module over $\mathbb{Z}$ by the simple quantities $\underline{T}_1, \ldots, \underline{T}_r$ such that they satisfy the axioms:

- $T_1 = \{e\}$, $T_i \cap T_j = \emptyset$ for all $i \neq j$,
- $\sum_{i=1}^r \underline{T_i} = \underline{H}$,
- for each $i \in \{1, \ldots, r\}$ there exists some $j \in \{1, \ldots, r\}$ such that $\underline{T_i}^\top = \underline{T_j}$.

The sets T_i are called the *basic sets* of $\mathfrak{S}$. We will denote by $B(\mathfrak{S})$ the set of all basic sets of $\mathfrak{S}$.

Trivial examples for S-rings are provided by the full group ring $\mathbb{Z}[H]$, and the module generated by the basic sets $\{e\}$ and $H \setminus \{e\}$. The latter one is also called the *trivial* S-ring over H.

The notion of an S-ring was created by I. Schur to use them in his investigation of permutation groups, see [10]. Later it was developed to a powerful tool in group theory, see [11, 13].

It was observed later that S-rings can also be applied in algebraic combinatorics. For a given subset $S \subseteq H$, the *Cayley digraph* of H with respect to S is defined as the digraph (V, E), where $V = H$ and $E = \{(h, hs) : h \in H, s \in S\}$. Cayley digraphs of cyclic groups are also called *circulant digraphs*. From now on Z_n will denote a cyclic group of order n. M. Klin and R. Pöschel started an approach based on S-rings to study circulant digraphs, see [3]. For a recent survey on this approach, see [9].

Let $\mathfrak{S}$ be an S-ring over Z_n. $\mathfrak{S}$ is called *wreath-decomposable* (or shortly *decomposable*), if there is a nontrivial, proper subgroup $H < Z_n$ such that for every basic

*This research was partially supported by grant OTKA T-043758, and by a grant provided by the University of Pécs.

set T, $T \subset H$ or $T = \bigcup_{h \in T} Hh$. Otherwise, $\mathfrak{S}$ is called *indecomposable*. If an S-ring is decomposable, then it can be obtained as the wreath product of two smaller S-rings, see [9]. Indecomposable S-rings play a crucial role in the description of the automorphism group of circulant graphs with p^m vertices, p a prime, see [4, 6].

In this paper we consider the problem of counting the number of indecomposable rings. For $m \in \mathbb{N}$ and a prime p, we set the notation:

$$I(m,p) = \#\{ \text{ indecomposable S-rings over } Z_{p^m}\}.$$

It was shown in [8] that if $p > 2$, then

$$I(m,p) = \delta(p-1)c_{m-1},$$

where $\delta(p-1)$ is equal to the number of positive divisors of $(p-1)$, and for $k \in \mathbb{N}_0$, c_k is the k-th *Catalan number*: $c_k = \frac{1}{k+1}\binom{2k}{k}$, cf. [12, page 172]. In this paper, a closed formula is derived for the numbers $I(m,2)$. For this purpose, besides the Catalan numbers, we will also need the so called *Schröder numbers*. For $k \in \mathbb{N}_0$, the k-th Schröder number is: $s_k = \sum_{k=0}^{n} \frac{1}{k+1}\binom{2k}{k}\binom{n+k}{2k}$, cf. [12]. In Section 4, the interpretation of both type of numbers will be recalled in terms of certain lattice paths. Our main result is the following theorem.

Theorem 1.1. *If $m \geq 3$ then*

$$I(m,2) = 1 + \frac{1}{3\sqrt{17}} \sum_{k=0}^{m-1} a_{m-1-k} \Big[\Big(\frac{11+3\sqrt{17}}{4}\Big)^{k+1} - \Big(\frac{11-3\sqrt{17}}{4}\Big)^{k+1} \Big],$$

where $a_0 = 2$, $a_1 = -9$ and

$$a_i = (2c_i - 4c_{i-1}) + (s_i - 2s_{i-1}) - 3\sum_{j=0}^{i-1} c_i s_{i-1-j}, \quad i \geq 2.$$

Here, c_i and s_i are the i-th Catalan and Schröder number, respectively.

It is easy to derive that $I(1,2) = 1$ and $I(2,2) = 2$. The values of $I(m,2)$ for $m \leq 10$ are shown in the following table.

m	1	2	3	4	5	6	7	8	9	10
$I(m,2)$	1	2	5	16	63	271	1225	5726	27461	134461

We refer to the characterization of S-rings over Z_{2^m} given in [2]. This paper contains a table which lists all S-rings over Z_{2^m}, $m \leq 5$. One can select the indecomposable ones to find that their total numbers completely agree with the numerical data presented above.

We conclude the introduction with a brief outline of our paper. The starting point of our examinations is the classification of S-rings over Z_{2^m} proved in [1, 2]. This will be shortly recalled in Section 2. In Section 3, this classification will be used to establish a bijection between the set of all nontrivial, indecomposable S-rings over Z_{2^m} and the collection of so-called indecomposable parameter vectors of length m (see also [5]). In Section 4, the initial counting problem will be turned into a lattice path counting problem. It will be shown that the set indecomposable parameter vectors of length m is in one-to-one correspondence with a nicely described set of paths in the $(m-1)\times(m-1)$ plane integer lattice consisting of steps $(1,0)$, $(0,1)$, and $(1,1)$. Theorem 1.1 will be settled in Section 5 based on this correspondence.

2. S-rings over cyclic 2-groups

Throughout the section $n = 2^m$ and $m \geq 2$ are assumed. Let $Z_n = \langle g \rangle$. Denote by H_i the subgroup of Z_n of order 2^i, $i = 0, \dots, m$, i.e., $H_i = \langle g^{2^{m-i}} \rangle$. We set the notation $L_i = H_{m-i} \setminus H_{m-1-i}$, $i = 0, \dots, m-1$, and $L_m = \{e\}$.

Let $\mathfrak{S}$ be an S-ring over Z_n. Next we describe its basic sets following [1, 2]. Let $T \in B(\mathfrak{S})$, $T \neq \{e\}$. It was proved in [1, 2] (cf. also [7]) that there are two main possibilities for T: either $T = H_j \setminus H_k$ for some $0 \leq k < j \leq m$, or T is contained in some set L_i. The *basic relation* θ of $\mathfrak{S}$ is an equivalence relation which is defined on the set $\{0, 1, \dots, m-1\}$ in such a manner that it has equivalence classes of the form $\{i, \dots, i+j\}$, $i \in \{0, \dots, m-1\}$, $j \in \{0, \dots, m-1-i\}$. The set $\{i, \dots, i+j\}$ with $j > 0$ is an equivalence class of θ if and only if $H_{m-i} \setminus H_{m-i-j-1}$ is a basic set of $\mathfrak{S}$. The set $\{i\}$ is an equivalence class if and only if L_i cannot be obtained as a proper subset of a basic set of $\mathfrak{S}$.

Assume that $T \subseteq L_i$. According to the classical theory of S-rings, see [13], the basic sets of $\mathfrak{S}$ contained in L_i are the orbits of some subgroup $K \leq \mathrm{Aut}(Z_n)$. Consequently, T can be obtained as one of the orbits of K. For every $i \in \{0, \dots, m-1\}$, denote by K_i the maximal subgroup of $\mathrm{Aut}(Z_n)$ such that the sets $L_i \cap T$, $T \in B(\mathfrak{S})$ are orbits of K_i. We refer to the groups $K_0, \dots, K_{m-1}$ as the *basic groups* of $\mathfrak{S}$.

