Sandpile groups of generalized de Bruijn and Kautz graphs and circulant matrices over finite fields

Swee Hong Chan[*]   Henk D.L. Hollmann[*]   Dmitrii V. Pasechnik[†]

August 22, 2018

Abstract

A maximal minor M of the Laplacian of an n-vertex Eulerian digraph Γ gives rise to a finite group $\mathbb{Z}^{n-1}/\mathbb{Z}^{n-1}M$ known as the *sandpile* (or *critical*) *group* $S(\Gamma)$ of Γ. We determine $S(\Gamma)$ of the *generalized de Bruijn graphs* $\Gamma = \mathrm{DB}(n, d)$ with vertices $0, \ldots, n-1$ and arcs $(i, di + k)$ for $0 \leq i \leq n-1$ and $0 \leq k \leq d-1$, and closely related *generalized Kautz graphs*, extending and completing earlier results for the classical de Bruijn and Kautz graphs.

Moreover, for a prime p and an n-cycle permutation matrix $X \in \mathrm{GL}_n(p)$ we show that $S(\mathrm{DB}(n, p))$ is isomorphic to the quotient by $\langle X \rangle$ of the centraliser of X in $\mathrm{PGL}_n(p)$. This offers an explanation for the coincidence of numerical data in sequences A027362 and A003473 of the OEIS, and allows one to speculate upon a possibility to construct normal bases in the finite field $\mathbb{F}_{p^n}$ from spanning trees in $\mathrm{DB}(n, p)$.

Dedicated to the memory of Ákos Seress.

---

[*]Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore, email: {sweehong, henk.hollmann}@ntu.edu.sg

[†]Department of Computer Science, University of Oxford, UK, email: dmitrii.pasechnik@cs.ox.ac.uk (corresponding author)

1 Introduction

The *critical group* $S(G)$ of a directed graph G is an abelian group obtained from the Laplacian matrix Δ of G. It carries the same information as the Smith Normal Form (SNF) of Δ. (For precise definitions of these and other terms, we refer to the next section.) The *sandpile group* $S(G, v)$ of a directed graph or *digraph* G at a vertex v is an abelian group obtained from the reduced Laplacian Δ_v of G; by the Matrix Tree Theorem [32], its order is equal to the number of directed trees rooted at v, see for example [19]. If the graph G is Eulerian, then the sandpile group does not depend on the vertex v and is equal to the critical group $S(G)$ of G [15]. Most of the literature on sandpile groups is concerned with *undirected* graphs, which can be considered as a special case, namely for directed graphs that are obtained by replacing each undirected edge in a graph by a pair of directed edges oriented in opposite directions.

   The critical group has been studied in other contexts under variuos other names, such as group of components (in arithmetic geometry), Jacobian group and Picard group (for algebraic curves), and Smith group (for matrices). For more details and background, see, for example, [21, 29, 1] for the undirected case and [15, 33] for the directed case.

   Critical groups have been determined for many families of (mostly undirected) graphs. For some examples, see [8, 16, 26, 27, 9, 10, 30, 22, 5], and the references in [1]. Here, we determine the critical group of the generalized de Bruijn graphs $\mathrm{DB}(n, d)$ and generalized Kautz graphs $\mathrm{Ktz}(n, d)$ (which are in fact both directed graphs), thereby extending and completing the results from [19] for the binary de Bruijn graphs $\mathrm{DB}(2^\ell, 2)$ and Kautz graphs $\mathrm{Ktz}((p-1)p^{\ell-1}, p)$ for primes p, and [4] for the classical de Bruijn graphs $\mathrm{DB}(d^\ell, d)$ and Kautz graphs $\mathrm{Ktz}((d-1)d^{\ell-1}, d)$. Unlike the classical case, the generalized versions are not necessarily iterated line graphs, so to obtain their critical groups, techniques different from these in [19] and [4] have to be applied.

   As set out in [14], our original motivation for studying the sandpile groups of generalized de Bruijn graphs was to explain their apparent relation to some other algebraic objects, such as the groups $C(n, p)$ of invertible $n \times n$-circulant matrices over $\mathbb{F}_p$ (mysterious numerical coincidences of the OEIS entries A027362 and A003473 were noted by the third author [24], while running extensive computer experiments using Sage [31, 25]), and *normal bases* (cf. e.g. [20]) of finite fields $\mathbb{F}_{p^n}$, in the case where $(n, p) = 1$. The latter were noted to be closely related to circulant matrices and to *necklaces* by Reutenauer [28, Sect. 7.6.2], see also [14] and the related numeric data collected in [2]. Here we show that the critical group of $\mathrm{DB}(n, p)$ is isomorphic to $C(n, p)/\langle Q_n \rangle \times \mathbb{F}_p^*$, where Q_n denotes the permutation matrix of the n-cycle. Although we were not able to construct an explicit bijection between the former and the latter, we could speculate that potentially one might be able to design a new deterministic way to construct normal bases of $\mathbb{F}_{p^n}$ from spanning trees in $\mathrm{DB}(n, p)$. For more details and background on this connection with aperiodic necklaces, we refer the interested reader to [14]. Most of the results for the case d prime were first derived in the undergraduate thesis [6] by the first author, supervised by the third author. Results in this text were announced in an extended abstract [7].

2 Preliminaries

In this section, we introduce the necessary terminology and background. First, in Section 2.1, we discuss the Smith Normal Form and the Smith group, and the critical group and sandpile group of a directed graph, as well as the relations between these notions. Then in Section 2.2, we define the generalized De Bruijn and Kautz graphs. The group of invertible circulants is defined in Section 2.3. Finally, in Section 2.4, we derive expressions for the sandpile group of generalized De Bruijn and Kautz graphs as embeddings in a group that we refer to as sand dune group.

2.1 Smith group, Critical Group, and Sandpile Group

Let M be an rank r integer $m \times n$ matrix. There exist positive integers $s_1, \ldots, s_r$ with $s_i | s_{i+1}$ for $i = 1, \ldots, r$ and unimodular matrices P and Q such that $PMQ = D = \operatorname{diag}(s_1, \ldots, s_r, 0, \ldots, 0)$. The diagonal matrix D is called the *Smith Normal Form* (SNF) of M, and the numbers $s_1, \ldots, s_r$ are the nonzero *invariant factors* of M. The SNF, and hence the invariant factors, are *uniquely* determined by the matrix M. For background on the SNF and invariant factors, see, e.g., [23]. The *Smith group* [29] of M is $\Gamma(M) = \mathbb{Z}^n / \mathbb{Z}^m M$; the submodule $\overline{\Gamma}(M) = \mathbb{Z}^n / \mathbb{Q}^m M \cap \mathbb{Z}^n$ of $\Gamma(M)$ is the torsion subgroup of $\Gamma(M)$. Indeed, if M has rank r, then $\Gamma(M) = \mathbb{Z}^{n-r} \oplus \overline{\Gamma}(M)$ with $\overline{\Gamma}(M) = \oplus_{i=1}^{r} \mathbb{Z}_{s_i}$, where $s_1, \ldots, s_r$ are the nonzero invariant factors of M. See [29] for further details and proofs.

Let $G = (V, E)$ be a finite directed graph with with vertex set V and edge set E (we allow loops and multiple edges). The *adjacency matrix* of G is the $|V| \times |V|$ matrix $A = (A_{v,w})$, with rows and columns indexed by V, where the entry $A_{v,w}$ in position (v, w) is the number of edges from v to w. The indegree $d^-(v)$ and outdegree $d^+(v)$ is the number of edges ending or starting in vertex v, respectively. The *Laplacian* of G is the matrix $\Delta = D - A$, where D is diagonal with $D_{v,v} = d_v^+$. The *critical group* $S(G)$ of G is the torsion subgroup $\overline{\Gamma}(\Delta)$ of the Smith group of the Laplacian Δ of G. The *sandpile group* $S(G, v)$ of G at a vertex v is the torsion subgroup of the Smith group of the *reduced Laplacian* Δ_v, obtained from Δ by deleting the row and the column of Δ indexed by v. Note that by the Matrix Tree Theorem for directed graphs, the order of $S(G, v)$ equals the number of directed spanning trees rooted at v. The directed graph G is called *Eulerian* if $d^+(v) = d^-(v)$ for every vertex v. In that case, $S(G, v)$ does not depend on the vertex v and is equal to the critical group $S(G)$ of G, essentially because in that case, not only the columns, but also the rows of the Laplacian Δ of G sum to zero; for a detailed proof, see [15] (note that the proof as given there does not use the assumption that the directed graph is connected). For more details on sandpile groups and the critical group of a directed graph, we refer for example to [15] or [33].

2.2 Generalized de Bruijn and Kautz graphs

Generalized de Bruijn graphs [13] and generalized Kautz graphs [11] are known to have a relatively small diameter and attractive connectivity properties, and have been studied intensively due to their applications in interconnection networks. The generalized Kautz graphs were first investigated in [18], [17], and are also known as *Imase-Itoh digraphs*. Both classes of directed graphs are Eulerian.

Let n and d be integers with $n \geq 1$ and $d \geq 0$. The *generalized de Bruijn graph* $\mathrm{DB}(n,d)$ has vertex set $\mathbb{Z}_n$, the set of integers modulo n, and d (directed) edges $v \to dv + i$, for $0 \leq i \leq d-1$, for $0 \leq v \leq n-1$. The *generalized Kautz graph* $\mathrm{Ktz}(n,d)$ has vertex set $\mathbb{Z}_n$ and d directed edges $v \to -d(v+1) + i$, for $0 \leq i \leq d-1$, for $0 \leq v \leq n-1$. (For both generalized de Bruijn and Kautz graphs, we allow multiple edges when $d > n$.) These directed graphs are important special cases of the so-called *consecutive-d digraphs*. Here a consecutive-d digraph $G(d,n,q,r)$, defined for $q \in \mathbb{Z}_n \setminus \{0\}$ and $r \in \mathbb{Z}_n$, has vertex set $\mathbb{Z}_n$ and directed edges $v \to qv + r + i$ for $0 \leq i \leq d-1$ and $0 \leq v \leq n-1$. Note that the generalized de Bruijn and Kautz graphs are the cases $q = d, r = 0$ and $q = -d, r = -d$, respectively. It is easily verified that both $\mathrm{DB}(n,d)$ and $\mathrm{Ktz}(n,d)$ are indeed Eulerian for all integers $n \geq 1$ and $d \geq 0$. It is easily seen that for $d = 0$ or 1, the critical groups for both the de Bruijn graph and the Kautz graph are trivial.

2.3 The group of invertible circulant matrices

Let $q = p^r$ be a prime power. An $n \times n$ circulant matrix over a finite field $\mathbb{F}_q$ is a matrix C of the form

$$C = \begin{pmatrix} c_0 & c_{n-1} & \cdots & c_1 \\ c_1 & c_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & c_{n-1} \\ c_{n-1} & \cdots & c_1 & c_0 \end{pmatrix}, \tag{1}$$

where $c_0, \ldots, c_{n-1} \in \mathbb{F}_q$. With C as in (1) we associate the polynomial $c_C(x) := c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_q[x]$. Let X denote the matrix of the multiplication by x map on the ring $\mathcal{R} := \mathbb{F}_q[x]/(x^n - 1)$ with respect to the basis $1, x, \ldots, x^{n-1}$. Every C in (1) can be written as $C = \sum_{i=0}^{n-1} c_i X^i$, where $c(x) = c_C(x)$. Note that $c_X(x) = x$, and the map $x \mapsto X$ induces an isomorphism between $\mathcal{R}$ and the algebra $\mathbb{F}_q[X]$ of circular matrices.

The units of $\mathbb{F}_q[X]$ form a commutative group under multiplication; we denote this group by $C(n,q)$. Under the isomorphism induced by $x \mapsto X$, the group $C(n,q)$ corresponds to

$$\mathcal{R}^* = \{c(x) \in \mathbb{F}_q[x], \deg c < n \mid (c(x), x^n - 1) = 1\}.$$

Indeed, by the extended Euclidean algorithm, $(c(x), x^n - 1) = 1$ if and only if there exist $u, v \in \mathbb{F}_q[x]$ such that $cu = 1 - (x^n - 1)v$, i.e. $u = c^{-1} \in \mathcal{R}$. On the other hand, $c(X)u(X) = I - (X^n - I)v(X) = I$, i.e. $u(X) = c(X)^{-1} \in C(n,q)$.

