

# A Simple Group Generated by Involutions Interchanging Residue Classes of the Integers

Stefan Kohl

Institut für Geometrie und Topologie, Universität Stuttgart, 70550 Stuttgart / Germany,  
e-mail: kohl@mathematik.uni-stuttgart.de

**Abstract.** We present a new countable simple group, which arises in a natural way from the arithmetical structure of the ring of integers.

## 1. Introduction

Several types of infinite simple groups are treated in the literature so far: We refer to Carter [4] for the simple groups of Lie type, to Higman [8] and Stein [19] for finitely presented simple groups, to Kegel, Wehrfritz [10] for locally finite simple groups, to Baer [1] for composition factors of infinite symmetric groups, and to Ol'shanskii [18] and Chehata [5] for constructions of simple groups with certain given special properties.

Here we present and investigate a new infinite simple group, which does not belong to any of the moderately well-investigated classes mentioned above. Our group emerges in a natural way from the arithmetical structure of the ring of integers:

**1.1 Definition** Let  $\text{CT}(\mathbb{Z})$  be the group which is generated by the set of all *class transpositions*: Given disjoint residue classes  $r_1(m_1)$  and  $r_2(m_2)$  of  $\mathbb{Z}$ , we define the *class transposition*  $\tau_{r_1(m_1), r_2(m_2)} \in \text{Sym}(\mathbb{Z})$  by

$$\tau_{r_1(m_1), r_2(m_2)} : n \longmapsto \begin{cases} (m_2n + m_1r_2 - m_2r_1)/m_1 & \text{if } n \in r_1(m_1), \\ (m_1n + m_2r_1 - m_1r_2)/m_2 & \text{if } n \in r_2(m_2), \\ n & \text{otherwise,} \end{cases}$$

where we assume that  $0 \leq r_1 < m_1$  and that  $0 \leq r_2 < m_2$ . For reasons of convenience, we set  $\tau := \tau_{0(2), 1(2)} : n \mapsto n + (-1)^n$ .

The following theorems list various properties of  $\text{CT}(\mathbb{Z})$ . Their proof is the main subject of this article. In addition, in the last section we identify two simple supergroups of  $\text{CT}(\mathbb{Z})$  which are in a certain sense canonical.

**1.2 Theorem** (Properties of  $\text{CT}(\mathbb{Z})$ )

1. The group  $\text{CT}(\mathbb{Z})$  is simple.
2. The group  $\text{CT}(\mathbb{Z})$  is countable, but it has uncountably many simple subgroups.
3. The group  $\text{CT}(\mathbb{Z})$  is not finitely generated.
4. The torsion subgroups of  $\text{CT}(\mathbb{Z})$  are divisible.
5. The group  $\text{CT}(\mathbb{Z})$  acts highly transitively on  $\mathbb{N}_0$ .

**1.3 Theorem** (Richness of the class of subgroups of  $\text{CT}(\mathbb{Z})$ )

1. Every finite group embeds into  $\text{CT}(\mathbb{Z})$ .
2. Every free group of finite rank embeds into  $\text{CT}(\mathbb{Z})$ .
3. The modular group  $\text{PSL}(2, \mathbb{Z})$  embeds into  $\text{CT}(\mathbb{Z})$ .
4. Every free product of finitely many finite groups embeds into  $\text{CT}(\mathbb{Z})$ .
5. The class of subgroups of  $\text{CT}(\mathbb{Z})$  is closed under taking
  - (a) direct products,
  - (b) wreath products with finite groups, and
  - (c) wreath products with  $(\mathbb{Z}, +)$ .
6. The group  $\text{CT}(\mathbb{Z})$  has
  - (a) finitely generated subgroups which are not finitely presented, and
  - (b) finitely generated subgroups with unsolvable membership problem.
7. The group  $\text{CT}(\mathbb{Z})$  has a locally finite simple subgroup which acts highly transitively on  $\mathbb{N}_0$ .

In 1932, Lothar Collatz investigated the permutation

$$\alpha \in \text{Sym}(\mathbb{Z}) : n \longmapsto \begin{cases} \frac{2n}{3} & \text{if } n \in 0(3), \\ \frac{4n-1}{3} & \text{if } n \in 1(3), \\ \frac{4n+1}{3} & \text{if } n \in 2(3) \end{cases}$$

of the integers. The cycle structure of this permutation is unknown so far (cp. Keller [11], Wirsching [20]). Anyway, determining an explicit factorization into generators we obtain the following result:

**1.4 Theorem** Collatz' permutation is an element of  $\text{CT}(\mathbb{Z})$ .

So far, the scope of computational group theory mainly comprises finite permutation groups, matrix groups, finitely presented groups, polycyclically presented groups and automata groups. For details, we refer to [9].

*En passant* this article presents a large new class of groups which are accessible to computational methods. This class includes the subgroups of  $\text{CT}(\mathbb{Z})$ . Algorithms to compute with such groups are implemented in the author's package **RCWA** [12] for the computer algebra system **GAP** [7]. Many of the results proven in this article have first been discovered during extensive experiments with the **RCWA** package.

## 2. Basic Properties of $\text{CT}(\mathbb{Z})$

In this section we prove that the group  $\text{CT}(\mathbb{Z})$  is not finitely generated, that every finite group embeds into it, that its torsion subgroups are divisible and that it acts highly transitively on  $\mathbb{N}_0$ . This covers Theorem 1.2, Assertion (3) – (5) and Theorem 1.3, Assertion (1). However, first we need to introduce a couple of basic terms:

**2.1 Definition** We call a mapping  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  *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. This means that for any residue class  $r(m)$  there are coefficients  $a_{r(m)}, b_{r(m)}, c_{r(m)} \in \mathbb{Z}$  such that the restriction of the mapping  $f$  to the set  $r(m) = \{r + km \mid k \in \mathbb{Z}\}$  is given by

$$f|_{r(m)} : r(m) \longrightarrow \mathbb{Z}, \quad n \longmapsto \frac{a_{r(m)} \cdot n + b_{r(m)}}{c_{r(m)}}.$$

We call the smallest possible  $m$  the *modulus* of  $f$ , written  $\text{Mod}(f)$ . 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 define the *multiplier*  $\text{Mult}(f)$  of  $f$  by  $\text{lcm}_{r(m) \in \mathbb{Z}/m\mathbb{Z}} a_{r(m)}$  and the *divisor*  $\text{Div}(f)$  of  $f$  by  $\text{lcm}_{r(m) \in \mathbb{Z}/m\mathbb{Z}} c_{r(m)}$ . We call  $f$  *integral* if  $\text{Div}(f) = 1$ . We call  $f$  *class-wise order-preserving* if all  $a_{r(m)}$  are positive.

It is easy to see that the permutations of this kind form a countable supergroup of  $\text{CT}(\mathbb{Z})$ .

