

CONTROLLABILITY IS HARDER TO DECIDE THAN ACCESSIBILITY

Eduardo D. Sontag*
Department of Mathematics
Rutgers University
New Brunswick, NJ 08903
(201)932-3072 – *sontag@fermat.rutgers.edu*

ABSTRACT

The present article compares the difficulties of deciding controllability and accessibility. These are standard properties of control systems, but complete algebraic characterizations of controllability have proved elusive. We show in particular that for subsystems of bilinear systems, accessibility can be decided in polynomial time, but controllability is NP-hard.

§1. Introduction.

One of the most important and basic outstanding problems in control theory is that of finding necessary and sufficient conditions for deciding when a continuous-time analytic nonlinear system is (locally or globally) controllable. The goal is to provide some sort of generalization of the classical Kalman controllability rank condition. An early success of this line of research was achieved with the characterization of the *accessibility property*: there is a Lie-algebraic rank condition for deciding if it is possible to reach an open set from a given initial state. When this accessibility rank condition does not hold, all trajectories must remain in a lower-dimensional submanifold of the state space. See for instance [HK], [Su1], or [I] for a discussion of this and related results. It is known that local controllability can also be *in principle* checked in terms of linear relations between Lie brackets of the vector fields defining the system ([Su1]), and recent research has succeeded in isolating a number of necessary as well as a number of sufficient explicit conditions for controllability. The literature regarding this question is very large; see for instance [Su2] and the references there. No complete characterization is yet available, however.

The purpose of this note is to point out that, whatever necessary and sufficient conditions are eventually found, these are likely to be rather hard to check. One way to quantify this difficulty is in terms of complexity of computation. There has been previous work dealing with difficulty of computation in the context of control and system theory. For instance, [So1] showed the undecidability of the realization problem, and more

* Research supported in part by US Air Force Grant 0247. Original manuscript for paper appeared in *SIAM J. Control and Opt.*, **26** (1988): 1106-1118

recently [PT] (and references there) dealt with the study of complexity of decentralized control problems, while [So2] characterized the complexity of decision problems for an algebra used to study piecewise linear control systems. More in the spirit of this paper, see [BW].

We shall show that the existence of easy to verify conditions for controllability –local or global, and even several “small time” variants,– would imply solutions to problems known to be hard. The relative difficulty of controllability vis a vis the already understood accessibility problem is clarified in the case of the class of systems that can appear as subsystems of bilinear ones. This is a large class of nonlinear systems, including for instance all minimal realizations of finite Volterra series, as well as of course all linear systems. In the context of this class, one can make the precise statement that the accessibility question can be decided in polynomial time, while controllability is (at least) NP-hard. Recall that NP-hard problems are widely believed to be intractable, and one of the main open problems in theoretical computer science is that of establishing rigorously this intractability, the famous “ $P \neq NP$ ” question ([GJ], [PS]). It could be argued that by proving that controllability is NP-hard, we are not in fact establishing precisely that this is harder than accessibility, only that this is true provided that the above open question in computer science is resolved. This is however the standard way in which one “proves” that a problem is hard in combinatorics, operations research, theoretical computer science, or, in a control-theoretic framework, [PT]. In any case, we conjecture that, even for the class of bilinear subsystems, it must be possible to establish exponential time lower bounds, as done in the area of decision methods for logical theories and certain problems in language theory (see e.g. [AHU], chapter 11). We have not yet been able to prove this stronger fact, however.

§2. A few preliminaries.

The systems we shall deal with have equations

$$\dot{x}(t) = f(x(t), u(t)) ,$$

where the state $x(t)$ is in a differentiable manifold M for each t , and the control values $u(t) = (u_1(t), \dots, u_m(t))$ belong to an Euclidean space \mathbb{R}^m at each time t . We assume that the dynamics f are real-analytic. Generalizations to more arbitrary control value sets and to nonanalytic systems could be made, but since our purpose is mainly to provide negative results, we shall make these results stronger by restricting to even simpler kinds of systems below.

Given any fixed state $x_0 \in \mathbb{R}^n$, we can pose several types of problems relative to x_0 : reachability *from* x_0 , controllability *to* x_0 , controllability in any fixed time T . One may also consider the property of complete controllability, being able to find controls that transfer any desired state to any other state. We use the notation

$$A^T(x)$$

for the set of states that can be reached from x in time exactly T ; when T is negative, we mean states that from which x can be reached in time $-T$. We may take any reasonable family of controls: all measurable locally essentially bounded controls, piecewise continuous controls, or even piecewise constant controls; the results will be the same. The union of all the sets $A^T(x)$, over all nonnegative T , is denoted

$$A^+(x) ;$$

this is the set of states reachable from x . Similarly,

$$A^-(x)$$

is the union over $T \leq 0$, the set of states controllable to x . With these notations, for instance, controllability from x_0 means that $A^+(x_0) = M$, controllability to x_0 means that $A^-(x_0) = M$, and local reachability in small time means that for each $T > 0$, x_0 is in the interior of the union of the sets $A^\varepsilon(x_0), 0 \leq \varepsilon \leq T$.

