GRAPH THEORETICAL CRITERIA FOR THE WILDNESS OF RESIDUE-CLASS-WISE AFFINE PERMUTATIONS

STEFAN KOHL

ABSTRACT. A permutation of $\mathbb{Z}$ is called *residue-class-wise affine* if there is a positive integer m such that it is affine on residue classes (mod m). The smallest such integer is called the *modulus* of the respective permutation.

A residue-class-wise affine permutation is called *tame* if the moduli of its powers are bounded, and *wild* otherwise.

In this short note, we describe two criteria to decide whether a given residue-class-wise affine permutation is tame or wild. These criteria are based on properties of certain graphs assigned to residue-class-wise affine permutations, and they are suitable for computational purposes.

1. INTRODUCTION

The subject of this note are bijective mappings of the following type:

Definition 1.1. We call a mapping $f : \mathbb{Z} \to \mathbb{Z}$ *residue-class-wise affine* if there is a positive integer m such that the restrictions of f to the residue classes $r(m) \in \mathbb{Z}/m\mathbb{Z}$ are all affine, i.e. given by

$$f|_{r(m)} : \ r(m) \to \mathbb{Z}, \ \ n \ \mapsto \ \frac{a_{r(m)} \cdot n + b_{r(m)}}{c_{r(m)}}$$

for certain coefficients $a_{r(m)}$, $b_{r(m)}$, $c_{r(m)} \in \mathbb{Z}$ depending on $r(m)$. We call the smallest possible m the *modulus* of f, written $\mathrm{Mod}(f)$.

For reasons of uniqueness, we assume that $\gcd(a_{r(m)}, b_{r(m)}, c_{r(m)}) = 1$ and that $c_{r(m)} > 0$. We call the least common multiple of the coefficients $c_{r(m)}$ the *divisor* of f, and use the notation $\mathrm{Div}(f)$.

Computing with arbitrary permutation groups over infinite sets like $\mathbb{Z}$ is not feasible. However the groups formed by residue-class-wise affine permutations are very well accessible to computational methods:

Definition 1.2. We call a subgroup of $\mathrm{Sym}(\mathbb{Z})$ *residue-class-wise affine*, or in short an *rcwa* group, if its elements are residue-class-wise affine permutations.

Residue-class-wise affine groups have been introduced in [2], and information on the richness of this class of groups can be found in [3]. For a collection of algorithms and methods to compute with residue-class-wise affine groups, see [6]. All of the algorithms described there are implemented in the GAP [1] package RCWA [4].

There are two entirely different classes of rcwa permutations and -groups. Roughly speaking, the one class comprises the 'trivial' cases, and the other comprises the 'interesting' ones. For computational purposes, it is important to be able to determine which of these classes a given rcwa permutation or -group belongs to:

2000 *Mathematics Subject Classification.* Primary 20-04, secondary 11B99.

Definition 1.3. We call an rcwa permutation σ *tame* if it permutes a partition of $\mathbb{Z}$ into finitely many residue classes on all of which it is affine, and *wild* otherwise. We call an rcwa group G *tame* if there is a common such partition for all elements of G, and *wild* otherwise. We call the mentioned partitions *respected partitions* of σ respectively G.

It follows immediately from the definition that any tame group embeds into the wreath product of the infinite dihedral group with a finite symmetric group of certain degree.

On the one hand, tameness is invariant under conjugation, but on the other, products of tame rcwa permutations need *not* be tame – see [3], Section 6.

In [2], a generalization of the above notion of tameness to not necessarily bijective rcwa mappings is considered. Namely, an rcwa mapping is called *tame* if the set of moduli of its powers is bounded, and *wild* otherwise. In [5] it is shown that in this sense, a surjective, but not injective rcwa mapping is always wild. Theorem 2.5.8 in [2] establishes the compatibility of these characterizations of tameness, namely it states that an rcwa group is tame if and only if the set of the moduli of its elements is bounded.

2. The Criteria

Our criteria to decide whether a given rcwa permutation is tame or wild are based on properties of the following directed graphs:

Definition 2.1. Let σ be an rcwa permutation, and let m be a positive integer. We define the *transition graph* $\Gamma(\sigma, m)$ of σ for modulus m as follows:

- The vertices of $\Gamma(\sigma, m)$ are the residue classes (mod m).
- There is an edge from $r_1(m)$ to $r_2(m)$ if and only if $\sigma(r_1(m)) \cap r_2(m) \neq \emptyset$.

