WHY WORD PROBLEMS ARE HARD

KEITH CONRAD

1. Introduction

The title above is a joke. Many students in school hate word problems. We will discuss here a specific math question that happens to be named "the word problem" and in general it can't be solved. This does not mean word problems in school are therefore pointless.

A *decision problem* is, roughly, a question with a yes/no answer. Here are some examples.

- Are two positive integers relatively prime?
- Is a positive integer a prime number?
- Are two matrices in $\mathrm{GL}_n(\mathbf{Q})$ conjugate in this group?

We call a decision problem **decidable** if there is an algorithm that always determines (correctly!) whether or not *each* instance of the problem has the answer yes or no. Note we are asking for *one* algorithm that handles all cases: we want to settle all instances of the problem by common procedure. The decision problems above are all decidable:

- Euclid's algorithm tells us in finitely many steps if two positive integers are relatively prime.
- Trial division tells us in finitely many steps if a positive integer is prime. It may be very inefficient, but it works.
- Conjugacy of matrices in $\mathrm{GL}_n(\mathbf{Q})$ can be settled by comparing their rational canonical forms (which is a finite algorithm in part since rational numbers are exactly computable numbers).

We will not be giving a rigorous definition of an algorithm, but experience with standard procedures for solving math questions (Gaussian elimination in linear algebra, the Euclidean algorithm in number theory, and so on) suggests what the concept is all about. A key point is its finite nature: an algorithm is a procedure with finitely many steps, like a computer program (programs do not have infinite length!). A decision problem is decidable essentially if there is an algorithm that can take as input each instance of the problem and in finitely many steps (the number of steps may vary with the input) terminate with a (correct!) yes/no answer; no "infinite loops" are allowed. If two algorithms can settle a problem together, we can put them together and call it a single algorithm. Infinitely many different algorithms, one for each instance of a problem, isn't what we mean by an algorithm.

A decision problem is intended to have an inherently finite or countable character to it. Therefore a question like deciding if two real numbers are equal, or equivalently deciding if a real number is equal to 0, is *not* considered a decision problem because it is inherently not about countable objects. (You may think equality in $\mathbf{R}$ shouldn't be decidable because if we know $x = .000000\ldots$ to a large number of digits, at no finite point can we really be sure $x = 0$, but that's not why we consider equality in $\mathbf{R}$ not to be a decision problem: comparing two real numbers need not use their decimal expansions.)

In the 1930s, Church and Turing proved independently that there are decision problems that are undecidable. The particular decision problems they used (*e.g.*, the halting problem for Turing) were of interest in logic but were not based on another branch of mathematics (linear algebra, group theory, topology, *etc.*). Therefore their work did not have a practical effect on areas of math outside of logic. Only 20 years later, in the 1950s, were examples of undecidable decision problems found elsewhere in mathematics, namely in group theory.

To explain these group-theoretic problems (without proofs) we will be using groups that are described by a finite amount of information (even though the groups may be infinite), and this will made precise by the concepts of *finitely generated group*, *free group*, and *finitely presented group*. To get a feel for what finitely presented groups are, we should understand first what finitely generated groups and free groups are, including examples of each.

2. Finitely generated groups

Definition 2.1. A group G is called *finitely generated* if it has finitely many elements $g_1, \ldots, g_n$ such that every element of G is a finite product of powers of these elements, allowing arbitrary integer exponents. We call the g_i's generators of G and write $G = \langle g_1, \ldots, g_n \rangle$.

Example 2.2. Every finite group is finitely generated, using all of its elements as generators.

Example 2.3. The group $\mathbf{Z}^n$ is infinite, abelian, and finitely generated with generators the vectors $\mathbf{e}_i = (0, \ldots, 1 \ldots, 0)$ having 1 in the i-th component and 0 elsewhere.

Example 2.4. An infinite nonabelian finitely generated group is

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a = \pm 1, b \in \mathbf{Z} \right\}$$

with generators $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$:

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^b, \quad \begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^b \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

The matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ has order 2, while $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ has infinite order. This group is also generated by $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$, which both have order 2. So an infinite group can be generated by two elements of order 2.

There are groups with two generators in which *all* elements of the group have finite order, and in fact there are such examples where all non-identity elements have a common prime order (Tarski monster).

A finitely generated group is at most countable, but the converse is false: $\mathbf{Q}$ as an additive group is countable but not finitely generated: for any finite list of fractions, pick a prime p not dividing any of the denominators. Then $1/p$ is not a sum of integer multiples from that finite list.

