ILLINOIS JOURNAL OF MATHEMATICS
Volume 30, Number 2, Summer 1986

A SIMPLE PRESENTATION OF A GROUP WITH UNSOLVABLE WORD PROBLEM

BY

DONALD J. COLLINS

In memoriam—William W. Boone

In my experience, many topologists suffer acute anxiety when it occurs to them that some fundamental group they are working with may have unsolvable word problem. One form of therapy I have known to be employed is to say that groups with unsolvable word problems are monstrous, complicated objects and that no-one could ever write one down in his lifetime. The object of this note is to deny even this succour by giving, in a modest amount of space and in complete detail, a group presentation with unsolvable word problem. As will be apparent, such an example exists, implicitly, in the literature and this article simply makes the example explicit.

For the sake of clarity, let us rehearse the basic ideas involved. A *(group) word* on a set X of *generators* is a string

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$$

where $x_i \in X$, $\varepsilon_i = \pm 1$, $1 \leq i \leq n$.

We write uv for the juxtaposition of the words u and v, and $u \equiv v$ to indicate that u and v are identical words. The empty word is denoted by 1. A *relation* over X is a formal equality $r = s$, where r and s are words on X. Two words u and v are *immediately equivalent* under a set R of relations if, for some relation $r = s$ in R, either $u \equiv wrz$, $v \equiv wsz$ or $u \equiv wsz$, $v \equiv wrz$.

A *group presentation* is a pair $G = \langle X | R \rangle$ where R is a set of relations over X that includes the *trivial relations* $xx^{-1} = 1$, $x^{-1}x = 1$ for every $x \in X$. It is easy to see that, with multiplication defined by juxtaposition of representatives, the classes under the equivalence relation generated by immediate equivalence form a group. If

$$u \equiv x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$$

the inverse of the class of u is the class of $u^{-1} \equiv x_n^{-\varepsilon_n} \cdots x_2^{-\varepsilon_2} x_1^{-\varepsilon_1}$.

The *word problem* for $G = \langle X | R \rangle$ is the problem of deciding when two words u and v lie in the same equivalence class—in symbols—when $u =_G v$.

Received March 21, 1985.

Since $u =_G v$ if and only if $uv^{-1} =_G 1$, the word problem can also be posed as deciding whether or not a word is equivalent to 1. The problem is *solvable* if there is an algorithm that always gives the correct answer, and otherwise *unsolvable*.

To see something of where our example comes from, we need to understand the idea of a *semigroup presentation*. By a *semigroup word* on a set X is meant a string

$$x_1 x_2 \cdots x_n$$

where $x_1, x_2, \ldots, x_n \in X$, $1 \le i \le n$.

A semigroup presentation and its word problem are then defined exactly analogously—with the obvious exception that since "inverse symbols" x^{-1} are excluded there are no trivial relations requiring special consideration. The equivalence classes form a semigroup—strictly a monoid since the class of 1 acts as identity.

When the word problem was originally posed by M. Dehn in 1910 [6], the principal aim was to obtain algorithms for important presentations and it was not until the precise formulation of the notion of algorithm in the 1930's that it was possible to establish unsolvability results. As is well known, the first proofs that there exist semigroup presentations with unsolvable word problem were given by A.A. Markov [8] and E.L. Post [12]. While Post makes no attempt to assess how complex a presentation is needed, Markov in [9] does refine his basic argument to show that there is a presentation with only 33 relations, each requiring at most six occurrences of a generator, for which unsolvability occurs.

Remarkably simple semigroup presentations with unsolvable word problem were given by G.S. Céjtin [4] and D.S. Scott [13]. We spell out Céjtin's example (Scott's example is similar):

Generators:

$$a, b, c, d, e;$$

Relations:

$$ac = ca, \qquad ad = da,$$
$$bc = cb, \qquad bd = db,$$
$$ce = eca, \qquad de = edb,$$
$$cca = ccae$$

As the reader may check, the seven relations in total require only 33 occurrences of a generator. It is hard to believe that a significantly simpler example will ever be constructed. An interesting point to note is that both Céjtin and Scott, for technical reasons, rely on the existence of a *group* presentation with unsolvable word problem. The existence of such presentations had been established by W.W. Boone [1, V, VI] and P.S. Novikov [11].

The example of the title is based on another semigroup presentation due to Céjtin, that is a slight variant of that above. We call this presentation C and it is given by:

Generators:

$$a, b, c, d, e;$$

Relations:

$$ac = ca, \qquad ad = da,$$
$$bc = cb, \qquad bd = db,$$
$$ce = eca, \qquad de = edb,$$
$$cdca = cdcae,$$
$$caaa = aaa,$$
$$daaa = aaa,$$

Céjtin proves that the problem of deciding if $w =_C aaa$, for arbitrary w, is unsolvable—in technical language the *individual word problem* for aaa is unsolvable.

The transition from an individual word problem for a semigroup presentation to the word problem for a group presentation is the basis of Boone's construction [1], [2] and the example we give relies on an elegant simplification of Boone's approach by V.V. Borisov [3]. (Novikov [11] on the other hand, uses A.M. Turing's paper [14] on *cancellation* semigroups.)