Criterion 2.2. Let σ be an rcwa permutation. Assume that there is a positive integer m such that the transition graph $\Gamma(\sigma, m)$ has a weakly-connected component which is not strongly-connected. Then σ is wild.

Criterion 2.3. Let σ be an rcwa permutation, let m denote its modulus and assume that the transition graph $\Gamma(\sigma, m)$ has a non-isolated vertex which carries a loop. Then σ is wild.

Criteria 2.2 and 2.3 are sufficient conditions for an rcwa permutation to be wild. In order to check that a given rcwa permutation is tame, one can construct a respected partition. An algorithm for this is described in [6].

3. The Proofs of the Validity of the Criteria

In the proof of Criterion 2.2, we need a notion of density for set-theoretic unions of residue classes:

Definition 3.1. Given a residue class $r(m)$, we set $\mu(r(m)) := 1/m$. Given $S \subseteq \mathbb{Z}$ we further set $\mu(\mathbb{Z} \setminus S) := 1 - \mu(S)$, and given two subsets $S_1, S_2 \subseteq \mathbb{Z}$, we set $\mu(S_1 \cup S_2) := \mu(S_1) + \mu(S_2) - \mu(S_1 \cap S_2)$. We call $\mu(S)$ the *natural density* of S.

These settings induce a notion of density for open and closed subsets of $\mathbb{Z}$ in the topology induced by taking the set of all residue classes as a basis.

We also need a parameter which describes how ‘smooth’ a union of residue classes is:

Definition 3.2. Let $S \subseteq \mathbb{Z}$ be an open set in the topology induced by taking the set of all residue classes as a basis. We define the *modulus* $\mathrm{Mod}(S)$ of S by the least positive integer m such that S can be written as a union of residue classes (mod m) if such an m exists, and by ∞ otherwise.

Further we need the following lemmata:

Lemma 3.3. *Let $S \subseteq \mathbb{Z}$ be a union of finitely many residue classes, and let σ be an rcwa permutation. Then the following hold:*

(1) It is $\mu(\sigma(S)) \leqslant \mu(S) \cdot \mathrm{Div}(\sigma)$.
(2) The modulus of the preimage of S under σ divides $\mathrm{Mod}(\sigma) \cdot \mathrm{Mod}(S)$.

Proof. Assertion (1) is immediate. We prove Assertion (2). Let $m := \mathrm{Mod}(\sigma)$, and let n be an integer. It depends on $\sigma(n)$ mod $\mathrm{Mod}(S)$ whether $\sigma(n)$ is in S or not. The residue $\sigma(n)$ mod $\mathrm{Mod}(S)$ is determined by n mod m and $\sigma|_{n(m)}(n)$ mod $\mathrm{Mod}(S)$, hence by n mod $\mathrm{lcm}(m, \mathrm{Div}(\sigma) \cdot \mathrm{Mod}(S))$. The assertion follows, since the divisor of an rcwa mapping divides its modulus. □

Lemma 3.4. *Let σ be an rcwa permutation. Assume that there is a union of finitely many residue classes of $\mathbb{Z}$ which is a proper subset of its image and a proper superset of its preimage under σ. Then σ is wild.*

Proof. Let $S_0 \subset \mathbb{Z}$ be a union of finitely many residue classes as described, and let S_1 be the preimage of S_0 under σ. Obviously, the set S_1 is a union of finitely many residue classes as well, and hence has a strictly smaller natural density than S_0. Images of integers outside S_1 lie outside S_0, hence in particular outside S_1. Thus since the image of S_1 under σ is a proper superset of S_1, the preimage S_2 of S_1 under σ is a proper subset of S_1. We can iterate this, and get a descending chain $S_0 \supset S_1 \supset S_2 \supset \dots$ of unions of finitely many residue classes such that for any k, the set S_{k+1} is the full preimage of S_k under σ.