Finitely generated abelian groups have an elementary abstract structure: they are each isomorphic to a direct product $\mathbf{Z}^r \times C_1 \times \cdots \times C_k$, where $r \geq 0$ and the C_i's are finite cyclic groups. But this does *not* mean finitely generated abelian groups that show up in mathematics are always easy to understand! There are hard theorems in number theory (*e.g.*, Dirichlet's unit theorem and the Mordell-Weil theorem) asserting that certain abelian groups are finitely generated, and determining an explicit set of generators for such a group (or perhaps even the number of generators of such a group) can be a difficult computational task.

3. Free groups

Definition 3.1. The *free group on n letters*, F_n, is a group generated by n elements $x_1, \ldots, x_n$ that have "no relations". Every element of F_n is just a string of symbols, like

$$x_1 x_2^2 x_3^{-1} x_2 x_1^5 x_2^{-3},$$

with the only cancellation allowed coming from $x_i x_i^{-1} = 1$ and $x_i^{-1} x_i = 1$.

The group F_1 is $\mathbf{Z}$, which is commutative, but F_n for $n \geq 2$ is noncommutative. In fact, two elements of F_n commute if and only they are powers of a common element of F_n. Every element in F_n can be written in just one way as a string of powers of the x_i's, so when $n \geq 2$ they are like a noncommutative basis.

Where do free groups naturally arise? Topology is one source of them.

Example 3.2. Consider the plane with 2 points removed. Every path in the plane that doesn't go through the two missing points will go a definite number of times around one point and the other, with (say) counterclockwise turns counting positively and clockwise turns counting negatively. Focusing only on paths that are loops starting and ending at a common point in this twice-punctured plane, going once around each point in succession depends on which point is looped around first: the fundamental group of a twice-punctured plane is nonabelian[1] and turns out to be isomorphic to the free group F_2, with the two generators being loops (up to homotopy) going once around just one of the two points.

More generally, the fundamental group of the plane with n points removed is isomorphic to the free group on n loops. This shows that free groups are mathematical objects arising in areas other than pure group theory.

A free group is called "free" because we can build homomorphisms out of it by sending the x_i's anywhere we wish (free choice), in the same way that bases in vector spaces are "free" for building linear mappings to other vector spaces: when you say where you want a basis to go, there is a unique linear map with that effect on the basis. Similarly, if G is a group with n elements $g_1, \ldots, g_n$ in G (no restriction on them, and they could even all be equal), there is a unique group homomorphism $F_n \to G$ such that $x_i \mapsto g_i$.

All vector spaces have a basis, but not all groups are free, *e.g.*, a nontrivial finite group is not free: all elements have finite order, and an element of order 6, say, can be mapped under a homomorphism only to elements of order dividing 6, so there's a constraint on where it could go under a homomorphism.

Every finitely generated group can be linked to some free group F_n by using quotient groups.

Theorem 3.3. *Every finitely generated group with n generators is a quotient group of F_n.*

Proof. Let G have generators $g_1, \ldots, g_n$. There's a homomorphism $f \colon F_n \to G$ with $f(x_i) = g_i$. It's surjective since the image of f is a subgroup of G containing the generators $g_1, \ldots, g_n$. Therefore $G \cong F_n / \ker f$. □

We defined free groups only with a finite number of generators. If we replace $x_1, \ldots, x_n$ in the definition with a possibly infinite alphabet then we get the concept of a free group in general, and every group is a quotient of a free group.

[1] Pictures explaining this are at https://math.stackexchange.com/questions/1802198.

The definition of a finitely generated group may seem to be a nonabelian analogue of a finite-dimensional vector space. A subspace of an n-dimensional vector space has dimension at most n. If a group G has n generators, does every subgroup have at most n generators? Yes if G is abelian, but in general no.

Theorem 3.4. *Every subgroup of finite index in a finitely generated group is finitely generated.*

Watch out! Theorem 3.4 does not say the number of generators of the subgroup is at most the number of generators of the original group, and for nonabelian groups often it is not.

Example 3.5. If $G = F_n$ and $[G : H] = m$ then $H \cong F_{mn-m+1}$. If $n > 1$ and $m > 1$ then $mn - m + 1 > n$, so a proper subgroup of finite index in a free group on finitely many – and at least two – letters requires *more* generators than the original group.

Theorem 3.6. *A normal subgroup of F_n other than $\{1\}$ is finitely generated if and only if it has finite index.*

Therefore if we can write down a nontrivial normal subgroup of F_n with infinite index, it will not be finitely generated.

Example 3.7. The commutator subgroup $[F_n, F_n]$ of F_n is normal and $F_n/[F_n, F_n] \cong \mathbf{Z}^n$, so $[F_n, F_n]$ has infinite index in F_n, and $[F_n, F_n]$ is nontrivial for $n \geq 2$ (since F_n is nonabelian), so for $n \geq 2$, $[F_n, F_n]$ is not finitely generated by Theorem 3.6.

