Gröbner-Shirshov bases, Dehn's algorithm and small cancellation rings

Agatha Atkarskaya

Hebrew University of Jerusalem
Einstein Institute of Mathematics

17.09.2024

Question. Given a list of properties, does there exist an algebraic system (e.g. group, associative algebra, Lie algebra, etc.) that satisfies them?

Question. Given a list of properties, does there exist an algebraic system (e.g. group, associative algebra, Lie algebra, etc.) that satisfies them?

- To answer the above question it is natural to define the object using generators and defining relators;
- However, there can be unexpected corollaries of the initial relators and the final object may become trivial;
  Adian-Rabin theorem states that there is no algorithm that takes as an input a finite group presentation and decides if the given group is trivial.
- Which kinds of presentations are good?

Small cancellation groups

Let $G = \langle x_1, \ldots, x_n \mid R_1, \ldots, R_k, \ldots \rangle$ be a group, where all R_i are cyclically reduced, the list of relators is closed under taking inverses and cyclic shifts of relations.

If $R_i \neq R_j$ and $R_i = cR_i'$, $R_j = cR_j'$, then c is called a *small piece*.

We say that G satisfies condition $\mathrm{C}(m)$ if every R_i can not be written as a product of less than m small pieces.

If $m \geqslant 7$, then G is hyperbolic.

Small cancellation groups

Theorem (Geendlinger's Lemma)

If G satisfy $\mathrm{C}(7)$ and $A = 1$ in G, then $A = LuR$, where $uu' = R_i$ for some i and $|u| > \frac{1}{2}|R_i|$.

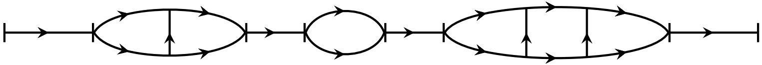
So, Dehn's algorithm solves the word problem in G.

Theorem (Geendlinger's Lemma)

If G satisfy $\mathrm{C}(7)$ and $A = 1$ in G, then $A = LuR$, where $uu' = R_i$ for some i and $|u| > \frac{1}{2}|R_i|$.

So, Dehn's algorithm solves the word problem in G.

It $A = B$ in such G and A, B do not contain $> \frac{1}{2}$ of any R_i, then A, B can be viewed as paths in a one-layer map.



Rips construction

There exist subgroups of small cancellation groups with exotic properties.

Theorem (E. Rips, 1982)

There is a finitely presented small cancellation group G such that:

- *G has finitely generated subgroups whose intersection is not finitely generated.*
- *G has a finitely generated but not finitely presented subgroup.*
- *The subgroup membership problem in G is not solvable.*

Iterated small cancellation theory

Given $G = \langle x_1, \dots, x_n \mid R_1, \dots, R_t, \dots \rangle$, our goal not small cancellation conditions, our real goal is Greendlinger's Lemma.

There are many group presentations with the following structure:

$$\{R_1, \dots, R_t, \dots\} = \mathcal{R}_1 \cup \mathcal{R}_2 \cup \dots,$$

where every $\mathcal{R}_i$ satisfies $C(m)$ and moreover $\mathcal{R}_i$ satisfies $C(m)$ modulo $\mathcal{R}_j$, $j \leqslant i$. Then every intermediate quotient $\mathrm{F}/\langle\langle R_1, \dots, R_i \rangle\rangle$ satisfies Greendlinger's Lemma. Thus, G satisfies it as well.

Iterated small cancellation theory

Given $G = \langle x_1, \ldots, x_n \mid R_1, \ldots, R_t, \ldots \rangle$, our goal not small cancellation conditions, our real goal is Greendlinger's Lemma.

There are many group presentations with the following structure:

$$\{R_1, \ldots, R_t, \ldots\} = \mathcal{R}_1 \cup \mathcal{R}_2 \cup \ldots,$$

where every $\mathcal{R}_i$ satisfies $C(m)$ and moreover $\mathcal{R}_i$ satisfies $C(m)$ modulo $\mathcal{R}_j$, $j \leqslant i$. Then every intermediate quotient $\mathrm{F}/\langle\langle R_1, \ldots, R_i \rangle\rangle$ satisfies Greendlinger's Lemma. Thus, G satisfies it as well.

- The Burnside group (f.g. group with identity $x^n = 1$) is infinite for odd $n \geqslant 557$ (S. Adian and P. Novikov, A. Olshanskii, E. Rips, K. Tent, A.A.), and even $n \geqslant 8000$ (S. Ivanov, I. Lysenok).
- Construction of Tarskii monster group (infinite group with all proper subgroups cyclic of the same order) by A. Olshanskii.

Constructing rings with exotic properties

This is a joint work with A. Kanel-Belov, E. Plotkin and E. Rips.