**2.2 Definition** We denote the group consisting of all residue class-wise affine permutations of  $\mathbb{Z}$  by  $\text{RCWA}(\mathbb{Z})$ , and call its subgroups *residue class-wise affine* groups.

The notation ‘ $\text{CT}(\mathbb{Z})$ ’ resp. ‘ $\text{RCWA}(\mathbb{Z})$ ’ reflects that generalizations to suitable rings other than  $\mathbb{Z}$  make perfect sense. For the sake of simplicity and to keep the article easy to read, we refrain from following this possibly fruitful direction of research at this point.

**2.3 Theorem** *The group  $\text{CT}(\mathbb{Z})$  is not finitely generated.*

**Proof:** It is easy to see that the multiplier resp. divisor of the product of two residue class-wise affine permutations divides the product of the multipliers resp. divisors of the factors. Further it is obvious that inversion interchanges multiplier and divisor. Therefore as there are infinitely many primes and as for any positive integer  $n$  there is a class transposition  $\tau_{1(2),0(2n)}$  with multiplier and divisor  $n$ , the assertion follows.  $\square$

**2.4 Theorem** *The group  $\text{CT}(\mathbb{Z})$  acts highly transitively on  $\mathbb{N}_0$ , and any finite group embeds into it.*

**Proof:** Any finite symmetric group  $S_m$  embeds into  $\text{CT}(\mathbb{Z})$ : Let  $m \in \mathbb{N}$ , and let  $S_m$  act naturally on the set  $\{0, 1, \dots, m-1\}$ . Then an example of a corresponding monomorphism is

$$\begin{aligned} \varphi_m : S_m &\hookrightarrow \text{CT}(\mathbb{Z}), \\ \sigma &\mapsto (\sigma^{\varphi_m} : n \mapsto n + (n \bmod m)^\sigma - n \bmod m). \end{aligned}$$

Just like the group  $S_m$  itself, its image under  $\varphi_m$  acts  $m$ -transitively on the set  $\{0, 1, \dots, m-1\}$ . Since  $m$  can be chosen arbitrary large and as class transpositions map nonnegative integers to nonnegative integers, the group  $\text{CT}(\mathbb{Z})$  acts highly transitively on  $\mathbb{N}_0$ .  $\square$

**2.5 Theorem** *The torsion subgroups of  $\text{CT}(\mathbb{Z})$  are divisible.*

**Proof:** We show that given an element  $g \in \text{CT}(\mathbb{Z})$  of finite order and a positive integer  $k$ , there is always an  $h \in \text{CT}(\mathbb{Z})$  such that  $h^k = g$ : Since the element  $g$  has finite order, it permutes a partition  $\mathcal{P}$  of  $\mathbb{Z}$  into finitely many residue classes on all of which it is affine. A  $k$ -th root  $h$  can be constructed from  $g$  by ‘slicing’ cycles  $\prod_{i=2}^l \tau_{r_1(m_1), r_i(m_i)}$  on  $\mathcal{P}$  into cycles  $\prod_{i=1}^l \prod_{j=\max(2-i, 0)}^{k-1} \tau_{r_1(km_1), r_i + jm_i(km_i)}$  of the  $k$ -fold length on the refined partition which one gets from  $\mathcal{P}$  by decomposing any  $r_i(m_i) \in \mathcal{P}$  into residue classes  $(\bmod km_i)$ .  $\square$

### 3. The Simplicity of $\text{CT}(\mathbb{Z})$

The aim of this section is to show that the group  $\text{CT}(\mathbb{Z})$  is simple, and that it has uncountably many simple subgroups. This covers Theorem 1.2, Assertion (1) and (2).

We need a couple of lemmata:

**3.1 Lemma** *Given two class transpositions  $\tau_{r_1(m_1), r_2(m_2)}, \tau_{r_3(m_3), r_4(m_4)}$  not equal to  $\tau$ , there is always a product  $\pi$  of 6 class transpositions such that  $\tau_{r_1(m_1), r_2(m_2)}^\pi = \tau_{r_3(m_3), r_4(m_4)}$ .*

**Proof:** Let  $r_5(m_5), r_6(m_6) \subset \mathbb{Z} \setminus (r_1(m_1) \cup r_2(m_2))$  be disjoint residue classes such that  $\cup_{i=3}^6 r_i(m_i) \neq \mathbb{Z}$ , and  $r_7(m_7), r_8(m_8) \subset \mathbb{Z} \setminus \cup_{i=3}^6 r_i(m_i)$  be disjoint residue classes. Then the following hold:

1.  $\tau_{r_1(m_1), r_2(m_2)}^{\tau_{r_1(m_1), r_5(m_5)} \cdot \tau_{r_2(m_2), r_6(m_6)}} = \tau_{r_5(m_5), r_6(m_6)}$ .
2.  $\tau_{r_5(m_5), r_6(m_6)}^{\tau_{r_5(m_5), r_7(m_7)} \cdot \tau_{r_6(m_6), r_8(m_8)}} = \tau_{r_7(m_7), r_8(m_8)}$ .
3.  $\tau_{r_7(m_7), r_8(m_8)}^{\tau_{r_3(m_3), r_7(m_7)} \cdot \tau_{r_4(m_4), r_8(m_8)}} = \tau_{r_3(m_3), r_4(m_4)}$ .

The assertion follows.  $\square$

**3.2 Lemma** *Let  $\sigma, v \in \text{RCWA}(\mathbb{Z})$ , and put  $m := \text{Mod}(\sigma)$ . If  $v$  is integral and fixes all residue classes (mod  $m$ ) setwisely, then  $[\sigma, v]$  is also integral.*

**Proof:** Since  $v$  fixes residue classes (mod  $m$ ), an affine partial mapping  $\alpha$  of  $[\sigma, v]$  is a product  $\alpha_\sigma^{-1} \alpha_{v^{-1}} \alpha_\sigma \alpha_v$  of affine partial mappings  $\alpha_\sigma, \alpha_v$  and  $\alpha_{v^{-1}}$  of  $\sigma, v$  resp.  $v^{-1}$ . The assertion follows since the subgroup generated by translations and reflections is normal in the affine group of  $\mathbb{Q}$ .  $\square$

**3.3 Lemma** *Let  $G$  be a subgroup of  $\text{RCWA}(\mathbb{Z})$  which contains  $\text{CT}(\mathbb{Z})$ . Then any nontrivial normal subgroup  $N \trianglelefteq G$  has an integral element  $\iota \neq 1$ .*

**Proof:** Let  $\sigma \in N \setminus \{1\}$ , and let  $m := \text{Mod}(\sigma)$ . Without loss of generality we can assume that there is a residue class  $r(m)$  such that  $r(m)^\sigma \neq r(m)$ . Put  $\iota := [\sigma, \tau_{r(2m), r+m(2m)}] \in N \setminus \{1\}$ . By Lemma 3.2,  $\iota$  is integral.  $\square$

Now we can prove our theorem:

**3.4 Theorem** *The group  $\text{CT}(\mathbb{Z})$  is simple.*

**Proof:** We have to show that any nontrivial normal subgroup  $N \trianglelefteq \text{CT}(\mathbb{Z})$  contains any class transposition.