Note that $C(n,q)$ contains a subgroup isomorphic to $\mathbb{Z}_{q-1} \oplus \mathbb{Z}_n$, namely the direct product of the group of scalar matrices $F_q^* I := \{\lambda I \mid \lambda \in \mathbb{F}_q^*\}$ and the cyclic subgroup $\langle X \rangle$ generated by X. Each $C \in \mathbb{F}_q[X]$ has the all-ones vector $\mathbf{1} := (1, \ldots, 1)^\top$ as an eigenvector. Thus $C'(n,q) := \{C \in C(n,q) \mid C\mathbf{1} = \mathbf{1}\} \leq C(n,q)$, and we have the following direct product decomposition.

$$C(n,q) = C'(n,q) \times F_q^* I, \tag{2}$$

where, as usual, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. In view of (2) one has $C'(n,q) \leq \mathrm{PLG}_n(q)$. Note that

$$C'(n,q) \cong \{a(x) \in \mathbb{F}_q[x], \deg a < n \mid (a(x), x^n - 1) = 1 \text{ and } a(1) = 1\}. \tag{3}$$

We also note that although $\langle X \rangle \leq C'(n,q)$, it is not necessarily a *direct summand* of $C'(n,q)$ (for example, take $n = 2$ and $q = 4$: then $C'(n,q) \cong \mathbb{Z}_4$ and $\langle X \rangle \cong \mathbb{Z}_2$).

Remark: Note that $C(n, q)$ is the centralizer of X in $\mathrm{GL}_n(q)$. It also can be viewed as the group of units of the group algebra $\mathbb{F}_q[\langle X \rangle]$.

2.4 The sandpile and sand dune groups

We determine the sandpile group $S_{\mathrm{DB}}(n, d)$ (resp. $S_{\mathrm{Ktz}}(n, d)$) of a generalized de Bruijn (resp. Kautz graph) on n vertices by embedding this group as a subgroup of index n in a group that, for lack of a better name, we refer to as the *sand dune* group of the corresponding directed graph. This embedding method can in fact be applied to the much wider class of *consecutive-d digraphs* [12], and the idea may have other applications as well.

Let us represent the elements of $\mathbb{Z}_n$ by $1, x, \ldots x^{n-1}$, and think of elements in the group algebra $\mathbb{Q}[\mathbb{Z}_n]$ as Laurent polynomials modulo $x^n - 1$, that is, identify $\mathbb{Q}[\mathbb{Z}_n]$ with $\mathbb{Q}[x, x^{-1}]$ mod $x^n - 1$, and its subring $\mathbb{Z}[\mathbb{Z}_n]$ with $\mathbb{Z}[x, x^{-1}]$ mod $x^n - 1$. Furthermore, we identify a vector $c = (c_0, \ldots, c_{n-1})$ in $\mathbb{Q}^n$ with its associated polynomial $c(x) = c_0 + \cdots + c_{n-1}x^{n-1}$ in $\mathbb{Q}[x, x^{-1}]$ mod $x^n - 1$; note that this association is in fact an isomorphism between $\mathbb{Q}^n$ and $\mathbb{Q}[x, x^{-1}]$ mod $x^n - 1$, considered as vector spaces over $\mathbb{Q}$. The advantage of this identification is that we now also have a multiplication available. Given a collection of vectors $V = \{v_i \mid i \in I\}$ in $\mathbb{Z}^n$, we denote the $\mathbb{Z}$-span of the associated polynomials by $\langle v_i(x) \mid i \in I \rangle_{\mathbb{Z}}$.

We now derive a useful description of both $S_{\mathrm{DB}}(n, d)$ and $S_{\mathrm{Ktz}}(n, d)$ using the Smith group $\Gamma(\Delta)$ of the Laplacian Δ of these digraphs as defined in Section 2.1. To this end, for every integer d we define the Laurent polynomial $f^{(n,d)}(x)$ in $\mathbb{Z}[x, x^{-1}]$ mod $x^n - 1$ as

$$f_v^{(n,d)}(x) = dx^v - x^{dv}(x^d - 1)/x - 1).\tag{4}$$

For $d \geq 0$, we have

$$f_v^{(n,d)}(x) = dx^v - x^{dv}\sum_{i=0}^{d-1}x^i = \sum_{w \in \mathbb{Z}_n}\Delta_{v,w}x^w$$

with $\Delta = \Delta_{\mathrm{DB}}$ the Laplacian of $\mathrm{DB}(n, d)$, while for $d < 0$, we have

$$f_v^{(n,d)}(x) = -|d|x^v - x^{-|d|v}(x^{-|d|} - 1)/(x - 1) = -|d|x^v + x^{-|d|(v+1)}\sum_{i=0}^{|d|-1}x^i = -\sum_{w \in \mathbb{Z}_n}\Delta_{v,w}x^w$$

with $\Delta = \Delta_{\mathrm{Ktz}}$ now the Laplacian of $\mathrm{Ktz}(n, |d|)$. In what follows, we simply write Δ to denote the Laplacian of either $\mathrm{DB}(n, d)$ or $\mathrm{Ktz}(n, d)$. For later use, we also define

$$g_v^{(n,d)}(x) = (x - 1)f_v^{(n,d)}(x) = dx^v(x - 1) - x^{dv}(x^d - 1)$$

for every $0 \leq v < n$. For the remainder of this paper, we let

$$e_v^{(n)} = x^v - 1, \qquad \epsilon_v^{(n,d)} = de_v^{(n)} - e_{dv}^{(n)}, \quad \text{for every } 0 \leq v \leq n - 1;\tag{5}$$

note that $e_0^{(n)} = \epsilon_0^{(n,d)} = 0$. We simply write $f_v(x)$, $g_v(x)$, e_v and ϵ_v if the intended values for n and d are evident from the context. Finally, we set

$$\mathcal{Z}_n = \langle e_v \mid 1 \leq v \leq n - 1 \rangle_{\mathbb{Z}}, \qquad \mathcal{E}_{n,d} = \langle \epsilon_v \mid 1 \leq v \leq n - 1 \rangle_{\mathbb{Z}}.$$

In the next lemma, we collect some simple facts.

Lemma 2.1.
(1) We have that $\sum_{v=0}^{n-1} f_v(x) = 0$ and $f_v(1) = 0$;
(2) $\mathcal{Z}_n$ consists of all polynomials $c(x) \in \mathbb{Z}[x]$ for which $\deg c \leq n-1$ and $c(1) = 0$;
(3) We have that $\epsilon_v = g_0(x) + \cdots + g_{v-1}(x)$ and $\mathcal{E}_{n,d} = \langle g_v(x) \mid 0 < v < n \rangle_{\mathbb{Z}}$.

Proof. (1) Since the columns of the Laplacian Δ add up to 0, we have that $f_v(1) = 0$; moreover, since both $\mathrm{DB}(n,d)$ and $\mathrm{Ktz}(n,d)$ are Eulerian, in both cases the rows of Δ also add up to 0, so that $\sum_{v \in \mathbb{Z}_n} f_v(x) = 0$ (these claims are also easily verified directly). Part (2) is obvious from the observation that $e_{v+1} - e_v = (x-1)x^v$, and to see (3), simply note that from (1), after multiplication by $x-1$, we obtain $g_0(x) + \cdots + g_{n-1} = 0$. $\qquad\square$

We can now derive an expression for the Smith group $\Gamma(\Delta)$ in terms of polynomials.

Lemma 2.2. For the Smith group $\Gamma(\Delta)$ we have

$$\Gamma(\Delta) = \mathbb{Z}^n/\mathbb{Z}^n\Delta = (\mathbb{Z}[x] \bmod x^n-1)/\langle f_v(x) \mid 0 \leq v \leq n-1 \rangle_{\mathbb{Z}} = \mathbb{Z} \oplus \mathcal{Z}_n/\langle f_v(x) \mid 1 \leq v \leq n-1 \rangle_{\mathbb{Z}}.$$

Proof. First note that the vectors $\mathbb{Z}^n$ correspond to the polynomials in $\mathbb{Z}[x] \bmod x^n - 1$ and, since the rows of Δ correspond to the polynomials $f_v(x)$ or $-f_v(x)$, the vectors in the row space $\mathbb{Z}^n\Delta$ correspond to the elements of $\langle f_v(x) \mid 0 \leq v \leq n-1 \rangle_{\mathbb{Z}}$. This shows the second equality in the lemma. Then, by Lemma 2.1 (2) and the Chinese Remainder Theorem, we have that $\mathbb{Z}_n[x] \bmod x^n - 1 \cong \mathbb{Z} \oplus \mathcal{Z}_n$. Again by Lemma 2.1, every $f_v(x)$ is contained in $\mathcal{Z}_n$ and $f_0(x)$ depends on the other $f_v(x)$, so the lemma follows. $\qquad\square$

The next result is one of the key points in our approach.

Theorem 2.3. Let n and d be integers, with $n \geq 1$. If $|d| \geq 2$, then the polynomials ϵ_v, for $1 \leq v \leq n-1$ (resp., the polynomials $g_v(x)$ $(1 \leq v \leq n-1)$) are independent over $\mathbb{Q}$, and $\dim_{\mathbb{Q}} \mathcal{E}_{n,d} = n-1$.

Proof. In view of Lemma 2.1 (3), it suffices to show that the $g_v(x)$ for $1 \leq v \leq n-1$ are independent over $\mathbb{Q}$. To see this, suppose that

$$0 \bmod x^n - 1 = \sum_{v \neq 0} a_v g_v(x) = d(x-1)\sum_{v \neq 0} a_v x^v - (x^d - 1)\sum_{v \neq 0} a_v x^{dv}, \quad a_v \in \mathbb{Q}.$$

Writing $a(x) = \sum_{v>0} a_v x^v$ and $c(x) = \sum_{v>0} a_v x^v(x-1) = (x-1)a(x) = \sum_i c_i x^i$, we have that $c(x^d) = dc(x) \bmod x^n - 1$. Subsituting x with x^d, one obtains $c((x^d)^d) = c(x^{d^2}) = dc(x^d) = d^2 c(x)$. Similarly, $c(x^{d^3}) = dc(x^{d^2}) = d^3 c(x)$, etc. Hence $c(x^{d^e}) = d^e c(x)$ in $\mathbb{Q}[x] \bmod x^n - 1$, for every integer $e \geq 1$. However, if $|d| \geq 2$ and $c(x) \neq 0$, then the left-hand side has bounded coefficients while the right-hand side has an unbounded coefficient $d^e c_i$ if $c_i \neq 0$, a contradiction. It follows that $c(x) = (x-1)a(x) = 0$, hence $a(x) \equiv 0 \bmod 1 + x + \cdots + x^{n-1}$. But as $a(0) = 0$ and $\deg a < n$, it follows that $a_v = 0$ for all v. $\qquad\square$

Corollary 2.4. For integers d with $|d| \geq 2$, the sandpile group (or equivalently, the critical group) $S(n,d)$ of the generalized de Bruijn graph $\mathrm{DB}(n,d)$ (if $d > 0$) or of the generalized Kautz graph $\mathrm{DB}(n,|d|)$ (if $d < 0$) can be expressed as

$$S(n,d) = \mathcal{Z}_n/\langle f_v^{(n,d)}(x) \mid 1 \leq v \leq n-1 \rangle_{\mathbb{Z}} \tag{6}$$

5

Proof. First, we claim that the polynomials f_v for $1 \leq v \leq n-1$ are independent over $\mathbb{Q}$. Indeed, every nontrivial relation between the $f_v(x)$ implies (after multiplication by $x-1$) a similar relation between the $g_v(x)$; however, according to Theorem 2.3, such relation cannot exist if $|d| \geq 2$. As a consequence, for $K := \langle f_v(x) \mid 1 \leq v \leq n-1 \rangle_{\mathbb{Z}}$ one has $\dim_{\mathbb{Q}} K = n-1$. In view of what was stated in Section 2.1, this implies that the quotient $\mathcal{Z}_n/K$ in Lemma 2.2 is a finite group, and the lemma follows. $\square$

It is not so easy to determine the structure of $S(n,d)$ by employing (6), due to the complicated form of the polynomials $f_v(x)$. The polynomials $g_v(x) = (x-1)f_v(x)$ have a much easier structure, which motivates the following approach. We define the *sand dune group* $\Sigma(n,d)$ of the generalized de Bruijn graph $\mathrm{DB}(n,d)$ for $d \geq 2$ (resp. of the generalized Kautz graph $\mathrm{Ktz}(n,|d|)$ for $d \leq -2$) as

$$\Sigma(n,d) = \mathcal{Z}_n/\langle g_v(x) \mid 1 \leq v \leq n-1 \rangle_{\mathbb{Z}} = \mathcal{Z}_n/\mathcal{E}_{n,d}.$$

The next result is crucial to our approach: it shows that $S(n,d) < \Sigma(n,d)$, and identifies the elements of $\Sigma(n,d)$ that are contained in $S(n,d)$.

Theorem 2.5. The sand dune group $\Sigma(n,d)$ is finite, and the sandpile group $S(n,d)$ is a subgroup of $\Sigma(n,d)$. Moreover, if $a = \sum_{v=1}^{n-1} a_v e_v \in \Sigma(n,d)$, then $a \in S(n,d)$ if and only if $\sum_{v=1}^{n-1} v a_v \equiv 0 \bmod n$.

