PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 149, Number 5, May 2021, Pages 2249–2255
https://doi.org/10.1090/proc/15391
Article electronically published on February 24, 2021

AN ALGEBRAIC CHARACTERIZATION OF k–COLORABILITY

RAMÓN FLORES, DELARAM KAHROBAEI, AND THOMAS KOBERDA

(Communicated by David Futer)

ABSTRACT. We characterize k–colorability of a simplicial graph via the intrinsic algebraic structure of the associated right-angled Artin group. As a consequence, we show that a certain problem about the existence of homomorphisms from right-angled Artin groups to products of free groups is NP–complete.

1. INTRODUCTION

Let Γ be a finite simplicial graph with vertex set $V = V(\Gamma)$ and edge set $E = E(\Gamma)$. We say that Γ is *k–colorable* if there is a map $\kappa\colon V \to \{1, \dots, k\}$ such that if $\{v, w\} \in E$ then $\kappa(v) \neq \kappa(w)$. The map κ is called a *k–coloring* of Γ. The minimal k for which there exists such a map κ is called the *chromatic number* of Γ and is denoted $\chi(\Gamma)$.

The problem of finding a k–coloring of a given graph is fundamental in graph theory, and has many applications in discrete mathematics, computational complexity, and computer science. Determining whether a given graph is 3–colorable is known to be NP–complete, as is determining a graph's chromatic number [1,7,15].

As such, determining the existence of a k–coloring of a graph is a fundamental problem in theoretical complexity theory, with a plethora of applications to both theoretical and applied computer science; for instance, several cryptographic schemes based on the 3–colorability problem have been proposed, such as a post-quantum public key encryption known as Polly Cracker [17], and a zero-knowledge proof system for graph 3–colorability [8].

This paper studies k–colorings of graphs via algebraic methods, specifically right-angled Artin groups [3]. To a finite simplicial graph Γ, we associate the right-angled Artin group $A(\Gamma)$ via

$$A(\Gamma) = \langle V(\Gamma) \mid [v, w] = 1 \text{ if and only if } \{v, w\} \in E(\Gamma)\rangle.$$

It is well-known that the isomorphism type of $A(\Gamma)$ determines the isomorphism type of Γ [4,14,16], so that the graph theoretic properties of Γ should be reflected in the algebra of $A(\Gamma)$. We are generally interested in the following problem:

Received by the editors March 23, 2020, and, in revised form, September 27, 2020.
2020 *Mathematics Subject Classification.* Primary 57M15; Secondary 05C90.
The first author was supported by FEDER-MEC grant MTM2016-76453-C2-1-P and FEDER grant US-1263032 from the Andalusian Government.
The second author was supported in part by a Canada's New Frontiers in Research Fund, under the Exploration grant entitled "Algebraic Techniques for Quantum Security".
The third author was partially supported by an Alfred P. Sloan Foundation Research Fellowship, by NSF Grant DMS-1711488, and by NSF Grant DMS-2002596.

Problem 1.1. Let P be a property of finite simplicial graphs. Find a property Q of groups such that Γ has P if and only if $A(\Gamma)$ has Q.

In order for Problem 1.1 to be interesting, one should insist that Q be a property of the isomorphism type of a group only. In particular, one should disallow reference to a generating set.

One reason for interest in Problem 1.1 is that it can provide insight into various graph theoretic problems and their computational complexity from the more flexible point of view of the algebraic structure of $A(\Gamma)$. Moreover, algebraically formulated problems can be approached using an arbitrary presentation for $A(\Gamma)$, without reconstructing the full underlying graph of $A(\Gamma)$.

