Geometry and the Word Problem for Special Monoids

Carl-Fredrik Nyberg Brodda
(Supervised by Dr Bob Gray)

University of East Anglia

York Semigroup Seminar
3 February 2021

Pretalk Preprints

The work in this talk is based on the following pre-prints:

1. `arXiv:2011.04536` (*The Geometry of Special Monoids*)
2. `arXiv:2011.09466` (*On the Word Problem for Special Monoids*)
3. `arXiv:2102.00745` (*We'll get back to this one!*)

Special Monoids

Every monoid/group can be expressed as a quotient of a free monoid/group. We write this as $\mathrm{Mon}\langle A \mid u_i = v_i \ (i \in I)\rangle$, resp. $\mathrm{Gp}\langle A \mid u_i = v_i \ (i \in I)\rangle$.

Note that $\mathrm{Mon}\langle A \mid u_i = v_i \ (i \in I)\rangle$ is different from $\mathrm{Mon}\langle A \mid w_i = 1 \ (i \in I)\rangle$!

Definition

A monoid is called *special* if it admits a presentation $\mathrm{Mon}\langle A \mid w_i = 1 \ (i \in I)\rangle$.

Every group is a special monoid, but not every monoid is special.

Examples

1. *The* ***bicyclic monoid*** $\mathrm{Mon}\langle b, c \mid bc = 1\rangle$.
2. $\mathbb{Z} \times \mathbb{Z} \cong \mathrm{Mon}\langle a, b, a', b' \mid aba'b' = 1, aa' = 1, a'a = 1, bb' = 1, b'b = 1\rangle$.
3. $\mathrm{Mon}\langle a, b \mid ab = a\rangle$ *has* ***no*** *special presentation.*

The Word Problem

If M is presented by $\mathrm{Mon}\langle A \mid w_i = 1 \ (i \in I)\rangle$, there is a natural homomorphism

$$\pi : A^* \to M.$$

The Word Problem for $\mathrm{Mon}\langle A \mid w_i = 1 \ (i \in I)\rangle$

INPUT : Two elements $u, v \in A^*$.
QUESTION : Is $\pi(u) = \pi(v)$?

We say the word problem is *decidable* if there is an algorithm which always decides this question in finite time. Otherwise, the word problem is *undecidable*.

Special Monoids

An element $m \in M$ of a monoid is *invertible* if there exists some $m' \in M$ such that

$$m'm = mm' = 1$$

i.e. if m is *left* and *right* invertible.

The *group of units* $U(M)$ is the subgroup of all invertible elements of M.
We always have $1 \in U(M)$.

Theorem (Adjan, 1960)

Let $M = \mathrm{Mon}\langle A \mid w = 1 \rangle$ *be a special one-relator monoid. Then*

1. *The word problem for* M *reduces to the word problem for* $U(M)$.
2. $U(M)$ *is a one-relator group.*

k-relator Special Monoids

G. S. Makanin studied special monoids in his 1966 Ph.D. thesis.

Theorem (Makanin, 1966)

Let $M = \mathrm{Mon}\langle A \mid w_1 = 1, w_2 = 1, \dots, w_k = 1\rangle$ *be a special k-relator monoid. Then*

1. *The word problem for M reduces to the word problem for $U(M)$.*
2. *$U(M)$ is a k-relator group.*

Zhang later showed that the word problem for M reduces to the *identity problem* for M, i.e. the problem of deciding if $u = 1$.

Thus: special monoids *really* are like generalised groups!

G. S. Makanin

USSR Academy of Sciences
Steklov Mathematical Institute

G. S. Makanin

On The Identity Problem For Finitely Presented Groups and Semigroups

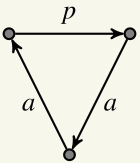
Dissertation for the degree of Candidate of Physical and Mathematical Sciences.

This translation can now be found at `arXiv:2102.00745`

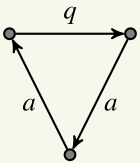
Graphical Approach

Idea: study the graphical properties of a special monoid modulo its group of units.

Consider $\mathrm{Mon}\langle a, p, q \mid apa = 1, aqa = 1 \rangle$.
We can interpret these relations graphically as loops labelled by the relator words.
I.e.



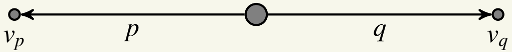
$apa = 1$

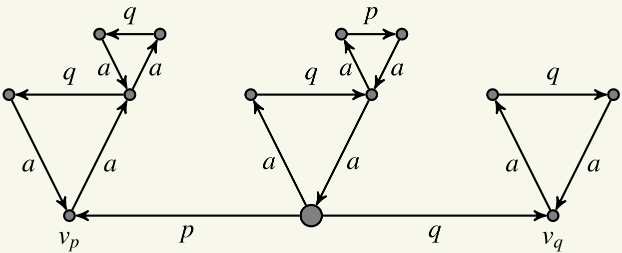


$aqa = 1$

Equality in $M = \mathrm{Mon}\langle a, p, q \mid apa = 1, aqa = 1\rangle$.