Proof. The finiteness of $\Sigma(n,d)$ follows from the fact that $\dim_{\mathbb{Q}} \mathcal{E}_{n,d} = n-1$, as proved in Lemma 2.3. Next, write $T_v(x) = e_v(x)/(x-1) = 1 + \cdots + x^{v-1}$ for $0 \leq v \leq n-1$. Consider the map ϕ on $\mathbb{Q}[x] \bmod x^n - 1$ for which $\phi(c(x)) = (x-1)c(x)$. It is $\mathbb{Q}$-linear, and $\mathrm{Ker}\phi = \langle T_n(x) \rangle_{\mathbb{Q}}$. Since $T_n(1) = n \neq 0$, the restriction of ϕ to $\mathcal{Z}_n$ is one-to-one, and ϕ maps $\langle f_v(x) \mid 1 \leq v \leq n-1 \rangle_{\mathbb{Z}}$ onto $\mathcal{E}_{n,d}$. As $\phi(\mathcal{Z}_n) \subseteq \mathcal{Z}_n$, one sees that ϕ embeds $S(n,d)$ as a subgroup $\phi(\mathcal{Z}_n)/\mathcal{E}_{n,d}$ in $\Sigma(n,d)$. To determine that subgroup, we need to determine $\phi(\mathcal{Z}_n)$.

To this end, let $a(x) = \sum_v a_v e_v(x) \in \mathcal{Z}_n$. Then we can write $a(x) = h(x)(x-1)$ with $h(x) = a(x)/(x-1) = \sum_v a_v T_v(x)$. Note that since $T_v(1) = v$, we have $h(1) = \sum_v v a_v$. Now $a(x) = \phi(b(x)) = b(x)(x-1)$ with $\deg b < n$ precisely when $b(x)$ is of the form $b(x) = h(x) - \lambda T_n(x)$ with $\lambda \in \mathbb{Q}$; note that $b(x) \in \mathcal{Z}_n$ precisely when $\lambda \in \mathbb{Z}$ and $b(1) = h(1) - \lambda T_n(1) = \sum_v v a_v - \lambda n = 0$; such a λ exists precisely when $\sum_v v a_v \equiv 0 \bmod n$. $\square$

Corollary 2.6. We have $\Sigma(n,d)/S(n,d) = \mathbb{Z}_n$ and in particular $|\Sigma(n,d)| = n|S(n,d)|$.

Proof. The map $\theta : \mathbb{Q}[x]/(x^n - 1) \to \mathbb{Z}_n$ given by $\theta(\sum_v a_v e_v) = \sum_v v a_v$ has the property that $\theta(\epsilon_v) = \theta(d e_v - e_{dv}) = 0$. Hence it is well-defined as a map on $\Sigma(n,d)$; it is obviously a homomorphism, and it is surjective since $\theta(e_v) = v$ for all $v \in \mathbb{Z}_n$. As a consequence, $n = |\mathbb{Z}_n| = |\mathrm{Im}(\theta)| = |\Sigma(n,d)|/|\mathrm{Ker}(\theta)| = |\Sigma(n,d)|/|S(n,d)|$. $\square$

We remark that the determination of $S(n,d)$ is complicated by the fact that $S(n,d)$ is not always a *direct summand* of $\Sigma(n,d)$, as is illustrated by the following.

Example 2.7. Let $n = 4$ and $d = 3$. Then $\Sigma(n,d) = \mathbb{Z}_8 \oplus \mathbb{Z}_2$ and $S(n,d) = \mathbb{Z}_4$, which is not a direct summand of $\mathbb{Z}_8 \oplus \mathbb{Z}_2$.

The above descriptions of $S(n,d)$ and $\Sigma(n,d)$, and the embedding of $S(n,d) < \Sigma(n,d)$, are quite suitable for the determination of these groups. In that process, at several places information is required about the order of various group elements. Our next few results provide that information.

Lemma 2.8. Every element $\alpha \in \Sigma(n,d)$ can be expressed as $\alpha = \sum_{v>0} \alpha_v \epsilon_v$, with $\alpha_v \in \mathbb{Q}$ satisfying $0 \leq a_v < 1$ for each $1 \leq v \leq n-1$; then the order of α in $\Sigma(n,d)$ is the smallest positive integer m such that $m\alpha_v \in \mathbb{Z}$ for each $1 \leq v \leq n-1$.

Proof. According to Theorem 2.3, the ϵ_v are independent in $\mathbb{Q}[x] \bmod x^n - 1$. Therefore, every polynomial $f(x)$ in $\mathbb{Q}[x]$ with $f(1) = 0$ and $\deg f < n$ has a unique expression $f = \sum_{v>0} f_v \epsilon_v$ as linear combination of the ϵ_v. Such an expression is 0 modulo $\mathcal{E}_{n,d}$ if and only if all coefficients f_v are integers. Now the claim is obvious. $\square$

In order to use this result, we must be able to express the polynomials e_v in terms of the ϵ_v. This can be done as follows.

Definition 2.9. Let $v \in \mathbb{Z}_n$. Given $d \in \mathbb{Z}$, there are unique $\mathbb{Z} \ni e > 0$ and $\mathbb{Z} \ni f \geq 0$ such that the $d^i v$ in $\mathbb{Z}_n$ are distinct for $0 \leq i \leq e + f - 1$, while $d^{e+f} v = d^f v$. We say that v has d-type $[f,e]$ in $\mathbb{Z}_n$.

Lemma 2.10. Let n and d be integers with $n \geq 1$ and $|d| \geq 2$. If v has d-type $[f,e]$ in $\mathbb{Z}_n$ then in $\mathbb{Q}[x] \bmod x^n - 1$, we have

$$ e_v = \sum_{i=0}^{f-1} \frac{1}{d^{i+1}} \epsilon_{d^i v} + \sum_{j=0}^{e-1} \frac{d^j}{d^f (d^e - 1)} \epsilon_{d^{f+j} v}. $$

Proof. First note that by a simple "telescoping" summation

$$ e_v = d^{-1} \epsilon_v + \cdots + d^{-f} \epsilon_{d^{f-1} v} + d^{-f} e_{d^f v}. $$

Put $w = d^f v$. Then

$$ e_w = d^{-1} \epsilon_w + \cdots + d^{-e} \epsilon_{d^{e-1} w} + d^{-e} e_{d^e w}, $$

and since $d^e w = w$, we conclude that

$$ (d^e - 1) e_w = d^{e-1} \epsilon_w + \cdots + \epsilon_{d^{e-1} w}. $$

By combining these two results, the lemma follows. $\square$

In view of Lemma 2.8, we immediately obtain the following.

Corollary 2.11. Let $|d| \geq 2$. If v has d-type $[f,e]$ in $\mathbb{Z}_n$ then e_v has order $|d^f (d^e - 1)|$ in $\Sigma(n,d)$.

Remark 2.12. As we have seen, the group $S(n,d)$ is equal to the sandpile group of $\mathrm{DB}(n,d)$ if $d \geq 2$ (resp. of $\mathrm{Ktz}(n, |d|)$ if $d \leq -2$). In what follows, we concentrate on the generalized de Bruijn graph and therefore we assume $d \geq 2$. We leave it to the reader to make the necessary adaptations for the generalized Kautz graphs.

3   Main results

Let n and d be fixed integers with $n \geq 1$ and $|d| \geq 2$. The description of the sandpile group $S(n,d)$ and the sand-dune group $\Sigma(n,d)$ involves a sequence of numbers defined as follows. Put $n_0 = n$, and for $i = 1, 2, \ldots$, define $d_i = (n_i, |d|)$ and $n_{i+1} = n_i/d_i$. We have $n_0 > \cdots > n_k = n_{k+1}$, where $k \geq 0$ is the smallest integer for which $d_k = 1$. We refer to the sequence $n_0 > \cdots > n_k = n_{k+1}$ as the *d-sequence* of n. In what follows, we write $m = n_k$. Note that $n = d_0 \cdots d_{k-1} m$ with $(m, d) = 1$.

Since $(m, d) = 1$, the map $x \mapsto dx$ is invertible and partitions $\mathbb{Z}_m$ into orbits of the form $O(v) = \{v, dv, \ldots, d^{o(v)-1}v\}$. Here, $O(v)$ is sometimes referred to as the *d-ary cyclotomic coset of v modulo m*. We refer to $o(v) = |O(v)|$ as the *order* of v.

For every prime $p|m$, we define $\pi_p(m)$ to be the largest power of p dividing m. Let $\mathcal{V}$ be a set of representatives of the orbits $O(v)$ different from $\{0\}$, where we ensure that for every prime divisor p of m, all integer numbers of the form m/p^j are contained in $\mathcal{V}$. (This is possible since no two of these numbers are in the same cyclotomic coset.)

Theorem 3.1. Let $n = d_0 \cdots d_{k-1} m$ with $(m, d) = 1$. The groups $S(n,d)$ and $\Sigma(n,d)$ are the sandpile and sand dune group of the generalized de Bruijn graph $\mathrm{DB}(n,d)$ if $d \geq 2$ (resp. of the generalized Kautz graph $\mathrm{Ktz}(n, |d|)$ if $d \leq -2$). With the above definitions and notation,

$$\Sigma(n,d) = \left[\bigoplus_{i=0}^{k-1} \mathbb{Z}_{|d|^{i+1}}^{n_i - 2n_{i+1} + n_{i+2}}\right] \oplus \left[\bigoplus_{v \in \mathcal{V}} \mathbb{Z}_{|d^{o(v)} - 1|}\right] \tag{7}$$

and

$$S(n,d) = \left[\bigoplus_{i=0}^{k-1} \mathbb{Z}_{|d|^{i+1}/d_i} \oplus \mathbb{Z}_{|d|^{i+1}}^{n_i - 2n_{i+1} + n_{i+2} - 1}\right] \oplus \left[\bigoplus_{v \in \mathcal{V}} \mathbb{Z}_{|d^{o(v)} - 1|/c(v)}\right], \tag{8}$$

where, for each prime $p \mid m$,

$$c(v) = \begin{cases} \pi_p(m) & v = m/\pi_p(m), \ p \neq 2 \text{ or } d \equiv 1 \bmod 4 \text{ or } 4 \nmid m \\ \pi_2(m)/2 & v = m/\pi_2(m), \ d \equiv 3 \bmod 4, \text{ and } 4 \mid m \\ 2 & v = m/2, \ 4 \mid m \text{ and } d \equiv 3 \bmod 4 \\ 1 & \text{otherwise.} \end{cases}$$

Remark that since $n = d_0 \cdots d_{k-1} m$ with $m = \prod_{p|m} \pi_p(m)$, the above result implies that $\Sigma(n,d)/S(n,d) = \mathbb{Z}_n$, in accordance with the results in Section 2.

With the notation from Section 2.3, we have the following isomorphisms, connecting critical groups and circulant matrices.

Theorem 3.2. Let $d > 0$ be a prime. Then $\Sigma(n,d) \cong C'(n,d)$ and $S(n,d) \cong C'(n,d)/\langle X \rangle$. For d a proper prime power, this result also holds if $(n,d) = 1$, but not always if $(n,d) \neq 1$.

The above results are proved in a number of steps. In what follows, we outline the method for the generalized de Bruijn graphs; for the generalized Kautz graphs, a similar approach can be used. First, we investigate the "multiplication-by-d" map d given by $x \mapsto dx$ on the sandpile and sand dune groups. Let $\Sigma_0(n,d)$ and $S_0(n,d)$ denote the kernel of the map $x \mapsto d^k x$ on

8

$\Sigma(n,d)$ and $S(n,d)$, respectively. It is not difficult to see that $\Sigma(n,d) \cong \Sigma_0(n,d) \oplus \Sigma(m,d)$ and $S(n,d) \cong S_0(n,d) \oplus S(m,d)$. Then, we use the map d to determine $\Sigma_0(n,d)$ and $S_0(n,d)$. It is easy to see that for *any* n, we have $d\Sigma(n,d) \cong \Sigma(n/(n,d),d)$ and $dS(n,d) \cong S(n/(n,d),d)$. With some more effort, it can be shows that the kernel of the map d on $\Sigma(n,d)$ (resp. on $S(n,d)$) is isomorphic to $\mathbb{Z}_d^{n-n/(n,d)}$ (resp. to $\mathbb{Z}_{d/(n,d)} \oplus \mathbb{Z}_d^{n-1-n/(n,d)}$). Then we use induction on the length $k+1$ of the d-sequence of n to show that $\Sigma_0(n,d)$ and $S_0(n,d)$ have the form of the left hand parts of (7) and (8), respectively. This part of the proof, although much more complicated, resembles the method used by [19] and [4].