Our initial motivation is the following old problem in Ring Theory (which is still not solved):

Problem (1970s, Kaplansky, L'vov, Latyshev)

Does there exist a division algebra infinite dimensional over its center with finitely generated multiplicative group?

Constructing rings with exotic properties

This is a joint work with A. Kanel-Belov, E. Plotkin and E. Rips.

Our initial motivation is the following old problem in Ring Theory (which is still not solved):

Problem (1970s, Kaplansky, L'vov, Latyshev)

Does there exist a division algebra infinite dimensional over its center with finitely generated multiplicative group?

One can quickly see that such algebra can not be commutative.

Constructing rings with exotic properties

This is a joint work with A. Kanel-Belov, E. Plotkin and E. Rips.

Our initial motivation is the following old problem in Ring Theory (which is still not solved):

Problem (1970s, Kaplansky, L'vov, Latyshev)

Does there exist a division algebra infinite dimensional over its center with finitely generated multiplicative group?

One can quickly see that such algebra can not be commutative.

Our general idea is as follows. We want to take such a quotient of $\mathbb{Z}_2\mathrm{F}$, F is a non-abelian free group, that it is infinite dimensional over its center and its every element is equal to a monomial.

Clearly, it is sufficient that every binomial $1 + w$ is equal to a monomial. So, we enumerate all elements of F, $\{w_1, w_2, \ldots\}$, and impose the relations $1 + w_i = v_i$ on $\mathbb{Z}_2\mathrm{F}$. Now the question is if $\mathbb{Z}_2\mathrm{F}/\mathcal{I}$, where $\mathcal{I} = \langle\langle 1 + w_i = v_i; i = 1, 2, \ldots\rangle\rangle$, is infinite dimensional over its center (or at least non-trivial).

Clearly, it is sufficient that every binomial $1 + w$ is equal to a monomial. So, we enumerate all elements of F, $\{w_1, w_2, \dots\}$, and impose the relations $1 + w_i = v_i$ on $\mathbb{Z}_2\mathrm{F}$. Now the question is if $\mathbb{Z}_2\mathrm{F}/\mathcal{I}$, where $\mathcal{I} = \langle\langle 1 + w_i = v_i; i = 1, 2, \dots\rangle\rangle$, is infinite dimensional over its center (or at least non-trivial).

Notice that it is easy to produce a quotient of $\mathbb{Z}_2\langle x, y\rangle$ that is infinite dimensional over $\mathbb{Z}_2$ and with every element equal to a monomial (everything what we want except inverting).

Gröbner-Shirshov bases of polynomial ideals

We fix deglex order on monomials. Let $I = \langle\langle f_1, f_2, \ldots\rangle\rangle \triangleleft k\langle x_1, \ldots, x_m\rangle$. Then $f_1, f_2, \ldots$ is a Gröbner-Shirshov basis of I if for every $Q \in I$ the leading monomial of Q is of the form $L\overline{f}_i R$, where $\overline{f}_i$ is the leading monomial of f_i.

So $Q \in I$ can be transformed to 0 by the greedy algorithm, which consists of steps: $Q \longmapsto Q - Lf_iR$, etc.. (the steps are called *reductions*).

If $L_1 f_i R_1$ and $L_2 f_j R_2$ have the same highest monomials, then $S(f_i, f_j) = L_1 f_i R_1 - L_2 f_j R_2$ is called *s-polynomial*.

Theorem

$\{f_1, f_2, \ldots\}$ is a Gröbner-Shirshov basis of the ideal I if and only if all s-polynomials of f_i, f_j can be reduced to 0.

We consider words of the form $u_i = x^2 y^i xy$ for $i > 0$. Now we enumerate all pairs of words in the semigroup $\langle x, y \rangle$ and impose the relations $w_j + w_k = u_{i(j,k)}$ on $\mathbb{Z}_2\langle x, y \rangle$, where we choose $i(j,k) > 2(|w_j| + |w_k|)$. Then $u_{i(j,k)}$ is the leading monomial of $w_j + w_k = u_{i(j,k)}$. Clearly, u_s, u_t do not have overlaps for $s \neq t$. Therefore, $\{w_j + w_k = u_{i(j,k)}\}_{j,k}$ is a Gröbner-Shirshov basis of the corresponding ideal I.

We consider words of the form $u_i = x^2 y^i xy$ for $i > 0$. Now we enumerate all pairs of words in the semigroup $\langle x, y \rangle$ and impose the relations $w_j + w_k = u_{i(j,k)}$ on $\mathbb{Z}_2\langle x, y \rangle$, where we choose $i(j, k) > 2(|w_j| + |w_k|)$. Then $u_{i(j,k)}$ is the leading monomial of $w_j + w_k = u_{i(j,k)}$. Clearly, u_s, u_t do not have overlaps for $s \neq t$. Therefore, $\{w_j + w_k = u_{i(j,k)}\}_{j,k}$ is a Gröbner-Shirshov basis of the corresponding ideal I.