By Lemma 3.1 all class transpositions  $\neq \tau$  are conjugate in  $\text{CT}(\mathbb{Z})$ . Further we have  $\tau = \tau_{0(4), 1(4)} \cdot \tau_{2(4), 3(4)}$ . Thus it is already sufficient to show that one class transposition  $\neq \tau$  lies in  $N$ .

By Lemma 3.3 the normal subgroup  $N$  has an integral element  $\iota_1 \neq 1$ . Let  $m \geq 3$  be a large enough multiple of the modulus of  $\iota_1$  such that there is a residue class  $r(m) \in \mathbb{Z}/m\mathbb{Z}$  which  $\iota_1$  does not fix setwisely. Then put  $\iota_2 := \tau_{r(2m), r+m(2m)} \cdot \tau_{r(2m)^{\iota_1}, r+m(2m)^{\iota_1}} = [\tau_{r(2m), r+m(2m)}, \iota_1] \in N$ .

By the choice of  $m$  we can now choose two distinct residue classes  $r_1(2m), r_2(2m) \notin \{r(2m), r+m(2m), r(2m)^{\iota_1}, r+m(2m)^{\iota_1}\}$ . Then we have

$$\begin{aligned} \tau_{r_1(2m), r_2(2m)} &= \iota_2^{\tau_{r(2m), r_1(4m)} \cdot \tau_{r+m(2m), r_2(4m)}} \\ &\quad \cdot \iota_2^{\tau_{r(2m), r_1+2m(4m)} \cdot \tau_{r+m(2m), r_2+2m(4m)}} \in N, \end{aligned}$$

which completes the proof of the theorem.  $\square$

**3.5 Remark** Assume  $\text{CT}(\mathbb{Z}) \leq G \leq \text{RCWA}(\mathbb{Z})$ , and let  $N$  be a nontrivial normal subgroup of  $G$ . Then the proof of Theorem 3.4 shows in fact that  $N$  contains  $\text{CT}(\mathbb{Z})$ .

**3.6 Definition** Given a set of primes  $\mathbb{P}$ , let  $\text{CT}_{\mathbb{P}}(\mathbb{Z}) < \text{CT}(\mathbb{Z})$  denote the subgroup which is generated by all class transpositions whose moduli have only prime factors in  $\mathbb{P}$ .

**3.7 Corollary** *If the set  $\mathbb{P}$  contains 2, then  $\text{CT}_{\mathbb{P}}(\mathbb{Z})$  is simple as well. Hence the group  $\text{CT}(\mathbb{Z})$  has uncountably many simple subgroups.*

**Proof:** In case  $2 \in \mathbb{P}$ , all of our arguments in this section apply to  $\text{CT}_{\mathbb{P}}(\mathbb{Z})$  as well: In the proof of Lemma 3.1, we can choose the four residue classes  $r_5(m_5), \dots, r_8(m_8)$  in such a way that all prime factors of their moduli already divide  $m_1 m_2 m_3 m_4$ . The proofs of Lemma 3.2, Lemma 3.3 and Theorem 3.4 likewise do not require the presence of class transpositions whose moduli have certain odd factors.  $\square$

**3.8 Remark** It remains open whether there are distinct sets of primes  $\mathbb{P}_1$  and  $\mathbb{P}_2$  such that  $\text{CT}_{\mathbb{P}_1}(\mathbb{Z}) \cong \text{CT}_{\mathbb{P}_2}(\mathbb{Z})$ .

#### 4. Richness of the Class of Subgroups of $\text{CT}(\mathbb{Z})$

In this section we prove Theorem 1.3, Assertion (2) – (7).

**4.1 Theorem** *Free groups of finite rank and the modular group  $\text{PSL}(2, \mathbb{Z})$  embed into  $\text{CT}(\mathbb{Z})$ .*

**Proof:** To prove the assertion concerning free groups, it suffices to show that the free group of rank 2 embeds. An example of an embedding is

$$\begin{aligned} \varphi_{F_2} : F_2 = \langle a, b \rangle &\hookrightarrow \text{CT}(\mathbb{Z}), \\ a &\mapsto (\tau \cdot \tau_{0(2),1(4)})^2, \quad b \mapsto (\tau \cdot \tau_{0(2),3(4)})^2. \end{aligned}$$

This can be seen by applying the Table-Tennis Lemma (see for example la Harpe [6], Section II.B.) to the infinite cyclic groups generated by the images of  $a$  and  $b$  under  $\varphi_{F_2}$  and the sets  $0(4) \cup 1(4)$  and  $2(4) \cup 3(4)$ . Likewise, the Table-Tennis Lemma can be used to show that

$$\begin{aligned} \varphi_{\text{PSL}(2,\mathbb{Z})} : \text{PSL}(2, \mathbb{Z}) \cong C_3 \star C_2 &\cong \langle a, b \mid a^3 = b^2 = 1 \rangle \hookrightarrow \text{CT}(\mathbb{Z}), \\ a &\mapsto \tau_{0(4),2(4)} \cdot \tau_{1(2),0(4)}, \quad b \mapsto \tau \end{aligned}$$

is an embedding of the modular group  $\text{PSL}(2, \mathbb{Z})$ . In this case one can use the sets  $0(2)$  and  $1(2)$  in place of  $0(4) \cup 1(4)$  and  $2(4) \cup 3(4)$ .  $\square$

**4.2 Theorem** *Every free product of finitely many finite groups embeds into  $\text{CT}(\mathbb{Z})$ .*

**Proof:** Let  $G_0, \dots, G_{m-1}$  be finite groups. To see that their free product embeds in  $\text{CT}(\mathbb{Z})$ , proceed as follows: First consider regular permutation representations  $\varphi_r$  of the groups  $G_r$  on the residue classes  $(\text{mod } |G_r|)$ . Then take conjugates  $H_r := (\text{im } \varphi_r)^{\sigma_r}$  of the images of these representations under mappings  $\sigma_r \in \text{CT}(\mathbb{Z})$  which map  $0(|G_r|)$  to  $\mathbb{Z} \setminus r(m)$ . Finally use that point stabilizers in regular permutation groups are trivial and apply the Table-Tennis Lemma to the groups  $H_r$  and the residue classes  $r(m)$  to see that the group generated by the  $H_r$ 's is isomorphic to their free product.  $\square$

The group  $\text{RCWA}(\mathbb{Z})$  is not co-Hopfian. In the proof of the next theorem, we need the following monomorphisms:

**4.3 Definition** Let  $f$  be an injective residue class-wise affine mapping, and let  $\pi_f : \text{RCWA}(\mathbb{Z}) \hookrightarrow \text{RCWA}(\mathbb{Z})$ ,  $\sigma \mapsto \sigma_f$  be the monomorphism defined by the properties  $\forall \sigma \in \text{RCWA}(\mathbb{Z})$   $f\sigma_f = \sigma f$  and  $\text{supp}(\text{im } \pi_f) \subseteq \text{im } f$ . Then we call  $\pi_f$  the *restriction monomorphism* associated to  $f$ .

