A New Class of Groups Accessible to Methods from Computational Group Theory

Stefan Kohl

Computational Algebra Day, Brussels, 07/11/2006

Classical Ways to Represent Groups in CGT

Today, in CGT groups are commonly represented as

- subgroups of finite symmetric groups, as
- subgroups of general linear groups, or as
- quotients of free groups of finite rank by a finite number of relations.

The class of groups which can be represented this way is however quite limited. For example, already trying to represent the restricted wreath product $\mathbb{Z} \wr \mathbb{Z}$ of the infinite cyclic group with itself causes severe problems. Further, the third-mentioned way to represent groups has major algorithmic disadvantages.

$\rightsquigarrow$ The need to look for another large group which admits computations, and which has a richer class of subgroups.

Our 'Universe'

Definition 1. Let $r_1(m_1), r_2(m_2) \subset \mathbb{Z}$ be disjoint residue classes. We define the *class transposition* $\tau_{r_1(m_1),r_2(m_2)} \in \mathrm{Sym}(\mathbb{Z})$ by

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

where we assume that $0 \leqslant r_i < m_i, i \in \{1, 2\}$. We put $\tau := \tau_{0(2),1(2)} : n \mapsto n + (-1)^n$.

Remark. The class transposition $\tau_{r_1(m_1),r_2(m_2)}$ is an involution which interchanges the residue classes $r_1(m_1)$ and $r_2(m_2)$, and which maps nonnegative integers to nonnegative integers.

Definition 2. Let $\mathrm{CT}(\mathbb{Z})$ denote the group which is generated by the set of all class transpositions.

On $\mathrm{CT}(\mathbb{Z})$

Remark. The group $\mathrm{CT}(\mathbb{Z})$ has a couple of nice properties. For example it is a countable simple group, and it has an uncountable family of simple subgroups which is parametrized by the sets of odd primes.

The purpose of **this** talk however is to describe some classes of groups which embed into $\mathrm{CT}(\mathbb{Z})$.

'The' tool for computing with these groups is the GAP package RCWA , which is available at

http://www.gap-system.org/Packages/rcwa.html.

Richness of the Class of Subgroups of $\mathrm{CT}(\mathbb{Z})$

Theorem 1. These groups embed into $\mathrm{CT}(\mathbb{Z})$:

1. Finite groups.
2. Free groups of finite rank.
3. The modular group $\mathrm{PSL}(2, \mathbb{Z})$.
4. Free products of finitely many finite groups.
5. Direct products of subgroups of $\mathrm{CT}(\mathbb{Z})$.
6. Wreath products of subgroups of $\mathrm{CT}(\mathbb{Z})$ with finite groups.
7. Restricted wreath products of subgroups of $\mathrm{CT}(\mathbb{Z})$ with $(\mathbb{Z}, +)$.

The Class of Subgroups of $\mathrm{CT}(\mathbb{Z})$, continued

Corollary. The group $\mathrm{CT}(\mathbb{Z})$ has

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

Remark. Subgroups of $\mathrm{CT}(\mathbb{Z})$ which are not finitely presented are quite common. For example we have

$$\mathbb{Z} \wr \mathbb{Z} \cong \langle \tau \cdot \tau_{0(2),1(4)}, \tau_{3(8),7(8)} \cdot \tau_{3(8),7(16)} \rangle.$$

In practice, in spite of being undecidable in general, the membership problem for a subgroup of $\mathrm{CT}(\mathbb{Z})$ given by generators can be solved in many cases, anyway. Often in particular deciding nonmembership is even quite cheap.

Proof of Theorem 1, Assertion (2) and (3)

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

Proof. An example of an embedding of the free group of rank 2 is

$$\varphi_{\mathrm{F}_2} : \mathrm{F}_2 = \langle a, b \rangle \hookrightarrow \mathrm{CT}(\mathbb{Z}), \quad a \mapsto (\tau \cdot \tau_{0(2),1(4)})^2,\ b \mapsto (\tau \cdot \tau_{0(2),3(4)})^2.$$

This can be seen by applying the Table-Tennis Lemma to the cyclic groups generated by the images of a and b under φ_{F_2} and the sets $0(4) \cup 1(4)$ and $2(4) \cup 3(4)$. The free groups of higher rank embed into F_2. Likewise it follows from the Table-Tennis Lemma that

$$\begin{aligned} \varphi_{\mathrm{PSL}(2,\mathbb{Z})} : \ \mathrm{PSL}(2, \mathbb{Z}) &\cong \mathrm{C}_3 \star \mathrm{C}_2 \\ &\cong \langle a, b \mid a^3 = b^2 = 1 \rangle \hookrightarrow \mathrm{CT}(\mathbb{Z}), \\ a &\mapsto \tau_{0(4),2(4)} \cdot \tau_{1(2),0(4)}, \quad b \mapsto \tau \end{aligned}$$

is an embedding of $\mathrm{PSL}(2, \mathbb{Z})$. This time one can use the sets $0(2)$ and $1(2)$ in place of $0(4) \cup 1(4)$ and $2(4) \cup 3(4)$. □