It follows from the above observations that $\mathfrak{S}$ is uniquely determined by its basic relation and basic groups. In [1, 2] the basic relation together with the basic groups were called the *S-system* of $\mathfrak{S}$. To recall the characterization of S-rings in terms of their basic relation and basic groups we need to give explicitly the subgroups of $\mathrm{Aut}(Z_n)$. It is clear that $\mathrm{Aut}(Z_n) = \{g^i \mapsto g^{i\cdot k} : 1 \leq k < n,\ \gcd(k,n) = 1\}$. In what follows, we identify $\mathrm{Aut}(Z_n)$ with the multiplicative group modulo n of elements $1 \leq k \leq n$, $\gcd(k,n) = 1$. It is well-known that $\mathrm{Aut}(Z_{2^m}) = \langle -1, 5 \rangle$. (Operations are taken modulo $n = 2^m$.) The subgroups of $\mathrm{Aut}(Z_n)$ are

$$\begin{aligned}
G_{3i+1} &= \{\pm 1 + 2^{i+2}k \mid 0 \leq k < 2^{m-i-2}\} \quad (i = 0, \dots, m-2), \\
G_{3i+2} &= \{1 + 2^{i+2}k \mid 0 \leq k < 2^{m-i-2}\} \quad (i = 0, \dots, m-2), \\
G_{3i} &= \{(-1)^k + 2^{i+1}k \mid 0 \leq k < 2^{m-i-1}\} \quad (i = 1, \dots, m-2).
\end{aligned} \tag{1}$$

In fact, it is not hard to see that $G_{3i+1} = \langle -1, 5^{2^i} \rangle$, $G_{3i+2} = \langle 5^{2^i} \rangle$, and $G_{3i} = \langle -5^{2^{i-1}} \rangle$. The S-rings over Z_{2^m} ($m \geq 2$) are characterized in the following theorem.

Theorem 2.1. [1, 2]
Let θ be a relation on $\{0, \dots, m-1\}$, and let $K_i \leq Aut(Z_n)$, $i = 0, \dots, m-1$ ($m \geq 2$). Then they form the basic relation and basic groups, respectively, of some S-ring over Z_{2^m} if and only if the following properties hold:

(i) *Every equivalence class of θ is of the form $\{i, \dots, i+j\}$,*

(ii) *If* $\{i, \dots, i+j\}$ *is an equivalence class of* θ *with* $j > 0$*, then* $K_i = K_{i+1} = \dots = K_{i+j} = G_1$*, and* $K_{i-1} = G_1$*,* $K_{i-2} \in \{G_1, G_2\}$ *(if* $i = 0$ *or* $i = 1$*, then delete the conditions where negative indices appear),*

(iii) $K_{m-1} = G_1$*,* $K_{m-2} \in \{G_1, G_2\}$*,*

(iv) *Let* $1 \le j \le m-2$*. If* $K_j = G_{3i+1}$ *or* $K_j = G_{3i+3}$ *for some* $0 \le i \le m-2$*, then*

$$K_{j-1} \in \{G_2\} \cup \{G_{3s+1} \mid 0 \le s \le i+1\} \cup \{G_{3r+3} \mid 0 \le r \le i\},$$

If $K_j = G_{3i+2}$ *for some* $0 \le i \le m-2$*, then*

$$K_{j-1} \in \{G_1\} \cup \{G_{3s+2} \mid 0 \le s \le i+1\}.$$

Denote by $\mathcal{S}(m)$ the set of all S-rings over Z_{2^m}. It follows immediately that the trivial S-ring is indecomposable. In what follows, we will ignore this possibility. Actually, the first summand 1 in the main formula (Theorem 1.1) will be responsible for the trivial S-ring. In the rest of this section it will be shown: if $\mathfrak{S}$ is a nontrivial, indecomposable S-ring over Z_{2^m}, $m \ge 2$, then its basic relation is equal to the identity relation ω_m on $\{0, \dots, m-1\}$, i.e., ω_m consists of singleton classes. We introduce the notation $\mathcal{S}^*(m)$ for the collection of S-rings over Z_{2^m} that have basic relation ω_m. We remark that not all members of $\mathcal{S}^*(m)$ are indecomposable. The description of the indecomposable rings will be completed in the next section.

We introduce the functions $f_i : \mathcal{S}(m) \to \mathbb{Z}$, $i = 0, \dots, m-1$, which act on an $\mathfrak{S} \in \mathcal{S}(m)$ by

$$f_i(\mathfrak{S}) = \max\{k : \, H_k g^{2^i} \subseteq T \cap L_i, \, T \in B(\mathfrak{S})\}.$$

In particular, if T' is a basic set of $\mathfrak{S}$ which is contained in L_i, then $f_i(\mathfrak{S})$ is the maximal number k such that T' is the union of H_k-cosets. The value $f_i(\mathfrak{S})$ can be calculated from the basic group K_i of $\mathfrak{S}$ by using (1). We have

$$f_i(\mathfrak{S}) = \begin{cases} m-2-a-i, & \text{if } K_i = G_{3a+b} \ne G_1, \\ m-1-i, & \text{if } K_i = G_1. \end{cases} \tag{2}$$

Proposition 2.2. *Let* $\mathfrak{S}$ *be an S-ring over* Z_{2^m} *having basic groups* $K_0, \dots, K_{m-1}$*. If* $K_1 \ne G_1$*, then* $f_0(\mathfrak{S}) \ge f_1(\mathfrak{S})$*.*

Proof. Let $K_1 = G_k$, $k = 3a+b$. Since we assumed $k > 1$, by (2) we have

$$f_1(\mathfrak{S}) = m-3-a.$$

Let $K_0 = G_{k'}$, $k' = 3a' + b'$. Because of Theorem 2.1(iv), we have $a' \le a+1$. If $k' = 1$, then $f_0(\mathfrak{S}) = m-1$, which is clearly larger than $f_1(\mathfrak{S})$. If $k' > 1$, then (2) and $a' \le a+1$ imply

$$f_0(\mathfrak{S}) = m-2-a' \ge m-3-a = f_1(\mathfrak{S}).$$

□

Proposition 2.3. *If* $\mathfrak{S}$ *is a nontrivial, indecomposable S-ring over* Z_{2^m}*, then its basic relation is* ω_m*.*

Proof. Let $\mathfrak{S}$ have basic relation θ and let it have basic groups $K_0, \dots, K_{m-1}$. We are going to show that if $\theta \neq \omega_m$, then $\mathfrak{S}$ is decomposable. We proceed by induction on m. The cases $m \leq 3$ can be checked directly, hence we assume that $m \geq 4$.

If $K_0 = G_1$, then there is a subgroup H_k such that $Z_n \setminus H_k$ is a basic set of $\mathfrak{S}$. If $k = 0$, then $\mathfrak{S}$ is the trivial S-ring. This possibility is excluded, hence $k > 0$, and by definition it follows that $\mathfrak{S}$ is decomposable.

Assume that $K_0 \neq G_1$. Then $\underline{H_{m-1}} \in \mathfrak{S}$, hence we can consider the S-ring over H_{m-1} generated by the basic sets of $\mathfrak{S}$ contained in H_{m-1}. Denote this S-ring by $\mathfrak{S}^*$. It follows that the basic relation of $\mathfrak{S}^*$ is equal to $\theta^* = \{(i,j) : (i+1, j+1) \in \theta\}$. Thus $\theta^* \neq \omega_{m-1}$, and, because of the induction hypothesis, $\mathfrak{S}^*$ is decomposable. This means by definition that there is some $1 \leq r \leq m-2$ such that every basic set of $\mathfrak{S}^*$ (which are the basic sets of $\mathfrak{S}$ contained in H_{m-1}) not contained in H_r is the union of some H_r-cosets. This implies that $f_1(\mathfrak{S}) \geq r$. A basic set in $L_0 = H_m \setminus H_{m-1}$ is the union of H_d-cosets, where $d = f_0(\mathfrak{S})$. Thus if $d \geq r$, then $\mathfrak{S}$ is decomposable. In case $K_1 \neq G_1$ this follows from Proposition 2.2, for $d = f_0(\mathfrak{S}) \geq f_1(\mathfrak{S}) \geq r$.

