

Chapter 2

Preliminaries

In this chapter, we define some basic notions and notations that will be used in the sequel, and meanwhile give an elementary description of several relevant mathematical theories, including dynamical and control systems, algebraic geometry, first-order theory of reals and so on, which are fundamental to the understanding of this book. For a comprehensive introduction of these theories the readers may refer to the cited literatures.

Throughout this chapter and in the rest of this book, we use $\mathbb{N}, \mathbb{Q}, \mathbb{R}$ to denote the set of *natural*, *rational*, and *real* numbers, respectively. Given a set A , the Cartesian product of its n duplicates is denoted by A^n ; for instance, \mathbb{R}^n stands for the n -dimensional Euclidean space. A vector element $(a_1, a_2, \dots, a_n) \in A^n$ is usually abbreviated by a boldface letter \mathbf{a} when its dimension is clear from the context.

2.1 Continuous Dynamical System

We introduce some basic theories of continuous dynamical systems here. For details please refer to [103, 189].

Typically, a continuous dynamical system (CDS for short) is modelled by first-order autonomous ordinary differential equations (ODE for short)

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}), \quad (2.1)$$

where $\mathbf{x} \in \mathbb{R}^n$ and $\mathbf{f} : U \rightarrow \mathbb{R}^n$ is a vector function defined on an open set $U \subseteq \mathbb{R}^n$, called a *vector field* on U .

We say that \mathbf{f} in (2.1) satisfies the *local Lipschitz condition* if for any $\mathbf{x}_0 \in U$, there exist $\delta > 0$ and $L > 0$, s.t.

$$\|\mathbf{f}(\mathbf{x}_1) - \mathbf{f}(\mathbf{x}_2)\| \leq L\|\mathbf{x}_1 - \mathbf{x}_2\|, \quad \forall \mathbf{x}_1, \mathbf{x}_2 \in \mathcal{B}_\delta(\mathbf{x}_0), \quad (2.2)$$

where $\|\cdot\|$ denotes the Euclidean norm¹ and $\mathcal{B}_\delta(\mathbf{x}_0) \triangleq \{\mathbf{x} \in U \mid \|\mathbf{x} - \mathbf{x}_0\| < \delta\}$ (\triangleq means *defined as*).

If \mathbf{f} satisfies the local Lipschitz condition, then given $\mathbf{x}_0 \in U$, there exists a unique *differentiable* vector function $\mathbf{x}(\mathbf{x}_0; t) : (a, b) \rightarrow \mathbb{R}^n$, where (a, b) is an open interval containing 0, such that $\mathbf{x}(\mathbf{x}_0; 0) = \mathbf{x}_0$ and the derivative of $\mathbf{x}(\mathbf{x}_0; t)$ w.r.t. t satisfies

$$\forall t \in (a, b). \quad \frac{d\mathbf{x}(\mathbf{x}_0; t)}{dt} = \mathbf{f}(\mathbf{x}(\mathbf{x}_0; t)).$$

Such $\mathbf{x}(\mathbf{x}_0; t)$ is called the solution to (2.1) with initial value \mathbf{x}_0 .

If \mathbf{f} is *analytic* at $\mathbf{x}_0 \in U$, i.e., each element function of \mathbf{f} can be written as a convergent power series in a neighborhood of \mathbf{x}_0 , then there exists a unique *analytic* solution $\mathbf{x}(\mathbf{x}_0; t)$ to (2.1) defined in a neighborhood of \mathbf{x}_0 .

In this paper, we will consider a special type of CDS in the following form:

Definition 2.1 (Constrained CDS). A constrained continuous dynamical system (CCDS for short) is a pair (B, \mathbf{f}) , where $B \subseteq \mathbb{R}^n$ is the domain restriction of continuous evolution, and $\mathbf{f} : B \rightarrow \mathbb{R}^n$ is a locally Lipschitz continuous vector field.

2.2 Stability and Feedback Control

In this section, we first introduce the classic theory of stability in the sense of Lyapunov.

Definition 2.2. A point $\mathbf{x}_e \in U$ is called an *equilibrium point* of (2.1), if $\mathbf{f}(\mathbf{x}_e) = \mathbf{0}$.