Two issues which must be clarified are the meanings of the words “given” (a system, and possibly also an initial state x_0) and “decide” (if the system is controllable from x_0 , reachable, etc.) . In its weakest sense, *given* could be taken to mean “given a recursive description” of the system, that is, one should provide a *computable* real function f , as well as a *computable* vector x_0 if a fixed initial state is of interest. (See [A] for a discussion of computable analysis, as well as [K] for an alternative viewpoint.) *Decide* should mean *provide a computer algorithm* which, when presented as an input with the description of f (and x_0), will answer “yes” or “no” after a finite number of steps. At this level, controllability is undecidable for trivial reasons, even for linear systems. For example, the one-dimensional system

$$\dot{x} = bx$$

is controllable if and only if b is nonzero. But it is impossible to decide if a “given” real number is zero or not: see [A], theorem 6.1. We obviously want to avoid such logical traps, which have to do with the fact that a recursive description of the dynamics is not necessarily in what one would intuitively call “explicit form”. For linear systems, the simplest way to get around this difficulty is to restrict to systems with rational coefficients, explicitly given in some notation, for instance in binary. More generally, one could look for instance at a class like that of systems with polynomial or rational functions f , again requiring rational coefficients.

In order to avoid such trivial counterexamples, and to give a stronger negative result, we shall restrict to bilinear subsystems. These are systems with a finite dimensional Lie algebra, specified as follows. Given are integers N , m , and l , and $m + 2$ matrices

$$A, G_1, \dots, G_m, B$$

over the rational numbers. Each of A, G_1, \dots, G_m is square of size $N \times N$, and B is of size $N \times m$. Also given is a set of l polynomials with rational coefficients

$$\phi_i(x_1, \dots, x_N), i = 1, \dots, l$$

with $\phi_i(0) = 0$ and such that the Jacobian of $(\phi_1, \dots, \phi_l)'$ (prime indicates transpose) has constant rank, say equal to $N - n$. Further, we assume that the n -dimensional manifold M where all the ϕ_i simultaneously vanish is invariant for the differential equation

$$\dot{x} = (A + \sum_{i=1}^m u_i G_i)x + Bu, \quad (2.1)$$

no matter what the control $u(\cdot)$ is. The latter can be expressed algebraically by the requirement that the Lie derivatives

$$L_X \phi_i \quad (2.2)$$

vanish identically on M , for each vector field X of the type $(A + \sum \alpha_i G_i)x + B\alpha$, $\alpha \in \mathbb{R}^m$. Then, to the data

$$(A, G_1, \dots, G_m, B, \phi_1, \dots, \phi_l) \quad (2.3)$$

we associate the system Σ whose state space is

$$M = \{x \mid \forall i, \phi_i(x) = 0\}$$

and whose dynamics are given by the restriction of (2.1). We shall call a system of this type a *bilinear subsystem*.

The above definition is meant to capture the idea of a system whose dynamics can be embedded algebraically into a bilinear system. This is a rich enough class of systems for the purposes of this note, and in fact includes many subclasses of interest. For instance, *bilinear* systems result when one takes all the $\phi_i \equiv 0$ (so $n = N$, $M = \mathbb{R}^N$), and in particular *linear* systems result when also all the G_i are zero. Further, minimal realizations of finite Volterra series are always of this type ([Cr]).

In order to express difficulty of computation, we associate to each Σ as in (2.3) a *size*. This is the total number of bits needed in order to store the data (2.3). We assume a fixed data structure for the matrices, say that they are listed by row, and that each entry is listed as a quotient of integers by giving sign, and the numerator and denominator in binary. Similarly, each of the polynomials ϕ_i may be given by specifying (again in binary) all coefficients in a fixed order. We denote by

$$\text{size } \Sigma$$

the resulting integer. When we say that a certain property can be *decided in polynomial time* for such systems, we mean that there is a (fixed) polynomial P and an algorithm which, when given the data (2.3), will answer correctly in time at most

$$P(\text{size } \Sigma)$$

whether this property holds or not. The precise definition of “algorithm” is not very critical in this context; for instance multitape Turing machines as in [AHU], or several types of

abstract computer models. For this and other related notions, we refer the reader to the standard literature in complexity theory, which we shall not repeat here.

Remark 2.1. A somewhat subtle point: note that when presented with a bilinear subsystem we assume that it is true that the Jacobians have constant rank and that the derivatives (2.2) vanish on M , and we shall only be interested in answering questions related to controllability. Checking the consistency of the data, for instance via Tarski-Seidenberg theory, could require a large computational effort, and we do not wish to make the problem even harder due to such reasons; we want to show that controllability is hard to check even if the data is reliable. ■

§3. Accessibility.

As an illustration of the terminology, we now restate in complexity terms the simplicity of the controllability problem for linear systems. Consider the property

The linear system (A, B) is controllable.

The classical condition is that the rank of the $n \times nm$ Kalman block matrix

$$(B, AB, A^2B, \dots, A^{n-1}B) \tag{3.1}$$

must equal the dimension n of the state space. Without loss of generality, we may assume that A and B are integer matrices; if they are not, we can multiply by a common denominator, which increases the total size of the data at most polynomially and doesn't affect controllability. Whether the rank of the Kalman matrix is n can be checked by Gaussian elimination, which (see e.g. [PS], proof of theorem 8.2,) requires a number of algebraic operations which is polynomial in n , m , and in the size of the integers appearing in the composite matrix (3.1). The size of these integers is in turn polynomial in the size of the original data; more generally the size in binary of each entry of a product matrix

$$A = A_1 \dots A_k$$

is bounded by a polynomial in k and in the size of the integer matrices A_i .

