CRITICAL GROUPS OF GENERALIZED DE BRUIJN AND KAUTZ GRAPHS AND CIRCULANT MATRICES OVER FINITE FIELDS

SWEE HONG CHAN, HENK D. L. HOLLMANN, DMITRII V. PASECHNIK

School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371

ABSTRACT. We determine the critical groups of the generalized de Bruijn graphs $\mathrm{DB}(n,d)$ and generalized Kautz graphs $\mathrm{Kautz}(n,d)$, thus extending and completing earlier results for the classical de Bruijn and Kautz graphs. Moreover, for a prime p the critical groups of $\mathrm{DB}(n,p)$ are shown to be in close correspondence with groups of $n\times n$ circulant matrices over $\mathbb{F}_p$, which explains numerical data in [11], and suggests the possibility to construct normal bases in $\mathbb{F}_{p^n}$ from spanning trees in $\mathrm{DB}(n,p)$.

1. INTRODUCTION

The *critical group* of a directed graph G is an abelian group obtained from the Laplacian matrix Δ of G; it determines and is determined by 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 G at a vertex v is an abelian group obtained from the reduced Laplacian Δ_v of G; its order is equal to the *complexity* $\kappa(G)$ of G, the number of directed trees rooted at v, a fact that is related to the Matrix Tree Theorem, see for example [8] and its references. If G is Eulerian, then $S(G,v)$ does not depend on v, and is then simply written as $S(G)$; in that case, it is equal to the critical group of G. The critical group has been studied in other contexts under several other names, such as group of components, Picard or Jacobian group, and Smith group. For more details and background, see, e.g., [6].

Critical groups have been determined for a large number of graph families. For some examples, see the references in [1]. Here, we determine the critical group of the generalized de Bruijn graphs $\mathrm{DB}(n,d)$ and generalized Kautz graphs $\mathrm{Kautz}(n,d)$, thus extending and completing the results from [8] for the binary de Bruijn graphs $\mathrm{DB}(2^\ell,2)$ and Kautz graphs (with p prime) $\mathrm{Kautz}((p-1)p^{\ell-1},p)$, and [3] for the classical de Bruijn graphs $\mathrm{DB}(d^\ell,d)$ and Kautz graphs $\mathrm{Kautz}((d-1)d^{\ell-1},d)$. Unlike the classical case, the generalized versions are not necessarily iterated line graphs, so to obtain their critical groups, different techniques have to be applied.

E-mail address: {sweehong, henk.hollmann, dima}@ntu.edu.sg.

Our original motivation for studying these groups stems from their relations to some algebraic objects, such as the groups $C(n,p)$ of invertible $n \times n$-circulant matrices over $\mathbb{F}_p$ (mysterious numerical coincidences were noted in the OIES entry A027362 [11] by the third author, computed with the help of [15, 12]), and *normal bases* (cf. e.g. [9]) of the finite fields $\mathbb{F}_{p^n}$. The latter were noted to be closely related to circulant matrices and to *necklaces* by Reutenauer [13, Sect. 7.6.2], see also [5], and the related numeric data collected in [2]. In particular, we show that $C(n,p)/(\mathbb{Z}_{p-1} \times \mathbb{Z}_n)$ is isomorphic to the critical group of $\mathrm{DB}(n,p)$. 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 $\mathbb{F}_{p^n}$.

2. PRELIMINARIES

Let M be an $m \times n$ integer matrix of rank r. For a ring F, we write $R_F(M) = M^\top F^n$, the F-module generated by the rows of M. The *Smith group* [14] of M is defined as $\Gamma(M) = \mathbb{Z}^n / R_\mathbb{Z}(M)$. The submodule $\overline{\Gamma}(M) = \mathbb{Z}^n / R_\mathbb{Q}(M) \cap \mathbb{Z}^n$ of $\Gamma(M)$ is a finite abelian group called the *finite part* of $\Gamma(M)$. Indeed, if M has rank r, then $\Gamma(M) = \mathbb{Z}^{n-r} \oplus \overline{\Gamma}(M)$ with $\overline{\Gamma}(M) = \oplus_{i=1}^r \mathbb{Z}_{d_i}$, where $d_1, \ldots, d_r$ are the nonzero invariant factors of M, so that $d_i | d_{i+1}$ for $i = 1, \ldots, r-1$. For invariant factors and the Smith Normal Form, we refer to [10]. See [14] for further details and proofs.

