Fault Tolerant Control: A Simultaneous Stabilization Result
Jakob Stoustrup and Vincent D. Blondel

Abstract—This note discusses the problem of designing fault tolerant compensators that stabilize a given system both in the nominal situation, as well as in the situation where one of the sensors or one of the actuators has failed. It is shown that such compensators always exist, provided that the system is detectable from each output and that it is stabilizable. The proof of this result is constructive, and a worked example shows how to design a fault tolerant compensator for a simple, yet challenging system. A family of second order systems is described that requires fault tolerant compensators for arbitrarily high order.

Index Terms—Controller order, fault tolerant control, sensor faults, simultaneous stabilization.

I. INTRODUCTION

The interest for using fault tolerant controllers is increasing. A number of theoretical results as well as application examples has now been described in the literature; see, e.g., [1]–[9] to mention some of the relevant references in this area.

The approaches to fault tolerant control can be divided into two main classes: Active fault tolerant control and passive fault tolerant control. In active fault tolerant control, the idea is to introduce a fault detection and isolation block in the control system. Whenever a fault is detected and isolated, a supervisory system takes action, and modifies the structure and/or the parameters of the feedback control system. In contrast, in the passive fault tolerant control approach, a fixed compensator is designed, that will maintain (at least) stability if a fault occurs in the system.

This note will only discuss the passive fault tolerant control approach, also sometimes referred to as reliable control. This approach has mainly two motivations. First, designing a fixed compensator can be made in much simpler hardware and software, and might thus be admissible in more applications. Second, classical reliability theory states that the reliability of a system decreases rapidly with the complexity of the system. Hence, although an active fault tolerant control system might in principle accommodate specific faults very efficiently, the added complexity of the overall system by the fault detection system and the supervisory system itself, might in fact sometimes deteriorate plant reliability.

In [10], a fault tolerant control problem has been addressed for systems, where specific sensors could potentially fail such that the corresponding outputs were unavailable for feedback, whereas other outputs were assumed to be available at all times.

In [11, Sec 5.5], the question of fault tolerant parallel compensation has been discussed, i.e., whether it is possible to design two compensators such that any of them alone or both in parallel will internally stabilize the closed loop system.

The existence results given in [10] and [11] can be considered to be special cases of the main results of this note.

In this note, we shall consider systems for which any sensor (or in the dual case any actuator) might fail, and we wish to determine for which systems such (passive) fault tolerant compensators exist. The main results state that the only precondition for the existence of solutions to this fault tolerant control problem is just stabilizability from each input and detectability of the system from each output.

Throughout this note, \( \mathbb{R}^{p \times m} \) shall denote the set of proper, real-rational functions taking values in \( \mathbb{C}^{p \times m} \), and \( \mathbb{R}^{SP} \) shall denote the set of strictly proper, real-rational functions taking values in \( \mathbb{C}^{p \times m} \). \( \mathbb{R}^{H} \) shall denote the set of stable, proper, real-rational functions taking values in \( \mathbb{C}^{p \times m} \). The notation \( \{ s \in \mathbb{R} : B(s) = 0 \} \) shall be used as shorthand for zeros of \( B(\cdot) \) on the positive real line. The set includes the point at infinity if \( \lim_{s \to \infty} B(s) = 0 \). For matrices \( A, B, C, D \) of compatible dimensions, the expression

\[
G(s) = \begin{pmatrix} A & B \\ C & D \end{pmatrix}
\]

will be used to denote the transfer function \( G(s) = C(sI - A)^{-1} B + D \). Real-rational functions will be indicated by their dependency of a complex variable \( s \) (as in \( G(s), K(s) \)), although the dependency of \( s \) will be suppressed in the notation (as in \( G, K \)), where no misunderstanding should be possible.