The analogue of the above for nonlinear systems will be obtained, as may be expected, for the accessibility problem. It turns out indeed that accessibility can be also decided in polynomial time for the class of bilinear subsystems, as we shall prove next.

In general, a system Σ is said to be *accessible from* the state x_0 if and only if the reachable set from x_0 has full dimension, that is if

$$\text{int } A^+(x_0) \neq \emptyset. \tag{3.2}$$

For bilinear subsystems (2.3), we shall take $x_0 := 0$ and just say that Σ is *accessible*. Note that the state space is M , so in (3.2) one means of course the interior with respect to M . When Σ is in particular linear, accessibility is equivalent to controllability, but these concepts are in general different.

Assume now given a bilinear subsystem Σ . Consider the $m + 1$ affine vector fields

$$X_0(x) := Ax$$

and

$$X_i(x) := G_i x + b_i$$

for each $i = 1, \dots, m$, where b_i denotes the i -th column of B . The set \mathcal{A} of all affine vector fields on \mathbb{R}^N is a Lie algebra of dimension

$$k := N^2 + N ,$$

with multiplication

$$[Ax + b, Cx + d] := (CA - AC)x + (Cb - Ad) .$$

Let $\mathcal{L}_i, i \geq 1$, be the sequence of linear subspaces of \mathcal{A} defined as follows:

$$\mathcal{L}_1 := \text{span} \{X_0, X_1, \dots, X_m\}$$

and inductively,

$$\mathcal{L}_{i+1} := \mathcal{L}_i + \text{span} \{[X_i, X] \mid i = 0, \dots, m, X \in \mathcal{L}_i\} .$$

Let \mathcal{L} be the union of all the \mathcal{L}_i . It follows from the definition that if $\mathcal{L}_i = \mathcal{L}_{i+1}$ for some integer i then also $\mathcal{L}_i = \mathcal{L}$. By dimensionality we then conclude that

$$\mathcal{L}_k := \mathcal{L} .$$

For any subspace $L \subseteq \mathcal{A}$, denote

$$L(0) := \{b \mid Ax + b \in L \text{ for some } A\} .$$

This is the tangent space at the state $x_0 = 0$, corresponding to the distribution L . With these notations, we can state the by now classical characterization of accessibility (see e.g. [I], theorem 6.15.):

Proposition 3.1. The system Σ is accessible if and only if $\mathcal{L}_k(0)$ has dimension n . ■

Note that the rank at the origin of the Jacobian matrix of (ϕ_1, \dots, ϕ_l) is $N - n$; this Jacobian can be computed in polynomial time, and its rank can be obtained again by Gaussian elimination. Thus n can be computed in this form, and it is only necessary to

find the dimension of $\mathcal{L}_k(0)$. We now show how to compute a basis of \mathcal{L}_k in polynomial time.

First of all, the problem is not changed by multiplying all the matrices in the description of Σ by the product of all the denominators of all the entries. This increases the size of Σ at most polynomially, so we assume from now on that A, G_1, \dots, G_m, B are matrices of integers.

We shall represent elements $X = Ax + b$ of \mathcal{A} as vectors of size k , listing first the entries of A in some fixed order and then those of b . For any such element, we let $\mu(X)$ denote the maximum of the absolute values of its entries. Also, we take $\bar{\mu}$ to be the largest of the values of the $\mu(X_i)$, $i = 0, \dots, m$, for the generators of \mathcal{L}_1 . Directly from the definition of matrix product, one obtains the formula

$$\mu([X, Y]) \leq 2N\mu(X)\mu(Y)$$

for any $X, Y \in \mathcal{A}$.

Next we show how to build in polynomial time, for each $i = 1, \dots, k$ a basis

$$\{Y_1, \dots, Y_{n_i}\}$$

(note that $n_i \leq k$) of \mathcal{L}_i such that

$$\mu(Y_j) \leq (2N\bar{\mu})^i$$

for each $j = 1, \dots, n_i$. The case $i = 1$ is clear by definition: start with the X_i and use Gaussian elimination to take a subset which forms a basis. By induction, it is necessary to consider now all Lie products

$$[X_j, Y_l] \tag{3.3}$$

for $j = 0, \dots, m$ and $l = 1, \dots, n_i$. There are at most k^2 of these. Each of them has entries of largest magnitude

$$\mu([X_j, Y_l]) \leq 2N\mu(X_j)(2N\bar{\mu})^i \leq (2N\bar{\mu})^{i+1}.$$

Let B be the matrix that lists all these generators (3.3). Each entry of B , expressed in binary, has length at most equal to

$$(i + 1)\log_2(2N\bar{\mu}),$$

(plus a bit for the sign). Since we may assume that $i + 1 \leq k = N^2 + N$, this quantity is bounded by a polynomial

$$a + bN^3 + cN^2 \log \bar{\mu},$$

which is in turn bounded by an expression of order $O(M^3)$, where M is the total size of the original data (A, G_1, \dots, G_m, B) . Thus Gaussian elimination can be performed in

polynomial time to select a subset of (3.3) which forms a basis. Note that it is essential that this elimination be performed at each step to the algorithm: otherwise we end up with an exponential number $-(m+1)^k$ of generators for the space \mathcal{L} . After at most k steps we have a basis for $\mathcal{L}_k = \mathcal{L}$, and hence also by evaluation at 0 and one last elimination step, we can determine the dimension of $\mathcal{L}(0)$. This establishes the following fact.