Then it remains to handle the parts $\Sigma(m,d)$ and $S(m,d)$, where $(m,d) = 1$. For the "helper" group $\Sigma(m,d)$ that embeds $S(m,d)$, this is trivial: it is easily seen that $\Sigma(m,d) = \oplus_{v \in \mathcal{V}} \langle e_v \rangle$, and the order of e_v is equal to the size $o(v)$ of its orbit $O(v)$ under the map d, so (7) follows immediately. The e_v are not contained in $S(m,d)$, but we can try to modify them slightly to obtain a similar decomposition for $S(m,d)$. The idea is to replace e_v by a modified version $\tilde{e}_v = e_v - \sum_{p|m} \lambda_p(v) e_{m\pi_p(v)/\pi_p(m)}$, where the numbers $\lambda_p(v)$ are chosen such that $\tilde{e}_v \in S(m,d)$, or by a suitable multiple of e_v, in some exceptional cases (these are the cases where $c(v) > 1$). It turns out that this is indeed possible, and in this way the proof of Theorem 3.1 can be completed.

The proof of Theorem 3.2 is by reducing to the case $(n,p) = 1$ by an explicit construction, and then by diagonalizing $C(n,p)$ over an appropriate extension of $\mathbb{F}_p$. Essentially, as soon as $(n,p) = 1$, one can read off a decomposition of $C(n,p)$ into cyclic factors from the irreducible factors of the polynomial $x^n - 1$ over $\mathbb{F}_p$.

In the next sections, we provide the details of the proofs as outlined above.

4 The multiplication-by-d map

In the remainder of this section, we use the map $x \mapsto dx$ on $\Sigma(n,d)$ to determine the structure of $\Sigma_0(n,d)$ and $S_0(n,d)$, i.e. the kernels of the map $x \mapsto d^k x$. We require the following simple result.

Theorem 4.1. For any pair n,d of positive integers, $d\Sigma(n,d) \cong \Sigma(n/(n,d),d)$ and $dS(n,d) = S(n/(n,d),d)$.

Proof. Write $n_1 = n/(n,d)$. Define $\varphi : d\Sigma(n,d) \to \Sigma(n_1,d)$ by $\varphi(de_v) = e_{v \bmod n_1}$ for $1 \leq v \leq n-1$ and extend φ by linearity. We claim that φ defines an isomorphism between $d\Sigma(n,d)$ and $\Sigma(n_1,d)$. To see this, proceed as follows. Since $de_v = e_{dv}$ in $\Sigma(n,d)$, we have that $d\sum_{v>0} \alpha_v e_v = \sum_{v>0} \alpha_v e_{dv}$, and from Lemma 2.10 we conclude that $\sum_{v>0} \alpha_v e_{dv}$ can be expressed as a linear combination of elements ϵ_{dv} in $\mathcal{E}_{n,d}$ with rational coefficients; the expression is 0 in $\Sigma(n,d)$ if and only if all coefficients can be chosen to be integer. So, noting that φ maps ϵ_{dv} in $\mathcal{E}_{n,d}$ to $\epsilon_{v \bmod n_1}$ in $\mathcal{E}_{n_1,d}$, we conclude that φ is well-defined and in fact one-to-one on $d\Sigma(n,d)$. Since φ is obviously onto $\Sigma(n_1,d)$, the desired conclusion follows.

To see that φ also induces an isomorphism between $dS(n,d)$ and $S(n_1,d)$, in view of Theorem 2.5 it is sufficient to remark that for an element $d\sum_{v>0} a_v e_v = \sum_{v>0} a_v e_{dv} \in d\Sigma(n,d)$, we have $\sum_{v>0} dva_v \equiv 0 \bmod n$ if and only if $\sum_{v>0} va_v \equiv 0 \bmod n_1$. $\square$

The next step is to determine the *kernel* of the multiplication-by-d map $d : \mathbb{Q}[x]/(x^n - 1) \to \mathbb{Q}[x]/(x^n - 1)$, defined by $x \mapsto dx$, on both $\Sigma(n,d)$ and $S(n,d)$. The result is as follows.

Theorem 4.2. (i) The kernel $\mathrm{Ker}_\Sigma(d)$ of the map d on $\Sigma(n,d)$ is isomorphic to $\mathbb{Z}_d^{n-n_1}$.
(ii) The kernel $\mathrm{Ker}_S(d)$ of the map d on $S(n,d)$ is isomorphic to $\mathbb{Z}_{d/d_0} \oplus \mathbb{Z}_d^{n-n_1}$.

Proof. The order of $\Sigma(n,d)$ is equal to the product of its invariant factors, which are the positive invariant factors of the $(n-1) \times (n-1)$ matrix $\Sigma = \Sigma^{(n,d)}$ that has as rows the vectors $\epsilon_v = de_v - e_{dv}$ with respect to the basis $\{e_v \mid 1 \leq v \leq n-1\}$. Since Σ is nonsingular, this product is equal to $\det \Sigma$. Now partition the set $\mathbb{Z}_n \setminus \{0\}$ of row and column indices of Σ into parts $\mathbb{Z} - d\mathbb{Z}_n$ and $(d\mathbb{Z}_n) \setminus \{0\}$. Under this ordering of the rows and columns, Σ takes the form

$$\Sigma = \Sigma^{(n,d)} = \left(\begin{array}{c|c} D & A \\ \hline O & \Sigma', \end{array} \right),$$

where $D = \mathrm{diag}(d, \ldots, d)$ is a $(n-n_1) \times (n-n_1)$ diagonal matrix and $\Sigma' = \Sigma^{(n_1,d)}$ is the matrix corresponding to $\Sigma(n_1, d)$. (Note that $d\mathbb{Z}_n \cong \mathbb{Z}_{n/(d,n)} = \mathbb{Z}_{n_1}$.) We conclude that

$$|\Sigma(n,d)| = d^{n-n_1}|\Sigma(n_1,d)|. \tag{9}$$

In view of Theorem 4.1, we have that $|\mathrm{Ker}_\Sigma(d)| = |\Sigma(n,d)|/|\mathrm{Im}_\Sigma(d)| = d^{n-n_1}$, and as a consequence of Corollary 2.6, we also have

$$|\mathrm{Ker}_S(d)| = |S(n,d)|/|S(n_1,d)| = (|\Sigma(n,d)|/n)/(|\Sigma(n,d)|/n_1) = d^{n-n_1}/d_0.$$

To actually construct a basis for these kernels, let us define

$$\Delta_{ab} := e_{a+bn_1} - e_a = d^{-1}(\epsilon_{a+bn_1} - \epsilon_a),$$

where the second equality follows directly from (5). By Lemma 2.8, each Δ_{ab} has order d. Hence they are contained in $\mathrm{Ker}_\Sigma(d)$. First, we claim that the set

$$\mathcal{B} = \{\Delta_{ab} \mid 0 \leq a \leq n_1 - 1, 1 \leq b \leq d_0 - 1\}$$

is independent in $\Sigma(n,d)$ and a basis for $\mathrm{Ker}_\Sigma(d)$. Indeed, consider a $\mathbb{Z}$-linear combination of the elements of $\mathcal{B}$. Since

$$\sum_{a=0}^{n_1-1} \sum_{b=1}^{d_0-1} \lambda_{ab} \Delta_{ab} = \sum_{a=0}^{n_1-1} \sum_{b=1}^{d_0-1} \lambda_{ab} d^{-1}(\epsilon_{a+bn_1} - \epsilon_a) = d^{-1} \sum_{a=0}^{n_1-1} \left(\sum_{b=1}^{d_0-1} \lambda_{a,b} \epsilon_{a+bn_1} - \left(\sum_{b=1}^{d_0-1} \lambda_{ab} \right) \epsilon_a \right),$$

and since $a + bn_1 = a' + b'n_1$ with $a, a' \in \{0, 1, \ldots, n_1 - 1\}$ and $b, b' \in \{0, \ldots, d_0 - 1\}$ is only possible when $(a,b) = (a',b')$, each ϵ_{a+bn_1} occurs only once in the expression. Hence the linear combination can be zero only if every term $d^{-1}\lambda_{ab}\epsilon_{a+bn_1}$ is zero, i.e. $d \mid \lambda_{ab}$, i.e. $\lambda_{ab}\Delta_{ab} = 0$.

Since every Δ_{ab} has order d, we conclude that

$$\mathrm{Ker}_\Sigma(d) = \bigoplus_{\substack{a \in \{0, \ldots, n_1-1\} \\ b \in \{1, \ldots, d_0-1\}}} \langle \Delta_{ab} \rangle \cong \mathbb{Z}^{n-n_1},$$

where the equality (instead of a containment) follows from the equality of the respective sizes.
Similarly, the set

$$B = \{\Delta_{ab} - b\Delta_{01} \mid 0 \leq a \leq n_1 - 1, 1 \leq b \leq d_0 - 1, (a,b) \neq (0,1)\} \cup \{d_0\Delta_{01}\}$$

spans $\mathrm{Ker}_S(d)$: according to Theorem 2.5, every element of B is contained in $S(n,d)$, and their independence easily follows from the independence of $\mathcal{B}$; a counting argument similar to the one above shows that they span the entire kernel. $\square$

10

In what follows we need a few simple properties of finite abelian groups. The first of these is a straightforward consequence of the uniqueness of decomposition of finite abelian groups into cyclic groups of prime power order.

Proposition 4.3. Let G, H, K be finite abelian groups. If $G \oplus K \cong H \oplus K$, then $G \cong H$. $\quad\square$

The next result are needed when we deal with invariant factors of a group. Recall that as a consequence of the uniqueness of the Smith Normal Form, every abelian group G also has a unique decomposition $G \cong \mathbb{Z}_{s_1} \oplus \cdots \oplus \mathbb{Z}_{s_r}$ with $1 < s_1 | \cdots | s_r$. We refer to $s_1, \ldots, s_r$ as the *invariant factors* of G.

Theorem 4.4. (i) We have that $\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{(m,n)} \oplus \mathbb{Z}_{[m,n]}$, where (m, n) and $[m, n]$ denote the greatest common divisor (gcd) and the least common multiple (lcm) of m and n.
(ii) If G has invariant factors $s_1, \ldots, s_r$, then $G \oplus \mathbb{Z}_m$ has invariant factors $s_1', \ldots, s_{r+1}'$ with $s_1' = (s_1, m)$, $s_i' = (s_i, [s_{i-1}, m])$ for $2 \leq i \leq r$, and $s_{r+1}' = [s_r, m]$, or invariant factors $s_2', \ldots, s_{r+1}'$ if $s_1' = (s_1, m) = 1$.

Proof. Part (i) is trivial, it follows immediately from the decomposition of $\mathbb{Z}_m$ and $\mathbb{Z}_n$ into their prime power summands. Part (ii) follows from part (i) and induction on r: we have that

$$\mathbb{Z}_{s_1} \oplus \cdots \oplus \mathbb{Z}_{s_r} \oplus \mathbb{Z}_m \cong \mathbb{Z}_{s_1'} \oplus \cdots \oplus \mathbb{Z}_{s_{r-1}'} \oplus \mathbb{Z}_{[s_{r-1}, m]} \oplus \mathbb{Z}_{s_r} \cong \mathbb{Z}_{s_1'} \oplus \cdots \oplus \mathbb{Z}_{s_{r-1}'} \oplus \mathbb{Z}_{s_r'} \oplus \mathbb{Z}_{s_{r+1}'}, \quad (10)$$

where we have used part (i) and the fact that $s_{r-1} | s_r$. Since $s_1' | \cdots | s_{r+1}'$ and $1 < s_1 | s_2'$, the invariant factors of $G \oplus \mathbb{Z}_m$ are $s_1', \ldots, s_{r+1}'$, or $s_2', \ldots, s_{r+1}'$ in case that $s_1' = (s_1, m) = 1$. $\quad\square$

We also require the following simple lemma.

Lemma 4.5. Let G be an abelian group, and let d, m be two positive integers. Let d' denote the maximal divisor of d for which $(d', m) = 1$. If $\mathbb{Z}_m$ is a direct summand of dG, then $\mathbb{Z}_{md/d'}$ is a direct summand of G. In particular, if $d | m$, then $\mathbb{Z}_{md}$ is a direct summand of G.

Proof. Consider a decomposition of G into cyclic groups of prime-power order. If $\mathbb{Z}_{p^t}$ is a direct summand of G and if $p^s || d$, then $d\mathbb{Z}_{p^t} = \mathbb{Z}_{p^t/(d,p^t)} = \mathbb{Z}_{p^{max(0,t-s)}}$ is the corresponding direct summand in dG. Therefore, if $p^r || m$, then the direct summand $\mathbb{Z}_{p^r}$ of $\mathbb{Z}_m \leq dG$ can only arise from a direct summand $\mathbb{Z}_{p^{r+s}}$ of G, i.e. the required direct summand of $\mathbb{Z}_{md/d'}$. $\quad\square$

Let $\delta = d_0 \cdots d_{k-1}$ and write $m = n_k$. Then $n = \delta m$ with $(\delta, m) = 1$. The Chinese Remainder Theorem (CRT) decomposition $\mathbb{Z}_n = \mathbb{Z}_\delta \oplus \mathbb{Z}_m$ induces a corresponding decompositions for the sand dune and sandpile groups.