Let $G = (V, E)$ be a directed graph on $n = |V|$ vertices. The indegree $d^-(v)$ and outdegree $d^+(v)$ is the number of edges ending or starting in $v \in V$, respectively. The *adjacency matrix* of G is the $n \times n$ matrix $A = (A_{v,w})$, with rows and columns indexed by V, where $A_{v,w}$ is the number of edges from v to w. The *Laplacian* of G is the matrix $\Delta = D - A$, where D is diagonal with $D_{v,v} = d_v^-$. The *critical group* $K(G)$ of G is the finite part of the Smith group of the Laplacian Δ of G. The *sandpile group* $S(G, v)$ of G at a $v \in V$ is the finite part of the Smith group of the $(n-1) \times (n-1)$ *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. G is called *Eulerian* if $d^+(v) = d^-(v)$ for every $v \in V$. In that case, $S(G, v)$ does not depend on v and is equal to the critical group $S(G)$ of G. For more details on sandpile groups and critical groups of directed graphs, we refer for example to [6] or [16].

2.1. **Generalized de Bruijn and Kautz graphs.**

Generalized de Bruijn graphs and generalized Kautz graphs [4] 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 [7], and are also known as *Imase-Itoh digraphs*. Both classes of graphs are Eulerian.

We will determine the critical group, or, equivalently, the sandpile group, of a generalized de Bruijn or Kautz graph on n vertices by embedding this group as a subgroup of index n in a group that we will refer to as the *sand dune* group of the corresponding digraph. Let us now turn to the details.

The *generalized de Bruijn graph* $\mathrm{DB}(n,d)$ has vertex set $\mathbb{Z}_n$, the set of integers modulo n, and (directed) edges $v \to dv+i$ for $i=0,\dots,d-1$ and all $v \in \mathbb{Z}_n$. The *generalized Kautz graph* $\mathrm{Kautz}(n,d)$ has vertex set $\mathbb{Z}_n$ and directed edges $v \to -d(v+1)+i$ for $i=0,\dots,d-1$ and all $v \in \mathbb{Z}_n$. Note that both $\mathrm{DB}(n,d)$ and $\mathrm{Kautz}(n,d)$ are Eulerian. In what follows, we will focus on the generalized de Bruijn graph; the generalized Kautz graph can be handled in a similar way, essentially by replacing d by $-d$ in certain places.

Let $\mathcal{Z}_n = \{a(x) \in \mathbb{Z}[x] \bmod x^n-1 \mid a(1)=0\}$. With each vertex $v \in \mathbb{Z}_n$, we associate the polynomial $f_v(x) = dx^v - x^{dv}\sum_{i=0}^{d-1} x^i \in \mathcal{Z}_n$. Since $f_v(x)$ is the associated polynomial of the vth row of the Laplacian $\Delta^{(n,d)}$ of the generalized de Bruijn graph $\mathrm{DB}(n,d)$, the Smith group $\Gamma(\Delta^{(n,d)})$ of the Laplacian of $\mathrm{DB}(n,d)$ is the quotient of $\mathbb{Z}[x] \bmod x^n-1$ by the $\mathbb{Z}_n$-span $\langle f_v(x) \mid v \in \mathbb{Z}_n\rangle_{\mathbb{Z}_n}$ of the polynomials $f_v(x)$. Now note that $\mathbb{Z}[x] \bmod x^n-1 \cong \mathbb{Z} \oplus \mathcal{Z}_n$, so since $\sum_{v\in\mathbb{Z}_n} f_v(x) = 0$, we have that

$$
\begin{aligned}
(1)\qquad \Gamma(\Delta^{(n,d)}) &= (\mathbb{Z}[x] \bmod x^n-1)/\langle f_v(x) \mid v \in \mathbb{Z}_n\rangle_{\mathbb{Z}_n} \\
&\cong \mathbb{Z} \oplus \mathcal{Z}_n/\langle f_v(x) \mid v \in \mathbb{Z}'_n\rangle_{\mathbb{Z}_n}
\end{aligned}
$$