Theorem 1. For bilinear subsystems, the accessibility property can be decided in polynomial time. ■

Remark 3.2. We made the convention that $x_0 = 0$ only for notational simplicity. It is equivalent to studying accessibility (and later controllability) from an *equilibrium* state. The results in the case of more general x_0 are entirely analogous, with accessibility as well as *strong* (fixed-time) accessibility both verifiable in polynomial time. ■

Remark 3.3. Another property that is sometimes of interest is that of *span reachability*, meaning that the linear span of the states reachable from the origin should be the entire space. This can also be checked in polynomial time, by an argument as above. In fact, the accessibility property is basically the same as a span-reachability property at the Lie algebra level.

§4. A controllability remark.

In this section we shall restrict our attention to systems of the very special type

$$\begin{aligned} \dot{y} &= w^2 f(z) \\ \dot{z} &= Az + bu_1 \\ \dot{w} &= u_2 . \end{aligned} \tag{4.1}$$

These are systems with state space

$$M = \mathbb{R} \times \mathbb{R}^k \times \mathbb{R}$$

of dimension $k+2$, and states partitioned as $x = (y, z, w)^\dagger$, with the block of variables z evolving as a linear system of dimension k . The control value set is \mathbb{R}^2 , and we assume that the single-input system (A, b) is controllable. We shall show that for systems (4.1), various variants of the notion of controllability are all equivalent to the indefiniteness of the mapping $f : \mathbb{R}^k \rightarrow \mathbb{R}$:

Definition 4.1. The mapping f is *definite* iff $f(z) \geq 0$ for all z or $f(z) \leq 0$ for all z . Otherwise, it is *indefinite*. ■

This allows us to reduce the problem of deciding if a polynomial is definite to a controllability question, and we conclude that controllability is at least as hard to decide as

† For simplicity, we write (y, z, w) instead of, more accurately, $(y, z', w)'$.

definiteness. Further, systems of the special form (4.1) with f polynomial can be rewritten as bilinear subsystems, and this rewriting can be done in polynomial time, relative to any class of polynomials f of fixed degree. Together with the NP-hardness of the the problem of deciding definiteness (next section), the desired negative result will follow.

It is clear that indefiniteness is necessary for any type of controllability: if f where definite, say $f(z) \geq 0$ for all z , then

$$y \geq y_0$$

whenever $x = (y, z, w) \in A^+(x_0)$, for each $x_0 = (y_0, z_0, w_0) \in M$. Thus it is impossible in that case for any x_0 to be in the interior of $A^+(x_0)$ or of $A^-(x_0)$.

Assume then that f is indefinite. We show now that, for each $\delta > 0$, and for each two states x_0 and \bar{x} , there is a control $u(\cdot)$ which steers x_0 into \bar{x} in time 4δ . We build u in 5 steps.

Step 1. Apply the control $u_1 \equiv 0, u_2(t) \equiv -w_0/\delta$ on the interval $[0, \delta]$. There results a state of the form $x_1 = (y_1, z_1, 0)$.

Consider now the number

$$y^* := \bar{y} - \left(\frac{\bar{w}}{\delta}\right)^2 \int_0^\delta s^2 f(e^{(s-\delta)A}\bar{z}) ds .$$

Either (a) $y_1 = y^*$ or (b) $y_1 \neq y^*$. Assume first that (b) holds. We know by indefiniteness of f that there exists some vector z_2 such that

$$\text{sign } f(z_2) = \text{sign}(y^* - y_1) .$$

Pick any such z_2 . By continuity of the exponential, there is some $0 < \varepsilon < \delta$ such that

$$\text{sign } f(e^{sA}z_2) = \text{sign}(y^* - y_1) \text{ for all } s \in [0, \varepsilon] . \quad (4.2)$$

Finally, pick any solution α of the equation

$$\alpha^2 \left[\int_0^{\varepsilon/2} s^2 f(e^{sA}z_2) ds + \int_{\varepsilon/2}^\varepsilon (\varepsilon - s)^2 f(e^{sA}z_2) ds \right] = y^* - y_1 .$$

There is some such α because of (4.2). In case (a), make an arbitrary choice, say $z_2 = z_1$, let $0 < \varepsilon < \delta$ be also arbitrary, and let $\alpha := 0$.

Step 2. Apply a control with $u_2 \equiv 0$, on the interval $[0, \delta - \varepsilon]$, that takes x_1 into the state $x_2 = (y_1, z_2, 0)$. A suitable $u_1(\cdot)$ exists because of the assumed controllability of the pair (A, b) .

Step 3. Apply a control on the interval $[0, \varepsilon]$ as follows. The u_1 component is identically zero, and

$$u_2(t) := \begin{cases} \alpha, & \text{if } t < \varepsilon/2, \\ -\alpha, & \text{if } t \geq \varepsilon/2. \end{cases}$$

There results the state $x_3 = (y^*, e^{\varepsilon A} z_2, 0)$; the total time elapsed is 2δ .