**4.4 Theorem** The class of subgroups of  $\text{CT}(\mathbb{Z})$  is closed under taking direct products, under taking wreath products with finite groups and under taking wreath products with  $(\mathbb{Z}, +)$ .

**Proof:** Given any two subgroups  $G, H \leq \text{RCWA}(\mathbb{Z})$ , the group generated by  $G^{\pi_{n \mapsto 2n}}$  and  $H^{\pi_{n \mapsto 2n+1}}$  is clearly isomorphic to  $G \times H$ . As the image of a class transposition  $\tau_{r_1(m_1), r_2(m_2)}$  under a restriction monomorphism  $\pi_{n \mapsto mn+r}$  is  $\tau_{mr_1+r(mm_1), mr_2+r(mm_2)}$ , the same argument can be used for our group  $\text{CT}(\mathbb{Z})$  as well.

Looking at the monomorphisms  $\pi_{mn+r}$  and  $\varphi_m$ , it is immediate to see that the classes of isomorphism types of subgroups of  $\text{RCWA}(\mathbb{Z})$  resp.  $\text{CT}(\mathbb{Z})$  are closed under forming wreath products with finite permutation groups as well.

Further given a subgroup  $G$ , a subgroup isomorphic to the wreath product  $G \wr (\mathbb{Z}, +)$  is generated by  $G^{\pi_{n \mapsto 4n+3}}$  and  $\tau \cdot \tau_{0(2), 1(4)}$ . This is seen best by checking that the orbit of the residue class  $3(4)$  under the action of the cyclic group  $\langle \tau \cdot \tau_{0(2), 1(4)} \rangle$  consists of disjoint residue classes, thus that the conjugates of  $G^{\pi_{n \mapsto 4n+3}}$  under powers of  $\tau \cdot \tau_{0(2), 1(4)}$  have pairwise disjoint supports.  $\square$

**4.5 Corollary** The group  $\text{CT}(\mathbb{Z})$  has

1. finitely generated subgroups which are not finitely presented, and
2. finitely generated subgroups with unsolvable membership problem.

**Proof:**

1. By Theorem 4.4, the group  $\text{CT}(\mathbb{Z})$  contains nontrivial wreath products  $G \wr (\mathbb{Z}, +)$ . By the main theorem in Baumslag [2], these are not finitely presented.
2. Let  $F_2 = \langle a, b \rangle$  be the free group of rank 2. Further let  $r_1, \dots, r_k \in F_2$  be the relators of a finitely presented group with unsolvable word problem – such a group exists by Novikov [17] and Boone [3]. Then the membership problem for the group

$$\langle (a, a), (b, b), (1, r_1), \dots, (1, r_k) \rangle < F_2 \times F_2$$

is unsolvable (cp. Mihailova [16]; see also Lyndon, Schupp [15], Chapter IV.4). Therefore as by Theorem 4.1 and Theorem 4.4 the group  $F_2 \times F_2$  embeds into  $\text{CT}(\mathbb{Z})$ , there exist finitely generated subgroups  $G < \text{CT}(\mathbb{Z})$  with unsolvable membership problem.  $\square$

The class transpositions which interchange residue classes with the same modulus generate a proper subgroup of  $\text{CT}(\mathbb{Z})$ :

**4.6 Definition** Let  $\text{CT}_{\text{int}}(\mathbb{Z})$  denote the subgroup of  $\text{CT}(\mathbb{Z})$  which is generated by all integral class transpositions.

The group  $\text{CT}_{\text{int}}(\mathbb{Z})$  acts highly transitively on  $\mathbb{N}_0$  for the same reasons as  $\text{CT}(\mathbb{Z})$  does so. Finitely generated subgroups of  $\text{CT}_{\text{int}}(\mathbb{Z})$  act faithfully on the set of residue classes modulo the lcm of the moduli of the generators. Therefore they are finite. Hence the group  $\text{CT}_{\text{int}}(\mathbb{Z})$  is locally finite.

**4.7 Theorem** *The group  $\text{CT}_{\text{int}}(\mathbb{Z})$  is simple.*

**Proof:** We have to show that any nontrivial normal subgroup  $N \trianglelefteq \text{CT}_{\text{int}}(\mathbb{Z})$  contains any class transposition of the form  $\tau_{r_1(m), r_2(m)}$ .

Let  $\iota_1 \in N \setminus \{1\}$ . Further let  $m$  be a large enough multiple of the modulus of  $\iota_1$  such that there is a residue class  $r(m) \in \mathbb{Z}/m\mathbb{Z}$  which  $\iota_1$  does not fix setwisely. Then

$\iota_2 := \tau_{r(2m), r+m(2m)} \cdot \tau_{r(2m)^{\iota_1}, r+m(2m)^{\iota_1}} = [\iota_1, \tau_{r(2m), r+m(2m)}] \in N$  is a product of two class transpositions with modulus  $2m$  and disjoint supports.

We make the following observations:

1. All products of two integral class transpositions with the same modulus  $m \geq 4$  and disjoint supports are conjugate in the group  $\text{CT}_{\text{int}}(\mathbb{Z})$ : Let  $(r_i(m))_{i \in \{1, \dots, 4\}}$  and  $(\tilde{r}_i(m))_{i \in \{1, \dots, 4\}}$  each be 4-tuples of pairwise disjoint residue classes. Then we have

$$(\tau_{r_1(m), r_2(m)} \cdot \tau_{r_3(m), r_4(m)})^{\prod_{i=1}^4 \tau_{r_i(m), \tilde{r}_i(m)}} = \tau_{\tilde{r}_1(m), \tilde{r}_2(m)} \cdot \tau_{\tilde{r}_3(m), \tilde{r}_4(m)},$$

where we read  $\tau_{r_i(m), \tilde{r}_i(m)}$  as the identity if  $r_i = \tilde{r}_i$ .

2. Given class transpositions  $\tau_1 = \tau_{r_1(m), r_2(m)}$  and  $\tau_2 = \tau_{r_3(2m), r_4(2m)}$  with disjoint supports, we have

$$\begin{aligned} \tau_1 &= \tau_2 \cdot \tau_{r_1(2m), r_2(2m)} \\ &\quad \cdot \tau_2 \cdot \tau_{r_1+m(2m), r_2+m(2m)}. \end{aligned}$$

Therefore any integral class transposition  $\neq \tau$  can be written as a product of two suitable products of two integral class transpositions with disjoint supports.

