The computation of the Betti numbers of an elliptic
space is a NP-hard problem

Antonio Garvín, Luis Lechuga *

Escuela Universitaria Politécnica, Universidad de Málaga, Departamento de Matemática Aplicada,
Campus de El Ejido, 29071 Málaga, Spain

Received 18 September 2002; received in revised form 15 October 2002

Abstract

Let $S$ a 1-connected space such that $\pi_*(S) \otimes \mathbb{Q}$ and $H^*(S; \mathbb{Q})$ are both finite-dimensional. Then, using the Sullivan model as a codification for $S$, we prove that the computation of the Betti numbers of $S$ is a NP-hard problem.

© 2002 Elsevier Science B.V. All rights reserved.

Keywords: Rational homotopy; Complexity; NP-hard problem

In studying the computational complexity of problems about spaces, a technical point immediately arises. How, exactly, does one describe a space? One possible answer was adopted by Brown [3] and consists of a simplicial decomposition, but this codification is extremely long for any space of even moderate complexity. Fortunately, in the case of a rational homotopy, Quillen’s Lie algebra model and Sullivan algebra model are both ways of providing such a description.

Anick in [2] proved, using the Quillen model for the spaces, that computing the rational homotopy groups of a CW complex having cells (other than the base point) in dimensions two and four only is a NP-hard problem. This result was obtained from the fact that computing the Betti numbers of an 12-algebra is a NP-hard problems. In [6, Theorem 7] is proven that for the class of formal finite complexes the computation of Betti numbers is again a NP-hard problem. In the proof of this result is implicitly shown that computing the Betti numbers of a finite-dimensional 12-algebra is a NP-hard problem. Unfortunately, in general, these 12-algebras cannot be obtained as the cohomology of an elliptic space. Thus,

* Corresponding author.
E-mail address: llechuga@uma.es (L. Lechuga).
in order to prove that computing the Betti number of an elliptic space is a NP-hard problem, is necessary to obtain a class of algebras that can be obtained as the cohomology of elliptic spaces and such that the computation of their Betti numbers be a NP-hard problem.

Our paper differs from Anick’s paper in two points. First, we assume that the space is elliptic and second, we encode the space via its Sullivan model while Anick’s codification is done via the Quillen model.

In principle, Anick’s results are not applicable to elliptic spaces. That is, even if is NP-hard to compute those results, it could happen that for the class of elliptic spaces the problem is not NP-hard. On the other hand, we recall that the generators of the Sullivan models corresponds to the rank of the rational homotopy groups and so when we use the Sullivan model, the rational homotopy of the space is known. When the space is encoded via its Quillen model is not the rational homotopy but the homology what is known, because the Quillen model of $S$ is a free differential graded Lie algebra whose generators correspond with, but lie in one degree lower than, a basis of $\overline{H}^*(S; \mathbb{Q})$.

We recall some definitions [5,1] in complexity theory. See [4] for standard definitions in rational homotopy. All spaces considered are 1-connected of finite type and the ground field is $\mathbb{Q}$.

Formally, a problem $\Pi = \{I_\alpha\}_{\alpha \in \Gamma} \subset \mathbb{N}$ is just a family of instances $I_\alpha$, each $I_\alpha$ can be encoded as a nonnegative integer. Thus, we see a problem, together with its solution, as a function $f : \Pi \subset \mathbb{N} \rightarrow \mathbb{N}$. If $I \in \Pi$, $f(I)$ is the answer to the instance $I$. A decision problem is a problem $f$ with just two possible values, usually $\{0, 1\}$ (Yes or No). The language of a decision problem is the set of instances $I$ for which the answer is yes, i.e., $f(I) = 1$.

A decision problem $f : \Pi \rightarrow \mathbb{N}$ (or simply $\Pi$ for convenience) belongs to the class P (polynomial) if there is an algorithm that solves the problem in polynomial time, i.e., there is a polynomial $p$ such that for each instance $I \in \Pi$ of length $n$, the algorithm produces $f(I)$ in a number of steps bounded by $p(n)$. The class NP consists of all those decision problems whose positive solutions can be verified in polynomial time once a solution is given. The question about $P = NP$ is one of the biggest open problems in complexity theory. A decision problem $A$ is NP-complete if it is in NP and if every other problem in NP is reducible to it. By reducible we mean that for every NP problem $B$, there is a polynomial time algorithm which transforms instances of $B$ into instances of $A$, such that the two instances have the same truth values. As a consequence, if we had a polynomial time algorithm for $A$, we could solve all NP problems in polynomial time. A problem $\Pi$ is NP-hard if every problem in NP can be reduced to it in polynomial time (although it is not required $\Pi \in NP$). In order to prove that a problem is NP-hard it suffices to reduce a known NP-complete problem to it. Note that if some problem $A$ is a particular case of problem $B$ and problem $A$ is NP-hard then problem $B$ is NP-hard if we assume that both problem are encoded in such a way that the inclusion transformation is a polynomial reduction.