II. PROBLEM FORMULATION

Consider a system of the form

\[
\begin{align*}
x & = Ax + Bu \\
y_1 & = C_1 x \\
& \vdots \\
y_p & = C_p x
\end{align*}
\]

where \( x \in \mathbb{R}^n, u \in \mathbb{R}^m, y_i \in \mathbb{R}, i = 1, \ldots, p \) and \( A, B, C_i, i = 1, \ldots, p \) are matrices of compatible dimensions. Each of the \( p \) measure-
ments $y_i, i = 1, \ldots, p$, is the output of a sensor, which can potentially fail.

In this note, we will determine whether it is possible to design a feedback compensator that is guaranteed to stabilize a given system, in case any sensor could potentially fail. To be more precise, we are looking for a dynamic compensator $u = K(s)y$, $K \in \mathcal{R}^{m \times p}$, with the property, that each of the following feedback laws:

$$u = K(s)y_1 \quad u = K(s)y_{1, \ldots, p}$$

are internally stabilizing, i.e., that both the nominal system as well as each of the systems resulting from one of the sensors failing are all stabilized by $K(s)$.

It is obvious, that the answer to this question immediately provides the answer to the corresponding dual question, i.e., whether is possible that $A(s)$ has an inverse in that ring. In particular, a unit in the ring of stable proper rational functions, if and only if $A(s)$ has constant sign for all $s \in \mathcal{R}_{+ \infty} : B(s) = 0$.

IV. MAIN RESULTS

In this section, we will present our main results which state that for systems with several outputs, it is always possible to find a compensator, that both stabilizes the nominal situation, as well as the situation where any of the sensors fails. In a similar fashion, it is shown, that it is always possible to design a fault tolerant feedback compensator for a system with several actuators. The only preconditions to these results, is in the first case that all unstable modes for the system are observable by each sensor and in the second (dual) case, that all modes are controllable by each actuator.

**Theorem 1:** Consider a system given by a state-space model of the form (1). Assume, that the pair $(A, B)$ is stabilizable, and that each of the pairs $(C_i, A), i = 1, \ldots, p$, is detectable. Then, there exists a dynamic compensator $K(s)$ such that each of the $p + 1$ control laws (2) internally stabilizes (1).

The proof will be constructive, and we shall give some comments on practical computations in the sequel of the proof.

**Proof:** First, let us note that it suffices to prove the result in the case where $m = 1$ and $p = 2$. To see that $m = 1$ can be assumed without loss of generality, one can just consider the system

$$\dot{x} = Ax + B\bar{u}$$

$$y_1 = C_1x$$

$$\vdots$$

$$y_p = C_p x$$

where $\bar{B} = BV, v \in \mathcal{R}^{m \times 1}, \bar{u} \in \mathcal{R}$, and $v$ is any vector such that the pair $(A, \bar{B})$ is also stabilizable. This is always possible (see, e.g., [14, Cor. 1.1, p. 43]). Thus, if $\bar{u} = \bar{K}(s)y$ is a fault tolerant feedback law for (4), then $u = K(s)y$ is a fault tolerant feedback law for (1) with $K(s) = v\bar{K}(s)$.

Next, if

$$K(s) = (K_1(s), K_2(s))$$

is a fault tolerant feedback compensator for this system

$$\dot{x} = Ax + Bu$$

$$y_1 = C_1x$$

$$y_2 = C_2x$$

then

$$K(s) = (K_1(s), K_2(s), 0, \ldots, 0)$$

is a fault tolerant feedback compensator for (1). Indeed, in the nominal situation or if one of the sensors corresponding to $y_i, i = 3, \ldots, p$, fails, the control signal generated by (7) will be the same as the control signal generated by (5) in the nominal situation. If $y_i, i = 1, 2$, fails, (7) will still generate the same control signal as (5) which is known to stabilize the shared dynamics of the two systems.

Thus, without loss of generality, we will assume that the system in consideration has the form (6), where $B$ is now a single column matrix, $C_i, i = 1, 2$ are single row matrices, $u, y_1, y_2 \in \mathcal{R}, i = 1, 2$. Thus, it will
be assumed that the transfer functions from $u$ to each of the outputs are scalar.