There is an isomorphism with $a \mapsto -1$ and $p, q \mapsto 2$ from M to $\mathbb{Z}$.
In particular, $p = q$ in M. How do we see this graphically?





If we determinise this graph, we will identify v_p and v_q!
This is the graphical version of saying $p = q$ in M.

More General Case

Consider $M = \mathrm{Mon}\langle A \mid w_1 = 1, \ldots, w_k = 1 \rangle$.

Take a single vertex, add loops everywhere (infinite graph) and "fold" the result.

Call the resulting graph $\mathfrak{R}_1(M)$ (this is the *Schützenberger graph of* 1).

Theorem (Stephen 1987, Zhang 1992)

If $\mathfrak{R}_1(M)$ can be effectively constructed, then the word problem for M is decidable.

So we really want to understand what $\mathfrak{R}_1(M)$ is like!

Proposition (Easy)

The Schützenberger graph $\mathfrak{R}_1(M)$ is isomorphic to the right Cayley graph of M induced on the set $\mathscr{R}_1$, the set of right invertible elements of M.

Important for later: $\mathfrak{R}_1(M)$ is deterministic!

Context-free Graphs

Let Γ be a connected, locally finite, rooted (at 1), labelled, directed graph, and consider Γ as a metric space with its undirected edge metric $d(u, v)$. We define:

$$\Gamma^{(n)} := \text{subgraph of } \Gamma \text{ induced on } \{v \in V(\Gamma) \mid d(1, v) < n\}.$$

Let C be a connected component of $\Gamma \setminus \Gamma^{(n)}$.
A *frontier point* of C is a vertex u of C such that $d(1, u) = n$.

If $v \in \Gamma$, then let $\Gamma(v)$ be the connected component of $\Gamma \setminus \Gamma^{(d(1,v))}$ containing v.
Let $\Delta(v)$ be the frontier points of $\Gamma(v)$.

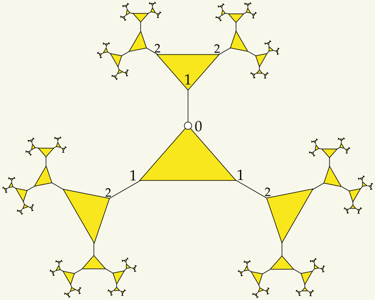
Definition (End-isomorphism)

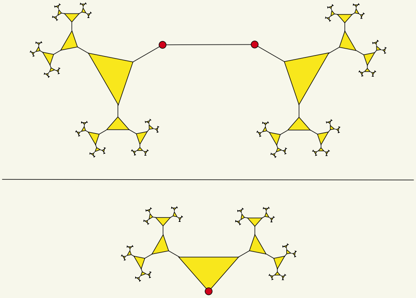
Let $u, v \in V(\Gamma)$. An *end-isomorphism* between the subgraphs $\Gamma(u)$ and $\Gamma(v)$ is a mapping $\psi \colon \Gamma(u) \to \Gamma(v)$ such that

1. ψ is a label-preserving graph isomorphism;
2. ψ maps $\Delta(u)$ onto $\Delta(v)$.

A graph Γ is **context-free** if there are only finitely many isomorphism classes of $\Gamma(u)$ up to end-isomorphism.

Context-free Graphs II

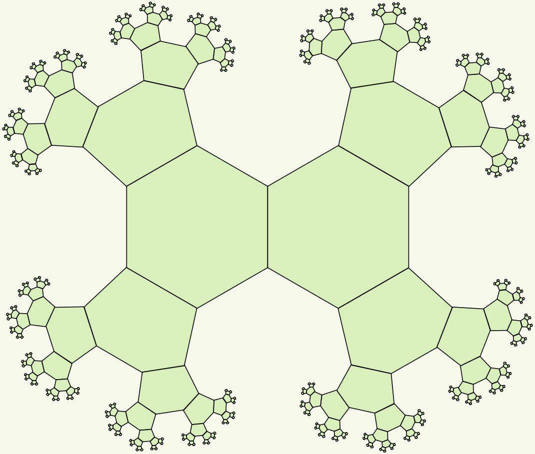




This graph has two end-spaces (excluding $\Gamma(1)$) up to end-isomorphism.
This is the Cayley graph $\mathfrak{R}_1(G)$ of the modular group $G = \mathrm{PSL}_2(\mathbb{Z})$.

$\mathrm{PSL}_2(\mathbb{Z})$ $\rightsquigarrow$ j-function $\rightsquigarrow$ modular curves $\rightsquigarrow$??? $\rightsquigarrow$ Fermat's Last Theorem

Arbres, Amalgames



This is the Cayley graph $\mathfrak{R}_1(G)$ of $G = \mathrm{SL}_2(\mathbb{Z})$. It is context-free!