The set of words $x^j, j > 0$, is linearly independent by the property of Gröbner-Shirshov basis.

We consider words of the form $u_i = x^2 y^i xy$ for $i > 0$. Now we enumerate all pairs of words in the semigroup $\langle x, y\rangle$ and impose the relations $w_j + w_k = u_{i(j,k)}$ on $\mathbb{Z}_2\langle x, y\rangle$, where we choose $i(j,k) > 2(|w_j| + |w_k|)$. Then $u_{i(j,k)}$ is the leading monomial of $w_j + w_k = u_{i(j,k)}$. Clearly, u_s, u_t do not have overlaps for $s \neq t$. Therefore, $\{w_j + w_k = u_{i(j,k)}\}_{j,k}$ is a Gröbner-Shirshov basis of the corresponding ideal I.

The set of words $x^j, j > 0$, is linearly independent by the property of Gröbner-Shirshov basis.

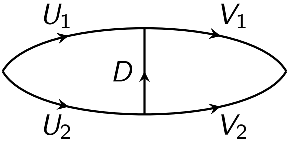
Now let us add inverses. Namely, take $\mathbb{Z}_2\langle x, y, a, b\rangle$, take the same $w_j + w_k = u_i$ and add $xa = ax = yb = by = 1$. Then we have overlaps in the set of the highest monomials. Take the s-polynomial for $ax - 1$ and $u_i - w_j - w_k$:

$$a(u_i - w_j - w_k) - (ax - 1)xy^i xy = xy^i xy - aw_j - aw_k.$$

The leading monomial $xy^i xy$ has an overlap with another u_t. Adding more and more s-polynomials produces more and more overlaps of the highest monomials.

Deglex ordering does not work well for "group-like" relations.

Let $G = \langle x, y \mid R_1, \ldots, R_n \rangle$ be given by a finite symmetrised Dehn's presentation. Then $kG \cong k\mathrm{F}/I$, where $I = \langle\langle R_1 - 1, \ldots, R_n - 1 \rangle\rangle$. Consider the following set of generators of I: $\{A_{ij} - B_{ij}\}_{i,j}$, where $A_{ij} B_{ij}^{-1} = R_i$. It is not a Gröbner-Shirshov basis of I with respect to deglex order.



$$R_s = U_1 D^{-1} V_1^{-1}$$

$$R_t = V_1 V_2^{-1} D$$

$U_1 U_2 - V_1 V_2 = 0$ in kG, but it do not contain leading monomials of any relators $A_{ij} - B_{ij}$. Notice that this can happen even if G satisfy $C(7)$.

Small cancellation rings

Let $\mathcal{I} = \langle\langle p_i = \sum_{j=1}^{n_j} \alpha_{ij} m_{ij}; i \geqslant 1 \rangle\rangle \lhd k\mathrm{F}$, $\mathcal{R} = \{p_i; i \geqslant 1\}$ and $\mathcal{M} = \{m_{ij}\}_{i,j}$.

Condition (Compatibility Condition)

- *For every* $\alpha \in k$ *we have* $\alpha \cdot p_i \in \mathcal{R}$.
- *If* $m_{ij} = xm'_{ij}$, *then* $x^{-1} \cdot p_i \in \mathcal{R}$.
- *If* $m_{ij} = m'_{ij}x$, *then* $p_i \cdot x^{-1} \in \mathcal{R}$.

Small pieces for rings

Let $C \in \mathcal{M}$,

$$p = \sum_{i=1}^{m_1} \alpha_i a_i + A_1 C A_2 \in \mathcal{R},\ \ q = \sum_{i=1}^{m_2} \beta_i b_i + B_1 C B_2 \in \mathcal{R}.$$

If at least one of $B_1 \cdot A_1^{-1} \cdot p$ and $p \cdot A_2^{-1} \cdot B_2$ does not belong to $\mathcal{R}$ (even after the cancellations), then C is called *a small piece with respect to* $\mathcal{R}$

We require that 1 is a small piece.

Small pieces for rings

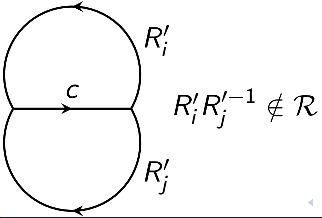
Let $C \in \mathcal{M}$,

$$p = \sum_{i=1}^{m_1} \alpha_i a_i + A_1 C A_2 \in \mathcal{R}, \; q = \sum_{i=1}^{m_2} \beta_i b_i + B_1 C B_2 \in \mathcal{R}.$$

If at least one of $B_1 \cdot A_1^{-1} \cdot p$ and $p \cdot A_2^{-1} \cdot B_2$ does not belong to $\mathcal{R}$ (even after the cancellations), then C is called *a small piece with respect to* $\mathcal{R}$

We require that 1 is a small piece.