Lemma 4.6. We have that
$$\Sigma(n, d) \cong \Sigma_0(n, d) \oplus \Sigma(m, d)$$

and

$$S(n, d) \cong S_0(n, d) \oplus S(m, d),$$

where $\Sigma_0(n, d) = \mathrm{Ker}_\Sigma(d^k)$ and $S_0(n, d) = \mathrm{Ker}_S(d^k)$ are the kernel of the map $x \mapsto d^k x$ on $\Sigma(n, d)$ and $S(n, d)$, respectively.

Proof. Since $n = \delta m$ with $(\delta, m) = 1$, by the CRT there are integers χ and η such that $\chi\delta$ and μm are mutually orthogonal idempotents, that is, $\chi\delta \equiv 1 \bmod m$ and $\mu m \equiv 1 \bmod \delta$. As a consequence, for each $v \in \mathbb{Z}_n$ we have $v = (v\mu m) + (v\chi\delta)$, and it is easily seen that the map $v \mapsto (v\mu m, v\chi\delta)$ induces a decomposition $\mathbb{Z}_n \cong \mathbb{Z}_\delta \oplus \mathbb{Z}_m$. Then we can write

$$e_v = (e_{v\chi\delta+v\mu m} - e_{v\chi\delta}) + e_{v\chi\delta},$$

and it is easily verified that the map

$$e_v \mapsto (e_{v\chi\delta+v\mu m} - e_{v\chi\delta}, e_{v\chi\delta})$$

induces a decomposition

$$\Sigma(n, d) \cong \Sigma_0(n, d) \oplus \Sigma(m, d),$$

where $\Sigma_0(n, d)$ denotes the subgroup generated by the elements $e_{v\chi\delta+v\mu m} - e_{v\chi\delta}$ for $v \in \mathbb{Z}_n$. Now $(d, m) = 1$, so the map $x \mapsto dx$ acts as a permutation on $\mathbb{Z}_m$; since $de_v = e_{dv}$ on $\Sigma(n, d)$, we conclude that $d\Sigma(m, d) \cong \Sigma(m, d)$. Next, since

$$\delta e_{v\chi\delta+v\mu m} = e_{v\chi\delta^2+v\mu m\delta} = e_{v\chi\delta^2} = \delta e_{v\chi\delta},$$

we have that $\delta(e_{v\chi\delta+v\mu m} - e_{v\chi\delta}) = 0$. Now $d_i = (d, n_i) | d$ for $i = 0, \ldots, k-1$, so that $\delta | d^k$. Combining these observations, we conclude that $\Sigma_0(n, d) = \mathrm{Ker}_{\sigma(n,d)}(d^k)$.

By Theorem 2.5, the element $a = \sum_{v \geq 0}^{n-1} a_v e_v \in S(n, d)$ iff $\chi := \sum_{v \geq 0} n - 1va_v \equiv 0 \bmod n$, which by CRT is the case if and only if χ is 0 both modulo δ and modulo m. Therefore, $a \in S(n, d)$ iff both projections $\sum_v a_v(e_{v\chi\delta+v\mu m} - e_{v\chi g})$ and $\sum_v a_v e_{v\chi\delta}$ are in $S(n, d)$. It follows that the above decomposition for $\Sigma(n, d)$ induces a similar decomposition for $S(n, d)$. $\square$

We now use the multiplication-by-d map to inductively determine the parts $\Sigma_0(n, d)$ and $S_0(n, d)$.

Theorem 4.7. Let n have d-sequence $n = n_0, n_1, \ldots, n_k = n_{k+1}$, with $d_i = n_i/n_{i+1} = (n_i, d)$ for $i = 0, \ldots, k$. Then

$$\Sigma_0(n, d) \cong \bigoplus_{i=0}^{k-1} \mathbb{Z}_{d^{i+1}}^{n_i - 2n_{i+1} + n_{i+2}}$$

and

$$S_0(n, d) \cong \bigoplus_{i=0}^{k-1} \left(\mathbb{Z}_{d^{i+1}/d_i} \oplus \mathbb{Z}_{d^{i+1}}^{n_i - 2n_{i+1} + n_{i+2} - 1} \right).$$

Proof. We use induction on k. If $k = 0$, then there is nothing to prove. Now, suppose that $k \geq 1$. By Theorem 4.1, we have $d\Sigma_0(n, d) \cong \Sigma_0(n_1, d)$. Since n_1 has d-sequence $(n_1, n_2, \ldots, n_k)$, by induction and by Lemma 4.5, we conclude that $\Sigma_0(n, d)$ is of the form

$$\Sigma_0(n, d) \cong \Lambda \oplus \bigoplus_{i=1}^{k-1} \mathbb{Z}_{d^{i+1}}^{n_i - 2n_{i+1} + n_{i+2}}$$

with $\Lambda \subseteq \mathrm{Ker}_\Sigma(d)$. Hence $\mathrm{Ker}_\Sigma(d) = \mathrm{Ker}_{\Sigma_0}(d) = \Lambda \oplus \mathbb{Z}_d^{n_1 - n_2}$ (to see this, note that $n_i - 2n_{i+1} + n_{i+2} = (n_i - n_{i+1}) - (n_{i+1} - n_{i+2})$ for all i and $n_k - n_{k+1} = 0$). So by Theorem 4.2 and Proposition 4.3, we have that $\Lambda \cong \mathbb{Z}_d^{(n-n_1)-(n_1-n_2)}$, as was to be proved.

12

Similarly, again using Lemma 4.5, we can conclude that

$$
S_0(n,d) \cong L \oplus \mathbb{Z}_{d^2}^{n_1 - 2n_2 + n_3 - 1} \oplus \bigoplus_{i=2}^{k-1} \left(\mathbb{Z}_{d^{i+1}/d_i} \oplus \mathbb{Z}_{d^{i+1}}^{n_i - 2n_{i+1} + n_{i+2} - 1} \right),
$$

where

$$
dL = \mathbb{Z}_{d/d_1}. \tag{11}
$$

From this expression, we read off that $\mathrm{Ker}_S(d) = \mathrm{Ker}_{S_0}(d) = \mathrm{Ker}_L(d) \oplus \mathbb{Z}_d^{n-n_1-1}$, hence by Theorem 4.2 and Proposition 4.3, we conclude that

$$
\mathrm{Ker}_L(d) = \mathbb{Z}_{d/d_0} \oplus \mathbb{Z}_d^{n-2n_1+n_2}. \tag{12}
$$

Suppose that L has invariant-factor decomposition

$$
L = \mathbb{Z}_{s_0} \oplus \cdots \oplus \mathbb{Z}_{s_r}
$$

with $s_0 | \cdots | s_r$. Then from (11) and (12), we conclude that

$$
\mathbb{Z}_{s_0/(s_0,d)} \oplus \cdots \oplus \mathbb{Z}_{s_r/(s_r,d)} = \mathbb{Z}_{d/d_1} \tag{13}
$$

and

$$
\mathbb{Z}_{(s_0,d)} \oplus \cdots \oplus \mathbb{Z}_{(s_r,d)} = \mathbb{Z}_{d/d_0} \oplus \mathbb{Z}_d^{n-2n_1+n_2}. \tag{14}
$$

Since $(s_i,d)|(s_{i+1},d)$ for $i = 0, \ldots, r-1$ and $(d/d_0)|d$, both direct sums in (14) are invariant-factor decompositions. Hence $(s_0,d) = d/d_0$ and $(s_i,d) = d$ for $i = 1, \ldots, r$. So we can write $s_0 = \tau d/d_0$ for some τ with $(\tau, d_0) = 1$ and $s_i = \sigma_i d$ for $i = 1, \ldots, r$, where $\sigma_1 | \cdots | \sigma_r$ and $\tau | \sigma_1 d_0$, so that $\tau | \sigma_1$. Moreover, from (13), we conclude that

$$
\mathbb{Z}_\tau \oplus \mathbb{Z}_{\sigma_1} \oplus \cdots \oplus \mathbb{Z}_{\sigma_r} = \mathbb{Z}_{d/d_1}.
$$

Now, using Theorem 4.4, we conclude that the left-hand side above has invariant factors (σ_1, τ), $(\sigma_{i+1}, [\sigma_i, \tau])$ for $i = 1, \ldots, r-1$, and $[\sigma_r, \tau]$, while the right-hand side has invariant factors d/d_1. Since the invariant factors are unique, we conclude that $(\sigma_1, \tau) = 1$ and $(\sigma_{i+1}, [\sigma_i, \tau]) = 1$ for $i = 1, \ldots, r-1$, while $[\sigma_r, \tau] = d/d_1$. Since $\sigma_i = (\sigma_{i+1}, \sigma_i)|(\sigma_{i+1}, [\sigma_i, \tau])$, we conclude that $\sigma_1 = \ldots = \sigma_{r-1} = 1$ and $(\sigma_r, \tau) = 1$, while $[\sigma_r, \tau] = \sigma_r \tau = d/d_1$. Since $\tau | \sigma_1 | \sigma_r$, we conclude that $\tau = 1$ and $\sigma_r = d/d_1$, hence $L = \mathbb{Z}_{d/d_0} \oplus \mathbb{Z}_d^{n-2n_1+n_2-1} \oplus \mathbb{Z}_{d^2/d_1}$, which is what we wanted to prove. $\qquad\square$

4.1 Adaptations for the case of generalized Kautz graphs

With minor adaptations, all the results in this section are also valid when $d < 0$, so for the sand dune group $\Sigma(n,d)$ and sandpile group $S(n,d)$ of the generalized Kautz graph $\mathrm{Ktz}(n,|d|)$. Like before, write $n_1 = n/(n,|d|)$ and $d_0 = (n,|d|)$. Using multiplication by d, we conclude in a similar way that $d\Sigma(n,d) \cong \Sigma(n_1,d)$ and $dS(n,d) \cong S(n_1,d)$, and also that $\mathrm{Ker}_\Sigma(d) \cong \mathbb{Z}_d^{n-n_1}$ and $\mathrm{Ker}_S(d) \cong \mathbb{Z}_{|d|/d_0} \oplus \mathbb{Z}_{|d|}^{n-n_1-1}$. And finally, we can use these facts to determine $\Sigma_0(n,d)$ and $S_0(n,d)$ in a similar way.

5 The sand dune and sandpile group in the relatively prime case

In this section, we determine the sand dune group $\Sigma(m, d)$ and the sandpile group $S(m, d)$ for fixed positive integers m and d with $(m, d) = 1$. In that case, the map $x \mapsto dx$ partitions $\mathbb{Z}_m$ into orbits of the form

$$O(v) = \{v, dv, \ldots, d^{e-1}v\},$$

where $d^e v \equiv v \bmod m$ and $d^i v \not\equiv d \bmod m$ for $1 \leq i < e$. Recall that we refer to $o(v) = |O(v)|$ as the *order* of v, and that $\mathcal{V}$ denotes a complete set of representatives of the orbits different from $\{0\}$, that is, $\mathcal{V}$ contains precisely one element from each orbit different from $\{0\}$. Recall that for p a prime, $\pi_p(v)$ denote the largest power of p dividing v. For the remainder of this section, we let

$$\mathbb{P} = \{p \mid p \text{ is a prime and } p|m\},$$

and write

$$M_p = m/\pi_p(m), \qquad p \in \mathbb{P}.$$

For later use, we define

$$\mathcal{V}^* = \{1 \leq v \leq m \mid v \equiv p^i M_p \bmod m \text{ for some } p \in \mathbb{P} \text{ and some integer } i \geq 0\}.$$

Since $(d, m) = 1$, it is easily seen that for $p, q \in \mathbb{P}$, if $p^i M_p \equiv d^k q^j M_q \bmod m$ then $p = q$ and $i = j$. Thus the elements in $\mathcal{V}^*$ are in different orbits on $\mathbb{Z}_m$. (Another way to see this is to note that every divisor $k|m$ is minimal in its orbit, which is contained in $d\mathbb{Z}_m$.)

For the remainder of this section, we assume that the set $\mathcal{V}$ of orbit representatives contains all the members of $\mathcal{V}^*$.

The determination of the sand dune group is easy.

Theorem 5.1. With the above notation, we have that $\Sigma(m, d) = \bigoplus_{v \in \mathcal{V}} \mathbb{Z}_{d^{o(v)}-1}$.

