On a Class of

Infinite Permutation Groups

Stefan Kohl

December 10, 2005
Nikolaus Conference 2005 in Aachen

Motivation (I)

3n+1 Conjecture: Iterated application of the Collatz mapping

$$T: \ \mathbb{Z} \longrightarrow \mathbb{Z},$$

$$n \ \longmapsto \ \begin{cases} \frac{n}{2} & \text{if } \ n \text{ even,} \\ \frac{3n+1}{2} & \text{if } \ n \text{ odd} \end{cases}$$

to any positive integer yields 1 after a finite number of steps, i.e.

$$\forall n \in \mathbb{N} \quad \exists k \in \mathbb{N}_0: \ n^{T^k} = 1.$$

This conjecture has been made by Lothar Collatz in the 1930s, and is still open today.

Example: Starting at $n = 7$ we get the sequence

$$7, 11, 17, 26, 13, 20, 10, 5, 8, 4, 2, 1.$$

Residue class-wise affine groups are permutation groups which are generated by bijective mappings ‘similar to the Collatz mapping’.

Motivation (II)

Very little is currently known about highly transitive permutation groups, i.e. those which are k-fold transitive for any k.

The group RCWA($\mathbb{Z}$) of residue class-wise affine bijections of $\mathbb{Z}$ belongs to this class, and it has a rich and interesting group theoretical structure. To my knowledge, nobody else has investigated this group so far.

Explicit machine computation in RCWA($\mathbb{Z}$) and its subgroups is quite feasible – see the GAP package RCWA.

The group RCWA($\mathbb{Z}$) acts as a group of homeomorphisms on $\mathbb{Z}$ endowed with a topology by taking the set of all residue classes as a basis ('Fürstenberg's Topology').

Basic Terms

Let R denote an infinite euclidean ring, which has at least one prime ideal and all of whose proper residue class rings are finite.

We call a mapping $f : R \to R$ *residue class-wise affine*, or in short an *rcwa* mapping, if there is an $m \in R \setminus \{0\}$ such that the restrictions of f to the residue classes $r(m) \in R/mR$ are all affine.

This means that for any residue class $r(m)$ there are coefficients $a_{r(m)}, b_{r(m)}, c_{r(m)} \in R$ such that the restriction of the mapping f to the set $r(m) = \{r + km | k \in R\}$ is given by

$$f|_{r(m)}: \; r(m) \to R,$$

$$n \; \mapsto \; \frac{a_{r(m)} \cdot n + b_{r(m)}}{c_{r(m)}} \; .$$

We call m the *modulus* of f. To make this unique, we always choose m multiplicatively minimal.

Examples

Examples of rcwa mappings of $\mathbb{Z}$:

1. $\nu : n \mapsto n + 1$, $\varsigma : n \mapsto -n$ and $\tau : n \mapsto n + (-1)^n$.

2. The Collatz mapping T.

3. The permutation

$$\alpha : \quad n \ \mapsto \begin{cases} \frac{3n}{2} & \text{if} \quad n \equiv 0 \bmod 2, \\ \frac{3n+1}{4} & \text{if} \quad n \equiv 1 \bmod 4, \\ \frac{3n-1}{4} & \text{if} \quad n \equiv 3 \bmod 4 \end{cases}$$

which has already been investigated by Lothar Collatz as well. The cycle structure of α is 'unknown'. For example, it is not known whether the cycle containing 8 is infinite.

Aim

The bijective rcwa mappings of the ring R form a group, denoted by $\mathrm{RCWA}(R)$.

So far, my main goal was to find out as much as possible about the group $\mathrm{RCWA}(\mathbb{Z})$ of the residue class-wise affine bijections of the ring of integers and its subgroups.

Results (I)

The group $\mathrm{RCWA}(\mathbb{Z})$

- has $\mathbb{Z}^\times \cong C_2$ as an epimorphic image,
- has a trivial centre,
- has no solvable normal subgroup $\neq 1$,
- is not finitely generated,
- has finite subgroups of any isomorphism type, and
- has only finitely many conjugacy classes of elements of any given odd order, but infinitely many conjugacy classes of elements of any given even order.