There exists a generalization of small pieces (in the group sense) called *graph small cancellation condition*. The above definition follows similar intuition.



Small cancellation condition for rings

Condition (Small Cancellation Condition)

Assume $q_1, \dots, q_n \in \mathcal{R}$ *and a linear combination* $\sum_{j=1}^{n} \gamma_j q_j$ *is non-zero after additive cancellations. Then there exists a monomial A in* $\sum_{j=1}^{n} \gamma_j q_j$ *with a non-zero coefficient such that*

- *either A can not be represented as a product of small pieces,*
- *or every representation of A of a form* $A = c_1 \cdots c_l$*,*
  where $c_1, \dots, c_l$ *are small pieces,*
  contains at least 11 small pieces.

Structure of small cancellation rings

"Informal structure theorem"

Theorem (A.A., A. Kanel-Belov, E. Plotkin, E. Rips, 2021)

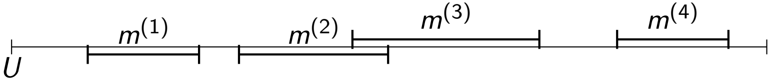
Let $k\mathrm{F}/\mathcal{I}$ be a small cancellation ring, $\mathcal{I} = \langle\langle p_i; i \geqslant 1\rangle\rangle$. Then it is non-trivial, its structure can be described in terms of "multi" one-layer maps, and $\{p_i\}_{i\geqslant 0}$ is a Gröbner-Shirshov basis of $\mathcal{I}$ with respect to a special monomial order.

Structure of small cancellation rings

“Informal structure theorem”

Theorem (A.A., A. Kanel-Belov, E. Plotkin, E. Rips, 2021)

Let $\mathrm{k}\mathrm{F}/\mathcal{I}$ be a small cancellation ring, $\mathcal{I} = \langle\langle p_i; i \geqslant 1\rangle\rangle$. Then it is non-trivial, its structure can be described in terms of “multi” one-layer maps, and $\{p_i\}_{i\geqslant 0}$ is a Gröbner-Shirshov basis of $\mathcal{I}$ with respect to a special monomial order.



$m^{(i)}$ are maximal occurrences of elements from $\mathcal{M}$ in a word U. They are used to define a complexity of U and the order on monomials is based on the complexity.

Small cancellation rings: examples

If $G = \langle x_1, \ldots, x_n \mid R_1, \ldots, R_t, \ldots \rangle$, then $kG \cong k\mathrm{F}/\mathcal{I}$, where $\mathcal{I} = \langle\langle R_i - 1; i \geqslant 1 \rangle\rangle$. If G satisfies $\mathrm{C}(m)$, $m \geqslant 22$, then kG is a small cancellation ring.

Notice that the above set of generators of $\mathcal{I}$ itself does not satisfy small cancellation conditions. We need to extend it.

Small cancellation rings: examples

If $G = \langle x_1, \ldots, x_n \mid R_1, \ldots, R_t, \ldots \rangle$, then $kG \cong k\mathrm{F}/\mathcal{I}$, where $\mathcal{I} = \langle\langle R_i - 1; i \geqslant 1 \rangle\rangle$. If G satisfies $\mathrm{C}(m)$, $m \geqslant 22$, then kG is a small cancellation ring.

Notice that the above set of generators of $\mathcal{I}$ itself does not satisfy small cancellation conditions. We need to extend it.

Let $\mathcal{I} = \langle\langle 1 + w = v \rangle\rangle \lhd k\mathrm{F}$, where $v = x^\alpha y x^{\alpha+1} y \ldots y x^\beta y$, and $|w| \ll \alpha \ll \beta$. Then $k\mathrm{F}/\mathcal{I}$ is a small cancellation ring.

Again we need to extend the generating set to fulfil small cancellation conditions. Small pieces here are subwords of $w^{\pm N}$ and subwords of $v^{\pm 1}$ that contain less than two letters $y^{\pm 1}$.

Further research

- Develop iterated small cancellation theory for rings.
- Study further properties of small cancellation rings.
  - Small cancellation rings are non-amenable and contain free associative subalgebras (A.A., 2023).
  - Prove generalisation of Bergman's centraliser theorem (N. Miasnikov gave a partial description of centralisers in $k\mathrm{F}$).
- Develop geometric theory for rings in parallel to geometric group theory.