We have seen that the property "finitely generated" doesn't behave well when passing to subgroups *in general*, but it does if we stick to subgroups of finite index (Theorem 3.4). Perhaps surprisingly, being "free" behaves well for all subgroups.

Theorem 3.8 (Nielsen, Schreier)**.** *Every subgroup of a free group is free.*

This theorem is not limited to the groups F_n: free groups in the theorem may have an infinite generating set. The theorem was proved by Nielsen for finitely generated subgroups and by Schreier for general subgroups. The theorem has a purely algebraic proof, but its first proof used topology: interpret a free group as a fundamental group and use the relation between normal subgroups of a fundamental group and covering spaces.

The Nielsen–Schreier theorem may at first seem trivial, because in a free group there are "no relations" among the generators other than what comes from axioms of group theory (like $xx^{-1} = 1$). So how could a subgroup of a free group *not* be free? The subtlety is that the generators of the original free group don't have to lie in the subgroup, so how do you know a subgroup has its own generators fitting the condition for being a free group? If you still don't see the subtlety, consider that a subgroup of a nonabelian group could be abelian: when you have a property (being cyclic, being nonabelian, being free) that is about a choice of elements in the group and you pass to a subgroup not containing those elements, it's not clear if the subgroup should still satisfy the same property. Sometimes the property may no longer hold (being nonabelian) and sometimes it does (being cyclic, being free).

4. Finitely presented groups

We have seen that a normal subgroup of a finitely generated group need not be finitely generated (Example 3.7). The property of a subgroup being finitely generated uses only the operations of multiplication and inversion in the subgroup to create new elements from an initial set of elements of the subgroup. In a normal subgroup, there is a further way to create new elements of it from elements we already have in the subgroup: conjugation by elements of the bigger group it's normal in. If a normal subgroup can't be built from finitely many of its elements by multiplication and inversion alone, it might be built from finitely many of its elements by multiplication, inversion, and also conjugation from the original group on those finitely many elements. (Analogy: when $\mathrm{SO}(n)$ acts on $\mathbf{R}^n$, an orbit is a sphere, but when $\mathrm{GL}_n(\mathbf{R})$ acts on $\mathbf{R}^n$, all nonzero vectors lie in the same orbit. Having a larger group act can link more elements of the set together.)

Example 4.1. In $F_2 = \langle x, y\rangle$, the subgroup $[F_2, F_2]$ is not finitely generated, but it contains the commutator $[x, y] = xyx^{-1}y^{-1}$ and $[F_2, F_2]$ is generated by $[x, y]$ together with all conjugates of $[x, y]$ by elements of F_2. That means we can get all of $[F_2, F_2]$ from $[x, y]$ by using in all possible ways the operations of multiplication, inversion, and conjugation from F_2. This makes $[F_2, F_2]$ "finitely generated" in a wider sense than just by using the group law within $[F_2, F_2]$ alone.

Definition 4.2. A group G is called *finitely presented* if it has the form F_n/N for some n where N is a normal subgroup of F_n whose elements are each constructed from a finite set R in F_n by using multiplication, inversion, and conjugation by F_n finitely many times on R.

What does this really mean? Writing $G = \langle g_1, \dots, g_n\rangle$, there's a homomorphism $F_n \twoheadrightarrow G$ sending each x_i to g_i, and N is the kernel. An element of F_n is in N when setting each x_i equal to g_i causes the element to turn into the identity in G. For instance, having $x_1^2x_2^3 \in N$ means $g_1^2g_2^3 = 1$ in G, or equivalently $g_1^2 = g_2^{-3}$. Thus N consists of the "relations" among the g_i's that generate G: the strings in the x_i's that are trivial when x_i is replaced by g_i. So R is a finite set of "relations" that explain all relations among the g_i's (all elements of N).

We write a finitely presented group as $\langle X \mid R\rangle$ where $X = \{x_1, \dots, x_n\}$ consists of the standard generators of F_n and R is the finite subset of F_n that generates N by multiplication, inversion, and conjugation by F_n: N is the smallest normal subgroup of F_n containing R. Here R need not be a generating set of N; we need conjugates of elements of R to get a generating set for N. The table below gives examples of finite presentations of groups.