Define $G_C = \begin{pmatrix} C_1 \\ C_2 \end{pmatrix}$ and let $K_0(s)$ be an internally stabilizing compensator for the system (6), which has the transfer function $G(s) = C(sI - A)^{-1} B$. Introduce a doubly coprime factorization of $G(s)$ and $K_0(s)$, i.e., stable proper functions $M, N, \hat{V}_0, \hat{U}_0$

$$G(s) = \frac{N(s)}{N_2(s)} M^{-1}(s)$$
$$K_0(s) = \frac{\hat{V}_0^{-1}(s)\hat{U}_0}{\hat{V}_0^{-1}(s)(\hat{V}_0, \hat{U}_0)}$$

satisfying the Bezout identity

$$\hat{V}_0 M - \hat{U}_0 N = \hat{V}_0 M - \hat{U}_0, N_1 - \hat{U}_0, N_2 = 1.$$  (8)

This can always be done—explicit formulas are given by (3).

Next, we note that replacing in (8) the triplet

$$(\hat{V}_0, \hat{U}_0, 1, \hat{U}_2)$$

where

$$\hat{V} = \hat{V}_0 - Q_2 N_1 - Q_3 N_2$$
$$\hat{U}_1 = \hat{U}_0, 1, Q_1, N_2 - Q_2 M$$
$$\hat{U}_2 = \hat{U}_0, 2 + Q_1, N_1 - Q_3 M$$

also provides a solution to (8), as this simple calculation shows

$$\hat{V}^{-1}(\hat{U}_1 \hat{U}_2) = (\hat{V}_0 - Q_2 N_1 - Q_3 N_2)^{-1}\times(\hat{U}_0, 1, Q_1, N_2 - Q_2 M, \hat{U}_0, 2 + Q_1, N_1 - Q_3 M)$$  (9)

where $Q_1, Q_2, Q_3$ are all stable proper rational functions, is also a stabilizing compensator.

In the sequel, we shall demonstrate, that $Q_1, Q_2, Q_3$ can be chosen such that $V^{-1}(U_1 U_2)$ stabilizes both the nominal and the faulty systems.

If the sensor corresponding to one of the outputs fails, the controller $V^{-1}(U_1 U_2)$ has to stabilize a system of the form:

$$G = \begin{pmatrix} N_1(s) \\ 0 \end{pmatrix} \quad \text{or} \quad G = \begin{pmatrix} 0 \\ N_2(s) \end{pmatrix}$$

which means that stability is obtained if and only if the compensator (9) satisfies the following two equations:

$$(\hat{V}_0 - Q_2 N_1 - Q_3 N_2)M$$
$$- (\hat{U}_0, 1, Q_1, N_2 - Q_2 M, \hat{U}_0, 2 + Q_1, N_1 - Q_3 M)$$
$$= V_0 M - \hat{U}_0, N_1 + Q_1, N_2 - Q_3 M$$

and

$$(\hat{V}_0 - Q_2 N_1 - Q_3 N_2)M$$
$$- (\hat{U}_0, 1, Q_1, N_2 - Q_2 M, \hat{U}_0, 2 + Q_1, N_1 - Q_3 M)$$
$$= V_0 M - \hat{U}_0, N_1 + Q_1, N_2 - Q_3 M.$$  (10)

The existence of a fault tolerant controller has now been shown to be inferred from the existence of stable proper rational functions $Q_1, Q_2, Q_3$, such that $u_1, u_2$ become units. We will prove this existence by first choosing $Q_1$ appropriately. Subsequently, (10) and (11) will be considered as equations for $Q_3$ and $Q_2$, which are no longer coupled, and show that each has an admissible solution.

To that end, first note that it is possible to determine a stabilizing proper function $Q_1$, such that:

$$Q_1(s)N_1(s)N_2(s) - \hat{U}_0, 1(s)\hat{U}_0, 1(s)\,|_{z_1 p} = \frac{1}{2}$$  (12)

for every value of $z_1 p \in \{z \in \mathbb{R} : M(z) = 0\}$, since $N_1(z_1 p)N_2(z_1 p)$ can not be zero for $M(z_1 p) = 0$ due to coprimeness of $M$ and $N_1$ and of $M$ and $N_2$. To determine $Q_1$ satisfying (12) in practice can be done by a standard rational interpolation.

