GROUPS ACTING ON NECKLACES AND SANDPILE GROUPS

S. V. Duzhin[*] and D. V. Pasechnik[†]

UDC 515.16

We introduce a group naturally acting on aperiodic necklaces of length n with two colors using a one-to-one correspondence between such necklaces and irreducible polynomials of degree n over the field $\mathbb{F}_2$ of two elements. We notice that this group is isomorphic to the quotient group of nondegenerate circulant matrices of size n over that field modulo a natural cyclic subgroup. Our groups turn out to be isomorphic to the sandpile groups for a special sequence of directed graphs. Bibliography: 15 *titles.*

1. Introduction

This work originated in the research of the first author related to the Drinfeld associator [6]. It is well known (e.g., see [5]) that the logarithm of the classical associator Φ_{KZ} is an element of the completed free Lie algebra on two generators with coefficients in the algebra $\mathcal{Z}$ of multiple zeta values [8]. The free Lie algebra has a basis whose elements are labelled by aperiodic necklaces [12]. However, the explicit expansion of $\log \Phi_{KZ}$ over this basis shown in [6] displays a highly chaotic behavior. Therefore, a natural idea arises to introduce some structure in the set of necklaces. In this paper, we introduce a group acting on the set of aperiodic necklaces of fixed length in the hope that the orbits of this group may shed some light on the structure of the embarrassing expression given in [6].

In the spirit proclaimed by V. I. Arnold in [2], this paper does not contain any proofs, only constructions, problems, motivations, examples, and statements of results proven elsewhere. It may be considered as an informal introduction to the paper [4].

2. General setting

In the most general setting, the approach we follow here consists in the following.

Suppose we have two sets A and B and a family of bijections $\varphi_i : A \to B$. This data can be used to define two groups: G_A, acting on the set A, and G_B, acting on the set B. Indeed, let G_A be the group generated by all bijections $\varphi_{ij} = \varphi_i^{-1} \circ \varphi_j$ and G_B the group generated by all $\varphi'_{ij} = \varphi_i \circ \varphi_j^{-1}$.

The following lemma is immediate.

Lemma 1. *The groups G_A and G_B are isomorphic, an isomorphism being given by the assignment $g \mapsto \varphi_i \circ g \circ \varphi_i^{-1}$ for any fixed i. In particular, the actions of these groups on the sets A and B are equivalent, any bijection φ_i maps the orbits of the group G_A onto the orbits of the group G_B, and this map on the set of orbits does not depend on the choice of a particular index i.*

3. History

The story began when the first author obtained the results of Sec. 6 (and also Sec. 11 which is, however, irrelevant to the main topic of this paper). This was done experimentally, by computer. The second author found the sequence of orders of the groups RG_n^2 in Sloane's encyclopaedia [14] under A027362 and conjectured that the groups are isomorphic to the sandpile groups of generalized de Bruijn graphs. This conjecture was checked by computer up to order 16 by the present authors and then proved by S. H. Chan in his Bachelor's thesis [3].[1] Finally, this theorem was generalized and extended in the paper [4].

4. Groups acting on necklaces

A p-colored *necklace* of length n is a sequence of n objects of p different kinds (called beads) considered up to cyclic shifts. Necklaces may be periodic (admitting a nontrivial shift that does not change it) or aperiodic. If the colors are linearly ordered, then the lexicographically minimal of all cyclic shifts of an aperiodic necklace is

[*] St.Petersburg Department of Steklov Mathematical Institute, St.Petersburg, Russia, e-mail: `duzhin@pdmi.ras.ru`.

[†] Department of Computer Science, University of Oxford, Oxford, UK, e-mail: `dimpase@cs.ox.ac.uk`.

[1] Actually, the correct proof appeared only in the updated version of the thesis paper.

Published in *Zapiski Nauchnykh Seminarov POMI*, Vol. 421, 2014, pp. 81–93. Original article submitted December 19, 2013.

called a *Lyndon* word. We will always suppose that p is prime and use the elements of a prime finite field $\mathbb{F}_p$ as the colors of beads. We will refer to such necklaces and Lyndon words as *arithmetical.*

The main case, which is most interesting from the point of view of Sec. 1, is $p = 2$.