3. Given  $k \in \mathbb{N}$ , any integral class transposition can be written as a product of  $k$  integral class transpositions with the  $k$ -fold modulus. This can be seen from the equality  $\tau_{r_1(m), r_2(m)} = \prod_{i=0}^{k-1} \tau_{r_1+im(km), r_2+im(km)}$ .

In the second paragraph of the proof we can choose  $m$  to be a multiple of any given positive integer. Therefore from Observation (1) – (3) we can conclude that  $N$  contains indeed any integral class transposition. Hence the group  $\text{CT}_{\text{int}}(\mathbb{Z})$  is simple, as claimed.  $\square$



### 5. Collatz' Permutation Lies in $\text{CT}(\mathbb{Z})$

In this section we show that Collatz' permutation

$$\alpha \in \text{RCWA}(\mathbb{Z}) : n \mapsto \begin{cases} \frac{2n}{3} & \text{if } n \in 0(3), \\ \frac{4n-1}{3} & \text{if } n \in 1(3), \\ \frac{4n+1}{3} & \text{if } n \in 2(3) \end{cases}$$

lies in  $\text{CT}(\mathbb{Z})$ , and thus prove Theorem 1.4 from the introduction.

In Keller [11] it is shown that  $\alpha$  has at most finitely many cycles of any given finite length. It further looks likely that except of the fixed points 0 and  $\pm 1$ , the only finite cycles are the transpositions  $\pm(2\ 3)$ , the 5-cycles  $\pm(4\ 5\ 7\ 9\ 6)$  and the 12-cycles  $\pm(44\ 59\ 79\ 105\ 70\ 93\ 62\ 83\ 111\ 74\ 99\ 66)$ . However according to Wirsching [20] the latter has still not been proven, and in particular it is not yet known whether the cycle

$$(\dots\ 32\ 43\ 57\ 38\ 51\ 34\ 45\ 30\ 20\ 27\ 18\ 12\ 8\ 11\ 15\ 10\ 13\ 17\ 23\ 31\ \dots)$$

of  $\alpha$  is finite or infinite.

In spite of this we can show that the permutation  $\alpha$  lies in  $\text{CT}(\mathbb{Z})$  by determining an explicit factorization into generators.

The major obstacle we are confronted with when trying to obtain such a factorization is the fact that multiplier and divisor of  $\alpha$  are coprime, whereas multiplier and divisor of a class transposition are always the same. We have already observed that the multiplier resp. divisor of a product of two residue class-wise affine mappings always divides the product of the multipliers resp. divisors of the factors. In the given case we need to form a product of class transpositions in such a way that one prime divisor gets eliminated from the multiplier of the product, but appears in the denominators of all of its affine partial mappings.

As a first step towards a solution of the factorization problem, we hence attempt to determine some product of class transpositions which has coprime multiplier and divisor. It turns out that 6 class transpositions are sufficient to form such a product: Given an odd prime  $p$ , the permutation

$$\begin{aligned} \sigma_p &:= \tau_{0(8),1(2p)} \cdot \tau_{4(8),2p-1(2p)} \\ &\quad \cdot \tau_{0(4),1(2p)} \cdot \tau_{2(4),2p-1(2p)} \\ &\quad \cdot \tau_{2(2p),1(4p)} \cdot \tau_{4(2p),2p+1(4p)} \in \text{CT}(\mathbb{Z}) \end{aligned}$$

has multiplier  $p$  and divisor 2. Indeed, evaluating this product yields

$$\sigma_p : n \mapsto \begin{cases} (pn + 2p - 2)/2 & \text{if } n \in 2(4), \\ n/2 & \text{if } n \in 0(4) \setminus (4(4p) \cup 8(4p)), \\ n + 2p - 7 & \text{if } n \in 8(4p), \\ n - 2p + 5 & \text{if } n \in 2p - 1(2p), \\ n + 1 & \text{if } n \in 1(2p), \\ n - 3 & \text{if } n \in 4(4p), \\ n & \text{if } n \in 1(2) \setminus (1(2p) \cup 2p - 1(2p)). \end{cases}$$

The GAP [7] package RCWA [12] provides a factorization routine for residue class-wise affine permutations, which uses certain elaborate heuristics. The permutations  $\sigma_p$  and their images under restriction monomorphisms  $\pi_{n \rightarrow mn+r}$  play a key role in this routine. It has been used to obtain the following factorization of  $\alpha$ :

$$\begin{aligned} \alpha = & \tau_{0(6),4(6)} \cdot \tau_{0(6),5(6)} \cdot \tau_{0(6),3(6)} \cdot \tau_{0(6),1(6)} \cdot \tau_{0(6),2(6)} \\ & \cdot \tau_{2(3),4(6)} \cdot \tau_{0(3),4(6)} \cdot \tau_{2(3),1(6)} \cdot \tau_{0(3),1(6)} \cdot \tau_{0(36),35(36)} \\ & \cdot \tau_{0(36),22(36)} \cdot \tau_{0(36),18(36)} \cdot \tau_{0(36),17(36)} \cdot \tau_{0(36),14(36)} \cdot \tau_{0(36),20(36)} \\ & \cdot \tau_{0(36),4(36)} \cdot \tau_{2(36),8(36)} \cdot \tau_{2(36),16(36)} \cdot \tau_{2(36),13(36)} \cdot \tau_{2(36),9(36)} \\ & \cdot \tau_{2(36),7(36)} \cdot \tau_{2(36),6(36)} \cdot \tau_{2(36),3(36)} \cdot \tau_{2(36),10(36)} \cdot \tau_{2(36),15(36)} \\ & \cdot \tau_{2(36),12(36)} \cdot \tau_{2(36),5(36)} \cdot \tau_{21(36),28(36)} \cdot \tau_{21(36),33(36)} \cdot \tau_{21(36),30(36)} \\ & \cdot \tau_{21(36),23(36)} \cdot \tau_{21(36),34(36)} \cdot \tau_{21(36),31(36)} \cdot \tau_{21(36),27(36)} \cdot \tau_{21(36),25(36)} \\ & \cdot \tau_{21(36),24(36)} \cdot \tau_{26(36),32(36)} \cdot \tau_{26(36),29(36)} \cdot \tau_{10(18),35(36)} \cdot \tau_{5(18),35(36)} \\ & \cdot \tau_{10(18),17(36)} \cdot \tau_{5(18),17(36)} \cdot \tau_{8(12),14(24)} \cdot \tau_{6(9),17(18)} \cdot \tau_{3(9),17(18)} \\ & \cdot \tau_{0(9),17(18)} \cdot \tau_{6(9),16(18)} \cdot \tau_{3(9),16(18)} \cdot \tau_{0(9),16(18)} \cdot \tau_{6(9),11(18)} \\ & \cdot \tau_{3(9),11(18)} \cdot \tau_{0(9),11(18)} \cdot \tau_{6(9),4(18)} \cdot \tau_{3(9),4(18)} \cdot \tau_{0(9),4(18)} \\ & \cdot \tau_{0(6),14(24)} \cdot \tau_{0(6),2(24)} \cdot \tau_{8(12),17(18)} \cdot \tau_{7(12),17(18)} \cdot \tau_{8(12),11(18)} \\ & \cdot \tau_{7(12),11(18)} \cdot \sigma_3^{-1} \cdot \tau_{7(12),17(18)} \cdot \tau_{2(6),17(18)} \cdot \tau_{0(3),17(18)} \cdot \sigma_3^{-3}. \end{aligned}$$

This shows constructively that  $\alpha \in \text{CT}(\mathbb{Z})$ .