Without loss of generality, we assume $\mathbf{x}_e = \mathbf{0} \in U$ in the sequel.

Definition 2.3 (Lyapunov Stability). Assuming $\mathbf{0}$ is an equilibrium point of (2.1), then

- $\mathbf{0}$ is called *stable*, if for any $\epsilon > 0$, there exists $\delta > 0$, s.t. for any \mathbf{x}_0 satisfying $\|\mathbf{x}_0\| < \delta$ the solution $\mathbf{x}(\mathbf{x}_0; t)$ exists on $[0, \infty)$ and $\|\mathbf{x}(\mathbf{x}_0; t)\| < \epsilon$ for all $t \geq 0$;
- $\mathbf{0}$ is called *asymptotically stable*, if $\mathbf{0}$ is stable and there exists $\delta > 0$, s.t. for any \mathbf{x}_0 satisfying $\|\mathbf{x}_0\| < \delta$, the solution $\mathbf{x}(\mathbf{x}_0; t)$ satisfies $\lim_{t \rightarrow \infty} \mathbf{x}(\mathbf{x}_0; t) = \mathbf{0}$.

The *Lyapunov's direct method* is an important method for deciding the stability of CDSs, by constructing the so-called *Lyapunov functions*.

¹For $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$, $\|\mathbf{x}\| = \sqrt{\sum_{i=1}^n x_i^2}$.

Theorem 2.1 (Lyapunov Stability Theorem). *Assuming $\mathbf{0}$ is an equilibrium point of (2.1), if there exist an open set $W \subseteq U$ containing $\mathbf{0}$ and a continuously differentiable function $V : W \rightarrow \mathbb{R}$ s.t.*

- (a) $V(\mathbf{0}) = 0$,
- (b) $V(\mathbf{x}) > 0$ for any $\mathbf{x} \in W \setminus \{\mathbf{0}\}$,
- (c) $\nabla V \cdot \mathbf{f} \leq 0$ for any $\mathbf{x} \in W$, where ∇ and \cdot denote the gradient and inner product operator, respectively,

then $\mathbf{0}$ is stable; in addition, if (c) is replaced by

- (c') $\nabla V \cdot \mathbf{f} < 0$ for any $\mathbf{x} \in W \setminus \{\mathbf{0}\}$,

then $\mathbf{0}$ is asymptotically stable. The function V satisfying (a), (b), (c) (or (c')) is called a Lyapunov function.

The output feedback stabilization problem for the following time-invariant system:

$$\begin{cases} \dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \mathbf{u}) \\ \mathbf{y} = \mathbf{h}(\mathbf{x}) \end{cases}, \quad (2.3)$$

where $\mathbf{f} : \mathbb{R}^n \times \mathbb{R}^m \rightarrow \mathbb{R}^n$ and $\mathbf{h} : \mathbb{R}^n \rightarrow \mathbb{R}^p$ are continuously differentiable functions satisfying $\mathbf{f}(\mathbf{0}, \mathbf{0}) = \mathbf{0}$ and $\mathbf{h}(\mathbf{0}) = \mathbf{0}$, is to design an output feedback control law $\mathbf{u} = \mathbf{g}(\mathbf{y})$, where $\mathbf{g} : \mathbb{R}^p \rightarrow \mathbb{R}^m$ is a continuously differentiable function with $\mathbf{g}(\mathbf{0}) = \mathbf{0}$, s.t. the closed loop system $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \mathbf{g}(\mathbf{h}(\mathbf{x})))$ has the origin as its asymptotically stable equilibrium point.

2.3 Polynomials and Polynomial Ideals

In this book, we will mainly focus on the class of *polynomial* expressions, which have powerful modelling ability and are easy to manipulate. We will give a brief overview of the theory of polynomials and polynomial ideals here. For more details please refer to [46].

A *monomial* in n variables x_1, x_2, \dots, x_n (or briefly \mathbf{x}) is a product form $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, or briefly \mathbf{x}^α , where $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{N}^n$. The number $\sum_{i=1}^n \alpha_i$ is called the *degree* of \mathbf{x}^α .