Example. There are exactly 6 aperiodic 2-colored necklaces of length 5, given by the Lyndon words 00001, 00011, 00111, 01111, 00101, 01011.

Denote the set of aperiodic necklaces with parameters n and p by N_n^p. There is a formula for the cardinality of this set in terms of the Möbius function:

$$|N_n^p| = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}.$$

It is remarkable that this number is equal to the number of irreducible polynomials over the field $\mathbb{F}_p$ of degree n, or, which is the same, to the number of orbits of maximal length n of the action of the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.[2] Denote the set of irreducible polynomials by I_n^p. There are two known explicit constructions of a one-to-one correspondence

$$\varphi : N_n^p \to I_n^p.$$

One of them (mentioned in Reutenauer [12] who ascribes it to E. Witt [15]) depends on the choice of a *normal* polynomial of degree n over $\mathbb{F}_p$. Another one belongs to Golomb [7] and depends on the choice of a *primitive* polynomial of degree n over $\mathbb{F}_p$. According to Sec. 2, either set of bijections generates a group of transformations on the set of aperiodic necklaces. We will call the first one the *Reutenauer* group and denote it by RG_n^p, and call the second one the *Golomb* group and denote it by GG_n^p.

5. The Galois group and irreducible polynomials

It is well known that the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n} : \mathbb{F}_p)$ is the cyclic group of order n generated by the Frobenius automorphism $\sigma(x) = x^p$. Each orbit of this group coincides with the set of roots of an irreducible polynomial over $\mathbb{F}_p$ of degree that divides n. The orbits of maximum length n correspond to irreducible polynomials of degree exactly n. The union of all such orbits is equal to the complement in $\mathbb{F}_{p^n}$ of all its proper subfields. A polynomial is called *normal* if the set of its roots constitutes a basis of the vector space $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$; it is called *primitive* if one (and hence any) of its roots is a generator of the multiplicative group $\mathbb{F}_{p^n}^*$.

Here is an example. Consider the extension $\mathbb{F}_{16} : \mathbb{F}_2$ of degree 4 as the quotient ring $\mathbb{F}_2[X]/(X^4 + X + 1)$. Denoting the class of X in this quotient by α, we can see that α is a generator of $\mathbb{F}_{16}$, and the following table lists the orbits of the Galois group $\mathrm{Gal}(\mathbb{F}_{16} : \mathbb{F}_2)$, the corresponding irreducible polynomials, and, for the polynomials of maximum degree, indicates their nature:

orbit	polynomial	normal?	primitive?
$\{0\}$	x		
$\{1\}$	$x+1$		
$\{\alpha^5, \alpha^{10}\}$	x^2+x+1		
$\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$	x^4+x+1	no	yes
$\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$	$x^4+x^3+x^2+x+1$	yes	no
$\{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$	x^4+x^3+1	yes	yes

6. Reutenauer's construction

By definition, a normal basis is an orbit of the Galois group that constitutes a basis of $\mathbb{F}_{p^n}$ as a vector space over $\mathbb{F}_p$. Given a normal basis $A = \{\alpha, \alpha^p, \alpha^{p^2}, \dots\}$ and a necklace $\nu_0, \nu_1, \dots, \nu_{n-1}$, we set up the sum $\nu_0\alpha + \nu_1\alpha^p + \cdots + \nu_{n-1}\alpha^{p^{n-1}}$. Cyclical shifts on the sequence $\nu_0, \nu_1, \dots$ lead to changes of the resulting element of the big field $\mathbb{F}_{p^n}$ within the same orbit of the Galois group, so that the minimal polynomial of that element remains the same.

We have therefore two finite sets of equal cardinality, N_n^p and I_n^p, equipped with a family of one-to-one maps $\varphi_A : N_n^p \to I_n^p$. It turns out that the group generated by this set according to the construction of Sec. 2 coincides in this case simply with the set of all maps $\varphi_A^{-1} \circ \varphi_B$ of the set of necklaces into itself. It forms an Abelian

[2] This is why we consider only the necklaces with a prime number of colors. Generalizing the theory for p^k instead of p is an interesting open problem.

group, earlier denoted by RG_n^p, whose order is equal to the number of normal bases (in the case $p = 2$ known as Sloane's sequence A027362 [14]).