Therefore, it remains to consider the case $K_1 = G_1$. The assertion that $L_1 = H_{m-1} \setminus H_{m-2}$ is not a basic set is equivalent to saying that θ has equivalence class $\{1, \dots, i\}$ with $i > 1$. According to Theorem 2.1(ii), we have $K_0 = G_1$, i.e., $d = m-1$, which clearly exceeds r and, consequently, $\mathfrak{S}$ is decomposable. Assume finally that L_1 is a basic set, i.e., $\underline{H_{m-2}} \in \mathfrak{S}^*$. This gives $K_0 = G_k$ with $k \leq 4$, see Theorem 2.1(iv). Thus, by (2),

$$d = f_0(\mathfrak{S}) \geq m - 3. \tag{3}$$

As before, the S-ring over H_{m-2} which is generated by the basic sets of $\mathfrak{S}$ contained in H_{m-2} is decomposable because of the induction hypothesis. This implies that every basic set of $\mathfrak{S}$ which is contained in $H_{m-2} \setminus H_s$ is the union of H_s-cosets for some $1 \leq s \leq m-3$. Since $d \geq m-3 \geq s$, see (3), and since L_1 is a basic set, we obtain finally that $\mathfrak{S}$ is decomposable as required. The proof now is completed. □

For our purpose, only the S-rings in $\mathcal{S}^*(m)$ need to be considered. An S-ring $\mathfrak{S} \in \mathcal{S}^*(m)$ is uniquely determined by its basic groups $K_0, \dots, K_{m-1}$ since, by definition, its basic relation is $\theta = \omega_m$. Now, $K_{m-1} = G_1$, $K_{m-2} \in \{G_1, G_2\}$ (Theorem 2.1(iii)), and for $i < m-2$ the basic group K_i is determined recursively from K_{i+1} (see Theorem 2.1(iv)). This can be interpreted via a rooted tree, which will be denoted by $T(m)$. Each vertex of $T(m)$ is labeled by one of the groups G_i. Label the root, which is also considered as the 0-th level of the tree, by G_1. Put two points on the 1-th level, label them by G_1 and G_2, respectively, and join the root with both using a directed edge. The i-th level, $1 < i \leq m-1$, is built based on the recursion in Theorem 2.1(iv). As an illustration, $T(4)$ is shown in Figure 1. Then the rings in $\mathcal{S}^*(m)$ can be naturally identified with the directed paths in $T(m)$ of length $m-1$. The S-ring $\mathfrak{S} \in \mathcal{S}^*(m)$ having basic groups $(K_0, \dots, K_{m-1})$ corresponds to the directed path of $T(m)$ that passes the i-th level at the vertex labeled with K_{m-1-i}; and conversely, any such directed path induces an ring in $\mathcal{S}^*(m)$ by considering the labels of its vertices.

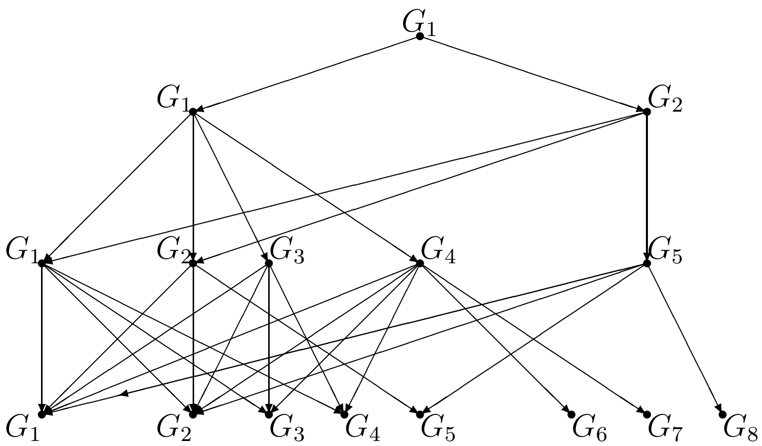


FIGURE 1. The directed rooted tree $T(4)$

3. PARAMETER VECTORS

In this section we will identify the S-rings in $\mathcal{S}^*(m)$, $m \geq 2$, with a collection of parameters. The main purpose is to give a formal description of the parameters that correspond to indecomposable rings in $\mathcal{S}^*(m)$. (Hence, they will also describe all nontrivial, indecomposable S-rings over Z_{2^m}.)

Introduce the set $M = \{0, \ldots, m-1\} \times \{0, +, -\}$. For the element $(s, \pm) \in M$ and $(s, 0) \in M$, respectively, we agree to use the notations $s^{\pm}$ and s, respectively.

Definition 3.1. *Let $\mathfrak{S} \in \mathcal{S}^*(m)$, and let it have basic groups $K_0, \ldots, K_{m-1}$ $(m \geq 2)$. The* **parameter vector** $\vec{u} = (u_0^{\varepsilon_0}, \ldots, u_{m-1}^{\varepsilon_{m-1}}) \in M^m$ *of $\mathfrak{S}$ is defined as*

$$u_i = f_i(\mathfrak{S}) = \begin{cases} m-2-a-i, & \text{if } K_i = G_{3a+b} \neq G_1, \\ m-1-i, & \text{if } K_i = G_1, \end{cases} \tag{4}$$

and

$$\varepsilon_i = \begin{cases} -, & \text{if } K_i = G_{3a}, \\ +, & \text{if } K_i = G_{3a+1} \text{ and } a > 0, \\ 0, & \text{if } K_i = G_1 \text{ or } K_i = G_{3a+2}. \end{cases} \tag{5}$$

The parameter vector $\vec{u}$ is called **indecomposable** *if and only if $\mathfrak{S}$ is indecomposable.*

As a direct consequence of Definition 3.1 we have the following proposition.

Proposition 3.2. *If $(u_i^{\varepsilon_i})$ is a parameter vector of length m, then*

$$u_i \leq \begin{cases} m-3-i, & \text{if } \varepsilon_i \neq 0, \\ m-1-i, & \text{if } \varepsilon_i = 0, \end{cases}$$

for all $i \in \{0, \ldots, m-1\}$.

The parameter vectors of length m can be easily obtained using $T(m)$. First, replace the labels of $T(m)$ by elements of M in the following manner: if a vertex on the i-th level is labeled by G_{3a+b}, then assign to it the "new" label $u^{\varepsilon} \in M$, where

$$u = \begin{cases} i - 1 - a, & \text{if } 3a + b > 1, \\ i, & \text{if } 3a + b = 1, \end{cases}$$

and

$$\varepsilon = \begin{cases} +, & \text{if } b = 1 \text{ and } a > 0, \\ -, & \text{if } b = 0, \\ 0, & \text{if } b = 2 \text{ or } 3a + b = 1. \end{cases}$$

See Figure 2 below, where the tree $T(4)$ is shown with its "new" labels.