where $\mathbb{Z}'_n = \mathbb{Z}_n \setminus \{0\}$. It is easily checked that the polynomials $f_v(x)$ with $v \in \mathbb{Z}'_n$ are independent over $\mathbb{Q}$, hence they constitute a basis for $\mathcal{Z}_n$ over $\mathbb{Q}$. As a consequence, each element in the quotient group

$$
(2)\qquad S(n,d) = S_{\mathrm{DB}}(n,d) = \mathcal{Z}_n/\langle f_v(x) \mid v \in \mathbb{Z}'_n\rangle_{\mathbb{Z}_n}
$$

has finite order, and so $S(n,d)$ is the critical group, or, equivalently, the sandpile group, of the generalized de Bruijn graph $\mathrm{DB}(n,d)$. We define the *sand dune group* $\Sigma(n,d) = \Sigma_{\mathrm{DB}}(n,d)$ of $\mathrm{DB}(n,d)$ as $\Sigma(n,d) = \mathcal{Z}_n/\langle g_v(x) \mid v \in \mathbb{Z}'_n\rangle_{\mathbb{Z}_n}$, where $g_v(x) = (x-1)f_v(x) = dx^v(x-1) - x^{dv}(x^d-1)$. Now let $e_v = x^v-1$; we have that $e_0 = 0$, and $\mathcal{Z}_n = \langle e_v \mid v \in \mathbb{Z}'_n\rangle_{\mathbb{Z}}$, the $\mathbb{Z}$-span of the polynomials e_v. Furthermore, let $\epsilon_v = de_v - e_{dv}$. The span in $\mathcal{Q}_n = \{a(x) \in \mathbb{Q}[x] \bmod x^n-1 \mid a(1)=0\}$ of the polynomials $g_v(x)$ with $v \in \mathbb{Z}_n$ is the set of polynomials of the form $dc(x) - c(x^d)$ with $c(1)=0$; since $\epsilon_v = g_0(x) + \cdots g_{v-1}(x)$ for all $v \in \mathbb{Z}_n$, we conclude that

$$
(3)\qquad \Sigma(n,d) = \mathcal{Z}_n/\mathcal{E}_{n,d},
$$

where $\mathcal{Z}_n = \langle e_v \mid v \in \mathbb{Z}'_n\rangle_{\mathbb{Z}}$ and $\mathcal{E}_{n,d} = \langle \epsilon_v \mid v \in \mathbb{Z}'_n\rangle_{\mathbb{Z}}$ is the $\mathbb{Z}$-submodule of $\mathcal{Z}_n$ generated by the polynomials $\epsilon_v = de_v - e_{dv}$. The next result is crucial: it identifies the elements of the sand dune group $\Sigma(n,d)$ that are actually contained in the sandpile group $S(n,d)$. (Due to lack of space, we omit the not too difficult proofs in the remainder of this section.)

Theorem 2.1. *If $a \in \Sigma(n,d)$ with $a = \sum_v a_v e_v$, then $a \in S(n,d)$ if and only if $\sum_v v a_v \equiv 0 \bmod n$.*

Corollary 2.2. *We have $\Sigma(n,d)/S(n,d) = \mathbb{Z}_n$ and so $|\Sigma(n,d)| = n|S(n,d)|$.*

The above descriptions of the sandpile group $S(n,d)$ and sand dune group $\Sigma(n,d)$, and the embedding of $S(n,d)$ as a subgroup of $\Sigma(n,d)$ are very suitable for the determination of these groups. In the process, repeatedly information is required about the order of various group elements. The following two results provide that information.

Lemma 2.3. *Let $a = \sum_v a_v \epsilon_v \in \Sigma(n,d)$. Then the order of a in $\Sigma(n,d)$ is the smallest positive integer m for which $ma_v \in \mathbb{Z}$ for each v.*

We say that $v \in \mathbb{Z}_n$ has d-*type* (f,e) in $\mathbb{Z}_n$ if $v, dv, \ldots, d^{e+f-1}v$ are all distinct, with $d^{e+f}v = d^f v$. Now, by expressing e_v in terms of the ϵ_v, we can determine the order of e_v. The result is as follows.