Results (II)

The following hold:

- A finite extension $G \trianglerighteq N$ of a subdirect product N of finitely many infinite dihedral groups has always a monomorphic image in $\mathrm{RCWA}(\mathbb{Z})$.

- The homomorphisms of a given finite group G of odd order into $\mathrm{RCWA}(\mathbb{Z})$ are parametrized by the non-empty subsets of the set of equivalence classes of transitive permutation representations of G up to inner automorphisms of $\mathrm{RCWA}(\mathbb{Z})$.

-

Most of the results listed so far can easily be generalized to groups $\mathrm{RCWA}(R)$ over euclidean rings R chosen suitably for the particular case.

Results (III)

An affine mapping $n \mapsto (an+b)/c$ of $\mathbb{Q}$ is order-preserving if and only if $a > 0$.

We call a residue class-wise affine mapping of $\mathbb{Z}$ *class-wise order-preserving*, if all of its affine partial mappings are order-preserving.

The following holds: The group $(\mathbb{Z}, +)$ is an epimorphic image of the subgroup

$$\mathrm{RCWA}^+(\mathbb{Z}) < \mathrm{RCWA}(\mathbb{Z})$$

of all class-wise order-preserving bijective rcwa mappings of $\mathbb{Z}$.

Methods (I)

Epimorphisms

$$\text{sgn}: \quad \text{RCWA}(\mathbb{Z}) \to \mathbb{Z}^\times$$

('sign') and

$$\det: \quad \text{RCWA}^+(\mathbb{Z}) \to (\mathbb{Z}, +)$$

('determinant') have been constructed explicitly.

In the notation used in the definition of an rcwa mapping, for $\sigma \in \text{RCWA}(\mathbb{Z})$ we have

$$\det(\sigma) \; = \; \frac{1}{m} \sum_{r(m) \in \mathbb{Z}/m\mathbb{Z}} \frac{b_{r(m)}}{|a_{r(m)}|}$$

and

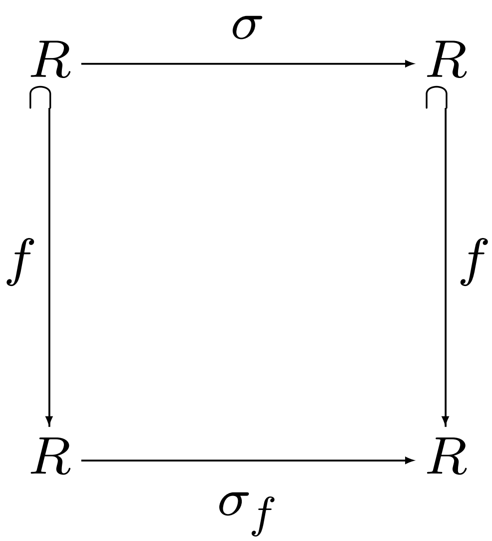
$$\text{sgn}(\sigma) \; = \; (-1)^{\det(\sigma) + \sum_{r(m):\, a_{r(m)}<0} \frac{m-2r}{m}}.$$

Methods (II)

Let $f : R \to R$ be an injective rcwa mapping. Let the *restriction monomorphism*

$$\pi_f : \ \mathrm{RCWA}(R) \to \mathrm{RCWA}(R), \quad \sigma \mapsto \sigma_f$$

associated to f be defined such that the diagram



commutes always, and that σ_f always fixes the complement of the image of f pointwise.

Methods (III)

Let $r(m) \subset \mathbb{Z}$ be a residue class, and define $\nu : n \mapsto n+1$ and $\varsigma : n \mapsto -n$. Further set $\nu_{r(m)} := \nu^{\pi_{n \mapsto mn+r}}$ and $\varsigma_{r(m)} := \varsigma^{\pi_{n \mapsto mn+r}}$. The mappings $\nu_{r(m)}$ and $\varsigma_{r(m)}$ generate an infinite dihedral group which acts on the residue class $r(m)$.