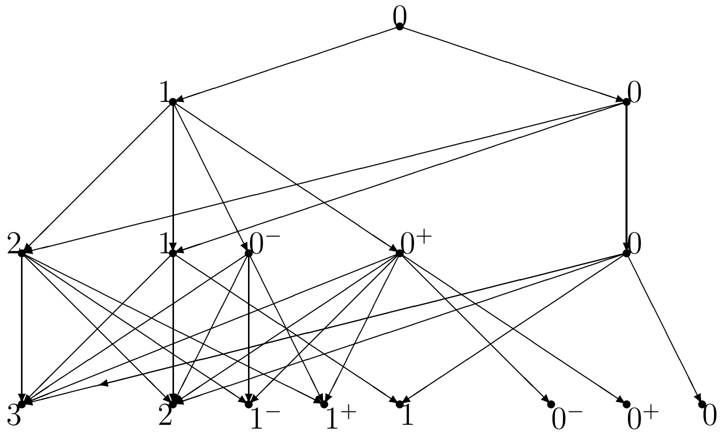


FIGURE 2. $T(4)$ with "new" labels

Now the parameter vector $(u_i^{\varepsilon_i})$ of a given S-ring $\mathfrak{S} \in \mathcal{S}^*(m)$ can be easily obtained. Consider the directed path of $T(m)$ corresponding to $\mathfrak{S}$, and then write down the "new" labels of $T(m)$ that are passed by the path. (Note: the label of the root provides $u_{m-1}^{\varepsilon_{m-1}}$, and so on.) Based on Figure 2, we list all parameter vectors of length at most 4 in Table 1.

m	parameter	vectors			
2	$(1,0)$	$(0,0)^*$			
3	$(2,1,0)$	$(2,0,0)$	$(1,1,0)$	$(1,0,0)^*$	$(0^-,1,0)^*$
	$(0^+,1,0)^*$	$(0,0,0)^*$			
4	$(3,2,1,0)$	$(3,2,0,0)$	$(3,1,1,0)$	$(3,1,0,0)$	$(3,0^-,1,0)$
	$(3,0^+,1,0)$	$(3,0,0,0)$	$(2,2,1,0)$	$(2,2,0,0)$	$(2,1,1,0)$
	$(2,1,0,0)^*$	$(2,0^-,1,0)^*$	$(2,0^+,1,0)^*$	$(2,0,0,0)^*$	$(1^-,2,1,0)$
	$(1^-,2,0,0)^*$	$(1^-,0^-,1,0)^*$	$(1^-,0^+,1,0)^*$	$(1^+,2,1,0)$	$(1^+,2,0,0)^*$
	$(1^+,0^-,1,0)^*$	$(1^+,0^+,1,0)^*$	$(1,1,1,0)$	$(1,1,0,0)^*$	$(1,0,0,0)^*$
	$(0^-,0^+,1,0)^*$	$(0^+,0^+,1,0)^*$	$(0,0,0,0)^*$		

TABLE 1. The parameter vectors of S-rings in $\mathcal{S}^*(m)$, $m = 2, 3, 4$.

The decomposability of an S-ring in $\mathcal{S}^*(m)$ can easily be checked in terms of its parameter vector as stated in the following proposition.

Proposition 3.3. *If $\vec{u} = (u_i^{\varepsilon_i})$ is the parameter vector of an S-ring $\mathfrak{S} \in \mathcal{S}^*(m)$, then $\mathfrak{S}$ is decomposable if and only if there exits some $r \in \{1, \dots, m-1\}$, such that $u_i \geq r$ for all $i = 0, \dots, m-1-r$.*

Proof. Recall that $u_i = f_i(\mathfrak{S})$, see (4). By the definition of f_i (cf. Section 2), the value u_i can also be regarded as the maximal number k that every basic set in L_i is the union of H_k-cosets. Our claim is an immediate consequence of this interpretation. $\mathfrak{S}$ is decomposable by definition if there exists some $r \in \{1, \dots, m-1\}$ such that every basic set is either contained in H_r or is the union of H_r-cosets (cf. Section 1). For our $\mathfrak{S} \in \mathcal{S}^*(m)$, this is equivalent to saying that every basic set in L_i, $i = 0, \dots, m-1-r$, is the union of some H_r-cosets for some $r \in \{1, \dots, m-1\}$. This is equivalent to saying that $u_i \geq r$ for all $i = 0, \dots, m-1-r$. $\square$

Using Proposition 3.3, it is easy to check that the indecomposable parameter vectors in Table 1 are exactly those that are marked with the sign *.

At the end of this section, we establish a formal description of indecomposable parameter vectors (Theorem 3.8). To prepare for this description, we give next further properties of the parameter vectors. Let $\mathfrak{S} \in \mathcal{S}^*(m)$, and let $\mathfrak{S}$ have basic groups

$$K_0 = G_{3a_0+b_0}, \dots, K_{m-2} = G_{3a_{m-2}+b_{m-2}}, K_{m-1} = G_1.$$

Let $\vec{u} = (u_i^{\varepsilon_i})$ denote the parameter vector of $\mathfrak{S}$. For the next three propositions assume that $i \in \{1, \dots, m-1\}$.

Proposition 3.4. *If $\varepsilon_{i-1} \neq 0$ and $\varepsilon_i = 0$, then $u_{i-1} = u_i - 1 = m-2-i$. Otherwise, $u_{i-1} \geq u_i$.*

Proof. Because of (5), the conditions $\varepsilon_{i-1} \neq 0$ and $\varepsilon_i = 0$ are equivalent with

$$\Big(b_{i-1} = 0 \vee (b_{i-1} = 1 \wedge a_{i-1} > 0)\Big) \wedge \Big(3a_i + b_i = 1 \vee b_i = 2\Big). \tag{6}$$

Theorem 2.1(iv) shows that (6) holds exactly when $3a_i + b_i = 1$ and $3a_{i-1} + b_{i-1} \in \{3, 4\}$. By (4), these equalities imply $u_{i-1} = m-2-1-(i-1) = m-2-i$ and $u_i = m-1-i$.

Assume that (6) does not hold. By Theorem 2.1(iv) we know that $a_{i-1} \leq a_i + 1$. If $3a_i + b_i \neq 1$, then, according to (4), we have $u_i = m-2-a_i-i$. Therefore,

$$u_i \leq m-2-(a_{i-1}-1)-i = m-2-a_{i-1}-(i-1) \leq u_{i-1}.$$

Let $3a_i + b_i = 1$. Since (6) does not hold, we have $3a_{i-1} + b_{i-1} \in \{1, 2\}$. This implies $u_i = m-1-i$ and $u_{i-1} \in \{m-i, m-1-i\}$, hence $u_{i-1} \geq u_i$ as required. The proof is completed. $\square$

Corollary 3.5. *If $\mathfrak{S}$ is indecomposable, then $u_i = m-1-i$ if and only if $i = m-1$ or $(i \geq 1 \wedge \varepsilon_{i-1} \neq 0 \wedge \varepsilon_i = 0)$.*

Proof. If $i = m-1$, then $K_{m-1} = G_1$, see Theorem 2.1(iii). This gives $u_{m-1} = m-1-(m-1) = 0$. If $i \geq 1$ and $\varepsilon_{i-1} \neq 0$ and $\varepsilon_i = 0$, then $u_i = m-1-i$ by Proposition 3.4.

Conversely, assume that $u_i = m-1-i$ holds and $i \in \{0, \dots, m-2\}$. Then $3a_i + b_i = 1$, see (4). If $i = 0$, then L_0 is a basic set, hence $\mathfrak{S}$ is decomposable, a contradiction. Thus $i \geq 1$ and we can consider u_{i-1}. According to Proposition 3.4, we have $u_{i-1} \geq u_i$ or $u_{i-1} = u_i - 1$.

Assume that $u_{i-1} \geq u_i$. We show next

$$u_j \geq m-1-i, \text{ for all } j = 0, \dots, i. \tag{7}$$

We use induction on j. The relation in (7) is clear for $j \in \{i, i-1\}$. Assume that $i > 1$ and that (7) holds for $j \in \{1, \dots, i-1\}$. By Proposition 3.4, either $u_{j-1} \geq u_j$ or $u_{j-1} = m-2-j$. Note that in both cases $u_{j-1} \geq m-1-i$, as required.