## 6. Two Simple Supergroups of $\text{CT}(\mathbb{Z})$

In this section we present two simple subgroups of  $\text{RCWA}(\mathbb{Z})$  which properly contain  $\text{CT}(\mathbb{Z})$  and which act highly transitively on  $\mathbb{Z}$ .

We identify these simple groups in the kernels of certain epimorphisms  $\pi^+ : \text{RCWA}^+(\mathbb{Z}) \rightarrow (\mathbb{Z}, +)$  and  $\pi^- : \text{RCWA}(\mathbb{Z}) \rightarrow \mathbb{Z}^\times \cong C_2$ , where  $\text{RCWA}^+(\mathbb{Z}) < \text{RCWA}(\mathbb{Z})$  denotes the subgroup consisting of all class-wise order-preserving elements. Using the notation for the coefficients introduced in Definition 2.1, these epimorphisms are given by

$$\pi^+ : \sigma \mapsto \frac{1}{m} \sum_{r(m) \in \mathbb{Z}/m\mathbb{Z}} \frac{b_{r(m)}}{a_{r(m)}}$$

and

$$\pi^- : \sigma \mapsto (-1)^{\sigma^{\pi^+} + \frac{1}{m} \sum_{r(m): a_{r(m)} < 0} (m - 2r)}$$

(see Sections 2.11 and 2.12 in Kohl [13]).

**6.1 Definition** We denote the kernels of  $\pi^+$  resp.  $\pi^-$  by  $K^+$  resp.  $K^-$ .

It is easy to see that  $\text{CT}(\mathbb{Z}) \leq K^+ \leq K^- \leq \text{RCWA}(\mathbb{Z})$ .

Our simple groups will be the subgroups of  $K^+$  and  $K^-$  which are generated by the elements which are *tame* in the following sense:

**6.2 Definition** We call an element  $\sigma \in \text{RCWA}(\mathbb{Z})$  *tame* if it permutes a partition  $\mathcal{P}$  of  $\mathbb{Z}$  into finitely many residue classes on all of which it is affine, and *wild* otherwise. We call a group  $G < \text{RCWA}(\mathbb{Z})$  *tame* if there is a common such partition for all elements of  $G$ , and *wild* otherwise. We call partitions with the described properties *respected partitions* of  $\sigma$  resp.  $G$ .

**6.3 Definition** We denote the normal subgroups of  $K^+$  resp.  $K^-$  which are generated by the tame elements by  $\tilde{K}^+$  resp.  $\tilde{K}^-$ .

Obviously, finite residue class-wise affine groups and integral residue class-wise affine permutations are tame. Tameness is invariant under conjugation: If  $\alpha \in \text{RCWA}(\mathbb{Z})$  respects a partition  $\mathcal{P}$ , then a conjugate  $\alpha^\beta$  respects the partition consisting of the images of the intersections of the residue classes in  $\mathcal{P}$  with the sources of the affine partial mappings of  $\beta$  under  $\beta$ . Of course the product of two tame permutations is in general not tame. Further, tameness of products does not induce an equivalence relation on the set of tame permutations: Let for example  $a := \tau_{1(6),4(6)}$ ,  $b := \tau_{0(5),2(5)}$  and  $c := \tau_{3(4),4(6)}$ . Then  $ab$  and  $bc$  are tame, but  $ac$  is not. If a tame group does not act faithfully on a respected partition, the kernel of the action clearly does not act on  $\mathbb{N}_0$ . Thus as the group  $\text{CT}(\mathbb{Z})$  acts on  $\mathbb{N}_0$ , its tame subgroups are finite. It can be shown that a residue class-wise affine group is tame if and only if the set of moduli of its elements is bounded (see Theorem 2.5.8 in [13]). An extension of the notion of tameness to non-bijective residue class-wise affine mappings is considered in [14].

It is easy to see that all tame elements of  $\text{RCWA}(\mathbb{Z})$  can be written as products of class transpositions and members of the following two series:

**6.4 Definition** Let  $r(m) \subset \mathbb{Z}$  be a residue class.

1. We define the *class shift*  $\nu_{r(m)} \in \text{RCWA}(\mathbb{Z})$  by

$$\nu_{r(m)} : n \mapsto \begin{cases} n + m & \text{if } n \in r(m), \\ n & \text{otherwise.} \end{cases}$$

2. We define the *class reflection*  $\varsigma_{r(m)} \in \text{RCWA}(\mathbb{Z})$  by

$$\varsigma_{r(m)} : n \mapsto \begin{cases} -n + 2r & \text{if } n \in r(m), \\ n & \text{otherwise,} \end{cases}$$

where we assume that  $0 \leq r < m$ .

For convenience, we set  $\nu := \nu_{\mathbb{Z}} : n \mapsto n + 1$  and  $\varsigma := \varsigma_{\mathbb{Z}} : n \mapsto -n$ .

Obviously, class shifts and class reflections do not lie in  $K^-$ .

**6.5 Theorem** *We have*

1.  $\tilde{K}^+ = \langle \text{CT}(\mathbb{Z}), \nu_{1(3)} \cdot \nu_{2(3)}^{-1} \rangle$ , and
2.  $\tilde{K}^- = \langle \text{CT}(\mathbb{Z}), \nu_{1(3)} \cdot \nu_{2(3)}, \varsigma_{0(2)} \cdot \nu_{0(2)} \rangle$ .

**Proof:** We identify 2 resp. 3 series of generators:

1. Looking at respected partitions, we check that  $\tilde{K}^+$  is generated by
  - (a) all class transpositions and
  - (b) all quotients of two class shifts with disjoint supports whose union has a nontrivial complement in  $\mathbb{Z}$ .