Here are some instances where a satisfactory answer to Problem 1.1 is known:

(1) The graph Γ is a nontrivial join if and only if $A(\Gamma)$ decomposes as a nontrivial direct product [18].
(2) The graph Γ is disconnected if and only if $A(\Gamma)$ decomposes as a nontrivial free product [2].
(3) The graph Γ is square–free if and only if $A(\Gamma)$ does not contain a subgroup isomorphic to a product $F_2 \times F_2$ of nonabelian free groups [11,12].
(4) The graph Γ admits an independent set D of vertices such that every cycle in Γ meets D at least twice if and only if the poly-free length of $A(\Gamma)$ is two [10].
(5) The graph Γ is a cograph (i.e. a P_4–free graph) if and only if $A(\Gamma)$ is contained in the class of finitely generated groups which contains $\mathbb{Z}$ and is closed under taking direct products and free products [12,13].
(6) The graph Γ is a finite tree or a finite complete bipartite graph if and only if $A(\Gamma)$ is a semidirect product of two free groups of finite rank [10].
(7) The graph Γ admits a nontrivial automorphism if and only if the group $\mathrm{Out}(A(\Gamma))$ of outer automorphisms of $A(\Gamma)$ contains a finite nonabelian group [5].
(8) A sequence of graphs $\{\Gamma_i\}_{i\in\mathbb{N}}$ forms a graph expander family if and only if the cohomology rings $\{H^*(A(\Gamma_i), F)\}$ over an arbitrary field F form a *vector space expander family* [6].

In this paper, we prove the following result which characterizes the existence of a k–coloring of a graph Γ (and in particular the chromatic number of Γ) via right-angled Artin groups, thus providing an answer to Problem 1.1 when P is k–colorability.

Theorem 1.2. *Let Γ be a finite simplicial graph with n vertices. The graph Γ is k–colorable if and only if there is a surjective map*

$$A(\Gamma) \to \prod_{i=1}^{k} F_i,$$

where for $1 \leq i \leq k$ the group F_i is a free group of rank m_i, and where

$$\sum_{i=1}^{k} m_i = n.$$

We note that the number of vertices of Γ is a canonical invariant of the isomorphism type of $A(\Gamma)$, since this is simply the rank of the abelianization of $A(\Gamma)$. We state Theorem 1.2 as we do because of the conciseness of the hypotheses and

the conclusion, though in the course of the proof it will become clear that we can weaken the hypotheses somewhat. For instance, the target groups need not be free, but may be replaced by groups with the correct Betti numbers in which infinite order elements have (virtually) cyclic centralizers. This last hypothesis is satisfied in all Gromov hyperbolic groups [9], for instance. Moreover, we need not assume that ϕ is surjective — it suffices that ϕ induces an isomorphism on first rational homology.

Theorem 1.2 has the following easy consequence, which is of interest from the point of view of complexity theory.

Corollary 1.3. *Fix $k \geq 3$. The problem of determining whether a right-angled Artin group $A(\Gamma)$ surjects to a product of k free groups, the sum of whose ranks equals $|V(\Gamma)|$, is NP–complete.*

Proof. It is a direct consequence of Theorem 1.2 and the fact that the k-colorability problem is NP–complete for $k \geq 3$ (see for example [7]). □

2. Proof of Theorem 1.2

There is only one difficult direction in our proof of Theorem 1.2. The following easy lemma handles the "only if" direction.

Lemma 2.1. *Suppose Γ is a simplicial graph on n vertices which is k–colorable. Then $A(\Gamma)$ admits a surjection as in Theorem 1.2.*

Proof. Let κ be a k–coloring, and write $V_i = \kappa^{-1}(i) \subset V$. If $\{v, w\} \in E$ then $v \in V_i$ and $w \in V_j$ for suitable indices $i \neq j$. We may thus form a quotient G of $A(\Gamma)$ by imposing the relation $[a, b] = 1$ for all pairs $a \in V_i$ and $b \in V_j$ for $i \neq j$. Clearly the result will be a right-angled Artin group $A(\Lambda)$, where

$$\Lambda = V_1 * V_2 * \cdots * V_k$$

is the join of the sets $\{V_1, \ldots, V_k\}$. Since for all i the set V_i is totally disconnected in Γ (and hence in Λ), it is easy to see that $A(\Lambda)$ is a direct product of free groups with ranks $\{|V_1|, \ldots, |V_k|\}$, and that

$$\sum_{i=1}^{k} |V_i| = n,$$

as desired. □

We now turn our attention to the "if" direction. Suppose

$$\phi\colon A(\Gamma) \to \prod_{i=1}^{k} F_i = G$$

is a surjection as in Theorem 1.2. We will fix notation and write $\{v_1, \ldots, v_n\}$ for the vertices of Γ and $w_i = \phi(v_i)$. Recall that m_i stands for the rank of F_i. We write $X = \{x_1, \ldots, x_n\}$ for a generating set of G, where

$$X_i = \{x_{1+\sum_{j<i} m_j}, x_{2+\sum_{j<i} m_j}, \ldots, x_{\sum_{j\leq i} m_j}\}$$

generates the subgroup

$$\{1\} \times \cdots \times \{1\} \times F_i \times \{1\} \times \cdots \times \{1\}.$$