Let \mathbb{K} be a field, which can be either \mathbb{Q} or \mathbb{R} in this chapter. A *polynomial* $p(\mathbf{x})$ (or briefly p) of degree d in \mathbf{x} with coefficients in \mathbb{K} is of the form

$$p(\mathbf{x}) \hat{=} \sum_{\substack{\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \\ \{\mathbb{N}^n \mid \alpha_1 + \alpha_2 + \cdots + \alpha_n \leq d\}}} c_\alpha \mathbf{x}^\alpha,$$

where all $c_\alpha \in \mathbb{K}$. It is easy to see that a polynomial in x_1, x_2, \dots, x_n with degree d has at most $\binom{n+d}{d}$ many non-zero coefficients.

The set of all polynomials in x_1, x_2, \dots, x_n with coefficients in \mathbb{K} form a *polynomial ring*, denoted by $\mathbb{K}[\mathbf{x}]$.

A vector field \mathbf{f} is called a *polynomial vector field* (PVF for short) if each element function of \mathbf{f} is a polynomial.

We next recall the basic theory of polynomial ideals.

Definition 2.4 (Polynomial Ideal). A subset $I \subseteq \mathbb{K}[\mathbf{x}]$ is called an **ideal** if the following conditions are satisfied:

1. $0 \in I$;
2. If $p, g \in I$, then $p + g \in I$;
3. If $p \in I$ and $h \in \mathbb{K}[\mathbf{x}]$, then $hp \in I$.

Let $g_1, g_2, \dots, g_s \in \mathbb{K}[\mathbf{x}]$. It is easy to check that the set

$$\langle g_1, g_2, \dots, g_s \rangle \hat{=} \left\{ \sum_{i=1}^s h_i g_i \mid h_1, h_2, \dots, h_s \in \mathbb{K}[\mathbf{x}] \right\}$$

is an ideal, called the ideal *generated* by g_1, g_2, \dots, g_s . If $I = \langle g_1, g_2, \dots, g_s \rangle$, then $\{g_1, g_2, \dots, g_s\}$ is called a *basis* of I .

Theorem 2.2 (Hilbert Basis Theorem). Every ideal $I \subseteq \mathbb{K}[\mathbf{x}]$ has a (finite) basis, that is, $I = \langle g_1, g_2, \dots, g_s \rangle$ for some $g_1, g_2, \dots, g_s \in \mathbb{K}[\mathbf{x}]$.

In particular, every ideal $I \subseteq \mathbb{K}[\mathbf{x}]$ has a *Gröbner basis* which possesses very nice properties. To illustrate this, we need to fix an ordering of monomials. First, suppose the list of variables x_1, x_2, \dots, x_n are ordered by $x_1 > x_2 > \dots > x_n$. Then $>$ induces a total ordering on the set of monomials \mathbf{x}^α with $\alpha \in \mathbb{N}^n$. One example is the *lexicographic* (lex for short) order, i.e., $\mathbf{x}^\alpha > \mathbf{x}^\beta$ if and only if there exists $1 \leq i \leq n$ such that $\alpha_i > \beta_i$, and $\alpha_j = \beta_j$ for all $1 \leq j < i$. It can be shown that the lex order of monomials is a *well-ordering*, that is, every non-empty set of monomials has a *least* element. Besides, the lex order is preserved under multiplication, i.e., $\mathbf{x}^\alpha > \mathbf{x}^\beta$ implies $\mathbf{x}^\alpha \mathbf{x}^\gamma > \mathbf{x}^\beta \mathbf{x}^\gamma$ for any $\gamma \in \mathbb{N}^n$. Such an ordering of monomials as the lex order is called a *monomial ordering*.