Context-free Graphs III

There is a full characterisation of which groups have context-free $\mathfrak{R}_1$ (Cayley graph).

Theorem (Muller & Schupp, 1985)

A group G has context-free $\mathfrak{R}_1(G)$ if and only if G has a free subgroup of finite index.

1. $\mathrm{PSL}_2(\mathbb{Z})$ has F_2 of index 6.
2. $\mathrm{SL}_2(\mathbb{Z})$ has F_2 of index 12.
3. $H * K$, where H, K are finite groups, as this surjects onto $H \times K$.

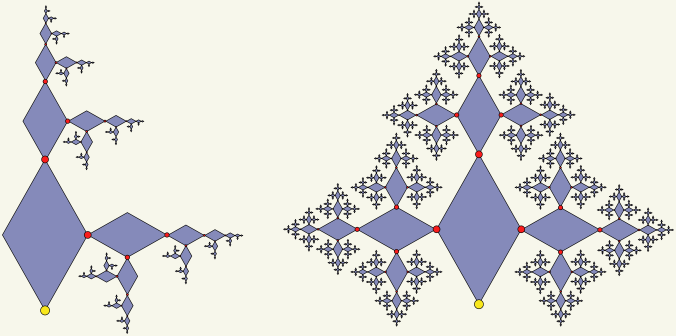
Theorem (Muller & Schupp, 1985)

If Γ is a context-free graph, then the monadic second-order theory of Γ is decidable.

For graphs with a high degree of symmetry, the above is an equivalence.

Trees of Copies

A way to build a context-free graph, starting from a context-free graph.
Starting with a graph Γ and a set of *attachment points* $S \subseteq V(\Gamma)$, construct $\mathrm{Tree}(\Gamma, S)$.



Proposition (NB, 2020)

If Γ *is context-free, then* $\mathrm{Tree}(\Gamma, S)$ *is context-free for any choice of attachment points.*

Bounded Folding

$\mathrm{Tree}(\Gamma, S)$ is generally not deterministic.
So when is $\mathrm{Tree}(\Gamma, S)_{\mathrm{det}}$ context-free?

Theorem (NB, 2020)

Let Γ *be a graph, and S a set of attachment points. Assume that the following hold:*

1. Γ *is deterministic and context-free;*
2. Γ *satisfies the "bounded folding condition".*

Then $\mathrm{Tree}(\Gamma, S)_{\mathrm{det}}$ *is context-free.*

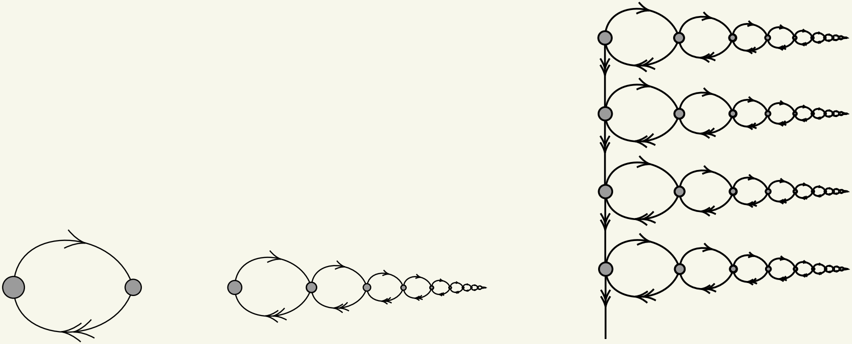
The proof is by horrible and lengthy induction!

Key point: the "bounded folding condition" is **local** to Γ!

The graph $\mathfrak{U}$

We now interpret $U(M)$ graphically as a graph $\mathfrak{U}$.
Idea: Turn the Cayley graph of $U(M)$ into an induced subgraph of $\mathfrak{R}_1(M)$.

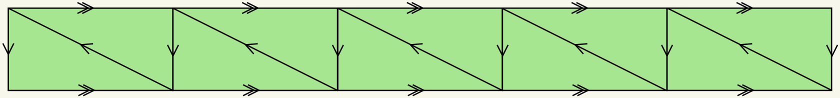
Let $M = \text{Mon}\langle b, c \mid bc = 1\rangle$. Then $1 = U(M) \cong \text{Gp}\langle b_1 \mid b_1 = 1\rangle$ via $b_1 \mapsto bc$.
Construct a tree of copies of "image" of the Cayley graph of $U(M)$ under this map.



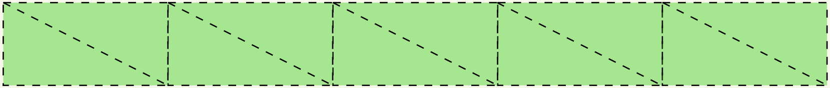
Thus the bicyclic monoid is made up of copies of its group of units!