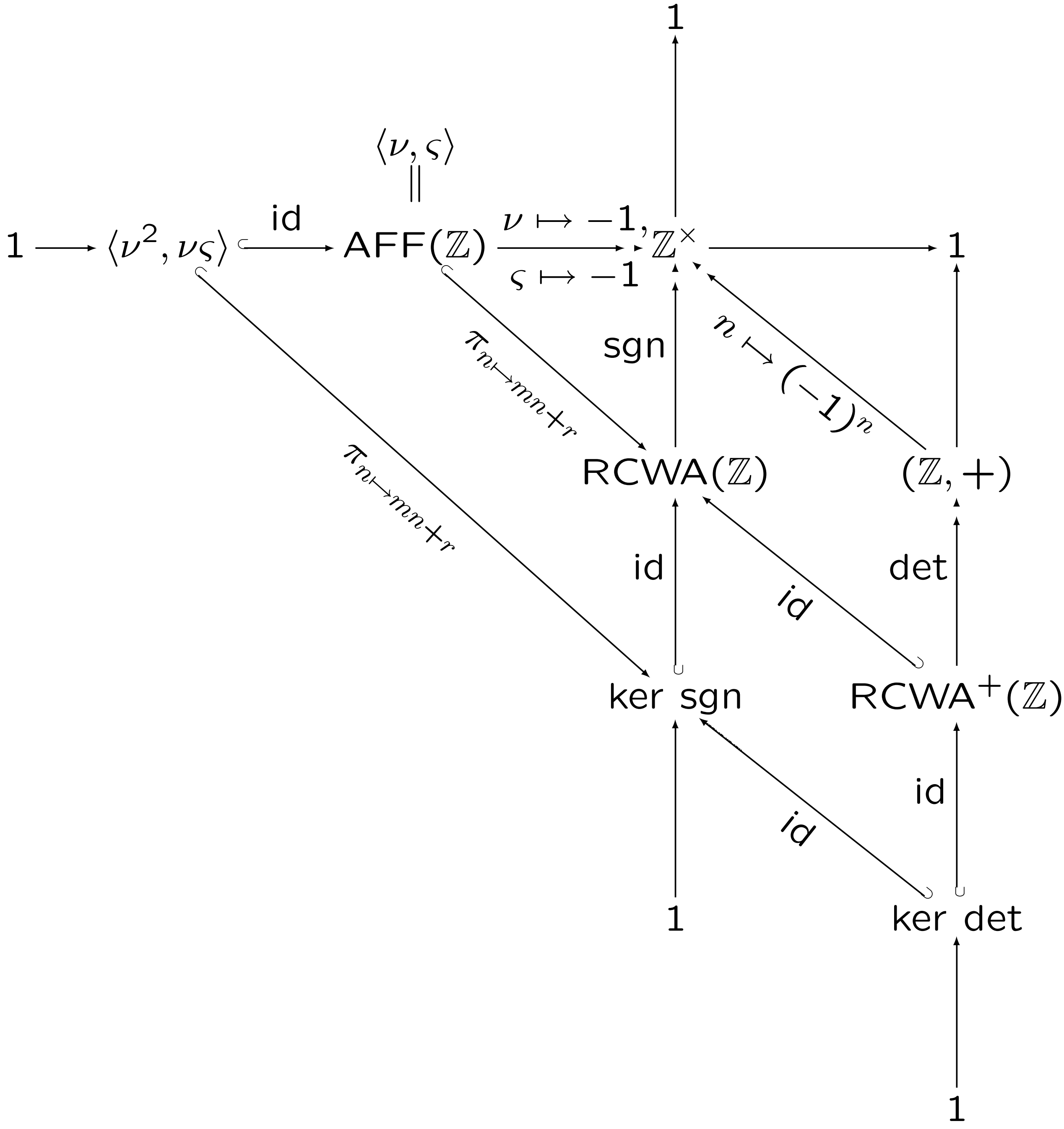
Let $r_1(m_1), r_2(m_2) \subset \mathbb{Z}$ be disjoint residue classes, and set $\tau : n \mapsto n + (-1)^n$. Further define

