Vladimir Shpilrain
The City College of New York
shpil@groups.sci.ccny.cuny.edu

March 1, 2012

Decision, witness, and search problems in group theory

Decision problems: given a property $\mathcal{P}$ and an object $\mathcal{O}$, find out whether or not the object $\mathcal{O}$ has the property $\mathcal{P}$.

Witness problems: given a property $\mathcal{P}$ and an object $\mathcal{O}$ with the property $\mathcal{P}$, find a proof (a "witness") of the fact that $\mathcal{O}$ has the property $\mathcal{P}$.

Search problems: given a property $\mathcal{P}$ and an object $\mathcal{O}$ with the property $\mathcal{P}$, find a "material evidence" of the fact that $\mathcal{O}$ has the property $\mathcal{P}$.

All decision problems in group theory have a "companion" witness version, and most of them also have a search version

Decision, witness, and search problems in group theory

Decision problems: given a property $\mathcal{P}$ and an object $\mathcal{O}$, find out whether or not the object $\mathcal{O}$ has the property $\mathcal{P}$.

Witness problems: given a property $\mathcal{P}$ and an object $\mathcal{O}$ with the property $\mathcal{P}$, find a proof (a "witness") of the fact that $\mathcal{O}$ has the property $\mathcal{P}$.

Search problems: given a property $\mathcal{P}$ and an object $\mathcal{O}$ with the property $\mathcal{P}$, find a "material evidence" of the fact that $\mathcal{O}$ has the property $\mathcal{P}$.

All decision problems in group theory have a "companion" witness version, and most of them also have a search version

Decision, witness, and search problems in group theory

Decision problems: given a property $\mathcal{P}$ and an object $\mathcal{O}$, find out whether or not the object $\mathcal{O}$ has the property $\mathcal{P}$.

Witness problems: given a property $\mathcal{P}$ and an object $\mathcal{O}$ with the property $\mathcal{P}$, find a proof (a "witness") of the fact that $\mathcal{O}$ has the property $\mathcal{P}$.

Search problems: given a property $\mathcal{P}$ and an object $\mathcal{O}$ with the property $\mathcal{P}$, find a "material evidence" of the fact that $\mathcal{O}$ has the property $\mathcal{P}$.

All decision problems in group theory have a "companion" witness version, and most of them also have a search version

Decision, witness, and search problems in group theory

Decision problems: given a property $\mathcal{P}$ and an object $\mathcal{O}$, find out whether or not the object $\mathcal{O}$ has the property $\mathcal{P}$.

Witness problems: given a property $\mathcal{P}$ and an object $\mathcal{O}$ with the property $\mathcal{P}$, find a proof (a "witness") of the fact that $\mathcal{O}$ has the property $\mathcal{P}$.

Search problems: given a property $\mathcal{P}$ and an object $\mathcal{O}$ with the property $\mathcal{P}$, find a "material evidence" of the fact that $\mathcal{O}$ has the property $\mathcal{P}$.

All decision problems in group theory have a "companion" witness version, and most of them also have a search version

The word problem

Let $G = \langle X; R \rangle = \langle x_1, \ldots, x_m;\ r_1, \ldots \rangle$ be a finite (or more generally, recursive) presentation of a group G by generators and defining relations.

Decision problem (WP): given a word w in the alphabet X, find out whether or not w is equal to 1 in G or, equivalently, whether or not w is in the normal closure of R.

Search problem (WSP): given that a word w is in the normal closure of R, find a presentation of w as a product of conjugates of r_i and r_i^{-1}.

Note: if in a group G the word problem is recursively unsolvable, then the length of a proof verifying that $w = 1$ in G is not bounded by any recursive function of the length of w.

The word problem

Let $G = \langle X; R \rangle = \langle x_1, \ldots, x_m;\ r_1, \ldots \rangle$ be a finite (or more generally, recursive) presentation of a group G by generators and defining relations.

Decision problem (WP): given a word w in the alphabet X, find out whether or not w is equal to 1 in G or, equivalently, whether or not w is in the normal closure of R.

Search problem (WSP): given that a word w is in the normal closure of R, find a presentation of w as a product of conjugates of r_i and r_i^{-1}.

Note: if in a group G the word problem is recursively unsolvable, then the length of a proof verifying that $w = 1$ in G is not bounded by any recursive function of the length of w.

The word problem

Let $G = \langle X; R \rangle = \langle x_1, \ldots, x_m;\ r_1, \ldots \rangle$ be a finite (or more generally, recursive) presentation of a group G by generators and defining relations.

Decision problem (WP): given a word w in the alphabet X, find out whether or not w is equal to 1 in G or, equivalently, whether or not w is in the normal closure of R.

Search problem (WSP): given that a word w is in the normal closure of R, find a presentation of w as a product of conjugates of r_i and r_i^{-1}.