Applied to Céjtin's presentation C, Borisov's method yields the following presentation B (where as customary the trivial relations are omitted).

Generators:

$$a, b, c, d, e, p, q, r, t, k.$$

Relations:

$$p^{10}a = ap,\ p^{10}b = bp,\ p^{10}c = cp,\ p^{10}d = dp,\ p^{10}e = ep,$$
$$qa = aq^{10},\ qb = bq^{10},\ qc = cq^{10},\ qd = dq^{10},\ qe = eq^{10},$$
$$ra = ar,\ rb = br,\ rc = cr,\ rd = dr,\ re = er,$$
$$pacqr = rpcaq, \qquad p^2adq^2r = rp^2daq^2,$$
$$p^3bcq^3r = rp^3cbq^3, \qquad p^4bdq^4r = rp^4dbq^4,$$
$$p^5ceq^5r = rp^5ecaq^5, \qquad p^6deq^6r = rp^6edbq^6,$$
$$p^7cdcq^7r = p^7cdceq^7,$$
$$p^8caaaq^8r = rp^8aaaq^8,$$
$$p^9daaaq^9r = rp^9aaaq^9,$$
$$pt = tp,\ qt = tq,$$
$$k(aaa)^{-1}t(aaa) = k(aaa)^{-1}t(aaa)$$

(We have cheated a little by using numerical exponents, but they are all small). The presentation B has 27 relations among 10 generators which require 421 occurrences of a generator. Borisov proves that for any semigroup word $w = w(a, b, c, d, e)$

$$(w^{-1}tw)k =_G k(w^{-1}tw) \text{ if and only if } w =_C aaa$$

and the unsolvability of the word problem for B follows from Céjtin's result for C.

The question of how many relations are needed, regardless of their length, to achieve unsolvability has received some attention and we record briefly the state of affairs as known to us at present.

For semigroups the best result is due to Ju.V. Matijasevic [10] who succeeds in obtaining unsolvability with only three defining relations. However, one relation requires several hundred occurrences of generators. This remarkable result has given rise to the pessimistic speculation that the still open word problem for one-relation semigroups will eventually be settled positively and that no-one will ever succeed in determining what happens for two relations.

For group presentations the results are a shade less striking. Borisov's construction can be applied to a form of Matijasevic's example, as can a construction of the author [5], based on [2], to yield unsolvability with 14 defining relations. In both cases a clever trick of Borisov [3] cuts the number of relations down to 12. On the positive side, the word problem is known to be solvable for one-relation presentations (W. Magnus [7]) and it is hard to believe that with only two relations to play with an unsolvable situation could be coded into a group—in this context, groups are less easily manipulated than semigroups. However, the general theory of two relation presentations is largely empty and one fears the worst.

References

1. W.W. Boone, *On certain simple undecidable problems in group theory*, V, VI, Indag. Math., vol. 19 (1957), 22–27, 227–232.
2. ______, *The word problem*, Ann. of Math., vol. 70 (1959), pp. 207–265.
3. V.V. Borisov, *Simple examples of groups with unsolvable word problems*, Math. Notes, vol. 6 (1969), pp. 768–775 (Mat. Zametki, vol. 6 (1969), pp. 521–532, in Russian).
4. G.S. Céjtin, *An associative calculus with an insoluble problem of equivalence*, Trudy Mat. Inst. Steklov, vol. 52 (1957), pp. 172–189, Russian).
5. D.J. Collins, *Word and conjugacy problems in groups with only a few defining relations*, Z. Math. Logik Grundlagen Math., vol. 15 (1969), pp. 303–324.
6. M. Dehn, *Über die Topologie des dreidimensionalen Raumes*, Math. Ann., vol. 69 (1910), pp 137–168.
7. W. Magnus, *Das Identitätsproblem fur Gruppen mit einer definierenden relation*, Math. Ann., vol. 106 (1932), pp. 295-307.
8. A.A. Markov, *The impossibility of certain algorithms in the theory of associative systems I*, Dokl. Akad. Nauk, vol. 55 (1947) pp. 583–586.
9. ______, *The impossibility of certain algorithms in the theory of associative systems II*, Dokl. Akad. Nauk, vol. 58 (1947), pp. 353–356.

10. JU. V. MATIJASEVIC, *Simple examples of undecidable associative calculi*, Soviet Math. Dokl, vol. 8 (1967), pp. 555--557.

11. P.S. NOVIKOV, *On the algorithmic unsolvability of the word problem in group theory*, Trudy Mat. Inst. Steklov, vol. 44 (1955), 143pp.

12. E.L. POST, *Recursive unsolvability of a problem of Thue*, J. Symbolic. Logic, vol. 12 (1947), pp. 1–11.

13. D.S. SCOTT, *A short recursively unsolvable problem*, J. Symbolic Logic, vol. 21 (1956), pp. 111–112.

14. A.M. TURING, *The word problem in semigroups with cancellation*, Ann. of Math. vol. 52 (1950), pp. 491–505.

UNIVERSITY OF LONDON
LONDON