For this we consider the process of factoring a given tame  $\vartheta \in K^+$  into these elements:

- ad (a) Let  $\mathcal{P}$  be a respected partition of  $\vartheta$ . Divide  $\vartheta$  by a product of class transpositions which respects  $\mathcal{P}$  as well and which induces on  $\mathcal{P}$  the same permutation as  $\vartheta$  does.
- ad (b) Factor the remaining quotient which is integral and fixes the partition  $\mathcal{P}$  into quotients of two class shifts with disjoint supports which respect  $\mathcal{P}$ . This works since the lattice in  $\mathbb{Z}^n$  consisting of all vectors with zero coordinate sum is spanned by the differences of two distinct canonical basis vectors.

2. Looking at respected partitions, we check that  $\tilde{K}^-$  is generated by
  - (a) all products of a class reflection and a class shift with the same support which has a nontrivial complement in  $\mathbb{Z}$ ,
  - (b) all class transpositions and
  - (c) all products of two class shifts with disjoint supports whose union has a nontrivial complement in  $\mathbb{Z}$ .

Similar as above, we consider the process of factoring a given tame permutation  $\vartheta \in K^-$  into these elements:

- ad (a) Let  $m \geq 2$  be a multiple of  $\text{Mod}(\vartheta)$ . Make  $\vartheta$  class-wise order-preserving via divisions from the left by products  $\varsigma_{r(m)} \cdot \nu_{r(m)}$ , where  $r(m)$  runs over all residue classes (mod  $m$ ) on which  $\vartheta$  is order-reversing.
- ad (b) Let  $\mathcal{P}$  be a respected partition of  $\vartheta$  of length at least 3. Divide  $\vartheta$  by a product of class transpositions which respects  $\mathcal{P}$  as well and which induces on  $\mathcal{P}$  the same permutation as  $\vartheta$  does.
- ad (c) Factor the remaining quotient which is integral and fixes  $\mathcal{P}$  into products of two class shifts with disjoint supports and inverses of such products. This works since for  $n \geq 3$  the lattice in  $\mathbb{Z}^n$  consisting of all vectors with even coordinate sum is spanned by the sums of two distinct canonical basis vectors.

Now we collapse series (1.b.), (2.a.) and (2.c) by taking orbit representatives under the conjugation action of  $\text{CT}(\mathbb{Z})$  to obtain the indicated single generators.  $\square$

**6.6 Theorem** *The groups  $\tilde{K}^+$  and  $\tilde{K}^-$  are simple.*

**Proof:** First we prove the simplicity of  $\tilde{K}^+$  and  $\tilde{K}^-$ . From Remark 3.5 we know that nontrivial normal subgroups of these groups contain  $\text{CT}(\mathbb{Z})$ .

1. Let  $N$  be a nontrivial normal subgroup of  $\tilde{K}^+$ . Let  $r_1(m_1)$  and  $r_2(m_2)$  be two disjoint residue classes whose union is not  $\mathbb{Z}$ . Then for any residue class  $r_3(m_3) \subset \mathbb{Z} \setminus (r_1(m_1) \cup r_2(m_2))$  we have

$$\nu_{r_1(m_1)} \cdot \nu_{r_2(m_2)}^{-1} = [\tau_{r_1(m_1), r_2(m_2)}, \nu_{r_3(m_3)} \cdot \nu_{r_2(m_2)}^{-1}] \in N.$$

Putting  $r_1(m_1) := 1(3)$  and  $r_2(m_2) := 2(3)$ , the simplicity of  $\tilde{K}^+$  follows from Theorem 6.5, Assertion (1).

2. Let  $N$  be a nontrivial normal subgroup of  $\tilde{K}^-$ . Given disjoint residue classes  $r_1(m_1)$  and  $r_2(m_2)$  whose union is not  $\mathbb{Z}$ , for any residue class  $r_3(m_3) \subset \mathbb{Z} \setminus (r_1(m_1) \cup r_2(m_2))$  we have

$$\begin{aligned} \nu_{r_1(m_1)} \cdot \nu_{r_2(m_2)} &= [\tau_{r_1(m_1), r_2(m_2)}, \nu_{r_3(m_3)} \cdot \varsigma_{r_1(m_1)}] \\ &\quad \cdot [\tau_{r_1(m_1), r_2(m_2)}, \varsigma_{r_1(m_1)} \cdot \nu_{r_1(m_1)}] \in N. \end{aligned}$$

This shows in particular that  $N$  contains  $\nu_{1(3)} \cdot \nu_{2(3)}$ .

Let  $r(m) \subsetneq \mathbb{Z}$  be a residue class. Then for an arbitrary residue class  $\tilde{r}(\tilde{m}) \subset \mathbb{Z} \setminus r(m)$  we have

$$\begin{aligned} \varsigma_{r(m)} \cdot \nu_{r(m)} &= [\tau_{r(m), \tilde{r}(\tilde{m})}, \varsigma_{r(m)} \cdot \nu_{\tilde{r}(\tilde{m})}] \\ &\quad \cdot [\tau_{\tilde{r}(2\tilde{m}), \tilde{r}+\tilde{m}(2\tilde{m})}, \varsigma_{\tilde{r}(2\tilde{m})} \cdot \nu_{\tilde{r}(2\tilde{m})}] \\ &\quad \cdot (\nu_{\tilde{r}(2\tilde{m})} \cdot \nu_{\tilde{r}+\tilde{m}(2\tilde{m})} \cdot \tau_{\tilde{r}(2\tilde{m}), \tilde{r}+\tilde{m}(2\tilde{m})})^{-1} \in N. \end{aligned}$$

This shows in particular that  $N$  contains also  $\varsigma_{0(2)} \cdot \nu_{0(2)}$ , and the simplicity of  $\tilde{K}^-$  follows from Theorem 6.5, Assertion (2).  $\square$

**6.7 Theorem** *The groups  $\tilde{K}^+$  and  $\tilde{K}^-$  act highly transitively on  $\mathbb{Z}$ .*

**Proof:** Since  $\tilde{K}^+ < \tilde{K}^-$  it is sufficient to prove the assertion for  $\tilde{K}^+$ . Let  $k$  be a positive integer, and let  $(n_1, \dots, n_k)$  and  $(\tilde{n}_1, \dots, \tilde{n}_k)$  be two  $k$ -tuples of pairwise distinct integers. We have to show that there is an element  $\sigma \in \tilde{K}^+$  such that  $(n_1^\sigma, \dots, n_k^\sigma) = (\tilde{n}_1, \dots, \tilde{n}_k)$ .