We will show how to reduce in polynomial time the subset sum problem, that is a NP-complete problem, into the problem of computing the Betti numbers of a certain elliptic minimal model. This proves that computing the Betti numbers of an elliptic Sullivan model is NP-hard.

The subset sum problem is an important problem in complexity theory and cryptography. The problem is this: Given a set of positive integers $T \subset \mathbb{N}$ and an integer $N$, is there
some subset $K \subset T$ such that $\sum_{p \in K} p = N$? The subset sum problem is NP-complete [5] and is perhaps the simplest such problem to describe.

We need to fix a codification of an elliptic space in order to prove results about reduction and complexity. Let $S$ an elliptic space an $(AZ, d)$ its Sullivan model. Choose $\{z_1, \ldots, z_m\}$ a homogeneous basis of $Z$. Then the codification string of $S$ consist of $m$, the degree of each $z_j$, and for each $z_j$ with $dz_j = \sum_p \lambda_{i_1, \ldots, i_p} z_{i_1} \cdots z_{i_p}$ where each $\lambda_{i_1, \ldots, i_p} \neq 0$ a list of elements $\{\lambda_{i_1, \ldots, i_p}, i_1, \ldots, i_p\}$. The codification for the subset sum problem with input $T$ and $N$ is simply a list of positive integers corresponding to the elements in $T$ and to the integer $N$.

**Theorem 1.** The computation of the Betti numbers of an elliptic space is a NP-hard problem.

**Proof.** Let $B$ be the subset sum problem and let $A$ be the following decision problem: Given as input an elliptic Sullivan model $(AZ, d)$ and a positive integer $N$, is the $N$th Betti number of $(AZ, d)$ positive?

We will show that problem $A$ is NP-hard via a polynomial reduction of problem $B$ to problem $A$, clearly this proves the theorem. Given an instance of problem $B$ with input $T$ and $N$, write $T = \{n_1, \ldots, n_q\}$ with $|n_i|$ odd for $i = 1, \ldots, p$ and $|n_i|$ even for $i = p + 1, \ldots, q$. We associate to $T$ the Sullivan model $(AZ_T, d)$ such that $Z_T = \langle x_1, \ldots, x_p, y_{p+1}, \ldots, y_q \rangle$ with the differential $d$ given by $dx_i = 0, i = 1, \ldots, q$ and $dy_i = x_i^2, i = p + 1, \ldots, q$. Clearly, with the given codifications, the transformation of the instance of problem $B$ corresponding to the input $(T, N)$ into the instance of problem $A$ corresponding to input $((AZ_T, d), N)$ is done in polynomial time.

Now $(AZ_T, d)$ is clearly elliptic and has cohomology

$$H(AZ_T, d) = (A^{p+1}_{i=1} (x_i)) \otimes (A^{q}_{i=p+1} H(\langle x_i, y_i \rangle, d)).$$

Observe that the $N$th Betti number of $(AZ, d)$ coincides with the number of solutions of $\sum_{p \in T} p_i = N$ and so the subset sum problem with input $T$ and $N$ has a solution iff the $N$th Betti number of $(AZ_T, d)$ is positive. Hence this establishes a polynomial time reduction of problem $B$ to problem $A$ and this shows that problem $A$ is NP-hard. $\square$

In [6, Theorem 7] is proven that computing the LS-category $\text{cat}_0(S)$ and the cup length $n_0(S)$ of the rational cohomology algebra of formal finite complexes are both NP-hard problems. These results cannot be applied to elliptic models. An interesting open problem is: Given an elliptic Sullivan model $(AZ, d)$, what is the computational complexity of computing $\text{cat}_0(AZ, d)$ and $n_0(AZ, d)$?

**References**