Proof. By Lemma 2.10, the expression for e_v in terms of the ϵ_w involves only ϵ_w with $w \in O(v)$. Hence the e_v with $v \in \mathcal{V}$ are independent. Moreover, since $d^i e_v = e_{d^i v}$, the subgroup $\langle e_v \rangle$ generated by e_v contains every e_w with $w \in O(v)$, so $\Sigma(m, d) = \oplus_{v \in \mathcal{V}} \langle e_v \rangle$, According to Corollary 2.11, the order of e_v is equal to $d^{o(v)} - 1$, so $\langle e_v \rangle \cong \mathbb{Z}_{d^{o(v)}-1}$, from which the theorem follows. $\square$

Remark 5.2. Aa alternative way to see the above result is to remark that the matrix $\Sigma = \Sigma^{(m,d)}$ is equivalent to a block-diagonal matrix with $|\mathcal{V}|$ blocks Σ_v ($v \in \mathcal{V}$), where the block Σ_v is the restriction of Σ to the rows and columns indexed by orbit $O(v)$; moreover, if within an orbit $O(v)$ we index in the order $v, dv, \ldots, d^{o(v)-1}v$, then Σ_v is $o(v) \times o(v)$ and of the form

$$\Sigma_v = \begin{pmatrix} d & -1 & 0 & \cdots & 0 \\ 0 & d & -1 & \cdots & 0 \\ & \ddots & \ddots & \ddots & \\ 0 & & 0 & d & -1 \\ -1 & 0 & & 0 & d \end{pmatrix}.$$

Now it is easy to see that Σ_v has invariant factors $(1, \ldots, 1, d^{o(v)} - 1)$, for example, by successively adding d times the first row to the second row, then d times the current second row to the

third row, ..., and finally d times the then current $(o(v) - 1)$th row to the last row, and then subtracting from the first column a suitable linear combination of the other columns.

As explained in Section 3, it is a bit more complicated to determine the structure of $S(m, d)$. First, we define the modified generators $\tilde{e}_v$ for $\Sigma(m, d)$. To this end, we need some preparation. Let $p \in \mathbb{P}$. Since $\pi_p(m)$ and $M_p = m/\pi_p(m)$ are relatively prime, there is a number η_p such that

$$\eta_p M_p \equiv 1 \bmod \pi_p(m).$$

Define

$$\lambda_p(v) = \eta_p v / \pi_p(v),$$

and for $v \in \mathcal{V} \setminus \mathcal{V}^*$, put

$$\tilde{e}_v = e_v - \sum_{p|m} \lambda_p(v) e_{\pi_p(v) M_p}.$$

Theorem 5.3. For $v \in \mathcal{V} \setminus \mathcal{V}^*$, let $\tilde{e}_v$ be defined as above. Then $\tilde{e}_v$ is contained in $S(m, d)$, and $\tilde{e}_v$ and e_v have the same the order in $S(m, d)$. Moreover, the $\tilde{e}_v$ for $v \in \mathcal{V} \setminus \mathcal{V}^*$ together with the e_v for $v \in \mathcal{V}^*$ are independent and generate $\Sigma(m, d)$.

Proof. To show that $\tilde{e}_v \in S(m, d)$, we use Theorem 2.5. For a fixed prime $q \in \mathbb{P}$, the numbers $M_p = m/\pi_p(m)$ with $p \in \mathbb{P} \setminus \{q\}$ are divisible by $\pi_q(n)$, so that modulo $\pi_q(v)$, we have

$$v - \sum_{p|m} \lambda_p(v) \pi_p(v) M_p \equiv v - \lambda_q(v) \pi_q(v) M_q \equiv v - \eta_q(v/\pi_q(v)) \pi_q(v) M_q \equiv 0 \bmod \pi_q(v).$$

Since this holds for every $q \in \mathbb{P}$, by the Chinese Remainder Theorem we have that $v - \sum_{p|m} \pi_p(v) \pi_p(v) m/\pi_p \equiv 0 \bmod m$, hence by Theorem 2.5, $\tilde{e}_v$ is in $S(m, d)$.

Next, recall that by Corollary 2.11, e_v has order $d^{o(v)} - 1$. To show that $\tilde{e}_v$ has order $d^{o(v)} - 1$, it is sufficient to show that $(d^{o(v)} - 1) e_{\pi_p(v) m/\pi_p(m)} = 0$ holds for every $p \in \mathbb{P}$. To see this, we proceed as follows. By the definition of $o(v)$, we have that $(d^{o(v)} - 1)v \equiv 0 \bmod m$, hence $(d^{o(v)} - 1)\pi_p(v) \equiv 0 \bmod \pi_p(m)$, and therefore $(d^{o(v)} - 1)\pi_p(v) m/\pi_p(m) \equiv 0 \bmod m$. So the order of $e_{\pi_p(v) M_p}$ divides $d^{o(v)} - 1$, and now the desired conclusion follows from the equality $d^{o(v)} e_{\pi_p(v) M_p} = e_{d^{o(v)} \pi_p(v) M_p}$.

Finally, by the definition of $\mathcal{V}^*$, it is obvious that the $\tilde{e}_v$ for $v \in \mathcal{V} \setminus \mathcal{V}^*$ together with the e_v for $v \in \mathcal{V}^*$ have the same span as the e_v for $v \in \mathcal{V}$, from which the claim follows immediately. $\square$

So now we are left with the choice of suitable elements $\tilde{e}_v$ for $v \in \mathcal{V}^*$. First, we need a simple number-theoretic result. For a prime p, let $\nu_p(n)$ denote the largest integer $e \geq 0$ for which $p^e | n$. We say that an integer d has *order e modulo p* if e is the smallest positive integer for which $p|d^e - 1$.

Lemma 5.4. For a prime p, with $(p, d) = 1$, let d have order e modulo p, and suppose that $\nu_p(d^e - 1) = a$. Then d has order ep^i modulo p^{a+i} for all $i \geq 0$, except when $p = 2$ and $d \equiv 3 \bmod 4$. In that exceptional case, $e = 1$ and $a = 1$, and if $\nu_2(d^2 - 1) = b$, then $b \geq 3$ and d has order 2^{i+1} modulo 2^{b+i} for all $i \geq 0$ (and order 1 modulo 2^i for $1 \leq i < b$).

Proof. For an integer $t \geq 1$, if d has order f mod p^t, then $p^t | d^n - 1$ if and only if $f | n$. So the order of d modulo p^{t+1} is of the form kf. Moreover, if $\nu_p(d^f - 1) = s \geq t$, then $d^f = 1 + qp^s$ for some integer q not divisible by p, so

$$d^{rf} = (1 + qp^s)^r \equiv 1 + rqp^s \bmod p^{2s};$$

hence for every integer $k \geq 1$,

$$d^{kf} - 1 = (d^f - 1)(1 + d^f + \cdots + d^{(k-1)f}) \equiv k + qp^a(0 + 1 + \cdots + (k-1)) \equiv qp^s \left(k + qp^s \binom{k}{2} \right) \bmod p^{3s}.$$

So the smallest $k > 1$ for which $p^{s+1} | d^{kf} - 1$ is $k = p$, in which case

$$d^{pf} - 1 \equiv qp^{s+1}(1 + qp^{s-1}\binom{p}{2}) \bmod p^{3s}.$$

Moreover, we see that $\nu_p(d^{pf} - 1) = s + 1$, except when $s = 1$ and $p = 2$. In that case, q is odd and $8 | d^{2e} - 1$, and $d \equiv 3 \bmod 4$ since $s = 1$. So we conclude that there is a "jump" in the order of d modulo powers p^s of p if and only if $s = 1$, $p = 2$, and $d \equiv 3 \bmod 4$, as claimed in the theorem. $\qquad \square$

Corollary 5.5. If $p \neq 2$ or $d \equiv 1 \bmod 4$, then $\nu_p(d^{o(M_p)} - 1) - \nu_p(d^{o(p^t M_p)} - 1) \leq t$ for $1 \leq t \leq \pi_p(m) - 1$. Otherwise, i.e. for $p = 2$ and $d \equiv 3 \bmod 4$, we have that $\nu_p(d^{o(M_p)} - 1) - \nu_p(d^{o(p^t M_p)} - 1) \leq t$ for $1 \leq t \leq \pi_p(m) - 2$.

Proof. Let $p \in \mathbb{P}$, and write $s = \nu_p(m)$, so that $M_p = m/p^s$. First we claim that the order of d modulo p^{s-t} is equal to $o(p^t M_p)$. To see this, note that by definition, $o(p^t M_p)$ is the smallest integer $e \geq 1$ for which $(d^e - 1)p^t M_p \equiv 0 \bmod m$, or, equivalently, for which $(d^e - 1)p^t \equiv 0 \bmod p^s$, from which the claim follows.

Now suppose that $o(p^{s-1}M_p) = e$ and $\nu_p(d^e - 1) = a$. Then we see from Lemma 5.4 that in the "non-exceptional" case, where $p \neq 2$ or $d \equiv 1 \bmod 4$, we have that $\nu_p(d^{ep^i} - 1) = a + i$ for all $i \geq 0$, so as a consequence of our claim, for $s - a \leq t \leq s - 1$, the order $o(p^t M_p)$ is still equal to e, with $\nu_p(d^{o(p^t M_p)} - 1) = \nu_p(d^e - 1) = a$, and for $t = s - a - i$ with $i \geq 1$, the order $o(p^t M_p)$ is equal to ep^i, with $\nu_p(d^{o(p^t M_p)} - 1) = \nu_p(d^{ep^i} - 1) = a + i$. This proves the result in the "non-exceptional" case.

In the "exceptional" case where $p = 2$ and $d \equiv 3 \bmod 4$, we have $e = 1$ and $a = 1$, and according to Lemma 5.4, for some integer $b \geq 3$ we have that $\nu_2(d^{2+i} - 1) = b + i$ for all $i \geq 0$. So as a consequence of our claim, $o(p^{s-2}M_2) = b$ and $\nu_2(d^2 - 1) = b$; then for $s - b \leq t \leq s - 3$, the order $o(2^t M_2)$ is still equal to b, with $\nu_2(d^{o(2^t M_2)} - 1) = \nu_2(d^2 - 1) = b$, and for $t = s - b - i$ with $i \geq 1$, the order $o(2^t M_2)$ is equal to $e2^i$, with $\nu_2(d^{o(2^t M_2)} - 1) = \nu_2(d^{e2^i} - 1) = b + i$. This proves the result in the "exceptional" case. $\qquad \square$

Now we are ready to define the $\tilde{e}_v$ in the cases where $v \in \mathcal{V}^*$, that is, when v is of the form $p^t M_p$ for some $p \in \mathbb{P}$ with $0 \leq t < \nu_p(m)$. In the "non-exceptional case", i.e. for p odd, or $p = 2$ and $d \equiv 1 \bmod 4$, and also for $4 \nmid m$, we let

$$\tilde{e}_{M_p} = \tilde{e}_{m/\pi_p(m)} = \pi_p(m)e_{M_p},$$

16

and for $1 \leq t < \nu_p(m)$, we let

$$\tilde{e}_{p^t M_p} = e_{p^t M_p} - \lambda_{p,t} e_{M_p},$$

where $\lambda_{p,t}$ is such that

$$\lambda_{p,t} = \frac{d^{o(M_p)} - 1}{d^{o(p^t M_p)} - 1} \mu_{p,t} \equiv p^t \bmod \pi_p(m) \tag{15}$$

for some suitable integer $\mu_{p,t}$. (We will show in a moment that this is indeed possible.) In the "exceptional case" where $p = 2$ and $d \equiv 3 \bmod 4$ and when also $4|m$, we we do not change the definition of $\tilde{e}_{p^t M_2}$ for $t = 1, \ldots, \pi_2(m) - 2$, but we let

$$\tilde{e}_{M_2} = e_{2^{s-1} M_2} - 2^{s-1} e_{M_2}, \qquad \tilde{e}_{2^{s-1} M_2} = \tilde{e}_{m/2} = 2 e_{2^{s-1} M_2}, \tag{16}$$

where $s = \pi_2(m)$.

Theorem 5.6. For $v \in \mathcal{V}^*$, let $\tilde{e}_v$ be defined as above. Then $\tilde{e}_v \in S(m, d)$. Moreover, $\tilde{e}_v$ and e_v have the same the order in $S(m, d)$, except in the following two cases.

    1. In the "non-exceptional" case where $p \in \mathbb{P}$ with $p \neq 2$ or $d \equiv 1 \bmod 4$, and also when $4 \nmid m$, the order of $\tilde{e}_{M_p} = \pi_p(m) e_{M_p}$ is $1/\pi_p(m)$ times the order of e_{M_p}.

    2. In the "exceptional" case where $p = 2$ and $d \equiv 3 \bmod 4$, if also $4|m$ then the order of $\tilde{e}_{m/2}$ is half the order of $e_{m/2}$ and the order of $\tilde{e}_{M_2}$ is $2/\pi_2(m)$ times the order of e_{M_2}.

    Finally, the $\tilde{e}_v$ for $v \in \mathcal{V}$ are independent and generate $S(m, d)$, and Theorem 3.1 holds.

Proof. We begin by showing that the $\tilde{e}_{p^t M_p}$ with $1 \leq t \leq \pi_p(v) - 1$ are well-defined. To this end, first observe that by definition of the order, we have that $o(\lambda v)|o(v)$, and hence $d^{o(\lambda v)} - 1$ divides $d^{o(v)} - 1$. So the fraction in (15) is an integer, and as a consequence of Corollary 5.5, in all relevant cases the exponent of the highest power of $p \in \mathbb{P}$ dividing this integer is at most t, so that an integer $\mu_{p,t}$ for which (15) holds indeed can be found.