Note: if in a group G the word problem is recursively unsolvable, then the length of a proof verifying that $w = 1$ in G is not bounded by any recursive function of the length of w.

The conjugacy problem

Decision problem (CP): given two words w_1, w_2, find out whether or not there is a word g such that the words $g^{-1}w_1g$ and w_2 represent the same element of the group G.

Search problem (CSP): given two words w_1, w_2 representing conjugate elements of G, find a conjugator.

The conjugacy problem

Decision problem (CP): given two words w_1, w_2, find out whether or not there is a word g such that the words $g^{-1}w_1g$ and w_2 represent the same element of the group G.

Search problem (CSP): given two words w_1, w_2 representing conjugate elements of G, find a conjugator.

The subgroup membership problem

Decision problem (MP): given a group G, a subgroup H generated by $h_1, \ldots, h_k$, and an element $g \in G$, find out whether or not $g \in H$.

Search problem (MSP): given a group G, a subgroup H generated by $h_1, \ldots, h_k$, and an element $h \in H$, find an expression of h as a word in $h_1, \ldots, h_k$.

The isomorphism problem

Decision problem (IP): given two finitely presented groups G_1 and G_2, find out whether or not they are isomorphic.

Search problem (ISP): given two isomorphic finitely presented groups G_1 and G_2, find an explicit isomorphism, i.e., a map $\varphi : G_1 \to G_2$ which is:

- a homomorphism
- injective
- surjective

The isomorphism problem

Decision problem (IP): given two finitely presented groups G_1 and G_2, find out whether or not they are isomorphic.

Search problem (ISP): given two isomorphic finitely presented groups G_1 and G_2, find an explicit isomorphism, i.e., a map $\varphi : G_1 \to G_2$ which is:

- a homomorphism
- injective
- surjective

The “no” part

“Yes” and “no” parts of decision problems are usually quite different!

- Non-identity witness problem
- Non-conjugacy witness problem
- Non-isomorphism witness problem
- Non-membership witness problem

Note: generically, i.e., on “most” inputs, the “no” answer can be given in linear time:
I. Kapovich, A. G. Myasnikov, P. Schupp, V. Shpilrain, *Generic-case complexity, decision problems in group theory and random walks*, J. Algebra **264** (2003), 665–694.

The “no” part

“Yes” and “no” parts of decision problems are usually quite different!

- Non-identity witness problem
- Non-conjugacy witness problem
- Non-isomorphism witness problem
- Non-membership witness problem

Note: generically, i.e., on “most” inputs, the “no” answer can be given in linear time:

I. Kapovich, A. G. Myasnikov, P. Schupp, V. Shpilrain, *Generic-case complexity, decision problems in group theory and random walks*, J. Algebra **264** (2003), 665–694.

The "no" part

"Yes" and "no" parts of decision problems are usually quite different!

- Non-identity witness problem
- Non-conjugacy witness problem
- Non-isomorphism witness problem
- Non-membership witness problem

Note: generically, i.e., on "most" inputs, the "no" answer can be given in linear time:
I. Kapovich, A. G. Myasnikov, P. Schupp, V. Shpilrain, *Generic-case complexity, decision problems in group theory and random walks*, J. Algebra **264** (2003), 665–694.

The "no" part

"Yes" and "no" parts of decision problems are usually quite different!

- Non-identity witness problem
- Non-conjugacy witness problem
- Non-isomorphism witness problem
- Non-membership witness problem

Note: generically, i.e., on "most" inputs, the "no" answer can be given in linear time:
I. Kapovich, A. G. Myasnikov, P. Schupp, V. Shpilrain, *Generic-case complexity, decision problems in group theory and random walks*, J. Algebra **264** (2003), 665–694.

The "no" part

"Yes" and "no" parts of decision problems are usually quite different!

- Non-identity witness problem
- Non-conjugacy witness problem
- Non-isomorphism witness problem
- Non-membership witness problem

Note: generically, i.e., on "most" inputs, the "no" answer can be given in linear time:
I. Kapovich, A. G. Myasnikov, P. Schupp, V. Shpilrain, *Generic-case complexity, decision problems in group theory and random walks*, J. Algebra **264** (2003), 665–694.

The "no" part

"Yes" and "no" parts of decision problems are usually quite different!

- Non-identity witness problem
- Non-conjugacy witness problem
- Non-isomorphism witness problem
- Non-membership witness problem

Note: generically, i.e., on "most" inputs, the "no" answer can be given in linear time:
I. Kapovich, A. G. Myasnikov, P. Schupp, V. Shpilrain, *Generic-case complexity, decision problems in group theory and random walks*, J. Algebra **264** (2003), 665–694.

Ramifications

- (M. Chiodo) Is there a general procedure to produce a non-trivial element from a finite presentation of a non-trivial group?