Here is the table of automorphism groups of necklaces for $p = 2$ and $n \leq 15$ (M_n stands for the number of normal bases, that is, the order of the group, and the next column lists the lengths of the orbits of RG_n^2 on the corresponding set of necklaces). To explain the meaning of the last column, let us first notice that to every polynomial P over a finite field, one can assign an integer $d(P)$ equal to the dimension (over the ground field) of the subspace spanned by the roots of P. Now, consider the orbits in the set of irreducible polynomials corresponding to the orbits in the set of necklaces. It turns out that $d(P)$ is constant over each orbit. For example, the biggest ("main") orbit consists of normal polynomials for which $d(P)$ is equal to n, the degree of the extension. The last column contains the lists of dimensions corresponding to the orbits listed in the previous column (it was obtained using the computer algebra Sage [13]).

n	$\lvert N_n^2\rvert$	M_n	group	orbits	$d(P)$
2	1	1	$\mathbb{Z}_1$	1	$[2]$
3	2	1	$\mathbb{Z}_1$	$2 \cdot 1$	$[3, 2]$
4	3	2	$\mathbb{Z}_2$	$2 + 1$	$[4, 3]$
5	6	3	$\mathbb{Z}_3$	$2 \cdot 3$	$[5, 4]$
6	9	4	$\mathbb{Z}_2^2$	$4 + 2 \cdot 2 + 1$	$[6, 5, 4, 4]$
7	18	7	$\mathbb{Z}_7$	$2 \cdot 7 + 4 \cdot 1$	$[7, 6, 4, 4, 3, 3]$
8	30	16	$\mathbb{Z}_2^2 \oplus \mathbb{Z}_4$	$16 + 8 + 4 + 2$	$[8, 7, 6, 5]$
9	56	21	$\mathbb{Z}_{21}$	$2 \cdot 21 + 2 \cdot 7$	$[9, 8, 7, 6]$
10	99	48	$\mathbb{Z}_2^3 \oplus \mathbb{Z}_6$	$48 + 2 \cdot 24 + 3$	$[10, 9, 8, 6]$
11	186	93	$\mathbb{Z}_{93}$	$2 \cdot 93$	$[11, 10]$
12	335	128	$\mathbb{Z}_2^3 \oplus \mathbb{Z}_4^2$	$128 + 64 + 2 \cdot 32 + 3 \cdot 16$ $+2 \cdot 8 + 3 \cdot 4 + 2 + 1$	$[12, 11, 10, 10, 9, 9,$ $8, 8, 8, 7, 7, 6, 6, 5]$
13	630	315	$\mathbb{Z}_{315}$	$2 \cdot 315$	$[13, 12]$
14	1161	448	$\mathbb{Z}_2^5 \oplus \mathbb{Z}_{14}$	$448 + 2 \cdot 224 + 2 \cdot 56$ $+4 \cdot 28 + 2 \cdot 8 + 7$ $+4 \cdot 4 + 2 \cdot 1$	$[14, 13, 12, 11, 11, 10, 10,$ $9, 9, 8, 8, 8, 7, 7, 6, 6, 5, 5]$
15	2182	675	$\mathbb{Z}_3 \oplus \mathbb{Z}_{15}^2$	$2 \cdot 675 + 2 \cdot 225$ $+6 \cdot 45 + 6 \cdot 15$ $+6 \cdot 3 + 4 \cdot 1$	$[15, 14, 12, 13, 11, 11, 11,$ $10, 10, 10, 9, 9, 9, 8, 8, 8,$ $7, 7, 7, 6, 6, 6, 5, 5, 4, 4]$

7. Orbits of the Reutenauer group

It is very interesting to study the *orbits* of the group RG_n^p acting on the set of aperiodic necklaces N_n^p. So far, we only have some empirical results in the case $p = 2$.

For example,

- If $n = 4$, the orbits are $O_1 = \{0001, 0111\}$ and $O_2 = \{0011\}$. The action of the group $\mathrm{RG}_4^2 = \mathbb{Z}_2$ on each orbit is obvious.
- If $n = 5$, we have $O_1 = \{00001, 00111, 01011\}$ and $O_2 = \{00011, 01111, 00101\}$. The action of the group is cyclic on each orbit.
- If $n = 6$, then $O_1 = \{000001, 011111, 001011, 001101\}$, $O_2 = \{000011, 010111\}$, $O_3 = \{000101, 001111\}$, and $O_4 = \{000111\}$. Here, the automorphism group acts as $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ on O_1, as $\mathbb{Z}_2$ on O_2 and O_3, and trivially on the last orbit.