By choosing $r = m-i-1$ in Proposition 3.3, one obtains via (7) that $\mathfrak{S}$ is decomposable, a contradiction. Therefore, we have $u_{i-1} = u_i - 1$. By Proposition 3.4, this implies that $\varepsilon_{i-1} \neq 0$ and $\varepsilon_i = 0$, and this completes the proof. □

Proposition 3.6. *If $\varepsilon_{i-1} = 0$ and $\varepsilon_i \neq 0$, then $u_{i-1} \in \{m-i, m-1-i\}$.*

Proof. Because of (5), the conditions $\varepsilon_{i-1} = 0$ and $\varepsilon_i \neq 0$ are equivalent with

$$\Big(3a_{i-1} + b_{i-1} = 1 \,\vee\, b_{i-1} = 2\Big) \wedge \Big(b_i = 0 \,\vee\, (b_i = 1 \,\wedge\, a_i > 0)\Big).$$

Theorem 2.1(iv) shows that the only possibility that this may occur is that $3a_{i-1} + b_{i-1} = 1$ or $3a_{i-1} + b_{i-1} = 2$. By (4), we have $u_{i-1} = m-1-(i-1)$ or $u_{i-1} = m-2-(i-1)$, i.e., $u_{i-1} \in \{m-i, m-1-i\}$. □

Proposition 3.7. *If $\varepsilon_{i-1} \neq 0$, $\varepsilon_i \neq 0$ and $u_{i-1} = u_i$, then $\varepsilon_i = +$.*

Proof. By (4) and (5), the conditions $\varepsilon_{i-1} \neq 0$, $\varepsilon_i \neq 0$ and $u_{i-1} = u_i$ give

$$u_{i-1} = m-2-a_{i-1}-(i-1) = m-2-a_i-i = u_i.$$

Thus $a_{i-1} = a_i + 1$. Theorem 2.1(iv) shows that this may occur only when $b_i = 1$, which, by (5), gives $\varepsilon_i = +$. □

In fact, the above properties completely describe the indecomposable parameter vectors among the elements of M^m.

Theorem 3.8. *The parameter vector $\vec{u} = (u_i^{\varepsilon_i}) \in M^m$ $(m \geq 2)$ is indecomposable if and only if it satisfies the properties:*

(i) *for all $i \in \{0, \dots, m-1\}$, $u_i \leq \begin{cases} m-3-i, & \text{if } \varepsilon_i \neq 0, \\ m-1-i, & \text{if } \varepsilon_i = 0, \end{cases}$*
(ii) *$u_i = m-1-i$ if and only if $i = m-1$ or $i \geq 1$ and $\varepsilon_{i-1} \neq 0$ and $\varepsilon_i = 0$,*
(iii) *if $\varepsilon_{i-1} \neq 0$ and $\varepsilon_i = 0$, then $u_{i-1} = u_i - 1$; otherwise, $u_{i-1} \geq u_i$,*
(iv) *if $\varepsilon_{i-1} = 0$ and $\varepsilon_i \neq 0$, then $u_{i-1} \in \{m-i, m-1-i\}$,*
(v) *if $\varepsilon_{i-1} \neq 0$, $\varepsilon_i \neq 0$ and $u_{i-1} = u_i$, then $\varepsilon_i = +$.*

Proof. If $\vec{u}$ is an indecomposable parameter vector, then the properties (i)-(v) are just a reformulation of Proposition 3.2, Propositions 3.4, 3.6, 3.7, and Corollary 3.5.

Conversely, assume that $\vec{u} = (u_i^{\varepsilon_i}) \in M^m$ satisfies (i)-(v). We are going to prove by induction on m that $\vec{u}$ is an indecomposable parameter vector, i.e., that it is the parameter vector of a nontrivial, indecomposable S-ring over Z_{2^m}. If $m = 2$, then it can be directly checked that $(0,0)$ is the only element of $M \times M$ satisfying all properties (i)-(v).

Assume that $m \geq 3$. For a given $u_i^{\varepsilon_i}$, $i \in \{0,\dots,m-1\}$, substitute u_i into the equation (4). This will determine a unique number a_i. Then consider the equation in (5) which corresponds to our given ε_i. It will hold for a unique $b_i \in \{0,1,2\}$ as a_i is already fixed. Then put $K_i = G_{3a_i+b_i}$.

In fact, it suffices to show that the groups $K_0,\dots,K_{m-1}$ are the basic groups of an indecomposable S-ring $\mathfrak{S} \in \mathfrak{S}^*(m)$, for then $\vec{u}$ is clearly the parameter vector of $\mathfrak{S}$. We prove first that they are the basic groups of an S-ring in $\mathfrak{S}^*(m)$ by showing that $K_0,\dots,K_{m-1}$ satisfy Theorem 2.1(iii)-(iv). We distinguish two cases.

Case 1: $u_1 < m-2$.

We set $\vec{u}' = (u_1^{\varepsilon_1},\dots,u_{m-1}^{\varepsilon_{m-1}}) \in M^{m-1}$. It can be checked that in this case $\vec{u}'$ satisfies all properties (i)-(v). Therefore, the induction hypothesis yields that $\vec{u}'$ is the parameter vector of an indecomposable S-ring $\mathfrak{S}'$ over $\mathbb{Z}_{2^{m-1}}$. It follows from this that the groups $K_1,\dots,K_{m-1}$ satisfy the conditions Theorem 2.1(iii)-(iv). Therefore, we only have to check K_0.

Assume that $\varepsilon_1 = 0$. Since $u_1 < m-2$, it follows that $K_1 = G_{3a_1+2}$. If $\varepsilon_0 \neq 0$, then, by (ii), we have $u_1 = m-2$, a contradiction. Also, $\varepsilon_0 = 0$. If $K_0 \neq G_1$, then $b_0 = 2$, and, by (2) and (i),

$$0 \leq a_0 = m-2-u_0 \leq m-3-(u_1)+1 = a_1+1.$$

Therefore, we obtain

$$K_0 \in \{G_1\} \cup \{G_{3i+2} \mid 0 \leq i \leq a_1+1\},$$

as stated in Theorem 2.1(iv).

Assume next that $\varepsilon_1 \neq 0$. This is the same as $K_1 = 3a_1+1$ or $K_1 = 3a_1$ for $a_1 > 0$. If now $\varepsilon_0 = 0$, then, by (iv), we have $u_0 \in \{m-1, m-2\}$. By (2), this implies that $K_0 \in \{G_1, G_2\}$. If $\varepsilon_0 \neq 0$, then $K_1 = 3a_0+1$ or $K_1 = 3a_0$ for $a_0 > 0$. By (2) and (i), we have $0 \leq a_0 \leq a_1+1$, and $a_0 = a_1+1$ is the same as $u_0 = u_1$. In this case, by (iii) it follows that $\varepsilon_1 = +$. Furthermore, we have $b_1 = 1$. Altogether we obtain that in case $K_1 = G_{3a_1+1}$ or $K_1 = G_{3a_1+3}$,

$$K_0 \in \{G_2\} \cup \{G_{3i+1} \mid 0 \leq i \leq a_1+1\} \cup \{G_{3i+3} \mid 0 \leq i \leq a_1\}.$$

Thus, K_0 satisfies Theorem 2.1(iv).

Case 2: $u_1 = m-2$.

Then, according to (4) and (5), we have $K_1 = G_1$ and $\varepsilon_1 = 0$. We set $\vec{u}' = (u_2^{\varepsilon_1},\dots,u_{m-1}^{\varepsilon_{m-1}}) \in M^{m-2}$. In this case, $u_2 < m-3$, since otherwise $\varepsilon_1 \neq 0$ would follow because of (iii). It follows from this that the groups $K_2,\dots,K_{m-1}$ satisfy the conditions Theorem 2.1(iii)-(iv). Therefore, we only have to check K_1 and K_0.