Let  $m := 2k + 1$ , and choose a residue class  $r(m)$  which does not contain one of the points  $n_i$  or  $\tilde{n}_i$ . Define  $\sigma_1, \tilde{\sigma}_1 \in \tilde{K}^+$  by

$$\sigma_1 := \prod_{i: n_i < 0} (\nu_{r(m)} \cdot \nu_{n_i(m)}^{-1})^{\lfloor \frac{n_i}{m} \rfloor} \quad \text{resp.} \quad \tilde{\sigma}_1 := \prod_{i: \tilde{n}_i < 0} (\nu_{r(m)} \cdot \nu_{\tilde{n}_i(m)}^{-1})^{\lfloor \frac{\tilde{n}_i}{m} \rfloor}.$$

Then the images of all points  $n_i$  resp.  $\tilde{n}_i$  under  $\sigma_1$  resp.  $\tilde{\sigma}_1$  are nonnegative. Since we know that  $\text{CT}(\mathbb{Z})$  acts highly transitively on  $\mathbb{N}_0$ , we can choose a  $\sigma_2 \in \text{CT}(\mathbb{Z}) < \tilde{K}^+$  which maps the images of the  $n_i$  under  $\sigma_1$  to the images of the  $\tilde{n}_i$  under  $\tilde{\sigma}_1$ . Now the permutation  $\sigma := \sigma_1 \cdot \sigma_2 \cdot \tilde{\sigma}_1^{-1}$  serves our purposes.  $\square$

**6.8 Conjecture** The group  $\text{RCWA}(\mathbb{Z})$  is generated by its tame elements.

**6.9 Remark** Conjecture 6.8 is equivalent to the assertion that  $\tilde{K}^+ = K^+$  and that  $\tilde{K}^- = K^-$ . If it holds, we have  $\text{RCWA}(\mathbb{Z}) = \langle \text{CT}(\mathbb{Z}), \varsigma_{0(2)} \rangle$ :

1. It is  $\nu = \varsigma_{0(2)} \cdot \tau \cdot (\varsigma_{0(2)}^{\tau_{1(4),2(4)}} \cdot \varsigma_{0(2)}^{\tau_{1(2),0(4)}})^{\tau_{0(2),1(4)}} \in \langle \text{CT}(\mathbb{Z}), \varsigma_{0(2)} \rangle$ .
2. It is  $\nu_{0(2)} = \tau\nu$ ,  $\nu_{1(2)} = \nu_{0(2)}^\tau$ ,  $\varsigma_{1(2)} = \varsigma_{0(2)}^\tau$  and  $\varsigma = \varsigma_{0(2)} \cdot \nu_{1(2)} \cdot \varsigma_{1(2)}$ .  
Therefore we know that  $\{\nu_{0(2)}, \nu_{1(2)}, \varsigma_{1(2)}, \varsigma\} \subset \langle \text{CT}(\mathbb{Z}), \varsigma_{0(2)} \rangle$ .
3. Let  $r(m) \subsetneq \mathbb{Z}$  be a residue class  $\neq 1(2)$ . We choose a residue class  $\tilde{r}(\tilde{m}) \subset \mathbb{Z} \setminus (0(2) \cup r(m))$ , and put  $\vartheta := \tau_{0(2),\tilde{r}(\tilde{m})} \cdot \tau_{\tilde{r}(\tilde{m}),r(m)} \in \text{CT}(\mathbb{Z})$ .  
Then we have  $\{\nu_{r(m)}, \varsigma_{r(m)}\} = \{\nu_{0(2)}^\vartheta, \varsigma_{0(2)}^\vartheta\} \subset \langle \text{CT}(\mathbb{Z}), \varsigma_{0(2)} \rangle$ .

The corresponding factorization routine in  $\text{RCWA}$  [12] provides some evidence for the validity of our conjecture.

## Acknowledgements

I would like to thank Bettina Eick for her continuing encouragement and for nicely drafting the introduction of this article.

Likewise I would like to thank Laurent Bartholdi for his hint that the classes of subgroups of  $\text{CT}(\mathbb{Z})$  and  $\text{RCWA}(\mathbb{Z})$  are closed under taking wreath products with  $(\mathbb{Z}, +)$ .

## References

1. Reinhold Baer. Die Kompositionsreihe der Gruppe aller eineindeutigen Abbildungen einer unendlichen Menge auf sich. *Studia Math.*, 5:15–17, 1934.
2. Gilbert Baumslag. Wreath products and finitely presented groups. *Math. Z.*, 75:22–28, 1961.
3. W. W. Boone. The word problem. *Ann. of Math.*, 70:207–265, 1959.
4. Roger W. Carter. *Simple Groups of Lie Type*. Wiley Classics Library Edition. John Wiley & Sons, 1972.
5. C. G. Chehata. An algebraically simple ordered group. *Proc. London Math. Soc. (3)*, 2:183–197, 1952.
6. Pierre de la Harpe. *Topics in Geometric Group Theory*. Chicago Lectures in Mathematics, 2000.
7. The GAP Group. *GAP – Groups, Algorithms, and Programming; Version 4.4.7*, 2006. <http://www.gap-system.org>.
8. Graham Higman. *Finitely Presented Infinite Simple Groups*. Notes on Pure Mathematics. Department of Pure Mathematics, Australian National University, Canberra, 1974.
9. Derek F. Holt, Bettina Eick, and Eamonn A. O’Brien. *Handbook of Computational Group Theory*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall / CRC, Boca Raton, FL, 2005.
10. Otto H. Kegel and Bertram A. F. Wehrfritz. *Locally Finite Groups*. North-Holland Publishing Company, 1973.
11. Timothy P. Keller. Finite cycles of certain periodically linear permutations. *Missouri J. Math. Sci.*, 11(3):152–157, 1999.

12. Stefan Kohl. *RCWA - Residue Class-Wise Affine Groups*, 2005. GAP package, <http://www.gap-system.org/Packages/rcwa.html>.
13. Stefan Kohl. *Restklassenweise affine Gruppen*. Dissertation, Universität Stuttgart, 2005. <http://deposit.ddb.de/cgi-bin/dokserv?idn=977164071>.
14. Stefan Kohl. Wildness of iteration of certain residue class-wise affine mappings. *Advances in Applied Mathematics*, ?(?):approx. 8 pages, 2006. to appear.
15. Roger C. Lyndon and Paul E. Schupp. *Combinatorial Group Theory*. Springer-Verlag, 1977. Reprinted in the Springer Classics in Mathematics Series, 2000.
16. K. A. Mihailova. The occurrence problem for direct products of groups. (Russian). *Mat. Sb.*, 70(112):241–251, 1966.
17. P. S. Novikov. On the algorithmic unsolvability of the word problem in group theory. (Russian). *Trudy Math. Inst. Steklov*, 44:143, 1955.
18. Alexander Yu. Ol'shanskii. Infinite groups with cyclic subgroups. (Russian). *Dokl. Akad. Nauk. SSSR*, 245(4):785–787, 1979.
19. Melanie Stein. Groups of piecewise linear homoeomorphisms. *Trans. Amer. Math. Soc.*, 332(2):477–514, 1992.
20. Günther J. Wirsching. The dynamical system on the natural numbers generated by the  $3n+1$  function. Habilitationsschrift, Katholische Universität Eichstätt, 1996.