Returning to the ideas of Sec. 1, we tried to evaluate various symmetric functions of the coefficients in the Drinfeld associator over the orbits in these cases, but could not arrive to any sensible conjecture.

It is also worthwhile to notice that there is an interesting operator on the set of necklaces, which sometimes turns an aperiodic necklace into a periodic one, but in general it takes whole orbits in the above lists into whole orbits. We call it the *averaging* operator; by definition, it acts as follows: $\{\nu_i\} \mapsto \{\nu_i + \nu_{i+1}\}$. For the above examples, we have

- $n = 4$: $O_1 \longrightarrow O_2 \longrightarrow \varnothing$.
- $n = 5$: $O_1 \longrightarrow O_2 \longrightarrow O_2$.
- $n = 6$: $O_1 \longrightarrow O_2 \longrightarrow O_3 \longrightarrow O_3$, $O_4 \longrightarrow \varnothing$.

(Here, going to $\varnothing$ means that the necklace becomes periodic.)

We noticed that in all examples with $n \le 15$, there is a *main* orbit, that is, an orbit of maximal length equal to the order of the group RG_n^2 which acts on this orbit simply transitively. Iterated averaging operators applied to the main orbit give the majority of orbits; some of the smallest orbits may go to $\varnothing$.

Note that here we spoke about the orbits of arithmetical groups in the sense of Sec. 4. From the point of view of studying the Drinfeld associator, however, it makes little sense to distinguish between the symbols 0 and 1: it is more reasonable to extend our groups RG_n^2 by the operator that flips 0's and 1's in each necklace. The orbits of such extended groups consist of either one or two orbits of the initial groups; it should be interesting to have their explicit description and try to study, for example, the sums of coefficients in the logarithm of the associator over these extended orbits.

8. Sandpile groups

Let Γ be a finite directed multigraph: it is defined by a finite set of vertices V and, for each pair of vertices $v, w \in V$, a nonnegative integer $e(v,w)$, called the number of arrows from v to w. The total number of arrows going out of v is referred to as the *outdegree* of v and denoted by $\mathrm{outdeg}(v)$; likewise, the *indegree* of v is the number of arrows going into v, denoted by $\mathrm{indeg}(v)$. (Computing these quantities, we do not take loops, if any, into consideration.) We will assume that the graph Γ is *strongly connected*, that is, there is a directed path from any vertex v to any other vertex w. We will also suppose that our graph is *Eulerian*, that is, for every vertex $v \in V$ we have $\mathrm{indeg}(v) = \mathrm{outdeg}(v)$. Under these assumptions, with the given graph Γ one can associate a certain finite Abelian group $S(\Gamma)$, called the *sandpile group* of Γ (see [9,10]). The group $S(\Gamma)$ is defined uniquely up to isomorphism, and the simplest way to define it is through the *Laplacian matrix* of Γ.

Let $V = \{v_1, \ldots, v_n\}$. The Laplacian matrix $L = (l_{ij})$ of size $n \times n$ is defined by its entries as

$$l_{ii} = -\,\mathrm{indeg}(v_i), \quad l_{ij} = e(v_i, v_j) \text{ if } i \ne j.$$

Let $\Lambda \subset \mathbb{Z}^n$ be the lattice spanned by the rows of L. Evidently, Λ is a sublattice of $\mathbb{Z}_0^n = \{(a_1, \ldots, a_n) \mid a_1 + \cdots + a_n = 0\}$. Then we set

$$S(\Gamma) = \mathbb{Z}_0^n / \Lambda.$$

It is known that the group $S(\Gamma)$ can also be defined as follows. Delete any row and any column from the matrix L and call the resulting $(n-1) \times (n-1)$ matrix L'. Let Λ' be the sublattice of $\mathbb{Z}^{n-1}$ spanned by the rows of L'. Then $S(\Gamma) \cong \mathbb{Z}^{n-1}/L'$. On the practical side, to compute the sandpile group, it is enough to reduce the Laplacian matrix by integral elementary operations on rows and columns to its Smith normal form, which is a diagonal matrix with integers $(d_1, \ldots, d_{n-1}, 0)$ on the diagonal, such that $d_i | d_{i+1}$ for any i; then the group is $\bigoplus_{i=1}^{n-1} \mathbb{Z}_{d_i}$. In general, we call it the Smith group of an integer matrix. In the next section, we will define a series of Eulerian directed multigraphs Γ_n^p labelled by a prime number p and a natural number n and explain the main idea of the proof that, for $p = 2$, their sandpile groups are isomorphic to the automorphism groups of necklaces defined above.

