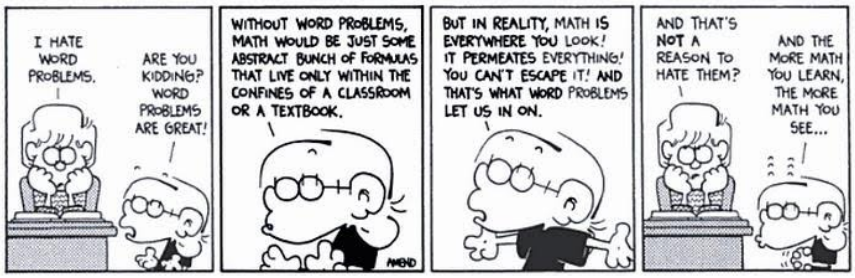
WHY WORD PROBLEMS ARE HARD

KEITH CONRAD

1. Introduction

The title above is a joke. Many students in school hate word problems. We will discuss here a specific question in group theory 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 pointless, despite what Paige thinks in the FoxTrot cartoon below.



Before explaining what "the word problem" is we discuss decision problems. A *decision problem* is, roughly, a question with a yes/no answer. Here are some examples.

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

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. This may be very inefficient (*e.g.,* for the number $2^{82{,}589{,}933} - 1$), but it works.
- Conjugacy of matrices in $\mathrm{GL}_n(\mathbf{Q})$ can be settled by comparing their rational canonical forms (which is an algorithm taking *finitely many steps*, in part since rational numbers are exactly computable numbers).

We will not give a rigorous definition of an algorithm, but standard ways to solve math problems (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 or proof: programs and proofs do not have infinite length! To say a decision problem is decidable essentially means there is an algorithm taking as input each instance of the problem and in finitely many steps (the number of steps may vary with the input) terminating with a (correct!)

yes/no answer; "infinite loops" aren't allowed. 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 deciding if a real number is equal to 0, is *not* considered a decision problem because it is inherently not about countable objects. For example, you may think showing a real number is 0 shouldn't be a decision problem 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 testing equality with 0 in $\mathbf{R}$ is not a decision problem: comparing a real number with 0 need not use decimal expansions. (In fact, the way we write something is part of the proper description of a decision problem. It is trivial to decide if an integer is prime if we choose to represent integers by their prime factorization, yet factoring is considered a hard problem! We normally think of decision problems for positive integers in terms of representing integers in a way computers would accept as input, such as their binary expansion.) Deciding if a real number equals 0 is not considered decision problem because $\mathbf{R}$ is uncountable.

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 had no practical effect on areas of math outside of logic. Only about 20 years later were examples of undecidable decision problems found elsewhere in mathematics, namely in group theory.

To explain these group-theoretic problems we will use groups described by a finite amount of information even if the groups are infinite, and this will made precise by the concepts of *finitely generated group*, *free group*, and *finitely presented group*. The last concept, finitely presented groups, is often not seen in abstract algebra courses. We will explain what each of the terms means, including examples of each. Theorems will be stated without proofs.

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 n generators: the vectors $\mathbf{e}_i = (0, \ldots, 1 \ldots, 0)$ with 1 in the i-th component and 0 elsewhere for $1 \leq i \leq n$.

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 the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ 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: 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 is not finitely generated: for each finite list of fractions, pick a prime p not dividing one of the denominators of those fractions. Then $1/p$ is not in the subgroup (additively) generated by that finite list. We don't really need prime numbers in that argument: for a finite list of fractions $a_1/b_1, \ldots, a_n/b_n$ with $a_i, b_i \in \mathbf{Z}$ and $b_i \geq 1$, the fraction $1/(b_1 \cdots b_n + 1)$ is not in the subgroup generated by the list since it is in reduced form with a denominator that is relatively prime to each b_i (and is greater than 1).

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 hard 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 infinite cyclic, so $F_1 \cong \mathbf{Z}$. For $n \geq 2$, F_n 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 product of powers of $x_1, \ldots, x_n$, so when $n \geq 2$ the generating set $\{x_1, \ldots, x_n\}$ is like a noncommutative basis.

A natural source of free groups in mathematics is topology.

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 each point, 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 F_n. This shows that free groups are mathematical objects arising in areas other than pure group theory.

The reason free groups are called "free" is that we can build homomorphisms out of them by sending the x_i's anywhere we wish (free choice). This is like bases in vector spaces being "free" for building linear mappings to other vector spaces: when you say where a basis goes,

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

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 $x_i \mapsto g_i$ for $i = 1, \ldots, n$.