Step 4. On the interval $[0, \delta]$, let $u_2 \equiv 0$ and let $u_1(\cdot)$ be a control steering $e^{\varepsilon A} z_2$ into $e^{-\delta A} \bar{z}$. Again such a control exists by the controllability of the linear system (A, b) . The resulting state is $x_4 = (y^*, e^{-\delta A} \bar{z}, 0)$.

Step 5. Finally, in one last interval of length δ , use $u_1 \equiv 0$ and $u_2 \equiv \bar{w}/\delta$. There results the desired state \bar{x} . ■

We can summarize the above discussion:

Proposition 4.2. Let Σ be a system as in (4.1), and pick any fixed $x_0 \in M$. The following properties are then equivalent:

- (i) $A(x) = M$ for each $x \in M$. (Complete controllability.)
- (ii) $A^T(x) = M$ for each T and each $x \in M$.
- (iii) $x_0 \in \text{int } A^+(x_0)$.
- (iv) $x_0 \in \text{int } A^-(x_0)$.
- (v) f is indefinite. ■

It follows that other intermediate properties are also equivalent to the above, for instance *local small-time reachability from x_0* :

$$x_0 \in \text{int } \bigcup_{t=0}^{\varepsilon} A^t(x_0) \text{ for each } \varepsilon > 0,$$

as well as local controllability to x_0 in small time. Thus checking either of these properties is equivalent to checking indefiniteness of f .

For accessibility, only that f not be identically zero is sufficient, which illustrates in this particular case the gap between the two concepts. Note that even for the very simple case in which f is a homogeneous quadratic form, already checking definiteness requires some computational effort.

§5. Deciding definiteness.

The previous section showed how, at least for some systems, controllability is no easier to check than definiteness of a map. This latter property can be checked for polynomials via decision methods for real closed fields (see e.g. [Co]) in doubly-exponential time, but it is not clear if there are faster algorithms. We remark here that the problem is NP-hard, and we do this by polynomial time reduction of the classical NP-complete problem, 3-SAT, to the definiteness question. Thus deciding definiteness is at least as hard as any problem in NP. The remark is not at all surprising, but it is the best lower bound that we have been able to obtain until now.

Recall the definition of the 3-SAT problem ([GJ], p.48). A *clause* $c(x, y, z)$ in the three (distinct) variables x, y, z is an expression of the type

$$\phi_1(x) \vee \phi_2(y) \vee \phi_3(z), \quad (5.1)$$

where each “literal” ϕ_i is of the form

$$\phi_i(a) = a$$

or

$$\phi_i(a) = 1 - a$$

and the binary variables x, y, z can take values in $\{0, 1\}$. We interpret the values 1 and 0 as “true” and “false” respectively. For any assignment (x^*, y^*, z^*) of values $\{0, 1\}$ to x, y, z , we say that $c(x^*, y^*, z^*)$ is *true* if at least one of $\phi_1(x^*)$, $\phi_2(y^*)$ or $\phi_3(z^*)$ is 1, and *false* otherwise. Equivalently, $c(x^*, y^*, z^*)$ is true if and only if the real polynomial

$$\tilde{c}(x, y, z) := \phi_1(x)^2 + \phi_2(y)^2 + \phi_3(z)^2$$

does not vanish at (x^*, y^*, z^*) . A set

$$\mathcal{S} = \{c_i(t_{i,1}, t_{i,2}, t_{i,3}), i = 1, \dots, L\}$$

of L clauses in the variables (t_1, \dots, t_n) , with each $t_{i,j} \in \{t_1, \dots, t_n\}$, is *satisfiable* iff there is some binary assignment $t^* = (t_1^*, \dots, t_n^*)$ to the variables (t_1, \dots, t_n) such that the clauses $c_i(t^*)$ become all simultaneously true. The 3-SAT problem is that of finding an algorithm for checking satisfiability. It was the first problem to be shown to be NP-complete, in the sense that if there were such an algorithm which runs in time polynomial in L then every other problem in the wide class NP, which includes many, if not most, combinatorial problems of interest, would also be decidable in polynomial time. It is a long-standing conjecture (“P \neq NP”) in theoretical computer science, widely believed to be true, that indeed none of these problems can be solved in polynomial time.

It is easy to reduce 3-SAT to the problem of deciding if a polynomial has any real zeroes, and hence to establish that the latter problem is NP-hard. We first show how to

do that, and then modify the construction to deal with the definiteness problem instead. Let \mathcal{S} be as above. Consider first the polynomial

$$\theta(t) = \theta(t_1, \dots, t_n) = \sum_{i=1}^n t_i^2 (1 - t_i)^2 . \quad (5.2)$$

Denote by B_n the set of binary n -vectors, $\{t = (t_1, \dots, t_n) \mid \forall i, t_i \in \{0, 1\}\}$, and note that B_n is the set of zeroes of θ . Now let $u = (u_1, \dots, u_n)$ be L new variables, and introduce

$$\psi(t, u) := \sum_{i=1}^L (u_i \tilde{c}_i(t) - 1)^2 + \theta(t) . \quad (5.3)$$

If $\psi(t^*, u^*) = 0$ then the last term in the sum vanishes, so t^* is binary, while the vanishing of the other terms implies that $\tilde{c}_i(t^*) \neq 0$ for all i . Conversely, if $t^* \in B_n$ is such that all $\tilde{c}_i(t^*) \neq 0$, there is some vector u^* such that $\psi(t^*, u^*) = 0$. We conclude that \mathcal{S} is satisfiable iff ψ has a real zero.