9. Generalized de Bruijn graphs

Let Γ_n^p be the graph with vertex set $V = \mathbb{Z}_n$, the residues modulo n, and p directed edges from every vertex i to each of pi, $pi+1$, …, $pi+p-1$. The outdegree of each vertex is thus equal to p. It is an easy exercise to check that the indegree of every vertex is also p and that the graph is strongly connected. Therefore, the sandpile group $S(\Gamma_n^p)$ is defined.

We call these graphs *generalized de Bruijn graphs*, because the well-known de Bruijn graphs appear as a particular case $\Gamma_{2^k}^2$, see, e.g., [1].

The structure of the group $S(\Gamma_n^2)$ for an arbitrary n is completely determined by the following two lemmas (Lemma 2 and Lemma 3), the first of which treats the case of odd n and the second shows how to pass from any n to $2n$. Before stating the lemmas, let us explain how one could actually arrive at the first, more difficult, one. Until the end of this section, we fix $p = 2$ and omit the superscripts 2 from various notations.

Suppose that n is odd. Ideologically, the problem is quite simple: it suffices to find the Smith normal form of the integer matrix A_n explicitly defined by $A_n[0,0] = A_n[n-1,n-1] = -1$, $A_n[0,1] = A_n[n-1,n-2] = 1$, $A_n[i,i] = -2$ for $0 < i < n-1$, and $A_n[i,2i] = A_n[i,2i+1] = 1$ for $i \in \mathbb{Z}_n$, $i \ne 0$, $i \ne n-1$. The problem is purely technical, but rather difficult: to understand this, it is enough to look at the table of the first 15 values of the sequence $S(\Gamma_n)$, which coincides with the table of Sec. 6 and is quite nontrivial. The key difficulty is that, as a rule, there are three nonzero elements in each column and each row of this matrix, e.g.,

$$A_9 = \begin{pmatrix} -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}.$$

It would be much easier to treat a matrix where there are only two nonzero elements in each row and column. This goal is almost achieved through a trick invented by S. H. Chan in his Bachelor's paper [3].

Let us consider the operator given by the Laplacian matrix of Γ_n in the basis $e_0 - e_1, \ldots, e_{n-2} - e_{n-1}, e_{n-1}$, that is, consider the matrix $A'_n = C_n^{-1} \cdot A_n \cdot C_n$ where C_n is the two-diagonal matrix with 1 on the main diagonal and -1 on the upper adjacent diagonal. Multiplying a matrix by either C_n or C_n^{-1} is equivalent to elementary operations on its rows and columns, hence the Smith normal forms of the matrices A_n and A'_n are the same. For the previous example we will obtain

$$A'_9 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & -2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -2 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 \end{pmatrix}.$$

We see that the lower-right minor of codimension 1 has the required property, and its Smith normal form can be found by drawing horizontal and vertical lines between the nonzero entries in each row and column of the matrix and considering the cycles obtained:

$$\begin{array}{ccccccccccccccc}
-2 & \cdots & 1 & & 0 & & 0 & & 0 & & 0 & & 0 & & 0 \\
\vdots & & \vdots & & & & & & & & & & & & \\
0 & & -2 & \cdots & 0 & \cdots & 1 & & 0 & & 0 & & 0 & & 0 \\
\vdots & & & & & & \vdots & & & & & & & & \\
0 & & 0 & & -2 & \cdots & 0 & \cdots & 0 & \cdots & 1 & & 0 & & 0 \\
\vdots & & & & \vdots & & \vdots & & & & \vdots & & & & \\
0 & & 0 & & 0 & & -2 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \\
\vdots & & & & \vdots & & & & & & \vdots & & & & \vdots \\
1 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & -2 & & 0 & & 0 & & 0 \\
 & & & & \vdots & & & & \vdots & & \vdots & & & & \vdots \\
0 & & 0 & & 1 & \cdots & 0 & \cdots & 0 & \cdots & -2 & & 0 & & 0 \\
 & & & & & & & & \vdots & & & & & & \vdots \\
0 & & 0 & & 0 & & 0 & & 1 & \cdots & 0 & \cdots & -2 & & 0 \\
 & & & & & & & & & & & & \vdots & & \vdots \\
0 & & 0 & & 0 & & 0 & & 0 & & 0 & & 1 & \cdots & -2
\end{array}$$