G	Presentation of G
$\mathbf{Z}$	$\langle x \mid \emptyset\rangle$
$\mathbf{Z}/(n)$	$\langle x \mid x^n\rangle$
D_n	$\langle r, s \mid r^n, s^2, srs^{-1}r\rangle$
$\mathbf{Z}^2$	$\langle x, y \mid xy(yx)^{-1}\rangle$

Table 1. Finitely Presented Groups

The elements of a finitely presented group $\langle X \mid R\rangle$ can be thought of as strings of symbols taken from X: we call these strings *words* in X. They may collapse in the group, but not in the free group whose quotient gives the presentation $\langle X \mid R\rangle$. It is in the free group where different words live as independent elements.

Example 4.3. Let

$$G = \langle x, y \mid xyx^{-1}y^{-2}, x^{-2}y^{-1}xy\rangle.$$

In G, $xyx^{-1}y^{-2} = 1$ and $x^{-2}y^{-1}xy = 1$, so $xy = y^2x$ and $yx^2 = xy$. Thus $y^2x = yx^2$. Canceling y on the left sides gives $yx = x^2$, and canceling x on the right gives $y = x$. Therefore the equation $yx^2 = xy$ in G says $x^3 = x^2$, so $x = 1$ and $y = 1$: G is trivial!

Often the elements of R in $\langle X \mid R\rangle$ are rewritten as equations to make the constraints more intuitive. In the case of G above, we might write $G = \langle x, y \mid xy = y^2x, xy = yx^2\rangle$.

Example 4.4. The finitely presented group $\langle x, y \mid x^{-1}y^2x = y^3, y^{-1}x^2y = x^3\rangle$ is trivial, but the proof that this group is trivial is rather tricky.[2]

There is an analogue of Theorem 3.4 for finitely presented groups.

Theorem 4.5. *Every subgroup of finite index in a finitely presented group is finitely presented.*

Not all subgroups of a finitely presented group are finitely presented.

Example 4.6. The group $F_2 \times F_2 = \langle x, y\rangle \times \langle z, w\rangle$ is finitely presented (it is not F_4!). Define $f \colon F_2 \times F_2 \to \mathbf{Z}$ by $x, y, z, w \mapsto 1$. Then $\ker f$ is generated by xy^{-1}, xz^{-1}, and xw^{-1}, but not finitely presented.

5. Decision problems about groups

Here are several decision problems about a finitely presented group $G = \langle X \mid R\rangle$.

1. Word Problem: Can we decide if two words in X are equal in G?
2. Generalized Word Problem: Given words $w_1, \ldots, w_n, w$ in X, can we decide if w is in the subgroup $\langle w_1, \ldots, w_n\rangle$ when viewed in G?
3. Conjugacy Problem: Can we decide if two words in X are conjugate in G?
4. Isomorphism Problem: Can we decide if two finitely presented groups $\langle X \mid R\rangle$ and $\langle Y \mid S\rangle$ are isomorphic? A special case of this: can we decide if a finitely presented group is trivial?

Dehn posed the word problem and the conjugacy problem in 1911, and Tietze posed the isomorphism problem for finitely presented groups in 1908. The generalized word problem was posed by Mihailova in 1958. For two finite presentations of a group, there is a systematic way (Tietze transformations) to convert one into the other in finitely many steps, so the above questions are each algorithmically insensitive to the *choice* of finite presentation.

Since $g = h$ if and only if $gh^{-1} = e$, the word problem in $G = \langle X \mid R\rangle$ is the same as asking if we can always decide if a word in X is trivial in G. If the conjugacy problem can be settled in a particular group, then so can the word problem: $g = h$ if and only if $gh^{-1} = e$, and $gh^{-1} = e$ if and only if gh^{-1} is *conjugate* to e. Therefore a group for which the word problem is undecidable also has the conjugacy problem being undecidable.

While the word problem is decidable for many types of groups (*e.g.*, Artin showed in 1926 that the word problem and the conjugacy problem are decidable in braid groups), in the 1950s Novikov and Boone independently proved there is a finitely presented group for which the word problem is undecidable. Eventually it was determined that *each* of the above decision problems for finitely presented groups is undecidable. The solution involves building a group that encodes a known undecidable decision problem from logic (the halting problem) in such a way that decidability of the group theory problem implies decidability of the logic problem. Thus the undecidability of the logic problem implies the group theory problem is undecidable too. While the original examples of undecidable decision problems (like the halting problem) were not initially of direct research interest to non-logicians, such problems were used in the construction of the groups that showed the group-theoretic decision problems

[2] See https://math.stackexchange.com/questions/66573.

are undecidable. Currently, the shortest description of a concrete finitely presented group with an undecidable word problem has the form $\langle X \mid R \rangle$ where $|X| = 2$ and $|R| = 27$.[3]

[3] See https://eprint.iacr.org/2014/528.pdf.