Assume that the rcwa permutation σ is tame, and let m be the least common multiple of the moduli of its powers. Since the divisor of an rcwa mapping divides its modulus, for any integer k we have $\mathrm{Div}(\sigma^k)|m$. Since S_0 is the image of S_k under σ^k, by Lemma 3.3, Assertion (1) the quotients $\mu(S_0)/\,\mu(S_k)$ are hence bounded by m. We conclude that $\lim_{k\to\infty} \mu(S_k)/\,\mu(S_{k+1}) = 1$, and hence that $\lim_{k\to\infty} \mathrm{Mod}(S_k) = \infty$. But since S_k is the preimage of S_0 under σ^k, by Lemma 3.3, Assertion (2) we also have $\forall k \in \mathbb{N}\ \mathrm{Mod}(S_k)|m \cdot \mathrm{Mod}(S_0)$. This contradicts our assumption that σ is tame. □

By switching to the inverse of σ, we see that Lemma 3.4 remains valid when we interchange the terms 'image' and 'preimage'.

Proof of the validity of Criterion 2.2.

Let σ be an rcwa permutation, and assume that there is a positive integer m such that the transition graph $\Gamma(\sigma, m)$ has a weakly-connected component which is not strongly-connected. We need to show that σ is wild.

We choose a strongly-connected component Γ_0 of $\Gamma(\sigma, m)$ which is a proper subgraph of a weakly-connected component $\tilde{\Gamma}_0$. Since $\tilde{\Gamma}_0$ is a finite graph, we can assume without loss of generality that Γ_0 is connected to the rest of $\tilde{\Gamma}_0$ by outgoing edges only – otherwise we could follow an ingoing edge in reverse direction and would enter another strongly-connected component and so on, until after a finite number of steps we would reach a 'source' which satisfies our condition.

Let $S \subset \mathbb{Z}$ be the union of the vertices of Γ_0. Since σ is surjective, $\sigma(S)$ is a proper superset of S. By the choice of Γ_0 this implies that the preimage of S under σ is a proper subset of S. Therefore by Lemma 3.4, the rcwa permutation σ is wild. □

Proof of the validity of Criterion 2.3.

Let σ be an rcwa permutation, let m denote its modulus and assume that the transition graph $\Gamma(\sigma, m)$ has a non-isolated vertex $r(m)$ which carries a loop. Further assume that the restriction of σ to the residue class $r(m)$ is given by $\alpha : n \mapsto (an + b)/c$ for coprime integers a, b and c. We need to show that σ is wild.

By Criterion 2.2, we can assume without loss of generality that $r(m)$ has both ingoing and outgoing edges. This implies that $c \neq 1$. Therefore as the divisor of an rcwa permutation divides its modulus, it suffices to show that a cycle of σ may pass the loop around $r(m)$ arbitrarily often without leaving $r(m)$ in between.

The mapping α has the rational fixed point $b/(c - a)$. Since a and c are coprime, c and $c - a$ are so as well. Further since by assumption $r(m)$ and $\alpha(r(m))$ intersect nontrivially, the congruence $n \equiv b/(c - a) \mod m$ is solvable. Given $k \in \mathbb{N}$, it is now easy to see that for any integer $n \equiv b/(c - a) \mod c^k m$, the first k iterates $\sigma(n), \sigma^2(n), \dots, \sigma^k(n)$ lie all in $r(m)$. The assertion follows. □

References

1. The GAP Group, *GAP – Groups, Algorithms, and Programming; Version 4.4.9*, 2006, http://www.gap-system.org.
2. Stefan Kohl, *Restklassenweise affine Gruppen*, Dissertation, Universität Stuttgart, 2005, published at http://deposit.d-nb.de/cgi-bin/dokserv?idn=977164071.
3. ______, *A simple group generated by involutions interchanging residue classes of the integers*, 2006, preprint, available at http://www.cip.mathematik.uni-stuttgart.de/ kohlsn/preprints/simplegp.pdf.
4. ______, *RCWA - Residue-Class-Wise Affine Groups; Version 2.4.3*, 2007, GAP package, published at http://www.gap-system.org/Packages/rcwa.html.
5. ______, *Wildness of iteration of certain residue-class-wise affine mappings*, Adv. in Appl. Math. **39** (2007), no. 3, 322–328. MR 2352043
6. ______, *Algorithms for a class of infinite permutation groups*, J. Symb. Comp. **43** (2008), no. 8, 545–581.

INSTITUT FÜR GEOMETRIE UND TOPOLOGIE, PFAFFENWALDRING 57, UNIVERSITÄT STUTTGART
70550 STUTTGART, GERMANY

E-mail address: kohl@mathematik.uni-stuttgart.de