Lemma 2.4. *Supposing v has d-type (f,e), then $e_v = \sum_{i=0}^{f-1} d^{-i-1}\epsilon_{d^i v} + \sum_{j=0}^{e-1} d^{j-f}(d^e-1)^{-1}\epsilon_{d^{f+j}v}$ in $\mathcal{Z}_n$, and hence e_v has order $d^f(d^e-1)$ in $\Sigma(n,d)$.*

2.2. **Invertible circulant matrices.** Let Q_n be the $n \times n$ permutation matrix over a field F corresponding to the cyclic permutation $(1,2,\ldots,n)$. An $n \times n$ *circulant matrix* over F is a matrix that can be written as $a_1Q_n + a_2Q_n^2 + \ldots + a_nQ_n^n$ with $a_i \in F$ for $1 \le i \le n$. All the invertible circulant matrices form a commutative group (w.r.t. matrix multiplication), namely, the centralizer of Q_n in $\mathrm{GL}_n(F)$. In the case $F = \mathbb{F}_p$ we consider here we denote this commutative group by $C(n,p)$. Note that $C(n,p)$ contains a subgroup isomorphic to $\mathbb{Z}_{p-1} \oplus \mathbb{Z}_n$, namely the direct product of the group of scalar matrices $F_p^*I := \{\lambda I \mid \lambda \in \mathbb{F}_p^*\}$ and the cyclic subgroup generated by Q_n. Each circulant matrix has all-ones vector $\mathbf{1} := (1,\ldots,1)^\top$ as an eigenvector. Thus $C'(n,p) := \{g \in C(n,p) \mid g\mathbf{1} = \mathbf{1}\}$ is a subgroup of $C(n,p)$, and we have the following formula.

$$C(n,p) = C'(n,p) \times F_p^* I. \tag{4}$$

3. Main results

Let $n, d > 0$ be fixed integers. The description of the sandpile group $S(n,d)$ and the sand-dune group $\Sigma(n,d)$ of the generalized the Bruin graph $\mathrm{DB}(n,d)$ involves a sequence of numbers defined as follows. Put $n_0 = n$, and for $i = 1,2,\ldots$, define $g_i = \gcd(n_i,d)$ and $n_{i+1} = n_i/g_i$. We have $n_0 > \cdots > n_k = n_{k+1}$, where k is the smallest integer for which $g_k = 1$. We will refer to the sequence $n_0 > \cdots > n_k = n_{k+1}$ as the d-*sequence* of n. In what follows, we will write $m = n_k$ and $g = g_0 \cdots g_{k-1}$. Note that $n = gm$ with $\gcd(m,d) = 1$.

Since $\gcd(m,d) = 1$, the map $x \to dx$ partitions $\mathbb{Z}_m$ into orbits of the form $O(v) = (v, dv, \ldots, d^{o(v)-1}v)$. We will 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 V be a complete set of representatives of the orbits $O(v)$ different from $\{0\}$, where we ensure that for every divisor p of m, all integers of the form m/p^j are contained in V.

Theorem 3.1. *With the above definitions and notation, we have that*

$$\Sigma(n,d) = \left[\bigoplus_{i=0}^{k-1} \mathbb{Z}_{d^{i+1}}^{n_i-2n_{i+1}+n_{i+2}}\right] \oplus \left[\bigoplus_{v\in V} \mathbb{Z}_{d^{o(v)}-1}\right], \tag{5}$$

and

$$S(n,d) = \left[\bigoplus_{i=0}^{k-1} \mathbb{Z}_{d^{i+1}/g_i} \oplus \mathbb{Z}_{d^{i+1}}^{n_i-2n_{i+1}+n_{i+2}-1}\right] \oplus \left[\bigoplus_{v\in V} \mathbb{Z}_{(d^{o(v)}-1)/c(v)}\right], \tag{6}$$

where $c(v) = 1$ except in the following cases. For any $p|m$,

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

and if $4|m$ and $d \equiv 3 \bmod 4$, then $c(m/2) = 2$.

For the generalized Kautz graph, a similar result holds. For $v \in \mathbb{Z}_m$, we let $O'(v)$ denote the orbit of v under the map $x \to -dv$, and we define $o'(v) = |O'(v)|$. Now take V' to be a complete set of representatives of the orbits on $\mathbb{Z}'_m$. Finally, define $c'(v)$ similar to $c(v)$, except that now d is replaced by $-d$ (so the special case now involves $d \equiv 1 \bmod 4$). Then we have the following.