Since $K_1 = G_1$, it satisfies Theorem 2.1(iii)-(iv) independently of K_2. According to (ii), we have $\varepsilon_0 \neq 0$ and $\varepsilon_1 = 0$. Thus, $u_0 = m-3$ because of (i), hence, from (4), we get that $K_0 \in \{G_3, G_4\}$. This shows that K_0 satisfies Theorem 2.1(iv), as required.

We proved that $\vec{u}$ is the parameter vector of an S-ring $\mathfrak{S} \in \mathfrak{S}^*(m)$. It remains to show that $\mathfrak{S}$ is indecomposable. By way of contradiction, assume that $\mathfrak{S}$ is decomposable. Because of Proposition 3.3, there is some $r \in \{1, \ldots, m-1\}$ such that

$$u_i \geq r \text{ for all } i = 0, \ldots, m-1-r. \tag{8}$$

In particular, $u_{m-1-r} \geq r = m-1-(m-1-r)$. Because of (i) and (ii), we have $u_{m-1-r} = r$, $m-1-r > 0$, $\varepsilon_{m-1-r} = 0$, and $\varepsilon_{u_{m-2-r}} \neq 0$. Now (iii) implies $u_{m-2-r} = u_{m-1-r} - 1 = r-1$, which contradicts (8). The proof of the theorem is now completed. □

4. Lattice paths

In this section, we consider lattice paths (for short *paths*) in the integer plane lattice, which consist of steps $\rightarrow = (1,0)$, $\uparrow = (0,1)$ and $\nearrow = (1,1)$. A path π is uniquely determined by its starting point and the sequence of its steps. We express this as $\pi = (s_1, \ldots, s_k)$, $s_i \in \{\rightarrow, \uparrow, \nearrow\}$. The path induced by $\pi' = (s_i, s_{i+1}, \ldots, s_j)$, $1 \leq i \leq j \leq k$, will be called a *subpath* of π.

In this section we are going to associate a path with any indecomposable parameter vector. Let $\vec{u} = (u_0^{\varepsilon_0}, \ldots, u_{m-1}^{\varepsilon_{m-1}})$ be an indecomposable parameter vector. The associated path will have starting point $(0,0)$, and its steps will be constructed recursively in $m-1$ steps. In each step, a subpath will be determined, which will be denoted by π_i, whose end point will be denoted by (x_i, y_i). As initial value, let π_0 be the empty path with starting point $(0,0)$, so that $(x_0, y_0) = (0,0)$.

Assume that π_i is already defined, connecting $(0,0)$ with (x_i, y_i), $0 \leq i < m-2$. Then define π_{i+1} as the concatenation of π_i with π', where π' has starting point (x_i, y_i), and where its steps are determined by the following rules:

If $\varepsilon_i = 0$ then

$$\pi' := \begin{cases} (\rightarrow, \uparrow), & \text{if } i \geq 1,\ \varepsilon_{i-1} \neq 0, \\ (\underbrace{\rightarrow, \ldots, \rightarrow}_{r}, \uparrow) & \text{if } i = 0 \text{ or } (i \geq 1,\ \varepsilon_{i-1} = 0), \end{cases} \tag{9}$$

where $r = \max(m-1-x_i-u_i, 0)$.

If $\varepsilon_i \neq 0$ then

$$\pi' := \begin{cases} (\overbrace{\uparrow, \ldots, \uparrow, \uparrow}^{s}, \rightarrow) & \text{if } \varepsilon_i = +, \\ (\underbrace{\uparrow, \ldots, \uparrow}_{s-1}, \nearrow) & \text{if } \varepsilon_i = -, \end{cases} \tag{10}$$

where $s = \max(m-2-y_i-u_i, 0)$.

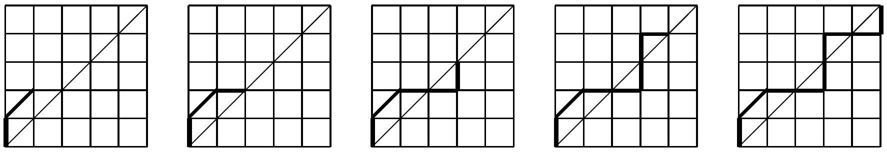
It is easy to see that for the end point of π_{i+1} we have

$$(x_{i+1}, y_{i+1}) = \begin{cases} (x_i+1, y_i+1), & \text{if } i \geq 1,\ \varepsilon_i = 0,\ \varepsilon_{i-1} \neq 0, \\ (x_i+r, y_i+1), & \text{if } \varepsilon_i = 0,\ (i = 0 \text{ or } i \geq 1,\ \varepsilon_{i-1} = 0), \\ (x_i+1, y_i+s), & \text{if } \varepsilon_i \neq 0. \end{cases}$$

Given this construction, we associate $\vec{u}$ with the path π_{m-1}. We set the notation $\pi(\vec{u}) = \pi_{m-1}$.

Example 4.1. $\pi(\vec{u})$, $\vec{u} = (2^-, 2^+, 3, 0^+, 1, 0)$.

By definition π_0 is the empty path, $(x_0, y_0) = (0, 0)$. As for π_1, since $u_0^{\varepsilon_0} = 2^-$, apply (10) with $s = 2$ to find $\pi_1 = \pi' = (\uparrow, \nearrow)$, $(x_1, y_1) = (1, 2)$. π_2 is the concatenation of π_1 with π', where π' starts at $(1, 2)$ and, according to (10), $\pi' = (\rightarrow)$. Continuing in this way, we obtain:



π_1 π_2 π_3 π_4 $\pi(\vec{u}) = \pi_5$

Next, we provide more paths associated with indecomposable parameter vectors. For sake of simplicity, we put $\pi(\vec{u}) = \pi(u_0^{\varepsilon_0}, \dots, u_m^{\varepsilon_m})$ if $\vec{u} = (u_0^{\varepsilon_0}, \dots, u_m^{\varepsilon_m})$.

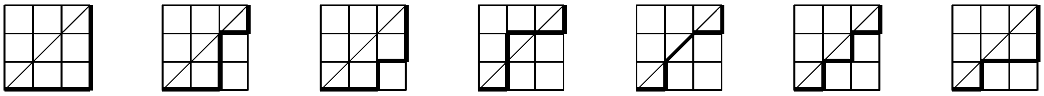
Example 4.2. *The paths associated with indecomposable parameter vectors of length m, $2 \leq m \leq 4$.*

<u>$m = 2$:</u> There is only one path: $\pi(0, 0) = (\rightarrow, \uparrow)$.

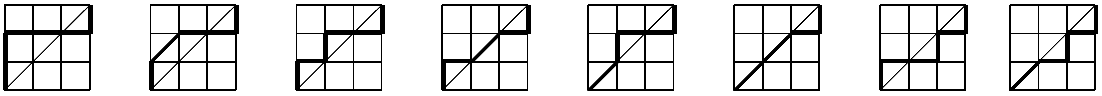
<u>$m = 3$:</u>

$\pi(0,0,0)$ $\pi(1,0,0)$ $\pi(0^+,1,0)$ $\pi(0^-,1,0)$

<u>$m = 4$:</u>



$\pi(0,0,0,0)$ $\pi(1,1,0,0)$ $\pi(1,0,0,0)$ $\pi(1,0^+,1,0)$ $\pi(1,0^-,1,0)$ $\pi(2,1,0,0)$ $\pi(2,0,0,0)$



$\pi(0^+,0^+,1,0)$ $\pi(0^-,0^+,1,0)$ $\pi(1^+,0^+,1,0)$ $\pi(1^+,0^-,1,0)$ $\pi(1^-,0^+,1,0)$ $\pi(1^-,0^-,1,0)$ $\pi(1^+,2,0,0)$ $\pi(1^-,2,0,0)$

It will turn out that the class of paths which can be obtained from indecomposable parameter vectors can be nicely described by using classical paths such as *Catalan* and *Schröder paths*.