For each $x_i \in X$ and $g \in G$, we write $\exp_{x_i}(g)$ for the *exponent sum* of x_i in g, i.e. the image of the element g under the homomorphism $G \to \mathbb{Z}$ which sends x_i to 1 and x_j to 0 for $j \neq i$.

If $g \in G$ is arbitrary, we write $g = g_1 \cdots g_k$, where $g_i \in \langle X_i \rangle$. It is easy to see that this expression for g is unique.

Lemma 2.2. *Suppose $g, h \in G$ are elements such that $[g, h] = 1$. Write $g = g_1 \cdots g_k$ and $h = h_1 \cdots h_k$. Then for all $1 \leq i \leq k$, the tuples*

$$(\exp_\alpha(g_i))_{\alpha \in X_i}, (\exp_\alpha(h_i))_{\alpha \in X_i}$$

are rational multiples of each other.

Note that the map

$$g_i \mapsto (\exp_\alpha(g_i))_{\alpha \in X_i}$$

just computes the image of g_i in the abelianization $H_1(F_i, \mathbb{Z})$, using the images of elements of X_i as an additive basis for $\mathbb{Z}^{m_i}$.

Proof of Lemma 2.2. Fix i arbitrarily. If one of these tuples consists of all zeros then there is nothing to show. Otherwise, we may suppose that these tuples are nontrivial for both g_i and h_i. In particular, we must have that both g_i and h_i are nontrivial group elements of $\langle X_i \rangle$. The centralizer of a nontrivial element of a free group is cyclic, so that then g_i and h_i must share a common nonzero power. Since the exponent sum map is a homomorphism, the lemma is now immediate. □

We will require the following fact from linear algebra, which we include for completeness.

Lemma 2.3. *Let M be a complex $n \times n$ matrix of rank n, let $1 \leq k \leq n-1$ be an integer, and consider the block decomposition $M = (M_1 \mid M_2)$, where M_1 is an $n \times k$ matrix. There exist k rows $\{r_1, \ldots, r_k\}$ which have the following properties:*

1. *The submatrix M_1' of M_1 spanned by the rows $\{r_1, \ldots, r_k\}$ has rank k.*
2. *The submatrix M_2' of M_2 obtained by deleting the rows $\{r_1, \ldots, r_k\}$ has rank $n - k$.*

Proof. We have that the determinant of M is nonzero, since M is invertible. We may now expand the determinant about $k \times k$–subminors of M_1. That is, we consider a submatrix M_1' of M_1 spanned by k rows, and the submatrix M_2' of M_2 obtained by deleting the k rows used to define M_1'. We then consider the complex number $\zeta = (\det M_1') \cdot (\det M_2')$. An easy application of the Leibniz formula shows that $\det M$ is an alternating sum of the complex numbers ζ, as M_1' ranges over all possible choices of k rows. Since $\det M \neq 0$, there is a choice of M_1' and M_2' so that the corresponding value of ζ is nonzero. In particular, such a choice of M_1' and M_2' gives the desired matrices of the correct ranks, whence the lemma follows. □

The following lemma completes the proof of Theorem 1.2.

Lemma 2.4. *Let $\phi\colon A(\Gamma) \to G$ be a surjective homomorphism as above. Then Γ admits a k–coloring.*

Proof. Since the abelianizations of $A(\Gamma)$ and G are both isomorphic to $\mathbb{Z}^n$, we have that the induced map

$$\phi_*\colon H_1(A(\Gamma), \mathbb{Q}) \to H_1(G, \mathbb{Q})$$

is an isomorphism. We express this map as a matrix with respect to the additive bases $\{v_1, \ldots, v_n\}$ for $H_1(A(\Gamma), \mathbb{Q})$ and $\{x_1, \ldots, x_n\}$ for $H_1(G, \mathbb{Q})$, so that

$$\phi_*(v_i) = [w_i] = \sum_{j=1}^{n} \beta_j^i x_j$$

for suitable coefficients β_j^i. With respect to these bases, ϕ_* is represented by an $n \times n$ matrix $A = (\beta_j^i)$ with rank exactly n, where here β_j^i denotes the (i, j)–entry of A. We write A as a block column matrix

$$A = (A_1 \mid \cdots \mid A_k),$$

where the column space of A_i has dimension exactly m_i.