    Next, Theorem 2.5 states that $\tilde{e}_{p^t M_p} - \lambda_{p,t} e_{M_p}$ is in $S(m, d)$ if and only if $p^t M_p - \lambda_{p,t} M_p \equiv 0 \bmod m$, or, equivalently, if $p^t \equiv \lambda_{p,t} \bmod m$, which holds since it is just the second requirement in (15). By the same theorem, obviously $\tilde{e}_{M_p} = \pi_p(m) e_{M_p}$ is also in $S(m, d)$, and the same holds for $\tilde{e}_{M_2}$ and $\tilde{e}_{m/2}$ as defined in (16).

    Then, we observe that $\tilde{e}_{p^t M_p} = e_{p^t M_p} - e_{M_p}$ and $e_{p^t M_p}$ have the same order if and only if $(d^{o(p^t M_p)} - 1)\lambda_{p,t} e_{M_p} = 0$, or, equivalently, if $d^{o(M_p)} - 1$ divides $(d^{o(p^t M_p)} - 1)\lambda_{p,t}$; this holds since it is just the first requirement in (15). Also, since $\pi_p(m)$ divides the order $d^{o(M_p)} - 1$ of e_{M_p} for $p \in \mathbb{P}$, we immediately have that $\pi_p(m) \tilde{e}_{M_p}$ has the order as claimed. Now consider the exceptional case where $p = 2$, $d \equiv 3 \bmod 4$ and $4|m$. Since $e_{m/2}$ has order $d - 1$, which is $2 \bmod 4$, the order of $\tilde{e}_{m/2}$ is as claimed. Now let $s = \nu_2(m)$. To determine the order of $\tilde{e}_{M_2}$, we first note that e_{M_2} has order $d^f - 1$, where f is the order of d modulo 2^s. Hence $2^{s-1} e_{M_2}$ has order $(d^f - 1)/2^{s-1}$. We claim that $\tilde{e}_{M_2}$ has the same order. To show this, it is sufficient to show that the order $d - 1$ of $e_{m/2}$ divides $(d^f - 1)/2^{s-1}$. To this end, note that both $(d - 1)/2$ and 2^s divide $d^f - 1$; since $d \equiv 3 \bmod 4$, we know that $(d - 1)/2$ is odd. Hence $((d - 1)/2, 2^s) = 1$, from which the conclusion follows.

    Finally, it is fairly obvious that the $\tilde{e}_{p^t M_p}$ for $p \in \mathbb{P}$ and $1 \leq t \leq \nu_p(m) - 2$ together with e_{M_p} and $e_{m/p}$ $p \in \mathbb{P}$ are independent and generate the same subgroup as the e_v for $v \in \mathcal{V}^*$. Applying Theorem 5.3, we conclude that the $\tilde{e}_v$ for $v \in \mathcal{V}$ are independent, and thus form a basis of a subgroup of $S(m, d)$. From the expressions for the orders derived above, we conclude

17

that this subgroup has order $|\Sigma(m,d)|/m$; now from Corollary 2.6 we see that in fact the $\tilde{e}_v$ with $v \in \mathcal{V}$ generate $S(m,d)$. So $S(m,d) = \bigoplus_{v \in \mathcal{V}} \langle \tilde{e}_v \rangle$, and now Theorem 3.1 follows from the order expressions. $\qquad \square$

5.1 Adaptations for the case of generalized Kautz graphs

Essentially, the above analysis for the case of the generalized de Bruijn graphs only depends on the orbits of the map $x \mapsto dx$ on $\mathbb{Z}_m \setminus \{0\}$ and the order of d modulo powers of p. Thus, similar results hold when $d < 0$; the only difference is that relevant group elements g now have orders of the form $|d^e - 1|/c$, so that the group $\langle g \rangle$ is isomorphic to $\mathbb{Z}_{|d^e-1|/c}$. We leave the details for the interested reader.

6 The group of invertible circulant matrices

In [14] it was shown that a family of bijections between the set of aperiodic necklaces of length n over the finite field $\mathbb{F}_q$, with q prime, and the set of degree n normal polynomials over $\mathbb{F}_q$, gives rise to a permutation group on any of these sets. This group turns out to be isomorphic to $C(n,q)$; as well, [14] conjectured a relation of $C(n,q)$ and $S(n,q)$. The present work confirms this relation[1] with the sandpile group $S(n,q)$ of DB(n,q). We show that indeed $C'(n,q)/\langle x \rangle$ is isomorphic to $S(n,q)$ for all n and all primes q, and also for all prime powers q provided that $(n,q) = 1$, by explicitly computing a decomposition into cyclic subgroups. While the case $(n,q) = 1$ appears to be well-understood, we did not find an explict reference in the literature. The general case is harder, and the only relevant reference we found was the case $n = 2^k$, $p = 2$ dealt with in [3, Prop. XI.5.7].

In what follows, we use the description for $C'(n,q)$ as given in (3).

Theorem 6.1. Let q be a prime power, and let m be a positive integer with $(m,q) = 1$. Then

$$C'(m,q) \cong \Sigma(m,q)$$

and

$$C'(m,q)/\langle x \rangle \cong S(m,q). \tag{17}$$

Example 6.2. We remark that the condition $(m,q) = 1$ (respectively $(n,d) = 1$) is necessary in Theorem 6.1 (respectvely in Theorem 3.2). Indeed, one may check directly that $C'(9,9)/\langle x \rangle \cong \mathbb{Z}_9^4 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_3^3$, while $S(9,9) \cong \mathbb{Z}_9^7$.

Proof. Let $\mathcal{V}$ be defined as in the beginning of Section 5, so that $\mathcal{V}^+ = \mathcal{V} \cup \{0\}$ is a complete set of orbit representatives for the map $x \mapsto qx$ on $\mathbf{Z}_m$ containing the set $\mathcal{V}^*$ of all numbers of the form $p^i M_p$ for a prime $p \in \mathbb{P}$, with $M_p = m/\pi_p(m)$. (Refer to the beginning of Section 5 for definitions of $\mathcal{V}^*$, M_p, and $\pi_p(m)$.) We write $o(v)$ to denote the size of the orbit of $v \in \mathcal{V}^+$. Next, let q have order k modulo q, so that $n | q^k - 1$, and let α be a primitive element of GF(q^k); put $\xi = \alpha^{(q^k-1)/n}$. For $v \in \mathcal{V}^+$, let $f_v(x)$ denote the minimal polynomial of ξ^v over $\mathbb{F}_q$; note

---

[1]In view of this relation, it would be desirable to have an explicit embedding of the group $S(n,q)$ as a subgroup of $C(n,q)$.

that $f_v(x) = \prod_{i=0}^{o(v)-1} (x - \xi^{q^i v})$ is $\mathbb{F}_q$-irreducible of degree $o(v)$. Then we can write $x^m - 1 = \prod_{v \in \mathcal{V}^+} f_v(x)$. Thus $C(m,q) \cong \prod_{v \in \mathcal{V}^+} (\mathbb{F}_q[x]/(f_v(x)))^*$ and

$$C'(m,q) \cong \prod_{v \in \mathcal{V}} (\mathbb{F}_q[x]/(f_v(x)))^* \cong \oplus_{v \in \mathcal{V}} \mathbb{F}^*_{q^{o(v)}} \cong \oplus_{v \in \mathcal{V}} \mathbb{Z}_{q^{o(v)}-1}.$$

Hence $C'(m,q) \cong \Sigma(m,q)$ by Theorem 5.1.

Next, we consider the quotient $C'(m,q)/\langle x \rangle$. The image of $x \bmod f_v(x)$ in $\mathbb{F}_{q^{o(v)}}$ is ξ^v; since ξ has order m, we see that x has order $m/(m,v)$ in $\mathbb{F}_{q^{o(v)}}$. Hence for each $v \in \mathcal{V}$, we can choose a primitive element β_v in $\mathbb{F}_{q^{o(v)}} \cong \mathbb{F}_q[x] \bmod f_v(x)$, so with β_v of order $q^{o(v)} - 1$, such that the image of x in $\mathbb{F}_{q^{o(v)}}$ is β^{r_v}, where

$$r_v = \frac{q^{o(v)} - 1}{m/(m,v)}; \tag{18}$$

as a consequence, we have that

$$G := C'(m,q)/\langle x \rangle \cong G = \langle \beta_v \mid v \in \mathcal{V}, \mathrm{ord}(\beta_v) = q^{o(v)} - 1 \; (v \in \mathcal{V}) \text{ and } \prod_{v \in \mathcal{V}} \beta_v^{r_v} = 1 \rangle. \tag{19}$$

To obtain the group structure of G in (19), we investigate the Sylow-p subgroup $G_p \leq G$ for each prime p. After some standard manipulations, i.e. writing $\beta_v = \prod_p \beta_{v,p}$ with $\mathrm{ord}(\beta_{v,p}) = \pi_p(q^{o(v)} - 1)$, then fixing a prime p and letting $\gamma_v = \beta_{v,p}$, we obtain that

$$G_p = \langle \gamma_v \mid v \in \mathcal{V}, \mathrm{ord}(\gamma_v) = \pi_p(q^{o(v)} - 1) \; (v \in \mathcal{V}) \text{ and } \prod_{v \in \mathcal{V}} \gamma_v^{s_v} = 1 \rangle,$$

where $s_v = \pi_p(r_v) = \pi_p((q^{o(v)} - 1)(v,m)/m)$ for all $v \in \mathcal{V}$. First, observe that if $p \nmid m$, then $s_v = \pi_p(q^{o(v)} - 1) = \mathrm{ord}(\gamma_v)$, and hence

$$G_p = \bigoplus_{v \in \mathcal{V}} \mathbb{Z}_{\pi_q(p^{o(v)}-1)}.$$

Now, let $p|m$. We need to determine for which $v \in \mathcal{V}$ the number s_v is minimal.

Claim 1: If $p|m$ and $\pi_p(v) = p^k$, then $s_v \geq s_{p^k M_p}$.

Indeed, first note that $p^k M_p(p^e - 1) \equiv 0 \bmod m$ precisely when $p^e - 1 \equiv 0 \bmod \pi_p(m)/p^k$. Then, writing $v = p^k w$ with $(p,w) = 1$, we see that $p^k w(p^e - 1) \equiv 0 \bmod m$ implies that $(p^e - 1) \equiv 0 \bmod \pi_p(m)/p^k$, and the claim is now obvious.

Claim 2: If $p \neq 2$ or $q \not\equiv 3 \bmod 4$ or $4 \nmid m$, then s_v is minimal for $v = M_p = m/\pi_p(m)$.

Indeed, if $p = 2$ and $4 \nmid m$, the claim follows immediately from claim 1. Otherwise, let $v_j = m/p^j$, and let $\lambda_j = \pi_p(q^{o(v_j)} - 1)$. As a consequence of Lemma 5.4, we have that

$$(\lambda_1, \lambda_2, \ldots) = (q^a, \ldots, q^a, q^{a+1}, q^{a+2}, \ldots),$$

where q^a occurs a times, for some $a \geq 1$. So, since $s_{v_j} = \lambda_j p^{-j}$, we see that s_{v_j} is minimal when j is as large as possible. Now the claim follows from claim 1.