Proof of Theorem 1, Assertion (4)

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

Proof. Let $G_0, \dots, G_{m-1}$ be finite groups. To see that their free product embeds into $\mathrm{CT}(\mathbb{Z})$, proceed as follows: First consider regular permutation representations φ_r of the groups G_r on the residue classes (mod $|G_r|$). Then take conjugates $H_r := (\mathrm{im}\, \varphi_r)^{\sigma_r}$ of the images of these representations under mappings $\sigma_r \in \mathrm{CT}(\mathbb{Z})$ which map $0(|G_r|)$ to $\mathbb{Z} \backslash r(m)$. 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 is isomorphic to their free product. □

This proof actually describes a practical algorithm for finding embeddings of free products of finite groups!

Proof of Theorem 1, Assertion (7)

Definition. Given a residue class $r(m)$, let

$$\pi_{n \mapsto mn+r}: \ \mathrm{CT}(\mathbb{Z}) \hookrightarrow \mathrm{CT}(\mathbb{Z})$$

be the monomorphism which maps a class transposition $\tau_{r_1(m_1),r_2(m_2)}$ to $\tau_{mr_1+r(mm_1),mr_2+r(mm_2)}$.

Theorem. Restricted wreath products of subgroups of $\mathrm{CT}(\mathbb{Z})$ with $(\mathbb{Z},+)$ embed into $\mathrm{CT}(\mathbb{Z})$.

Proof. Given a subgroup $G \leqslant \mathrm{CT}(\mathbb{Z})$, the group generated by $\pi_{n\mapsto 4n+3}(G)$ and $\tau \cdot \tau_{0(2),1(4)}$ is isomorphic to the restricted wreath product $G \wr (\mathbb{Z},+)$. This holds since 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 pairwise disjoint residue classes, which means that the conjugates of $\pi_{n\mapsto 4n+3}(G)$ under powers of $\tau \cdot \tau_{0(2),1(4)}$ have disjoint supports. □

This proof describes a practical construction as well.

Divisible Subgroups of $\mathrm{CT}(\mathbb{Z})$

Theorem 2. Any finite group embeds into a divisible torsion group which embeds into $\mathrm{CT}(\mathbb{Z})$.

Proof. Since every finite group embeds into $\mathrm{CT}(\mathbb{Z})$, it suffices to prove that the torsion subgroups of $\mathrm{CT}(\mathbb{Z})$ are divisible. We show that given an element $g \in \mathrm{CT}(\mathbb{Z})$ of finite order and a positive integer k, there is always an $h \in \mathrm{CT}(\mathbb{Z})$ such that $h^k = g$: Since 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 obtained from $\mathcal{P}$ by decomposing any $r_i(m_i) \in \mathcal{P}$ into residue classes (mod km_i). □

This proof actually describes a practical algorithm for extracting roots of torsion elements of $\mathrm{CT}(\mathbb{Z})$.

An Example

The class of subgroups of $\mathrm{CT}(\mathbb{Z})$ is in fact much richer than indicated by Theorem 1 and 2. To give a little glimpse of this, we give an example of a reasonably complicated wreath product construction:

Let $G_1 := \langle \tau_{0(4),3(4)}, \tau_{0(6),3(6)}, \tau_{1(4),0(6)} \rangle$.

This group acts faithfully on a certain partition $\mathcal{P}$ of $\mathbb{Z}$ into infinitely many residue classes. The orbits on $\mathcal{P}$ are all finite, and there is an orbit of any given odd length. The group G_1 induces full symmetric groups on these orbits. Let

$$G_2 := \langle G_1, \tau_{0(4),3(4)} \cdot \tau_{6(12),9(12)} \cdot \tau_{0(6),9(12)} \rangle.$$

The additional generator permutes the residue classes in $\mathcal{P}$ as well, but it moves residue classes between the finite orbits of G_1. In fact there are two infinite orbits on $\mathcal{P}$ under the action of G_2.

An Example, continued

We would like to construct a wreath product of $\mathrm{PSL}(2,\mathbb{Z})$ with G_2.

A representative for one of the infinite orbits of G_2 on $\mathcal{P}$ is the residue class $1(24)$. From above we know that

$\mathrm{PSL}(2,\mathbb{Z}) \cong \langle \tau_{0(2),1(2)}, \tau_{0(4),2(4)} \cdot \tau_{1(2),0(4)} \rangle$.

We compute the image under the restriction monomorphism $\pi_{n\mapsto 24n+1}$. This yields the group

$\langle \tau_{1(48),25(48)}, \tau_{1(96),49(96)} \cdot \tau_{25(48),1(96)} \rangle =: H$,

whose support is the residue class $1(24)$. Now, our wreath product is

$$\langle G2, H \rangle.$$

Of course this construction can be continued – for example we could restrict the group G_2 to the residue class $17(24)$, which belongs to the second infinite orbit on $\mathcal{P}$, and form the closure of $\langle G2, H \rangle$ and that group, and so on.