We next modify ψ in order to reduce to definiteness instead. Now let

$$\psi(t, u) := \sum_{i=1}^L (2u_i \tilde{c}_i(t) - u_i^2 - 1)^2 + \theta(t) . \quad (5.4)$$

It is again true that \mathcal{S} is satisfiable if ψ has a real zero. This is because an expression of the type $2u\tilde{c} - u^2 - 1$ is strictly negative unless $\tilde{c} \neq 0$. Conversely, assume that \mathcal{S} is satisfiable, and let $t^* \in B_n$ be such that all $\tilde{c}_i(t^*) \neq 0$. Consider each $2u\tilde{c}_i(t^*) - u^2 - 1 = 0$ as an equation on $u \in \mathbb{R}$. Writing this as

$$\tilde{c}_i(t^*) = \frac{u^2 + 1}{2u}$$

and using the fact that, since $t^* \in B_n$ and $\tilde{c}_i(t^*) \neq 0$, $\tilde{c}_i(t^*) \in \{1, 2, 3\}$, and that

$$\alpha : (0, \infty) \rightarrow [1, \infty) : u \mapsto \frac{u^2 + 1}{2u}$$

is onto, we conclude that (5.4) has a zero.

We show below that when \mathcal{S} is not satisfiable not only is ψ always positive but in fact it is bounded away from zero. Note that in general it is false that a positive polynomial must be bounded below by a positive constant, as evidenced by the example $x^2 + (1 - xy)^2$, so some care is required. Moreover, we need an explicit value for this lower bound, which in our case will turn out to be $1/4n^2$.

Assume then that \mathcal{S} is not satisfiable. Pick any element $t^* \in B_n$. There is some clause $c_i(t^*)$ which is false. Relabelling variables if necessary, we may assume that c_i involves the polynomials $\phi_1(t_1), \phi_2(t_2), \phi_3(t_3)$. Since these all vanish at t^* , we conclude that

$$\phi_j(t)^2 = (t_j^* - t)^2$$

for $j = 1, 2, 3$. In particular, using Euclidean norm, it holds that

$$\|t^* - t\|^2 > \tilde{c}_i(t) \tag{5.5}$$

for each $t \in \mathbb{R}^n$. Now consider any fixed element $(t, u) \in \mathbb{R}^{n+L}$. Either (1) $\|t^* - t\|^2 \leq 1/2$ for some $t^* \in B_n$, or (2) the distance from t to B_n is at least $1/\sqrt{2}$. If there is any t^* as in (1), pick a clause c_i as above. Then, for this fixed i , using (5.5),

$$\left| \left(\frac{2u_i}{u_i^2 + 1} \right) \tilde{c}_i(t) \right| \leq \tilde{c}_i(t) \leq 1/2,$$

so

$$\left| 2u_i \tilde{c}_i(t) - u_i^2 - 1 \right| = (u_i^2 + 1) \left| \left(\frac{2u_i}{u_i^2 + 1} \right) \tilde{c}_i(t) - 1 \right| \geq (u_i^2 + 1)/2 \geq 1/2.$$

Hence, $\psi(t, u) \geq 1/4 \geq 1/4n^2$. Suppose that (2) holds instead. Then necessarily

$$t_j^2(1 - t_j^2) \geq \frac{1}{4n^2}$$

for at least one j , and therefore again $\psi(t, u) \geq 1/4n^2$. Indeed, if this were not the case, then it would hold for each $j = 1, \dots, n$ that either

$$|t_j| < \frac{1}{\sqrt{2n}} \quad \text{or} \quad |t_j - 1| < \frac{1}{\sqrt{2n}}. \tag{5.6}$$

Choose $t^* \in B_n$ with $t_j^* = 0$ if the first case in (5.6) holds, and 1 otherwise. Then this particular t^* would satisfy that $\|t^* - t\|^2 \leq 1/2$, contradicting case (2).

The conclusion from the above discussion is that \mathcal{S} is satisfiable if and only if there is some pair (t, u) such that

$$f(t, u) := 4n^2\psi(t, u) - 1 < 0$$

On the other hand, since f certainly admits positive values, for instance

$$f((2, 2, \dots, 2), u) \geq 16n^3 - 1$$

for any u , it follows that f is indefinite iff it takes any negative values, that is, iff \mathcal{S} is satisfiable. The construction, including expanding f into a standard polynomial form, can be done in polynomial time, and we summarize:

Lemma 5.1. For each set \mathcal{S} of L clauses in n variables, there is a polynomial f of degree 6 in $n + L$ variables, whose coefficients have magnitude $\leq cLn^2$, such that \mathcal{S} is satisfiable iff f is indefinite. The polynomial f can be obtained in polynomial time from \mathcal{S} , and c is a constant independent of \mathcal{S} . ■

§6. A reduction to bilinear subsystems.

The idea behind the construction to be given in this section is basically a classical one in the field of bilinear systems, and can be traced at least as far back as the paper [B]. The point of giving the details is to keep track of the computational effort required and of the size of the numbers appearing.