The graph $\mathfrak{U}$, cont.

Let $M = \mathrm{Mon}\langle a, b, c \mid abaca = 1\rangle$. Then $U(M) \cong \mathrm{Gp}\langle b_1, b_2 \mid b_1 b_2 b_1 = 1\rangle \cong \mathbb{Z}$.



This is the Cayley graph of $U(M)$.



The graph $\mathfrak{U}$ looks very similar to the Cayley graph, but with subdivided edges.

$\mathfrak{R}_1$ from $\mathfrak{U}$

This construction can be applied to any special monoid.

Proposition (NB, 2020)

Let M be a special monoid. There exists an induced subgraph $\mathfrak{U}$ of $\mathfrak{R}_1(M)$ such that

1. *$\mathfrak{U}$ is a context-free graph if and only if $U(M)$ is context-free;*
2. *$\mathfrak{U}$ satisfies the bounded folding condition.*

As in the bicyclic monoid case, we can construct $\mathfrak{R}_1(M)$.

Theorem (NB, 2020)

Let M be a special monoid.

1. *There exists a set S of attachment points such that $\mathfrak{R}_1(M) \cong \mathrm{Tree}(\mathfrak{U}, S)_{\mathrm{det}}$.*
2. *The determinisation of $\mathrm{Tree}(\mathfrak{U}, S)$ is effectively constructible.*

In particular, if $\mathfrak{U}$ is effectively constructible, then $\mathfrak{R}_1$ is.

New (graphical) proof of the word problem reducing to the group of units.

Monoid Muller-Schupp

Thus we can assemble the following main theorem of `arXiv:2011.04536`.

Theorem (NB, 2020)

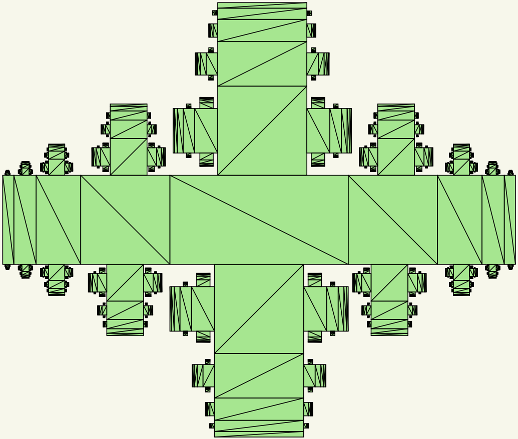
If M is a special monoid, then $\mathfrak{R}_1(M)$ is a context-free graph if and only if the group of units $U(M)$ has a free subgroup of finite index.

Proof.

$(\Longleftarrow)$ If $U(M)$ is virtually free, then $U(M)$ is context-free (Muller-Schupp). Thus $\mathfrak{U}$ is context-free, and so $\mathrm{Tree}(\mathfrak{U}, S)$ is context-free. As $\mathfrak{U}$ satisfies bounded folding, $\mathrm{Tree}(\mathfrak{U}, S)_{\mathrm{det}}$ is also context-free, and $\mathfrak{R}_1 \cong \mathrm{Tree}(\mathfrak{U}, S)_{\mathrm{det}}$.
$(\Longrightarrow)$ The group $U(M)$ is the full automorphism group of $\mathfrak{R}_1$ as 1 is an idempotent (Stephen). The automorphism group of any context-free graph is itself context-free. By Muller-Schupp, $U(M)$ is virtually free. □

All groups are special monoids, so this is a proper generalisation of Muller-Schupp.

Infinite Cyclic $U(M)$



This is $\mathfrak{R}_1$ of $\mathrm{Mon}\langle a, b, c \mid abaca = 1 \rangle$.
The central strip is $\mathfrak{U}$, with $U(M) \cong \mathrm{Mon}\langle b_1, b_2 \mid b_1 b_2 b_1 = 1 \rangle \cong \mathbb{Z}$.
As $U(M)$ is free, the theorem tells us that $\mathfrak{R}_1$ is a context-free graph.

More Characterisation

Theorem (NB, 2020)

Let M be a f.p. special monoid. Then the following are equivalent:

1. $U(M)$ *is virtually free.*
2. *The right Cayley graph of M is context-free.*
3. *The right Cayley graph of M is quasi-isometric to a tree.*
4. *The monadic second-order theory of the right Cayley graph of M is decidable.*
5. *The word problem for M is a context-free language.*

We can deduce decidability results in this way!

Corollary (NB, 2020)

Let M be a special monoid with virtually free group of units. Then the rational subset membership problem for M is decidable.

Previously only known for $\text{Mon}\langle b, c \mid bc = 1 \rangle$.

Thank you!