- Given a finitely presented group G, elements $h_1, \ldots, h_k \in G$, and the information that $h_1, \ldots, h_k$ freely generate a free subgroup of G, find a proof (a "witness") of that fact.

  Can both "yes" and "no" parts of a (natural) decision problem be non-recursive?

- Given a finitely presented group and the information that it is metabelian, find a proof (a "witness") of that fact.

- Given two finitely presented groups G_1 and G_2 and the information that there is an injective homomorphism (an embedding) of G_1 into G_2, find a proof (a "witness") of that fact.

Ramifications

- (M. Chiodo) Is there a general procedure to produce a non-trivial element from a finite presentation of a non-trivial group?

- Given a finitely presented group G, elements $h_1, \ldots, h_k \in G$, and the information that $h_1, \ldots, h_k$ freely generate a free subgroup of G, find a proof (a "witness") of that fact.

Can both "yes" and "no" parts of a (natural) decision problem be non-recursive?

- Given a finitely presented group and the information that it is metabelian, find a proof (a "witness") of that fact.

- Given two finitely presented groups G_1 and G_2 and the information that there is an injective homomorphism (an embedding) of G_1 into G_2, find a proof (a "witness") of that fact.

Ramifications

- (M. Chiodo) Is there a general procedure to produce a non-trivial element from a finite presentation of a non-trivial group?

- Given a finitely presented group G, elements $h_1, \ldots, h_k \in G$, and the information that $h_1, \ldots, h_k$ freely generate a free subgroup of G, find a proof (a "witness") of that fact.

Can both "yes" and "no" parts of a (natural) decision problem be non-recursive?

- Given a finitely presented group and the information that it is metabelian, find a proof (a "witness") of that fact.

- Given two finitely presented groups G_1 and G_2 and the information that there is an injective homomorphism (an embedding) of G_1 into G_2, find a proof (a "witness") of that fact.

Ramifications

- (M. Chiodo) Is there a general procedure to produce a non-trivial element from a finite presentation of a non-trivial group?

- Given a finitely presented group G, elements $h_1, \ldots, h_k \in G$, and the information that $h_1, \ldots, h_k$ freely generate a free subgroup of G, find a proof (a "witness") of that fact.

  Can both "yes" and "no" parts of a (natural) decision problem be non-recursive?

- Given a finitely presented group and the information that it is metabelian, find a proof (a "witness") of that fact.

- Given two finitely presented groups G_1 and G_2 and the information that there is an injective homomorphism (an embedding) of G_1 into G_2, find a proof (a "witness") of that fact.

Ramifications

- (M. Chiodo) Is there a general procedure to produce a non-trivial element from a finite presentation of a non-trivial group?

- Given a finitely presented group G, elements $h_1, \ldots, h_k \in G$, and the information that $h_1, \ldots, h_k$ freely generate a free subgroup of G, find a proof (a "witness") of that fact.

  Can both "yes" and "no" parts of a (natural) decision problem be non-recursive?

- Given a finitely presented group and the information that it is metabelian, find a proof (a "witness") of that fact.

- Given two finitely presented groups G_1 and G_2 and the information that there is an injective homomorphism (an embedding) of G_1 into G_2, find a proof (a "witness") of that fact.

Stratification: converting search problems to decision problems

Stratification of the conjugacy search problem

Given two words w_1, w_2 representing conjugate elements of G, and a positive integer k, is there a word g of length at most k such that $g^{-1}w_1g$ and w_2 represent the same element of G?

Warning. The conjugacy search problem is algorithmically solvable in any recursively presented group G, whereas the problem above may not be if the word problem in G is algorithmically unsolvable.

Stratification: converting search problems to decision problems

Stratification of the conjugacy search problem

Given two words w_1, w_2 representing conjugate elements of G, and a positive integer k, is there a word g of length at most k such that $g^{-1}w_1g$ and w_2 represent the same element of G?

Warning. The conjugacy search problem is algorithmically solvable in any recursively presented group G, whereas the problem above may not be if the word problem in G is algorithmically unsolvable.

Stratification: WSP

Geodesic problem:

Given a word w, a group G, and a positive integer k, is there a word g of length at most k, which is equal to w in G?

NP-hard in some groups G, including, somewhat surprisingly, the free metabelian group of rank 2 (Myasnikov-Roman'kov-Ushakov-Vershik), where it is actually **N**P-complete.

Stratification: ISP

• By the sum of the lengths of images of the generators under a given isomorphism.

• By the length of a sequence of Tietze transformations establishing an isomorphism between groups.

Stratification: ISP

• By the sum of the lengths of images of the generators under a given isomorphism.

• By the length of a sequence of Tietze transformations establishing an isomorphism between groups.

Thank you