Catalan paths are defined as paths connecting two points lying on the line $y = x$ such that they consist of steps $\rightarrow$ and $\uparrow$, and reach no point above the line $y = x$. The total number of Catalan paths from $(0, 0)$ to (n, n) is the n-th Catalan number c_n, [12, Exercise 6.20/c]. Schröder paths connect two points lying on the diagonal line, consist of steps $\rightarrow$, $\uparrow$ and $\nearrow$, and reach no point below the line $y = x$. The total number of Schröder paths from $(0, 0)$ to (n, n) is equal to n-th Schröder number s_n, [12, Exercise 6.39/j]. For our purpose we will need a slight modification of the Schröder paths. Namely, we call a path a *long Schröder path* if it is the extension of a Schröder path with two additional steps $\rightarrow$ and $\uparrow$.

By examining the paths in the examples, one might observe that they can be described as concatenation of Catalan and long Schröder paths. We are going to show that this is true in general.

Theorem 4.3. *If $m \geq 2$, then the mapping $\vec{u} \mapsto \pi(\vec{u})$ is a bijection from the set of all indecomposable parameter vectors of length m to the class of paths described by*

$$\text{concatenations of Catalan and long Schröder paths from } (0,0) \text{ to } (m-1, m-1). \tag{11}$$

The proof of Theorem 4.3 will be based on induction on m. This requires a few preparatory propositions. As these are straightforward consequences of the definitions, we leave the proofs to the reader.

Let $\vec{u} = (u_i^{\varepsilon_i}) \in M^m$ be an indecomposable parameter vector, and let $m \geq 3$. We introduce the vector $\vec{u}\,' = (w_0^{\xi_0}, \ldots, w_{m-2}^{\xi_{m-2}})$ by

$$w_0^{\xi_0} = \begin{cases} u_1^{\varepsilon_1}, & \text{if } u_1 < m-2, \\ m-3, & \text{otherwise,} \end{cases}$$

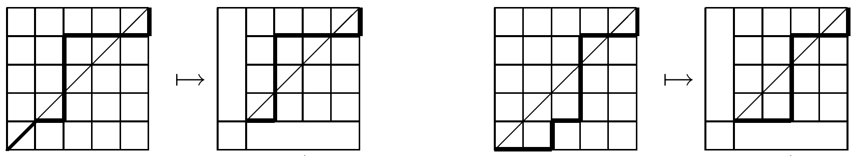
and for $i \in \{1, \ldots, m-2\}$ let $w_i^{\xi_i} = u_{i+1}^{\varepsilon_{i+1}}$. The vector $\vec{u}\,'$ will be called the *derivation* of $\vec{u}$.

Proposition 4.4. *If $\vec{u}$ is an indecomposable parameter vector of length $m \geq 3$, then so is its derivation $\vec{u}\,'$.*

Let $\pi = (s_1, \ldots, s_k)$ be a path starting at $(0,0)$. For the numbers $1 \leq i_1 < \cdots < i_t \leq k$, we denote by $\pi^{-i_1,\ldots,i_t}$ the path starting at $(0,0)$, and whose steps are obtained from those of π by deleting the steps $s_{i_1}, \ldots, s_{i_t}$. For a path $\pi = (s_1, \ldots, s_k)$ connecting $(0,0)$ with (m,m), we define its *derivation* as the path π' connecting $(0,0)$ with $(m-1, m-1)$ such that:

$$\pi' = \begin{cases} \pi^{-1}, & \text{if } s_1 = \nearrow, \\ \pi^{-1,l+1}, & \text{if } s_1 = \cdots = s_l = \rightarrow (\uparrow),\ s_{l+1} = \uparrow (\rightarrow), \\ \pi^{-(l+1)}, & \text{if } s_1 = \cdots s_l = \uparrow,\ s_{l+1} = \nearrow. \end{cases} \tag{12}$$

Example 4.5. *The derivation of $\pi = \pi(3^-, 4, 0^+, 0^+, 1, 0)$ and $\rho = \pi(3, 2, 2, 0^+, 1, 0)$. (The derivations are shown after translating them by the vector $(1,1)$.)*



π $\quad\pi'\quad$ ρ $\quad\rho'$

The vectors $(3^-, 4, 0^+, 0^+, 1, 0)$ and $(3, 2, 2, 0^+, 1, 0)$ are indecomposable parameter vectors, see Theorem 3.8. It can be seen that the derivation paths are also concatenations of Catalan and long Schröder paths. Moreover, $\pi' = \pi(3, 0^+, 0^+, 1, 0)$, $\rho' = \pi(2, 2, 0^+, 1, 0)$, and $(3, 0^+, 0^+, 1, 0)$ and $(2, 2, 0^+, 1, 0)$ are the derivations of $(3^-, 4, 0^+, 0^+, 1, 0)$ and $(3, 2, 2, 0^+, 1, 0)$, respectively. In general, we have the following relation between the derivation of vectors and paths.

Proposition 4.6.

(i) *If π is a path as described in (11) with $m \geq 3$, then π' is also a concatenation of Catalan and long Schröder paths, connecting $(0,0)$ with $(m-2, m-2)$.*

(ii) *If $\vec{u}$ is an indecomposable parameter vector of length m, $m \geq 3$, then $(\pi(\vec{u}))\,' = \pi(\vec{u}\,')$.*

Now everything is prepared to prove Theorem 4.3.

The proof of Theorem 4.3. We proceed by induction on m. The assertion is true for $m = 2$, see Table 1 and Example 4.2.

Assume that $m \geq 3$. It follows from (9) and (10) that $\vec{u} \mapsto \pi(\vec{u})$ is an injection. We show next that if $\vec{u}$ is an indecomposable parameter vector of length m, then $\pi(\vec{u})$ is a path as described in (11). Let $\pi = \pi(\vec{u})$. We have $\pi' = \pi(\vec{u}')$, see Proposition 4.6(ii). Since $\vec{u}'$ is an indecomposable parameter vector, see Proposition 4.4, π' is a concatenation of Catalan and long Schröder paths connecting $(0,0)$ with $(m-2, m-2)$. Now one can use (9), (10), and (12) to conclude that π must be a path as described in (11).

The proof will be completed by showing that if ρ is a path which connects $(0,0)$ with $(m-1, m-1)$ such that it is a concatenation of Catalan and long Schröder paths, then $\rho = \pi(\vec{u})$ for some indecomposable parameter vector $\vec{u}$ of length m. Let $\rho = (s_1, \ldots, s_k)$. Use Proposition 4.6(i) and the induction hypothesis to deduce $\rho' = \pi(\vec{v})$ for some indecomposable vector $\vec{v}$ of length $m-1$. Furthermore, let $\vec{v} = (v_0^{\xi_0}, \ldots, v_{m-2}^{\xi_{m-2}})$.

We distinguish two cases depending on whether ρ starts with a Catalan or with a long Schröder subpath. We consider only the first case as the second one can be settled along the same line of reasoning.