Given a monomial ordering $>$ and a polynomial $g \in \mathbb{K}[\mathbf{x}]$, rearrange the monomials in p in a descending order as

$$g = c_1 \mathbf{x}^{\alpha_1} + c_2 \mathbf{x}^{\alpha_2} + \dots + c_k \mathbf{x}^{\alpha_k},$$

where all c_i 's are non-zero. Then $c_1 \mathbf{x}^{\alpha_1}$ is called the *leading term* of g , denoted by $\text{lt}(g)$; c_1 is called the *leading coefficient* of g , denoted by $\text{lc}(g)$; and \mathbf{x}^{α_1} is called the *leading monomial* of g , denoted by $\text{lm}(g)$. For a polynomial $p \in \mathbb{K}[\mathbf{x}]$, if p has a non-zero term $c_\beta \mathbf{x}^\beta$ and \mathbf{x}^β is divisible by $\text{lm}(g)$, i.e., $\mathbf{x}^\beta = \mathbf{x}^\gamma \text{lm}(g)$ for some $\gamma \in \mathbb{N}^n$, then we say p is *reducible* modulo g , and call

$$p' = p - \frac{c_\beta}{\text{lc}(g)} \mathbf{x}^\gamma g$$

the one-step *reduction* of p modulo g .

Given a finite set of polynomials $G \subsetneq \mathbb{K}[\mathbf{x}]$ and a polynomial $p \in \mathbb{K}[\mathbf{x}]$, we can do a multi-step reduction on p using polynomials in G , until p is reduced to p^* which is not further reducible modulo G . Such p^* is called the *normal form* of p w.r.t. G , denoted by $\text{nf}(p, G)$. For general G , the above process of reduction is guaranteed to terminate; however, the final result $\text{nf}(p, G)$ may vary, depending on the sequence of polynomials chosen from G during reduction. Fortunately, we have

Proposition 2.1. *Given a monomial ordering, then every ideal $I \subseteq \mathbb{K}[\mathbf{x}]$ other than $\{0\}$ has a basis $G = \{g_1, g_2, \dots, g_s\}$, such that for any $p \in \mathbb{K}[\mathbf{x}]$, $\text{nf}(p, G)$ is unique. Such G is called a **Gröbner basis** of I .*

Furthermore,

Proposition 2.2. *Let G be a Gröbner basis of an ideal $I \subseteq \mathbb{K}[\mathbf{x}]$. Then for any $p \in \mathbb{K}[\mathbf{x}]$, $p \in I$ if and only if $\text{nf}(p, G) = 0$.*

Most importantly, for any ideal $I = \langle h_1, h_2, \dots, h_l \rangle \subseteq \mathbb{K}[\mathbf{x}]$, the Gröbner basis G of I can be computed from the h_i s using *Buchberger's Algorithm* [46]. Then by Proposition 2.2, we get that the *ideal membership* problem, that is to decide whether a polynomial $p \in \mathbb{K}[\mathbf{x}]$ lies in a given ideal $\langle h_1, h_2, \dots, h_l \rangle \subseteq \mathbb{K}[\mathbf{x}]$, is algorithmically solvable.

The following theorem, which can be deduced from Hilbert Basis Theorem, is key to the proof of several main results in this book (Chap. 9).

Theorem 2.3 (Ascending Chain Condition). *For any ascending chain of ideals*

$$I_1 \subseteq I_2 \subseteq \dots \subseteq I_l \subseteq \dots$$

in $\mathbb{K}[\mathbf{x}]$, there exists an $N \in \mathbb{N}$ such that $I_l = I_N$ for any $l \geq N$.

2.4 First-Order Theory of Reals

From a logical point of view, polynomials can be used to construct the first-order theory of *real numbers* (actually of all *real closed fields*), denoted by $\mathcal{T}(\mathbb{R})$. The language of $\mathcal{T}(\mathbb{R})$ consists of

- variables: $x, y, z, \dots, x_1, x_2, \dots$;
- constants: all the numbers in \mathbb{Q} ;
- function symbols: $+, -, \cdot$;
- relation symbols: $>, <, \geq, \leq, =, \neq$;
- Boolean connectives: $\wedge, \vee, \neg, \longrightarrow, \longleftrightarrow, \dots$; and
- quantifiers: \forall, \exists .

Note that we give a non-minimal set of constructs for convenience of expressing formulas. Besides, all variables are simply interpreted over \mathbb{R} , and all function and relation symbols are interpreted in the normal sense of real arithmetic.