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 $g_1, \ldots, g_n$, and the only such subgroup is G. Therefore $G = \mathrm{Im}(f) \cong F_n/\ker f$. □

We defined free groups with a finite number of generators. Replacing $x_1, \ldots, x_n$ in the definition of F_n with a possibly infinite alphabet, we get the concept of a free group in general, and the reasoning in the proof of Theorem 3.3 shows every group is a quotient of some free group.

A finitely generated group, as described in Definition 2.1, may look like 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 $H \cong F_{mn-m+1}$. When $n = 1$, $mn-m+1 = 1$ for all $m \geq 1$, so the theorem says every finite-index subgroup of an infinite cyclic group is infinite cyclic. When $n > 1$ and $m > 1$, $mn - m + 1 > n$ 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. For example, inside F_2 ($n = 2$) the subgroup $\langle x^2, y^2, xy\rangle$ has index 2 ($m = 2$) and is isomorphic to F_3 while the subgroup $\langle x^3, y^3, xy, yx\rangle$ has index 3 ($m = 3$) and is isomorphic to F_4.

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

Therefore a nontrivial normal subgroup of F_n with infinite index is not 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" is not preserved when passing to subgroups *in general*, but it is preserved if we stick to subgroups of finite index (Theorem 3.4). Perhaps surprisingly, being "free" is preserved for all subgroups.

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

This result is not limited to the groups F_n: free groups in Theorem 3.8 may have an infinite generating set (or an empty generating set: the trivial group is the free group on the empty alphabet). The theorem was proved by Nielsen (1921) for finitely generated subgroups and by Schreier (1926) for general subgroups. Their proofs were purely algebraic, but later a proof was found by Baer and Levi (1936) that interprets the theorem through the lens of topology: a free group can be made into a fundamental group of a space and each subgroup is the fundamental group of a covering space. A second proof using topology was found much later by Serre (1970).

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 the 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 the group $\mathbf{Z} = F_1$: proving every subgroup of $\mathbf{Z}$ is trivial or infinite cyclic (hence isomorphic to $F_\emptyset$ or F_1) requires some work since subgroups of $\mathbf{Z}$ need not be given in a form that makes them obviously cyclic, *e.g.*, $20\mathbf{Z} + 36\mathbf{Z}$ or the subgroup of $\mathbf{Z}$ generated by all perfect numbers. Since 6 and 28 are perfect and $(6, 28) = 2$, the subgroup generated by all perfect numbers is $2\mathbf{Z}$ if all perfect numbers are even or $\mathbf{Z}$ if there is an odd perfect number. Whether or not there is an odd perfect number is a famous unsolved problem (it is expected that there is no odd perfect number), and until the problem is settled it is impossible to compute the subgroup of $\mathbf{Z}$ generated by all perfect numbers. But we can still say the abstract structure of this subgroup is infinite cyclic.

Another property to compare between groups and subgroups is being nonabelian. Subgroups of a nonabelian group may or may not be nonabelian (the trivial subgroup certainly is abelian).

When you have a property of a group that involves a choice of elements in the group (being cyclic, being nonabelian, and being free are all such properties) 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 always does (being cyclic, being free). This is why Theorem 3.8 is substantial.

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 of a finitely generated group can't be built from finitely many of its own elements by multiplication and inversion, it might be built from finitely many of its own elements by multiplication, inversion, *and* conjugation by the larger group it is normal in. In other words, a normal subgroup that is not generated by finitely many of its elements might be generated by finitely many of its conjugacy classes.

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 the single commutator $[x, y]$ together with all of its (infinitely many) conjugates in F_2. That means we can get all of $[F_2, F_2]$ by using in all possible ways the operations of multiplication and inversion on the

elements in the conjugacy class of $[x, y]$ in F_2. This makes $[F_2, F_2]$ "finitely generated" in a wider sense than just by using the group law of F_2 on $[x, y]$ alone: we use the group law of F_2 on all conjugates of $[x, y]$ in F_2.

Definition 4.2. A group G is called *finitely presented* if it is isomorphic to F_n/N for some n, where N is a normal subgroup of F_n that is generated by a finite subset R in F_n and all the conjugates of elements of R in F_n.