In this example, we see two cycles of lengths 4 and 12, which are simply a visualization of the orbits of lengths 2 and 6 in the set $\mathbb{Z}_9 \setminus \{0\}$ under the doubling operator $x \mapsto 2x$ (in our case, the orbits are $\{1, 2, 4, 8, 7, 5\}$ and $\{3, 6\}$). It is readily verified that each orbit of length d adds a summand $\mathbb{Z}_{2^d-1}$ to the Smith group of such a matrix (where each row and each column contains one entry 1 and one entry -2), so for our example we obtain $\mathbb{Z}_{63}\oplus\mathbb{Z}_3$. Unfortunately, the presence of a nonzero first column spoils this clear picture, namely, it decreases the size of the group by a factor of n (more exactly, it leads to a subgroup of index n). For the example under study, any subgroup of index 9 is isomorphic to $\mathbb{Z}_{21}$. However, there are situations where such a group may have different subgroups of index n. S. H. Chan in a series of rather involved technical lemmas showed what exactly the resulting group $S(\Gamma_n)$ looks like. In most cases, one must simply divide by n the order of the first cyclic group, corresponding to the orbit of the number 1. This is so for all odd integers up to 19. For $n = 21$, however, the set $\mathbb{Z}_{21}\setminus\{0\}$ decomposes into five orbits $\{1,2,4,8,16,11\}$, $\{3,6,12\}$, $\{5,10,20,19,17,13\}$, $\{7,14\}$, and $\{9,18,15\}$ of lengths 6, 3, 6, 2, and 3, respectively, but the sandpile group is actually equal to $\mathbb{Z}_9^2\oplus\mathbb{Z}_7^3$, and not to $\mathbb{Z}_3^2\oplus\mathbb{Z}_9\oplus\mathbb{Z}_7^3$ as one might infer from the previous rule. To state the exact formula proven by S. H. Chan, we need some notations.

Let n be an odd number. For any element $v\in\mathbb{Z}_n\setminus 0$ let $l(v)$ be the length of its orbit under the doubling operator $x\mapsto 2x$. Let H_n be the set of minimal representatives of all orbits. Now, denote by $\mathbb{P}_n$ the set of all prime divisors of n. For each $q\in\mathbb{P}_n$ let q' stand for the maximal power of q that divides n, and let $q'' = n/q'$. Denote the set of all such residues q'' by V_n. Finally, for an Abelian group G and an integer k let kG be the subgroup of all elements of G of the form kx, $x\in G$.

Lemma 2. *If n is odd, then the group $S(\Gamma_n)$ has the following decomposition:*

$$S(\Gamma_n)\cong\bigoplus_{q\in\mathbb{P}_n} q' Z_{2^{l(q'')}-1}\oplus\bigoplus_{v\in H_n\setminus V_n} Z_{2^{l(v)}-1}.$$

Example. Take $n = 21$. Then $\mathbb{P}_n = \{3,7\}$, $q_1' = 3$, $q_1'' = 7$, $l(7) = 2$, $q_2' = 7$, $q_2'' = 3$, $l(3) = 3$, $H_{21} = \{1,3,5,7,9\}$, $V_{21} = \{3,7\}$, so the first direct summand in the above formula is trivial, and the second gives

$$S(\Gamma_{21}) = \mathbb{Z}_{63}\oplus\mathbb{Z}_{63}\oplus\mathbb{Z}_7.$$

The proof of the next lemma is much simpler: it follows from the fact that Γ_{2n} is the directed line graph of Γ_n (see [9]).