A *term* of $\mathcal{T}(\mathbb{R})$ over a finite set of variables $\{x_1, x_2, \dots, x_n\}$ is a polynomial $p \in \mathbb{Q}[x_1, x_2, \dots, x_n]$. An *atomic formula* of $\mathcal{T}(\mathbb{R})$ is of the form $p \triangleright 0$, where \triangleright is any relation symbol. A *quantifier-free formula* (QFF for short) of $\mathcal{T}(\mathbb{R})$ is a Boolean combination of atomic formulas. A generic formula of $\mathcal{T}(\mathbb{R})$ is built up from atomic formulas using Boolean connectives as well as quantifiers.

A profound result about $\mathcal{T}(\mathbb{R})$ is that it admits *quantifier elimination* (QE for short) [188]. That is, any (quantified) formula φ in $\mathcal{T}(\mathbb{R})$ has a quantifier-free equivalent φ_{QF} involving only *free* variables of φ , and φ_{QF} can be computed from φ using QE algorithms. An immediate consequence of this result is the *decidability* of $\mathcal{T}(\mathbb{R})$: the truth value of any closed formula in $\mathcal{T}(\mathbb{R})$ can be decided.

Formulas in $\mathcal{T}(\mathbb{R})$ define a special class of sets:

Definition 2.5 (Semi-algebraic Set). A subset $A \subseteq \mathbb{R}^n$ is called a *semi-algebraic set* (SAS for short), if there exists a QFF φ in $\mathcal{T}(\mathbb{R})$ over variables x_1, x_2, \dots, x_n (or briefly \mathbf{x}), such that

$$A = \{\mathbf{x} \in \mathbb{R}^n \mid \varphi(\mathbf{x}) \text{ is true}\}.$$

Let $\mathcal{A}(\varphi)$ denote the SAS defined by a QFF φ . Then from Definition 2.5 it is easy to check that SASs are closed under common set operations:

- $\mathcal{A}(\varphi_1) \cap \mathcal{A}(\varphi_2) = \mathcal{A}(\varphi_1 \wedge \varphi_2)$;
- $\mathcal{A}(\varphi_1) \cup \mathcal{A}(\varphi_2) = \mathcal{A}(\varphi_1 \vee \varphi_2)$;
- $\mathcal{A}(\varphi_1)^c = \mathcal{A}(\neg \varphi_1)$;
- $\mathcal{A}(\varphi_1) \setminus \mathcal{A}(\varphi_2) = \mathcal{A}(\varphi_1) \cap \mathcal{A}(\varphi_2)^c = \mathcal{A}(\varphi_1 \wedge \neg \varphi_2)$,

where A^c and $A \setminus B$ stand for the complement (in \mathbb{R}^n) and subtraction operations of sets, respectively. Moreover, we can easily check the emptiness, inclusion, and equality of SASs by the decidability of $\mathcal{T}(\mathbb{R})$.

For convenience, in the rest of this book, we do not distinguish between an SAS $\mathcal{A}(\varphi)$ and its defining formula φ . That is, we will use $\mathcal{T}(\mathbb{R})$ -formulas to represent SASs and use Boolean connectives as set operators. Besides, it is easy to check that any SAS can be represented by a QFF in the form of

$$\varphi(\mathbf{x}) \triangleq \bigvee_{k=1}^K \bigwedge_{j=1}^{J_k} p_{kj}(\mathbf{x}) \triangleright_{kj} 0,$$

where $p_{kj}(\mathbf{x}) \in \mathbb{Q}[\mathbf{x}]$ and $\triangleright_{kj} \in \{\geq, >\}$. Therefore restricting SASs to formulas of such shape will not lose any generality.

2.5 Summary

In this chapter, we fix some basic notations and introduce some basic notions and results of several fundamental theories, including continuous dynamical systems, feedback control systems and stability, polynomial ideals, and first-order theory of reals. These notations, notions, and theories are key to the understanding of the rest of this book. For detailed description of related materials the readers can resort to the cited references.

Formal Verification of Simulink/Stateflow Diagrams

A Deductive Approach

Zhan, N.; Shuling, W.; Zhao, H.

2017, XV, 258 p. 74 illus., 60 illus. in color., Hardcover

ISBN: 978-3-319-47014-6