Consider the matrix A_1. Since ϕ_* is an isomorphism, we have that the row space of A_1 has dimension m_1. We may therefore choose an $m_1 \times m_1$ minor B_1 of A_1 with rank m_1. By Lemma 2.3, we may assume that deleting the first m_1 columns of A and the rows which appear in B_1 results in a matrix of rank exactly $n - m_1$. We perform a row permutation of A to get a matrix A', so that the rows of B_1 are the restriction of the first m_1 rows of A' to the first m_1 columns of A'.

Deleting the first m_1 rows and columns of A' results in a matrix of rank exactly $n - m_1$. Repeating this process for each block column matrix results in an $n \times n$ block matrix

$$B = (B_1 \mid \cdots \mid B_k)$$

with the following properties:

(1) The matrix B is obtained from A by permuting rows.
(2) The rows with index set $J_i = \{(\sum_{j<i} m_j) + 1, \ldots, \sum_{j \leq i} m_j\}$ of B_i have rank m_i.

Observe that the rows of B correspond to the group elements

$$\{w_i = \phi(v_i)\}_{i=1}^{n},$$

where we have relabeled the elements $\{v_1, \ldots, v_n\}$ so that $\phi(v_i)$ corresponds to the i^{th} row of B. We define $\kappa \colon V \to \{1, \ldots, k\}$ by $\kappa(v_\ell) = i$ if $\ell \in J_i$. It remains to check that κ is a valid coloring of Γ. Suppose that $\kappa(v) = \kappa(w) = i$ for distinct vertices of V. Then the elements $[\phi(v)]$ and $[\phi(w)]$ in $H_1(G, \mathbb{Q})$ correspond to linearly independent rows of the block B_i. We have that if $\{v, w\} \in E$ then v and w commute. Lemma 2.2 implies that the rows corresponding to $[\phi(v)]$ and $[\phi(w)]$ in the block B_i are rational multiples of each other, which is a contradiction. We conclude that $\{v, w\} \notin E$, so that κ is a valid coloring of Γ. □

Observe that the proof of Theorem 1.2 builds an explicit coloring of Γ using the image of $V(\Gamma)$ under ϕ. In principle, an algorithm which takes as input the surjection from Theorem 1.2 and outputs a coloring of Γ can be implemented, and even in polynomial time.

More precisely, let Γ be a graph with n vertices and let ϕ be a surjection from $A(\Gamma)$ to a product of k free groups of total rank n, given in terms of generators. We can compute the map induced by ϕ on abelianizations in time which is linear in the complexity of ϕ. Let M be the resulting matrix and N a bound on the maximum of the entries of M, in absolute value. Following the proof of Theorem 1.2, we break M into submatrices M_1 and M_2, and compute a sequence of determinants of submatrices of M_1 and M_2, of which there are at most polynomially many as a

function of n. All this would require a computation time which is bounded by a polynomial in n and N. This allows us to sort the rows of M as in the proof of the theorem and therefore produce a k–coloring in polynomial computing time.

It it straightforward to see that one can start with a k–coloring of Γ and produce the surjection ϕ in polynomial time.

Acknowledgments

We thank Yago Antolín, Juan González-Meneses, Sang-hyun Kim, and Andrew Sale for helpful discussions and comments. We thank the University of York for hospitality while part of this research was conducted. Finally, we thank an anonymous referee for helpful comments.