Now, for a fixed $Q_1$, (10) can be recognized as a strong stabilization problem in the variable $Q_3$. It is known from Lemma 1 that such $Q_3$ exists if and only if

$$V_0 M - \hat{U}_0, N_1 + Q_1, N_2 - u_1 |_{z_1 p}$$

has constant sign for every value of $z_1 p \in \{z \in \mathbb{R} : M(z) = 0\}$ or $N_2(z) = 0$.

For $M(z_1 p) = 0$, we obtain

$$V_0(s)M(s) - \hat{U}_0, 1(s), N_1(s) + Q_1(s)N_2(s)N_1(s) |_{z_1 p} = \frac{1}{2}$$  (13)

from (12). For $N_2(z_1 p) = 0$, we get

$$V_0(s)M(s) - \hat{U}_0, 1(s), N_1(s) + Q_1(s)N_2(s)N_1(s) |_{z_1 p} = \frac{1}{2}$$  (14)

where (8) has been applied. This proves the existence of an admissible function $Q_3$. To determine $Q_3$ in practice, one approach is first to find $u_1$ that interpolates the constraints (13) and (14), and subsequently to determine $Q_3$ as a solution to (10). If $u_1$ in addition is chosen to interpolate all constraints arising from zeros of $M$ and $N_2$ in the right half plane (not just the positive half line), $Q_3$ can be computed by

$$Q_3 = \frac{V_0 M - \hat{U}_0, 1(s) + Q_1(s)N_2(s) |_{z_1 p}}{N_2 M}.$$  (15)

The proof of existence of an admissible $Q_2$ is completely analogous to the proof of existence of $Q_3$. The interpolation constraints for (11) corresponding to $M(z_1 p) = 0$ amounts to

$$V_0(s)M(s) - \hat{U}_0, 2(s)N_2(s) - Q_1(s)N_1(s)N_2(s) |_{z_1 p} = \frac{1}{2}$$

from (8), $Q_2$ can now be found as a solution to (11), and the resulting $u_2$ will interpolate the conditions (16) and (17). Again, $Q_2$ might be computed by first finding $u_2$ interpolating all constraints arising from zeros of $M$ and $N_1$ in the right half plane [not just (16) and (17)], and then computing $Q_2$ as

$$Q_2 = \frac{V_0 M - \hat{U}_0, 2(s)N_2 - Q_1(s)N_1(s) - u_2}{N_1 M}.$$  (18)
Thus, one possible fault tolerant compensator is
\[
K = (\hat{V}_0 - Q_2N_1 - Q_3N_2)^{-1} \\
\times (\hat{U}_{0,1} + \hat{Q}_1N_2 - \hat{Q}_3M \times \hat{U}_{0,2} + Q_1N_1 - Q_3M)
\]  
which stabilizes the system given by (6) in the nominal case, as well as in the case, where one of the two sensors fail. 

A corresponding result for actuator failures follows trivially from Theorem 1 by duality.

Theorem 2: Consider a system given by a state-space model of the form
\[
\hat{x} = Ax + B_1u_1 + \cdots + B_mu_m \\
y = Cx
\]
where \( x \in \mathbb{R}^n, u_i \in \mathcal{R}, i = 1, \ldots, m, y \in \mathbb{R}^{p} \) and \( A, B_i, i = 1, \ldots, m, C \) are matrices of compatible dimensions. Assume, that each of the pairs \((A, B_i), i = 1, \ldots, m,\) is stabilizable and that the pair \((C, A)\) is detectable. Then, there exists a dynamic compensator \(K(s)\) such that the nominal control law
\[
u = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_m \end{pmatrix} = K(s)y
\]
as well as each of the \(m\) control laws
\[
u = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_m \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_m \end{pmatrix}
\]
internally stabilizes (20).

Proof: Follows by transposing the system and the compensator.