$$\mu = \mu_{r_1(m_1),r_2(m_2)} \in \mathrm{Rcwa}(\mathbb{Z}),$$

$$n \mapsto \begin{cases} \dfrac{m_1 n + 2r_1}{2} & \text{if} \quad n \in 0(2), \\ \dfrac{m_2 n + (2r_2 - m_2)}{2} & \text{if} \quad n \in 1(2). \end{cases}$$

Then, $\tau_{r_1(m_1),r_2(m_2)} := \tau^{\pi_\mu}$ is an involution which interchanges the residue classes $r_1(m_1)$ and $r_2(m_2)$ ('class transposition').

Structure



1
$\langle \nu, \varsigma \rangle$
1
$\langle \nu^2, \nu\varsigma \rangle$
id
AFF($\mathbb{Z}$)
$\nu \mapsto -1,$
$\varsigma \mapsto -1$
$\mathbb{Z}^\times$
1
sgn
$\pi_{n \mapsto mn+r}$
$\pi_{n \mapsto mn+r}$
$n \mapsto (-1)^n$
RCWA($\mathbb{Z}$)
($\mathbb{Z}$, +)
id
det
id
ker sgn
RCWA$^+$($\mathbb{Z}$)
id
id
1
ker det
1

Example I

The group generated by the permutations

$$\nu: \ n \ \mapsto \ n+1$$

and

$$\tau_{1(2),0(4)}: \ n \ \mapsto \ \begin{cases} 2n-2 & \text{if} \ \ n \equiv 1 \bmod 2, \\ \frac{n+2}{2} & \text{if} \ \ n \equiv 0 \bmod 4, \\ n & \text{if} \ \ n \equiv 2 \bmod 4 \end{cases}$$

acts 3-transitive, but not 4-transitive on $\mathbb{Z}$.

(Proven by means of computation with my RCWA package.)

Example II

The group generated by the permutations

$$\alpha: \quad n \mapsto \begin{cases} \frac{3n}{2} & \text{if} \quad n \equiv 0 \bmod 2, \\ \frac{3n+1}{4} & \text{if} \quad n \equiv 1 \bmod 4, \\ \frac{3n-1}{4} & \text{if} \quad n \equiv 3 \bmod 4 \end{cases}$$

and

$$\beta: \quad n \mapsto \begin{cases} \frac{3n}{5} & \text{if} \quad n \equiv 0 \bmod 5, \\ \frac{9n+1}{5} & \text{if} \quad n \equiv 1 \bmod 5, \\ \frac{3n-1}{5} & \text{if} \quad n \equiv 2 \bmod 5, \\ \frac{9n-2}{5} & \text{if} \quad n \equiv 3 \bmod 5, \\ \frac{9n+4}{5} & \text{if} \quad n \equiv 4 \bmod 5 \end{cases}$$

acts (at least!) 4-transitive on the set of positive integers.

(Proven by means of computation with my RCWA package.)

Open Questions concerning $\mathrm{RCWA}(\mathbb{Z})$

- Is $\mathrm{RCWA}(\mathbb{Z}) \rhd \ker \mathrm{sgn} \rhd 1$ a composition series?

- What can be said about the structure of fin.-gen. subgroups of $\mathrm{RCWA}(\mathbb{Z})$? Are they all finitely presented? Can they have intermediate growth?

- Which degrees of transitivity can actions of fin.-gen. subgroups of $\mathrm{RCWA}(\mathbb{Z})$ on $\mathbb{Z}$ or other infinite orbits have?

- Does the group $\mathrm{RCWA}(\mathbb{Z})$ have non-trivial outer automorphisms?

- Find general algorithmic solutions to the membership- / conjugacy problem for fin.-gen. subgroups of $\mathrm{RCWA}(\mathbb{Z})$.