To complete the determination of G_p in the non-exceptional case where $p \neq 2$ or $q \not\equiv 3 \bmod 4$, or when $4 \nmid m$, we proceed as follows. Define $\delta = \gamma_{M_p} \prod_{v \neq M_p} \gamma_v^{s_v/s_{M_p}}$. Note that δ has order

19

$s_{M_p} = \pi_p(q^{M_p} - 1)/\pi_p(m)$ in G_p. Obviously, δ and the γ_v with $v \neq M_p$ generate G_p, so we conclude that

$$G_p \leq \mathbb{Z}_{\pi_p(q^{o(M_p)}-1)/\pi_p(m)} \oplus \bigoplus_{v \in \mathcal{V}\setminus\{M_p\}} \mathbb{Z}_{\pi_p(q^{o(v)}-1)}.$$

Now consider the exceptional case where $p = 2$ and $q \equiv 3 \bmod 4$ and $4|m$. With the same notation as after claim 2, Lemma 5.4 now implies that

$$(\lambda_1, \lambda_2, \ldots) = (2, 2^b, \ldots, 2^b, 2^{b+1}, 2^{b+2}, \ldots),$$

where 2^b occurs $b - 1$ times, for some $b \geq 3$. So

$$(s_{v_1}, s_{v_2}, \ldots) = (1, 2^{b-2}, \ldots, 2, 1, 1, \ldots).$$

Since $v_1 = m/2$, we see that $s_{m/2} = 1$ and $o(m/2) = 1$, so $\mathrm{ord}(m/2) = \pi_2(q^{o(m/2)} - 1) = \pi_2(q - 1) = 2$. Also, note that $s_{M_2} = \pi_2(q^{o(M_2)} - 1)/\pi_2(m)$. Now define $\delta = \gamma_{M_2} \prod_{v \neq M_2, m/2} \gamma_v^{s_v/s_{M_2}}$. Then $\delta^{s_{M_2}} = \gamma_{m/2}^{-s_{m/2}} = \gamma_{m/2}$, and since $\mathrm{ord}(\gamma_{m/2}) = 2$, we conclude that δ has order $2s_{M_2}$. Also, since $s_{m/2} = 1$, $\gamma_{m/2}$ can be expressed in terms of elements γ_v with $v \neq m/2$. It is now easy to see that G_p is generated by δ and γ_v for $v \in \mathcal{V} \setminus \{M_2, m/2\}$, and since $\pi_2(q^{o(m/2)} - 1) = 2$, we conclude that in this case

$$G_2 \leq \mathbb{Z}_{\pi_p(q^{o(M_2)}-1)/\pi_2(m)} \oplus \mathbb{Z}_{(q^{o(m/2)}-1)/2} \oplus \bigoplus_{v \in \mathcal{V}\setminus\{M_2, m/2\}} \mathbb{Z}_{\pi_2(q^{o(v)}-1)}.$$

If we combine the information about the various Sylow p-subgroups, we may conclude from Theorem 3.1 that G is a subgroup of $S(m, q)$. Since $|G| = |C'(m, q)/\langle x \rangle| = |C'(m.q)|/m = |S(m, q)|$, we conclude that $G = S(m, q)$ as desired. $\qquad\square$

7 The group $C(n, p)$ for general n and prime p

We work with $C(n, p)$ as the group of invertible circulant matrices over $\mathbb{F}_p$ and with $C^*(n, p) \leq C(n, p)$ as the subgroup of marices with eigenvalue 1 on the eigenvector $(1, \ldots, 1)$.

We first compute the group decomposition of $C^*(n, p)$ and then proceed to compute the group decomposition of $C^*(n, p)/\langle Q_n \rangle$.

Lemma 7.1. Let p be prime and $(m, p) = 1$. Then

$$C^*(p^k m, p) = \left[\bigoplus_{i=0}^{k-2} \mathbb{Z}_{p^{k-1-i}}^{p^i(p-1)^2 m} \right] \oplus \mathbb{Z}_{p^k}^{(p-1)m} \oplus C^*(p, m).$$

Proof. Note that $\phi : C^*(pn, p) \to C^*(pn, p)$ given by $x \mapsto x^p$ is a well-defined homomorphism, as ϕ preserves both the determinant and the eigenvalue of the common eigenvector $(1, \ldots 1)$. It can be easily checked that $|\mathrm{Ker}(\phi)| = p^{(p-1)n}$.

It can be also easily checked that $(C^*(pn, p))^p$ is isomorphic to $C^*(n, p)$, via $\sum_{i=0}^{n-1} a_i Q_{pn}^{pi} \mapsto \sum_{i=0}^{n-1} a_i Q_n^i$. Hence ϕ can be viewed as surjective homomorphism from $C^*(pn, p)$ to $C^*(n, p)$.

We prove the lemma by using induction on k. It is easy to see that $C^*(pm, p) = \mathbb{Z}_p^{a_1} \oplus C^*(m, p)$ since $(C^*(pm, p))^p \simeq C^*(m, p)$. Since in this case $|\text{Ker}(\phi)| = p^{(p-1)m}$, we can conclude that $a_i = (p-1)m$ and the statement is true for $k = 1$.

By using the fact that $(C^*(p^{k+1}m, p))^p \simeq C^*(p^k m, p)$, by induction we conclude that

$$C^*(p^{k+1}m, p) = Z_p^{a_1} \oplus \left[\bigoplus_{i=0}^{k-2} \mathbb{Z}_{p^{k-i}}^{p^i(p-1)^2 m} \right] \oplus \mathbb{Z}_{p^{k+1}}^{(p-1)m} \oplus C^*(p, m).$$

It remains to find a_1. Note that when $n = p^{k+1}m$, we have

$$\text{Ker}(\phi) = Z_p^{a_1} \oplus \left[\bigoplus_{i=0}^{k-2} \mathbb{Z}_p^{p^i(p-1)^2 m} \right] \oplus \mathbb{Z}_p^{(p-1)m}.$$

Recall that $|\text{Ker}(\phi)| = p^{(p-1)p^k m}$. Thus we have two expressions for $|\text{Ker}(\phi)|$. Equating them, we have:

$$(p-1)p^k m = a_1 + \left[\sum_{i=0}^{k-2} p^i (p-1)^2 m \right] + (p-1)m,$$

$$(p-1)p^k m = a_1 + (p^{k-1} - 1)(p-1)m + (p-1)m,$$

$$a_1 = p^{k-1}(p-1)^2 m,$$

which completes the induction. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Finally, we complete the proof of Theorem 3.2. Let $d = p$ be prime, $n = p^k m$ and $(p, m) = 1$. Since $\langle Q_n \rangle$ is cyclic of order $p^k m$, its Sylow p-subgroup is Z_{p^k}. Combined with Lemma 7.1, this implies that the Sylow p-subgroup of the quotient group $C^*(n, p)/\langle Q_n \rangle$ equals

$$\text{Syl}_p(C^*(p^k m, p)/\langle Q_n \rangle) = \left[\bigoplus_{i=0}^{k-2} \mathbb{Z}_{p^{k-1-i}}^{p^i(p-1)^2 m} \right] \oplus \mathbb{Z}_{p^k}^{(p-1)m-1}.$$

By Lemma 4.6 and Theorem 4.7 with $d = p$, the Sylow p-subgroup of $S(n, p)$ satisfies

$$\text{Syl}_p(S(n, p)) \cong S_0(n, p) \cong \bigoplus_{i=0}^{k-1} \left(\mathbb{Z}_{p^{i+1}/d_i} \oplus \mathbb{Z}_{p^{i+1}}^{n_i - 2n_{i+1} + n_{i+2} - 1} \right),$$

with $n = n_0, n_1, \ldots, n_k = n_{k+1}$ the p-sequence of n, and $d_i = n_i/n_{i+1} = (n_i, p)$ for $0 \le i \le k$. As $n = p^k m$, we have $n_i = p^{k-i} m$ and $d_i = p$ for $0 \le i \le k$, and $n_i = m$ otherwise. Plugging these values into above equation, we have

$$\text{Syl}_p(S(p^k m, p)) = \mathbb{Z}_{p^{k-1}} \oplus \mathbb{Z}_{p^k}^{(p-1)m-1} \oplus \bigoplus_{i=0}^{k-2} \left[\mathbb{Z}_{p^i} \oplus \mathbb{Z}_{p^{i+1}}^{p^{k-2-i}(p-1)^2 m - 1} \right].$$

Changing i to $k-2-i$ in the above summation, we have

$$\mathrm{Syl}_p(S(p^k m, p)) = \mathbb{Z}_{p^{k-1}} \oplus \mathbb{Z}_{p^k}^{(p-1)m-1} \oplus \bigoplus_{i=0}^{k-2} \left[\mathbb{Z}_{p^{k-2-i}} \oplus \mathbb{Z}_{p^{k-1-i}}^{p^i(p-1)^2 m-1} \right]$$

$$= \left[\bigoplus_{i=0}^{k-2} \mathbb{Z}_{p^{k-1-i}}^{p^i(p-1)^2 m} \right] \oplus \mathbb{Z}_{p^k}^{(p-1)m-1}$$

$$= \mathrm{Syl}_p(C^*(p^k m, p)/\langle Q_n \rangle)$$

and the proof of Theorem 3.2 is complete.

References

[1] C. A. Alfaro and C. E. Valencia. On the sandpile group of the cone of a graph. *Linear Algebra and its Applications*, 436(5):1154 – 1176, 2012.

[2] J. Arndt. *Matters Computational: Ideas, Algorithms, Source Code.* Springer, 2010. http://www.jjj.de/fxt/fxtbook.pdf.

[3] H. Bass. *Algebraic K-theory.* W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[4] H. Bidkhori and S. Kishore. A bijective proof of a theorem of Knuth. *Comb. Probab. Comput.*, 20(1):11–25, 2010.

[5] N. Biggs. Chip-firing and the critical group of a graph. *Journal of Algebraic Combinatorics*, 9:25–45, 1999.

[6] S. H. Chan. Final Year Project Thesis: Relations between sandpiles of some graphs and other combinatorial objects, 2012. School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore.

[7] S. H. Chan, H. Hollmann, and D. V. Pasechnik. Circulant matrices and sandpile groups of generalized de Bruijn graphs. In J. Nešetřil and M. Pellegrini, editors, *Proceedings of EuroComb 2013*, volume 16 of *Publications of the Scuola Normale Superiore*. Springer, 2013.

[8] P. Chen and Y. Hou. On the sandpile group of $P_4 \times C_n$. *Eur. J. Comb.*, 29(2):532–534, 2008.

[9] P. Chen, Y. Hou, and C. Woo. On the critical group of the möbius ladder graph. *Australasian Journal of Combinatorics*, 36:133–142, October 2006.

[10] A. Dartois, F. Fiorenzi, and P. Francini. Sandpile group on the graph D_n of the dihedral group. *European Journal of Combinatorics*, 24/7:815–824, 2003.

[11] D.-Z. Du, F. Cao, and D. F. Hsu. De Bruijn digraphs, Kautz digraphs, and their generalizations. In D.-Z. Du and D. F. Hsu, editors, *Combinatorial Network Theory*, pages 65–105. Kluwer Academic, 1996.

[12] D.-Z. Du, D. Hsu, and G. Peck. Connectivity of consecutive-d digraphs. *Discrete Applied Mathematics*, 37/38:169–177, 1992.

[13] D. Z. Du and F. K. Hwang. Generalized de Bruijn digraphs. *Networks*, 18:27–38, 1988.

[14] S. V. Duzhin and D. V. Pasechnik. Automorphisms of necklaces and sandpile groups, 2013. arXiv:1304.2563.

[15] A. E. Holroyd, L. Levine, K. Mészáros, Y. Peres, J. Propp, and D. B. Wilson. Chip-firing and rotor-routing on directed graphs. In *In and out of equilibrium. 2*, volume 60 of *Progr. Probab.*, pages 331–364. Birkhäuser, Basel, 2008.

[16] Y. Hou, C. Woo, and P. Chen. On the sandpile group of the square cycle C_n^2. *Linear Algebra and its Applications*, 418:457467, 2006.

[17] M. Imase and M. Itoh. Design to minimize diameter on building-block network. *Computers, IEEE Transactions on*, C-30(6):439 –442, june 1981.

[18] M. Imase and M. Itoh. A design for directed graphs with minimum diameter. *Computers, IEEE Transactions on*, C-32(8):782 –784, aug. 1983.

[19] L. Levine. Sandpile groups and spanning trees of directed line graphs. *J. Combin. Theory Ser. A*, 118(2):350–364, 2011.

[20] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[21] D. J. Lorenzini. A finite group attached to the laplacian of a graph. *Discrete Mathematics*, 91:277–282, 1991.

[22] R. Merris. Unimodular equivalence of graphs. *Linear Algebra and its Applications*, 173:181–189, Aug. 1992.

[23] M. Newman. *Integral Matrices*. Number v. 45 in Pure and Applied Mathematics - Academic Press. Acad. Press, 1972.

[24] The On-line Encyclopedia of Integer Sequences, entries A027362 and A003473, 2004-2011. see `http://oeis.org/A027362` and `http://oeis.org/A003473`.

[25] D. Perkinson. *Sage Sandpiles*, 2012. see `http://people.reed.edu/~davidp/sand/sage/sage.html`.

[26] Z. Raza. On the critical group of $\hat{W}_{3n}$. In *Proceedings of the 2011 international conference on Applied & computational mathematics*, ICACM'11, pages 98–106, Stevens Point, Wisconsin, USA, 2011. World Scientific and Engineering Academy and Society (WSEAS).

[27] Z. Raza and S. A. Waheed. On the critical group of $\hat{W}_{4n}$. *J. Appl. Math. & Informatics*, 30:993 – 1003, 2012.

[28] C. Reutenauer. *Free Lie Algebras*. Oxford University Press, 1993.

[29] J. J. Rushanan. *Topics in integral matrices and abelian group codes.* PhD thesis, California Institute of Technology, 1986.

[30] J. Shen and Y. Hou. On the sandpile group of $3 \times n$ twisted bracelets. *Linear Algebra and its Applications*, 429(8–9):1894–1904, Oct. 2008.

[31] W. Stein et al. *Sage Mathematics Software (Version 5.7).* The Sage Development Team, 2012. http://www.sagemath.org.

[32] N. G. d. B. T. van Aardenne, Ehrenfest. Circuits and trees in oriented linear graphs. *Simon Stevin*, (28):203–217, 1951.

[33] D. Wagner. The critical group of a directed graph, 2000. Available at http://arxiv.org/abs/math/0010241.