Lemma 6.1. Let Σ be a system of the form

$$\dot{\xi}_0 = \Psi(\xi), \quad \dot{\xi} = P\xi + Qu, \quad (6.1)$$

where Ψ is a polynomial of degree d in the r variables $\xi = (\xi_1, \xi_2, \dots, \xi_r)$ with integer coefficients and with $\Psi(0) = 0$, P is an integer matrix of dimensions $r \times r$, and Q is an integer matrix of dimensions $r \times m$. Assume that the coefficients of Ψ, P, Q are all of magnitude bounded by ρ . Then, there is a bilinear system

$$\Sigma_b = (A, G_1, \dots, G_m, B, \phi_1, \dots, \phi_l)$$

with $N = \binom{r+d}{r}$, $l = N - r - 1$, each coefficient of the matrices A, G_1, \dots, G_m, B of magnitude $\leq d\rho r^2$, and the polynomials ϕ_i of degree $\leq d$ and with each coefficient equal to 0, 1, or -1 , such that each of the following properties holds for the system Σ if and only if it holds for the system Σ_b :

- (a) $0 \in \text{int } A^+(0)$,
- (b) $0 \in \text{int } A^-(0)$,
- (c) $A^+(x) = M$ for all $x \in M$.

Further, the system Σ_b can be constructed in polynomial time from the data Ψ, P, Q .

Proof. Note that N is the number of possible monomials of degree $\leq d$ in the variables $\xi = \xi_1, \dots, \xi_r$. We shall use multiindices $\alpha = (\alpha_1, \dots, \alpha_r)$ with weight $|\alpha| := \sum \alpha_i \leq d$, and

$$\xi^\alpha := \xi_1^{\alpha_1} \dots \xi_r^{\alpha_r}$$

to denote these monomials. The coordinates of vectors in \mathbb{R}^N will be denoted as η_α , for such indices α , ordered lexicographically. In particular, we let $e_i := (0, 0, \dots, 0, 1, 0, \dots, 0)$ (1 in i -th position,) and write η_{e_i} just as η_i . For each of the $l = N - r - 1$ indices α with weight $|\alpha| \geq 2$, we introduce the polynomial in N variables

$$\phi_\alpha(\eta) := \eta_\alpha - \eta_1^{\alpha_1} \dots \eta_r^{\alpha_r}.$$

Note that the Jacobian matrix of the of the ϕ_α 's has constant rank $N - r - 1$. The idea of the construction is to introduce a variable for each monomial in Ψ (the η_α 's) in such a manner that the equation for ξ_0 becomes linear,

$$\dot{\eta}_0 = \sum_{\beta} \psi_\beta \eta_\beta,$$

where $\Psi(\xi) = \sum_{\beta} \psi_{\beta} \xi^{\beta}$, and to introduce a differential equation for each of the monomials ξ^{α} , thought of now as new variables η_{α} . Note that if $\xi(\cdot)$ is a solution of

$$\dot{\xi} = P\xi + Qu$$

and if $|\alpha| > 0$ then

$$d\xi^{\alpha}/dt = \sum_{|\beta|=|\alpha|} a_{\beta}^{\alpha} \xi^{\beta} + \sum_{|\beta|=|\alpha|-1} (g_{\beta}^{\alpha,1} u_1 + \cdots + g_{\beta}^{\alpha,m} u_m) \xi^{\beta}, \quad (6.2)$$

where the coefficients $a_{\beta}^{\alpha}, \dots$ are obtained as follows. Let $P = (p_{ij}), Q = (q_{ij})$; with these notations,

$$a_{\beta}^{\alpha} = \sum_{i,j} \alpha_i p_{ij}, \quad (6.3)$$

the sum over all those indices $1 \leq i, j \leq r$ for which $\beta + e_i = \alpha + e_j$, and for each j ,

$$g_{\beta}^{\alpha,j} = \sum_i \alpha_i q_{ij}, \quad (6.4)$$

the sum over all those indices $1 \leq i \leq r$ for which $\beta + e_i = \alpha$. We also denote, for the case $\alpha = (0, \dots, 0)$, each β , and each $j = 1, \dots, m$, $\alpha_{\beta}^{\alpha} := \psi_{\beta}$ and $g_{\beta}^{\alpha,j} := 0$. Finally, let A and $G_j, j = 1, \dots, m$ be the matrices (a_{β}^{α}) and $(g_{\beta}^{\alpha,j})$ respectively, and let B be the block matrix

$$\begin{pmatrix} 0 \\ Q \\ 0 \end{pmatrix}$$

where the first block is a row of size $1 \times m$ and the last one is of size $N - r - 1$ by m .

Since there are at most r^2 terms in each of (6.3) and (6.4), the claimed estimates for the magnitudes of the entries of these matrices do indeed hold. Further, the constructions can be clearly carried out in polynomial time.