Outlook (I)

Define a complete infinite binary tree $\mathcal{T}$ with integers as vertices as follows: Let 1 be the root, and let n^L resp. n^R be the left resp. right child of a vertex n, where

$$L : \mathbb{Z} \to \mathbb{Z}, \ n \mapsto \begin{cases} 4n+1 & \text{if } n \equiv 0 \text{ mod } 2, \\ 16n+12 & \text{if } n \equiv 1 \text{ mod } 2 \end{cases}$$

and

$$R : \mathbb{Z} \to \mathbb{Z}, \ n \mapsto \begin{cases} \frac{4n}{3} & \text{if } n \equiv 0 \text{ mod } 6, \\ \frac{8n+4}{3} & \text{if } n \equiv 1 \text{ mod } 6, \\ \frac{16n+4}{3} & \text{if } n \equiv 2 \text{ mod } 6, \\ \frac{2n}{3} & \text{if } n \equiv 3 \text{ mod } 6, \\ \frac{4n-1}{3} & \text{if } n \equiv 4 \text{ mod } 6, \\ \frac{2n-1}{3} & \text{if } n \equiv 5 \text{ mod } 6. \end{cases}$$

It is easy to see that all vertices of $\mathcal{T}$ are positive integers, and that no integer occurs twice. Now the $3n+1$ Conjecture is equivalent to the question whether any positive integer is indeed a vertex of $\mathcal{T}$.

Outlook (II)

The group generated by the permutations

$$\tau: \; n \mapsto n + (-1)^n$$

and

$$\tau_r := \prod_{k=1}^{\infty} \tau_{2^{k-1}-1(2^{k+1}),2^k+2^{k-1}-1(2^{k+1})}^{1-\delta_{r,k \bmod 3}}$$

($r \in \{0,1,2\}$) is isomorphic to Grigorchuk's first example of an infinite finitely generated periodic group of subexponential growth.

The generators τ, τ_0, τ_1 resp. τ_2 correspond to a, b, c resp. d in the notation used in

R. I. Grigorchuk.
Bernside's Problem on Periodic Groups.
Functional Anal. Appl. 14:41–43, 1980.

Outlook (III)

Consider the following ordering of the positive integers:

$$2^0 < 2^1 < 2^2 < 2^3 < \cdots < 4 \cdot 5 < 4 \cdot 3 < \ldots$$
$$< 2 \cdot 7 < 2 \cdot 5 < 2 \cdot 3 < \cdots < 9 < 7 < 5 < 3.$$

Sarkovskii's Theorem states that any continuous function $f : \mathbb{R} \to \mathbb{R}$ which has a cycle of length l has cycles of all lengths which are smaller in the above ordering as well. Thus if f has a cycle of length 3, it has cycles of any finite length.

Since the Collatz mapping T has the 3-cycle (-5, -7, -10), Sarkovskii's Theorem implies that any extension of T to a continuous function $\hat{T} : \mathbb{R} \to \mathbb{R}$ has finite cycles of any given length. The permutation α mentioned at the beginning has the 5-cycle (4, 6, 9, 7, 5), but no 3-cycle. This means that an extension of α to a continuous function $\widehat{\alpha} : \mathbb{R} \to \mathbb{R}$ must have cycles of any finite length except of 3.

References

RCWA -
[R]esidue [C]lass-[W]ise [A]ffine Groups.
GAP package, 2005.
`www.gap-system.org/Packages/rcwa.html`

Meenaxi Bhattacharjee, Dugald Macpherson, Rögnvaldur G. Möller, and Peter M. Neumann. *Notes on Infinite Permutation Groups*. Number 1698 in Lecture Notes in Mathematics. Springer-Verlag, 1998.

Jeffrey C. Lagarias.
The 3x+1 problem:
An annotated bibliography, 2005.
`arxiv.org/abs/math.NT/0309224`

O. M. Sarkovskii.
Co-existence of cycles of a continuous mapping of the line into itself.
Ukrain. Mat. Z. 16, 61–71, 1964.