Theorem 3.2. *The sandpile group $S_{\mathrm{Kautz}}(n,d)$ of the generalized Kautz graph $\mathrm{Kautz}(n,d)$ is obtained from $S(n,d)$ by replacing V by V', $o(v)$ by $o'(v)$, and $c(v)$ by $c'(v)$ in (6).*

The above results can be 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. Furthermore, we note that many of the steps below repeatedly use Theorem 2.1 and Lemma 2.4. First, we investigate the "multiplication-by-d" map $d : x \to dx$ on the sandpile and sand-dune group. Let $\Sigma_0(n,d)$ and $S_0(n,d)$ denote the kernel of the map d^k on $\Sigma(n,d)$ 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 much more effort, it can be show that the kernel of the map d on $\Sigma(n,d)$ and $S(n,d)$ is isomorphic to $\mathbb{Z}_d^{n-n/(n,d)}$ and $\mathbb{Z}_{d/(n,d)} \oplus \mathbb{Z}_d^{n-1-n/(n,d)}$, respectively. Then we use induction over 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 part of the right hand side in (5) and (6), respectively. This part of the proof, although much more complicated, resembles the method used by [8] and [3].

Now it remains to handle the parts $\Sigma(m,d)$ and $S(m,d)$ with $\gcd(m,d) = 1$. For the "helper" group $\Sigma(m,d)$ that embeds $S(m,d)$, this is trivial: it is easily seen that $\Sigma(m,d) = \oplus_{v\in V}\langle e_v\rangle$, and the order of e_v is equal to the size $o(v)$ of its orbit $O(v)$ under the map d, so (5) 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

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

Finally, with the notation from Subsect. 2.2, we have the following isomorphisms, connecting critical groups and circulant matrices.

Theorem 3.3. *Let d be a prime. Then*

$$S(n,d) \cong C'(n,d)/\langle Q_n \rangle, \qquad \textit{and} \qquad \Sigma(n,d) \cong C'(n,d).$$

The proof of Theorem 3.3 is by reducing to the case $\gcd(n,p) = 1$ by an explicit construction, and then by diagonalizing $C(n,p)$ over an appropriate extension of $\mathbb{F}_p$. Essentially, as soon as $\gcd(n,p) = 1$, one can read off a decomposition of $C(n,p)$ into cyclic factors from the irreducible factors of the polynomial $x^n - 1$ over $\mathbb{F}_p$.

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. Bidkhori and S. Kishore. A bijective proof of a theorem of Knuth. *Comb. Probab. Comput.*, 20(1):11–25, 2010.
[4] 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.
[5] S. Duzhin and D. Pasechnik. Automorphisms of necklaces and sandpile groups, 2013. see http://arxiv.org/abs/1304.2563.
[6] 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.
[7] M. Imase and M. Itoh. A design for directed graphs with minimum diameter. *Computers, IEEE Transactions on*, C-32(8):782 –784, aug. 1983.
[8] L. Levine. Sandpile groups and spanning trees of directed line graphs. *J. Combin. Theory Ser. A*, 118(2):350–364, 2011.
[9] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.
[10] M. Newman. *Integral Matrices*. Number v. 45 in Pure and Applied Mathematics - Academic Press. Acad. Press, 1972.
[11] The on-line encyclopedia of integer sequences, entry A027362, 2004-2011. see http://oeis.org/A027362.
[12] D. Perkinson. *Sage Sandpiles*, 2012. see http://people.reed.edu/~davidp/sand/sage/sage.html.
[13] C. Reutenauer. *Free Lie Algebras*. Oxford University Press, 1993.
[14] J. J. Rushanan. *Topics in integral matrices and abelian group codes*. ProQuest LLC, Ann Arbor, MI, 1986. Thesis (Ph.D.)–California Institute of Technology.
[15] W. Stein et al. *Sage Mathematics Software (Version 5.7)*. The Sage Development Team, 2012. http://www.sagemath.org.
[16] D. Wagner. The critical group of a directed graph, 2000. Available at http://arxiv.org/abs/math/0010241.