It is interesting to note that it might be necessary to resort to arbitrarily high controller orders even for a system of low order. As an example, consider for \( \varepsilon > 0 \)
\[
G_\varepsilon(s) = \frac{s - (1 + \varepsilon)}{s + 1}
\]
with the following coprime factorization:
\[
G_\varepsilon(s) = N(s)M(s)^{-1} = \left( \frac{s - (1 + \varepsilon)}{s + 1} \right)^{-1}
\]
for which the fault tolerant control problem is equivalent to finding \(K(s) = V^{-1}(U_1 \hat{U}_1)\) such that
\[
\hat{V} \frac{s - (1 + \varepsilon)}{s + 1} - \hat{U}_1 \frac{s - 1}{(s + 1)^2} - \hat{U}_2 \frac{s - 1}{(s + 1)^2} = u_1 \\
\hat{V} \frac{s - (1 + \varepsilon)}{s + 1} - \hat{U}_1 \frac{s - 1}{(s + 1)^2} = u_2 \\
\hat{V} \frac{s - (1 + \varepsilon)}{s + 1} - \hat{U}_1 \frac{s - 1}{(s + 1)^2} = u_3
\]
where \(u_1, u_2, u_3\) are all units in the ring of stable proper functions.

Evaluating these equations at \(s = 1\) at \(s = \infty\), we notice that
\[
u_1(1) = u_2(1) = u_3(1) \quad \text{and} \quad \nu_1(\infty) = u_2(\infty) = u_3(\infty).
\]
On the other hand, we also have
\[
u_1(1 + \varepsilon) = u_2(1 + \varepsilon) + u_3(1 + \varepsilon).
\]
Thus, one possible fault tolerant compensator is
\[
K = (\hat{V}_0 - Q_2N_1 - Q_3N_2)^{-1} \\
\times (\hat{U}_{0,1} + \hat{Q}_1N_2 - \hat{Q}_3M \times \hat{U}_{0,2} + Q_1N_1 - Q_3M)
\]
which stabilizes the system given by (6) in the nominal case, as well as in the case, where one of the two sensors fail.

The constraint at infinity, means that we can assume \(v_2\) to be of the form
\[
v_2(s) = \frac{s^n + \alpha_1s^{n-1} + \cdots + \alpha_n}{s^n + \beta_1s^{n-1} + \cdots + \beta_n}
\]
for some \(n\), which leads to the conditions
\[
1 + \alpha_1 + \cdots + \alpha_n = 1 + \beta_1 + \cdots + \beta_n
\]
and
\[
(1 + \varepsilon)^n + \cdots + (1 + \varepsilon)^{n-1}\alpha_1 + \cdots + (1 + \varepsilon)^{n-1}\beta_1
\]
\[= \gamma(1 + \varepsilon)^n + \cdots + \gamma(1 + \varepsilon)^{n-1}\beta_1 + \cdots + \gamma\beta_n.
\]
Subtracting (24) from (25) gives
\[
(1 + \varepsilon)^n - 1 + (1 + \varepsilon)^{n-1} - 1 = \gamma(1 + \varepsilon)^{n-1} - 1 \beta_1 + \cdots + (\gamma - 1)\beta_n.
\]
We remind the reader, that a necessary condition for (23) to be a unit is that \(\alpha_i > 0, \beta_i > 0, i = 1, \ldots, n\). Thus, all the terms on the left hand side of (26) are positive. This means, however, that (26) can only be true if
\[
\log 2 \frac{\log(1 + \varepsilon)}{\varepsilon} \rightarrow \infty \quad \text{for} \quad \varepsilon \rightarrow 0_+.
\]
From (22), we obtain
\[
u_2 = \frac{\hat{V} \frac{s - (1 + \varepsilon)}{s + 1} - \hat{U}_2 \frac{s - 1}{(s + 1)^2}}{\hat{V} \frac{s - (1 + \varepsilon)}{s + 1} - \hat{U}_2 \frac{s - 1}{(s + 1)^2} - \hat{U}_1 \frac{s - 1}{(s + 1)^2} = u_3}
\]
where \(u_1, u_2, u_3\) are all units in the ring of stable proper functions.