References

[1] Sanjeev Arora and Boaz Barak, *Computational complexity*, Cambridge University Press, Cambridge, 2009. A modern approach. MR2500087

[2] Noel Brady and John Meier, *Connectivity at infinity for right angled Artin groups*, Trans. Amer. Math. Soc. **353** (2001), no. 1, 117–132, DOI 10.1090/S0002-9947-00-02506-X. MR1675166

[3] Ruth Charney, *An introduction to right-angled Artin groups*, Geom. Dedicata **125** (2007), 141–158, DOI 10.1007/s10711-007-9148-6. MR2322545

[4] Carl Droms, *Isomorphisms of graph groups*, Proc. Amer. Math. Soc. **100** (1987), no. 3, 407–408, DOI 10.2307/2046419. MR891135

[5] Ramón Flores, Delaram Kahrobaei, and Thomas Koberda, *Algorithmic problems in right-angled Artin groups: complexity and applications*, J. Algebra **519** (2019), 111–129, DOI 10.1016/j.jalgebra.2018.10.023. MR3874519

[6] Ramón Flores, Delaram Kahrobaei, and Thomas Koberda, *Expanders and right-angled Artin groups*, preprint (2020).

[7] Michael R. Garey and David S. Johnson, *Computers and intractability*, W. H. Freeman and Co., San Francisco, Calif., 1979. A guide to the theory of NP-completeness; A Series of Books in the Mathematical Sciences. MR519066

[8] Oded Goldreich, Silvio Micali, and Avi Wigderson, *Proofs that yield nothing but their validity, or all languages in NP have zero-knowledge proof systems*, J. Assoc. Comput. Mach. **38** (1991), no. 3, 691–729, DOI 10.1145/116825.116852. MR1125927

[9] M. Gromov, *Hyperbolic groups*, Essays in group theory, Math. Sci. Res. Inst. Publ., vol. 8, Springer, New York, 1987, pp. 75–263, DOI 10.1007/978-1-4613-9586-7_3. MR919829

[10] Susan Hermiller and Zoran Šunić, *Poly-free constructions for right-angled Artin groups*, J. Group Theory **10** (2007), no. 1, 117–138, DOI 10.1515/JGT.2007.010. MR2288463

[11] Mark Kambites, *On commuting elements and embeddings of graph groups and monoids*, Proc. Edinb. Math. Soc. (2) **52** (2009), no. 1, 155–170, DOI 10.1017/S0013091507000119. MR2475886

[12] Sang-hyun Kim and Thomas Koberda, *Embedability between right-angled Artin groups*, Geom. Topol. **17** (2013), no. 1, 493–530, DOI 10.2140/gt.2013.17.493. MR3039768

[13] Sang-Hyun Kim and Thomas Koberda, *Free products and the algebraic structure of diffeomorphism groups*, J. Topol. **11** (2018), no. 4, 1054–1076, DOI 10.1112/topo.12079. MR3989437

[14] Thomas Koberda, *Right-angled Artin groups and a generalized isomorphism problem for finitely generated subgroups of mapping class groups*, Geom. Funct. Anal. **22** (2012), no. 6, 1541–1590, DOI 10.1007/s00039-012-0198-z. MR3000498

[15] Marvin L. Minsky, *Computation: finite and infinite machines*, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1967. Prentice-Hall Series in Automatic Computation. MR0356580

[16] Lucas Sabalka, *On rigidity and the isomorphism problem for tree braid groups*, Groups Geom. Dyn. **3** (2009), no. 3, 469–523, DOI 10.4171/GGD/67. MR2516176

[17] Massimiliano Sala, Teo Mora, Ludovic Perret, Shojiro Sakata, and Carlo Traverso (eds.), *Gröbner bases, coding, and cryptography*, Springer-Verlag, Berlin, 2009. MR2590633

[18] Herman Servatius, *Automorphisms of graph groups*, J. Algebra **126** (1989), no. 1, 34–60, DOI 10.1016/0021-8693(89)90319-0. MR1023285

Department of Geometry and Topology, Faculty of Mathematics, University of Seville, c/ Tarfia s/n, 41012 Seville, Spain
Email address: ramonjflores@us.es

Department of Computer Science, University of York, Deramore Lane, York YO10 5GH, United Kingdom; New York University, Tandon School of Engineering, PhD Program in Computer Science; and CUNY Graduate Center
Email address: dk2572@nyu.edu, delaram.kahrobaei@york.ac.uk

Department of Mathematics, University of Virginia, Charlottesville, Virginia 22904
Email address: thomas.koberda@gmail.com