Let the starting Catalan subpath of ρ have first steps $s_1 = \cdots = s_l = \rightarrow$, $s_{l+1} = \uparrow$, $1 \leq l \leq m-2$. Now define $\vec{u} = (u_i^{\varepsilon_i})$ by

$$u_i^{\varepsilon_i} = \begin{cases} (m-1-l)^0, & \text{if } i = 0, \\ v_{i-1}^{\xi_{i-1}}, & \text{if } 1 < i \leq m-1. \end{cases}$$

We are going to complete the proof by showing that $\vec{u}$ is an indecomposable parameter vector of length m, and $\rho = \pi(\vec{u})$. Now, $\vec{u}$ being an indecomposable parameter vector is equivalent to the conditions

$$\begin{aligned} u_0 &\leq m-2, \\ \varepsilon_1 \neq 0 &\Rightarrow u_0 = m-2, \\ u_0 &\geq u_1, \end{aligned}$$

see Theorem 3.8. It immediately follows that $u_0 \leq m-2$. Let $\varepsilon_1 \neq 0$. We have $\xi_0 \neq 0$. Moreover, ρ' starts with a long Schröder path, see (10). As ρ starts with a Catalan subpath, this can only occur if $l = 1$, see (12). Hence $u_0 = m-2$. It remains to show that $u_0 \geq u_1$. We have $u_1 = v_0 \leq m-3$ since $\vec{v}$ is an indecomposable parameter vector of length $m-1$. Hence we may assume that $u_1 < m-2$, so that $l > 1$. Thus, by (12), the path ρ' starts with the Catalan subpath $(s_2, \ldots, s_l, s_{l+1}, \ldots)$. Now use (9) to obtain $l - 1 \leq m - 2 - v_0$. It follows that $u_1 = v_0 \leq m - 1 - l = u_0$.

It is clear that $\vec{u}' = \vec{v}$. Therefore, we have $(\pi(\vec{u}))' = \rho'$, see Proposition 4.6(ii). Moreover, for $\pi(\vec{u}) = \rho$ it is enough to show that the two paths share the same first $l+1$ steps. This is however clear since it follows that the first iteration of $\pi(\vec{u})$ is $(s_1, \ldots, s_{l+1})$, see (9). $\square$

5. The proof of Theorem 1.1

Recall that $I(m,p)$ denotes the number of indecomposable S-rings over Z_{p^m}. If $m \geq 2$, then the nontrivial, indecomposable S-rings over Z_{2^m} were parameterized by the indecomposable parameter vectors of length m in Section 3. In Section 4 these vectors were shown to be in a one-to-one correspondence with paths as described in (11). Since the trivial S-ring is always indecomposable, for $m \geq 2$ we have

$$I(m,2) = 1 + \#\{\text{paths as described in (11)}\}. \tag{13}$$

Our derivation of the expression for $I(m,2)$ given in Theorem 1.1 will be based on this interpretation. If $n \geq 1$, let p_n denote the number of paths from $(0,0)$ to (n,n) as described in (11), and for convenience put $p_0 = 1$. Thus, $I(m,2) = 1 + p_{m-1}$ if $m \geq 2$. We set $P(x) = \sum_{n\geq 0} p_n x^n$.

Recall that the total numbers of Catalan and Schröder paths, respectively, connecting $(0,0)$ with (n,n) are given by

$$c_n = \frac{1}{n+1}\binom{2n}{n} \text{ and } s_n = \sum_{k=0}^{n} \frac{1}{k+1}\binom{2k}{k}\binom{n+k}{2k}. \tag{14}$$

The corresponding generating functions are, see [12, page 178],

$$C(x) = \sum_{n\geq 0} c_n x^n = \frac{1-\sqrt{1-4x}}{2x}, \quad S(x) = \sum_{n\geq 0} s_n x^n = \frac{1-x-\sqrt{1-6x+x^2}}{2x}. \tag{15}$$

If $\tilde{s}_n$ denotes the number of long Schröder paths, $n \in \mathbb{N}$, then the corresponding generating function is $\tilde{S}(x) = (S(x)-1)x$, as is immediate to see.

The proof of Theorem 1.1. $I(1,2) = 1$ is clear, hence assume $m \geq 2$. As our paths are concatenations of Catalan and long Schröder paths, we have the following recursion:

$$p_n = \sum_{i=0}^{n} \tilde{s}_i p_{n-i} + \sum_{i=0}^{n-1} c_i p_{n-1-i}, \quad n \geq 1.$$

In terms of generating functions, $P(x) = P(x)\tilde{S}(x) + P(x)C(x)x + 1$. Substitute $\tilde{S}(x) = (S(x)-1)x$ and use (15) to deduce

$$P(x) = \frac{2}{3x + \sqrt{1-4x} + \sqrt{1-6x+x^2}}.$$

By getting rid of the square roots in the denominator and using (15) again, one can obtain

$$P(x) = \frac{1 + 4x + (4x-2)C(x) + (2x-1)S(x) + 3xC(x)S(x)}{4x^2 + 11x - 2}.$$

From this, for the numerator we have:

$$-2 + 9x + \sum_{n\geq 2}\Big(4c_{n-1} - 2c_n + 2s_{n-1} - s_n + 3\sum_{i=0}^{n-1} c_i s_{n-1-i} \Big)x^n.$$

Using partial fraction decomposition, the denominator can be expanded to

$$\frac{1}{4x^2+11x-2} = \sum_{n\geq 0} \frac{1}{3\sqrt{17}}\Big[\Big(\frac{11-3\sqrt{17}}{4}\Big)^{n+1} - \Big(\frac{11+3\sqrt{17}}{4}\Big)^{n+1}\Big]x^n.$$

Eventually, these facts are combined to derive the desired expression for p_{m-1}. The proof now is completed. □

Acknowledgements

The author thanks Mikhail Klin for helpful remarks and suggestions. A three-week visit of the author at the University of Delaware was useful in producing the final version of the paper. This visit was partially supported by the University of Delaware. The author also thanks Christian Krattenthaler for his remarks regarding paths and their enumeration.

References

[1] Ja. Ju. Gol'fand, N. L. Najmark, R. Pöschel. *The structure of S-rings over* Z_{2^m}. Akad. der Wiss. der DDR Inst. für Math., Preprint P-MATH-01/85 (1985), 1–30.
[2] M. Ch. Klin, N. L. Najmark, R. Pöschel. *Schur rings over* Z_{2^m}. Akad. der Wiss. der DDR Inst. für Math., Preprint P-MATH-14/81 (1981), 1–30.
[3] M. H. Klin and R. Pöschel. *The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings.* Algebraic methods in graph theory, Vol. I,II (Szeged 1978), Colloq. Math. Soc. János Bolyai **25** (1981), 405–434.
[4] M. Ch. Klin, R. Pöschel. *Circulant graphs via Schur ring theory. Automorphism groups of circulant graphs on* p^m *vertices, p an odd prime.* Manuscript.
[5] I. Kovács, M. Klin. *Automorphism groups of circulant graphs on* 2^m *vertices.* (In preparation.)
[6] I. Kovács. *On automorphisms of circulant digraphs on* p^m *vertices, p an odd prime.* Linear Alg. and its Appl. **356** (2002), 231–252.
[7] K. H. Leung, S. L. Ma. *The structure of Schur rings over cyclic groups.* J. Pure Appl. Algebra **66** (1990), 287–302.
[8] V. Liskovets, R. Pöschel. *Counting circulant graphs of prime-power order by decomposing into orbit enumeration problems.* Discr. Math. **214** (2000), 173–191.
[9] M. Muzychuk, M. Klin and R. Pöschel. *The isomorphism problem for circulant graphs via Schur ring theory.* DIMACS Series in Discrete Mathematics and Theoretical Computer Science. Vol. **56** (2001), 241–264.
[10] I. Schur. *Zur Theorie der einfach transitiven Permutationsgruppen.* Sitzungsber. Preuss. Akad. Wiss. Phys.-Math. Kl. (1933), 598–623.
[11] W. R. Scott. *Group Theory.* Prentice-Hall, 1964.
[12] R. P. Stanley. *Enumerative Combinatorics vol II.* Cambridge University Press, Cambridge, 1999.
[13] H. Wielandt. *Finite Permutation Groups.* Academic Press, Berlin, 1964.

István Kovács
University of Primorska, Department of Mathematics and Computer Science
Cankarjeva 5, Koper 6000, Slovenia
kovacs@pef.upr.si