A finitely presented group is a special type of finitely generated group. In the homomorphism $F_n \twoheadrightarrow G$ with kernel N, let $g_i \in G$ be the image of x_i, so $G = \langle g_1, \ldots, g_n \rangle$. An element of F_n is in N when setting each x_i equal to g_i turns the element of F_n into the identity in G. For instance, having $x_1^2 x_2^3 \in N$ means $g_1^2 g_2^3 = 1$ in G, or equivalently $g_1^2 = g_2^{-3}$. View N as the "relations" among the g_i's generating G: all 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" explaining all relations among the g_i's (all elements of N). The conjugate of a relation is a relation: if $f(g_1, \ldots, g_n) = 1$ where $f(x_1, \ldots, x_n)$ is a product of powers of $x_1, \ldots, x_n$, then $w(g_1, \ldots, g_n) f(g_1 \ldots, g_n) w(g_1, \ldots, g_n)^{-1} = 1$ too where $w(x_1, \ldots, x_n)$ is an arbitrary element of F_n.

We write a finitely presented group as $\langle X \mid R \rangle$ where $X = \{x_1, \ldots, x_n\}$ consists of the standard generators of F_n and R is a 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. Equivalently, N is the subgroup generated by the conjugacy classes of the elements of R: N is generated by finitely many conjugacy classes rather than just finitely many elements.[2] Here R need not be a generating set of N; we need to include conjugates of elements of R to get a generating set for N, so it is the conjugacy classes of elements of R that generate 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, so these strings are called *words* in X. They may collapse in the group $\langle X \mid R \rangle$, but not in the free group $\langle X \rangle \cong F_n$ whose quotient F_n/N is the group $\langle X \mid R \rangle$. It is in the free group $\langle X \rangle$ 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 $xy = yx^2$. 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 $xy = yx^2$ in G says $x^2 = x^3$, so $x = 1$ and thus $y = 1$: G is trivial!

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

[2]If a subset S of a group is closed under conjugation then the subgroup generated by S is a normal subgroup. That is, the subgroup generated by a set of conjugacy classes in a group is a normal subgroup.

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.[3]

Since finitely presented groups are finitely generated, finite-index subgroups of finitely presented groups are finitely generated by Theorem 3.4. But are they finitely presented?

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

Some subgroups of a finitely presented group are not finitely presented. This was first shown by Dehn (1911). Here is an example.

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, since x and y commute with z and w). Define the homomorphism $f\colon F_2 \times F_2 \to \mathbf{Z}$ by $x, y, z, w \mapsto 1$. Then $\ker f$ is a finitely generated subgroup of $F_2 \times F_2$, with generators xy^{-1}, xz^{-1}, and xw^{-1}, but $\ker f$ is not finitely presented.

5. Decision problems about groups

Here are several decision problems about a finitely presented group $G = \langle X \mid R\rangle$. The first one is the problem in our title.

(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?

Tietze posed the isomorphism problem for finitely presented groups in 1908. Dehn posed the word problem and conjugacy problem in 1911. (Both Tietze and Dehn were topologists. Much of the early work on finitely presented groups was motivated by the occurrence of such groups in algebraic topology as fundamental groups.) 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 $g = h$ in a group if and only if $gh^{-1} = e$, the word problem in $G = \langle X \mid R\rangle$ is equivalent to the problem of deciding when words in X are trivial in G. If the conjugacy problem can be settled in a specific 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. Thus a group for which the word problem is undecidable is also a group for which the conjugacy problem is undecidable.

The word problem is decidable for some types of groups: Artin settled it for braid groups in 1926, and it can be settled for finitely generated free groups by writing each word as a "reduced word". But in the 1950s Novikov and Boone independently proved there is a finitely presented group for which the word problem is undecidable.[4] Eventually it was determined that *each* of the four decision problems above for finitely presented groups is

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

[4]In 1947, Markov and Post independently proved the word problem for finitely presented *semigroups* is undecidable. A semigroup is a set with an associative binary operation, like $\mathbf{Z}^+$ under addition. Groups have more structure than semigroups, such as inverses, so the undecidability of the word problem for finitely

undecidable. The solutions use 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 undecidability of the logic problem implies undecidability of the group theory problem. While the original examples of undecidable decision problems (like the halting problem) were not of direct research interest to non-logicians, such problems were used in the construction of the groups that showed the group-theoretic decision problems 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 $|R| = 27$.[5]

presented semigroups does not imply undecidability of the word problem for finitely presented groups even though every group is a semigroup.

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