Lemma 3. *Suppose that $n = 2^k m$ where m is odd. Then*

$$S(\Gamma_n)\cong S(\Gamma_m)\oplus\mathbb{Z}_{2^k}^{m-1}\oplus\left[\bigoplus_{i=2}^{k}\mathbb{Z}_{2^{k+1-i}}^{2^{i-2}m}\right].$$

10. Circulant matrices

An $n\times n$ matrix $A = a_{i,j}$, $i,j\in\mathbb{Z}_n$, over a field $\mathbb{K}$ is called *circulant* if its rows are the cyclic shifts of the first row, i.e.,

$$A_{i+1,j+1} = A_{ij}\quad\text{for all}\quad i,j\in\mathbb{Z}_n,$$

where $i+1$ and $j+1$ are taken modulo n.

In particular, the permutation matrices associated with the powers of the cyclic permutation $(0,1,\dots,n-1)$ are circulant; they form a basis of the algebra $C_n(\mathbb{K})\cong\mathbb{K}[\mathbb{Z}_n]$ of all $n\times n$ circulant matrices over $\mathbb{K}$. We see that the algebra $C_n(\mathbb{K})$ has dimension n and is commutative.

For a circulant matrix to be nondegenerate it is necessary (but not sufficient) that its rows (and columns) are aperiodic. Denote the group of nondegenerate circulants by $C_n(\mathbb{K})^*$. By the observation made above, it is commutative. In the case $\mathbb{K} = \mathbb{F}_p$, by studying the natural action of this group on the field $\mathbb{F}_{p^n}$ considered as a vector space over $\mathbb{F}_p$, it is easy to deduce that the Reutenauer group RG_n^p is isomorphic to the quotient $C_n(\mathbb{F}_p)^*/\mathbb{Z}_n$, where $\mathbb{Z}_n$ is the group of permutation circulant matrices, those associated with the powers of $(0,1,\dots,n-1)$.

In the case $p = 2$, it was proved in [3] that the series of these quotient groups satisfies the same relations as those given in Lemmas 2 and 3. The proof of these facts is not so involved as the proof of Lemma 2 and relies basically on the primary decomposition theorem from linear algebra. The main theorem follows.

Theorem (S. W. Chan). *For any natural n we have*

$$\mathrm{RG}_n^2\cong S(\Gamma_n^2).$$

This theorem is quite remarkable, because it relates objects coming from entirely different areas of mathematics. It is noteworthy that nobody knows any explicit isomorphism between the two groups in question, although the elements of both can be encoded by some sequences of 0's and 1's.

In the paper [4], this result is generalized to any prime number p as follows: $\mathrm{RG}_n^p \cong S(\Gamma_n^p) \oplus \mathbb{Z}_{p-1}$. Moreover, that paper describes the structure of the sandpile groups for the generalized de Bruijn graphs Γ_n^p for arbitrary values of p, not only prime. Of course, in the general case there is no analog of the isomorphism theorem; however, if p is a power of a prime, both groups are defined and the relation between them should be studied.

11. Golomb's construction

We conclude the paper with some experimental data related to another set of one-to-one correspondences between the necklaces and irreducible polynomials mentioned above.

Let α be a generator of the multiplicative group of the field $\mathbb{F}_q$, $q = p^n$. S. Golomb [7] defined a bijection $\psi_\alpha : N_n^p \to I_n^p$ that depends only on the orbit of the element α under the Galois group action, that is, ψ_α is completely determined by the primitive polynomial with one of the roots α. To a necklace $\nu = (\nu_0, ..., \nu_{n-1})$ we assign the element

$$\alpha^{\nu_0 + p\nu_1 + \cdots + p^{n-1}\nu_{n-1}}$$

of $\mathbb{F}_q$ and then take its minimal polynomial, which we denote by $\psi_\alpha(\nu)$. It is not hard to prove (see [7]) that the map ψ_α is one-to-one for any α that is a root of a primitive polynomial, and that these maps are the same for all roots of one primitive polynomial, and are distinct for different primitive polynomials, so that they generate a group of automorphisms of necklaces whose order equals the number of primitive polynomials $\phi(2^n - 1)/n$, where ϕ is Euler's totient function. This group turns out to be Abelian, too.