Given any vector $x = (x_0, \dots, x_r) \in \mathbb{R}^{r+1}$, let $h(x) \in \mathbb{R}^N$ be defined as follows: $h_{(0, \dots, 0)}(x) := x_0$, and

$$h_{\alpha}(x) := x_1^{\alpha_1} \dots x_r^{\alpha_r}$$

for $|\alpha| > 0$. Note that h is a diffeomorphism $\mathbb{R}^r \simeq M$, and $h(0) = 0$. Now assume that $x(\cdot) = (x_0(\cdot), x_1(\cdot), \dots, x_r(\cdot))$ solves (6.1) with respect to a given control $u(\cdot)$. It follows by construction that $\eta(t) := h(\xi(t))$ satisfies

$$\dot{\eta}(t) = (A + \sum u_i(t) G_i) \eta(t) + Bu(t).$$

Therefore $x(0)$ can be steered into $x(T)$ iff $h(x(0))$ can be steered into $h(x(T))$, and this establishes properties (a)-(c). ■

§7. Controllability is NP-hard.

We are only left to put together all the pieces from the previous sections. Assume that \mathcal{S} is any set of L clauses. Note that it can involve at most $n \leq 3L$ variables. By lemma 5.1 we may build in polynomial time an integer polynomial f of degree 6 in $n + L$ variables, with coefficients of magnitude bounded by cL^3 , such that f is indefinite iff \mathcal{S} is satisfiable. For this f , we now consider the system (4.1), where (A, b) is a cascade of integrators

$$\dot{z}_1 = z_2, \dot{z}_2 = z_3, \dots, \dot{z}_k = u_1,$$

and $k = n + L$. By proposition 4.2, the system is controllable, in either of the senses there, iff \mathcal{S} is satisfiable. We now apply lemma 6.1, with $r = k + 1$, $m = 2$,

$$\Psi(\xi_1, \dots, \xi_{k+1}) := \xi_{k+1}^2 f(\xi_1, \dots, \xi_r),$$

and P, Q found from A, b plus the last equation $\dot{w} = u_2$. Note that $d = 8$, and that we may take $\rho = cL^3$. We thus obtain, in polynomial time, the bilinear subsystem Σ_b in lemma 6.1. Listing all entries of A, \dots, ϕ_l results in a size of order at most $N^2 \log_2(r^2 \rho)$, which is bounded by a polynomial in L . A polynomial time decision method for controllability of Σ_b would thus imply one for 3-SAT. Thus our problem is at least as hard as that one:

Theorem 2. Each of the following decision problems is NP-hard, for bilinear subsystems:

- (a) $0 \in \text{int } A^+(0)$. (Local reachability at 0.)
- (b) $0 \in \text{int } A^-(0)$. (Local controllability at 0.)
- (c) $A^+(x) = M$ for all $x \in M$. (Complete controllability.) ■

As remarked earlier, many other questions, such as local small-time reachability, are shown to be NP-hard by the same argument. As directions for further research, we'd suggest looking for a similar result using only single-input systems –the above proof shows that it is hard to decide controllability if at least two controls are allowed,– and also for the case of controls constrained to compact sets. Alternatively, it would be interesting to establish better lower bounds for the problem studied here.

§8. References.

- [A] Aberth, O., *Computable Analysis*, McGraw-Hill, New York, 1980.
- [AHU] Aho, A.V., J. Hopcroft, and J.D. Ullman, *The Design and Analysis of Computer Algorithms*, Addison-Wesley, Reading, 1974.
- [BW] Boothby, W.M., and E.N. Wilson, "Determination of the transitivity of bilinear systems," *SIAM J. Control and Opt.* **17**(1979): 212-221.
- [B] Brockett, R., "On the algebraic structure of bilinear systems," in *Theory and Applications of Variable Structure Systems* (R. Mohler and A. Ruberti, eds.), Academic Press, NY, 1972, pp. 153-168.
- [Co] Collins, G., "Quantifier elimination for real-closed fields by cylindrical algebraic decomposition," in *Springer Lec. Notes in C.S.* **35**(1975): 134-183.
- [Cr] Crouch, P.E., "Dynamical realizations of finite Volterra series," Ph.D. Thesis, Harvard, 1977.
- [GJ] Garey, M.R., and D. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W.H. Freeman and Company, San Francisco, 1979.
- [HK] Hermann, R. and A.J. Krener, "Nonlinear controllability and observability," *IEEE Trans. Autom. Ctr.* **22**:728-740.
- [I] Isidori, A., *Nonlinear Control Systems: An Introduction*, Springer, Berlin, 1985.
- [K] Ko, K., "Applying techniques of discrete complexity theory to numerical computation," in *Studies in Complexity Theory*, (R.V. Book, ed.), Pitman, London, 1986.
- [PS] Papadimitriou, C.H., and K. Steiglitz, *Combinatorial Optimization: Algorithms and Complexity*, Prentice-Hall, Englewood Cliffs, 1982.
- [PT] Papadimitriou, C.H., and J. Tsitsiklis, "Intractable problems in control theory," *SIAM J. Control and Opt.* **24**(1986): 639-654.
- [So1] Sontag, E.D., "On certain questions of rationality and decidability," *J. Comp. Syst. Sci.* **11**(1975): 375-381.
- [So2] Sontag, E.D., "Real addition and the polynomial hierarchy," *Inform. Proc. Letters* **20**(1985): 115-120.
- [Su1] Sussmann, H.J., "Lie brackets, real analyticity, and geometric control," in *Differential Geometric Control theory* (R.W. Brockett, R.S. Millman, and H.J. Sussmann, eds.), Birkhauser, Boston, 1983.
- [Su2] Sussmann, H.J., "A general theorem on local controllability," *SIAM J. Control and Opt.*, **25**(1987): 158-194.