Here is the table of these groups for $p = 2$ and $2 \le n \le 12$ given together with the sizes of the orbits into which they split the set of necklaces (M_n stands for the order of the group):

n	$\lvert N_n^2 \rvert$	M_n	group	orbits
2	1	1	$\mathbb{Z}_1$	1
3	2	2	$\mathbb{Z}_2$	2
4	3	2	$\mathbb{Z}_2$	$2+1$
5	6	6	$\mathbb{Z}_6$	6
6	9	6	$\mathbb{Z}_6$	$6+2+1$
7	18	18	$\mathbb{Z}_{18}$	18
8	30	16	$\mathbb{Z}_2 \oplus \mathbb{Z}_8$	$16+8+4+2$
9	56	48	$\mathbb{Z}_2 \oplus \mathbb{Z}_{24}$	$48+8$
10	99	60	$\mathbb{Z}_2 \oplus \mathbb{Z}_{30}$	$60+30+6+2+1$
11	186	176	$\mathbb{Z}_2 \oplus \mathbb{Z}_{88}$	$176+8+2$
12	335	144	$\mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{12}$	$144+48+36+2\cdot 24+2\cdot 12$ $+8+2\cdot 6+2\cdot 4+3\cdot 2+1$

Note that the sequence of orders of these groups is not monotonous. As yet, nobody knows any relations between these groups and other mathematical objects, which was the case for the Reutenauer groups.

Acknowledgments. We are grateful to M. Vsemirnov who draw our attention to the close relation between the Reutenauer groups and circulant matrices. The first author acknowledges the hospitality of the Nanyang Technological University, Singapore, and Max-Planck Institute for Mathematics, Germany, where this paper was accomplished.

This paper was supported by Singapore MOE Tier 2, Grant MOE2011-T2-1-090; the first author was also supported by the grant NSh-4850.2012.1.

REFERENCES

1. T. van Aardenne-Ehrenfest and N. G. de Bruijn, "Circuits and trees in oriented linear graphs," *Simon Stevin*, **28**, 203–217 (1951).
2. V. I. Arnold, "From Hilbert's superposition problem to dynamical dystems," transcript of a lecture given at the Fields Institute (1997); `http://www.pdmi.ras.ru/~arnsem/Arnold/arnlect1.ps.gz`.
3. S. H. Chan, Bachelor's Thesis, NTU, Singapore (2012).

4. S. H. Chan, H. D. L. Hollmann, and D. V. Pasechnik, "Critical groups of generalized de Bruijn and Kautz graphs and circulant matrices over finite fields," in: J. Nešetřil and M. Pellegrini (eds.), *Proceedings of EuroComb* 2013, The Seventh European Conference on Combinatorics, Graph Theory and Applications, Springer (2013); ISBN 978-88-7642-474-8.
5. S. Chmutov, S. Duzhin, and J. Mostovoy, *Introduction to Vassiliev Knot Invariants*, Cambridge Univ. Press, Cambridge (2012); draft version: `http://www.pdmi.ras.ru/~duzhin/papers/cdbook`.
6. S. Duzhin, "An explicit expansion of the Drinfeld associator up to degree 12," web publication `http://www.pdmi.ras.ru/~arnsem/dataprog`.
7. S. W. Golomb, "Irreducible polynomials, synchronization codes, primitive necklaces and the cyclotomic algebra," in: *Combinatorial Mathematics and Its Applications* (Proc. Conf. Univ. North Carolina), Univ. North Carolina Press, Chapel Hill (1969), pp. 358–370.
8. M. E. Hoffman, "The algebra of multiple harmonic series," *J. Algebra*, **194**, 477–495 (1997).
9. L. Levine, "Sandpile groups and spanning trees of directed line graphs," *J. Combin. Theory, Ser. A*, **118**, No. 2, 350–364 (2011).
10. L. Levine and J. Propp, "What is ... a sandpile?" *Notices Amer. Math. Soc.*, **57**, No. 8, 976–979 (2010).
11. R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, Cambridge (2008).
12. Ch. Reutenauer, *Free Lie Algebras*, The Clarendon Press, New York (1993).
13. "Computer algebra system Sage," `http://www.sagemath.org`.
14. N. J. A. Sloane, "Online encyclopaedia of integer sequences," `http://oeis.org/`.
15. E. Witt, "Treue Darstellung Liescher Ringe," *J. reine angew. Math.*, **177**, 152–160 (1937).