Evaluating these equations at \(s = 1\) at \(s = \infty\), we notice that
\[
u_1(1) = u_2(1) = u_3(1) \quad \text{and} \quad \nu_1(\infty) = u_2(\infty) = u_3(\infty).
\]
On the other hand, we also have
\[
u_1(1 + \varepsilon) = u_2(1 + \varepsilon) + u_3(1 + \varepsilon).
\]
Let us define the units \(v_2 = u_2/u_1\) and \(v_3 = u_3/u_1\). Then, we have
\[
v_2(1) = v_3(1) = 1 \\
v_2(\infty) = v_3(\infty) = 1 \\
v_2(1 + \varepsilon) + v_3(1 + \varepsilon) = 1.
\]
From the last equation, we infer that either \(v_2(1 + \varepsilon) \leq 1/2\) or \(v_3(1 + \varepsilon) \leq 1/2\). Assume without loss of generality that \(v_2(1 + \varepsilon) \leq 1/2\). Then, \(v_2\) is a unit such that
\[
v_2(1) = 1 \quad \gamma := v_2(1 + \varepsilon) \leq 1/2 \quad \text{and} \quad v_2(\infty) = 1.
\]
V. FAULT TOLERANT CONTROL DESIGN EXAMPLE

In this section, we shall apply the method of the constructive existence proof for a system which is only of second order, but yet difficult to reliably stabilize
\[
\dot{x} = \begin{pmatrix} 3 & 0 \\ -1 & -1 \end{pmatrix} x + \begin{pmatrix} 1 \\ 0 \end{pmatrix} u \\
y_1 = \begin{pmatrix} 1 & 2 \end{pmatrix} x \\
y_2 = \begin{pmatrix} 1 & 3 \end{pmatrix} x.
\]
This system has a stable pole in \(-1\) and an unstable pole in 3. The transfer function from \(u\) to \(y_1\) has a zero in 1, whereas the transfer function from \(u\) to \(y_2\) has a zero in 2.
The objective is now to find a compensator $K(s)$, such that all the three control laws
\[ u = K(s) \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}, \quad u = K(s) \begin{pmatrix} 0 \\ y_2 \end{pmatrix}, \quad u = K(s) \begin{pmatrix} y_1 \\ 0 \end{pmatrix} \]
internally stabilize (27).

We will find the doubly coprime factorization by designing an observer based compensator. One possible observer gain matrix (there are infinitely many) that assigns the observer poles to the set \{-2, -1\} is the following gain:
\[ L = \begin{pmatrix} -12 & 8 \\ 4 & -3 \end{pmatrix}. \]
The (unique) feedback gain that also assigns poles to the set \{-2, -1\} is
\[ F = \begin{pmatrix} -5 & 0 \end{pmatrix}. \]
Consequently, the transfer matrix for the system
\[ G(s) = \frac{1}{s^2 - 2s - 3} \begin{pmatrix} s - 1 \\ s - 2 \end{pmatrix} \]
can be written in the following coprime factorization form:
\[ G(s) = \begin{pmatrix} N_1(s) \\ N_2(s) \end{pmatrix} M^{-1}(s) \]
where
\[ M(s) = 1 + F(sI - A - BF)^{-1}B = \frac{s - 3}{s + 2} \]
\[ \begin{pmatrix} N_1(s) \\ N_2(s) \end{pmatrix} = C(sI - A - BF)^{-1}B = \begin{pmatrix} \frac{s - 1}{s + 2} \\ \frac{s^2 + 3s + 2}{s + 2} \end{pmatrix}. \]
The compensator has the following factorization:
\[ K_0 = \tilde{V}_0^{-1}(\tilde{U}_{0,1} \quad \tilde{U}_{0,2}) \]
with
\[ \tilde{V}_0 = 1 - F(sI - A - LC)^{-1}B = \frac{s^2 + 8s + 12}{s^2 + 3s + 2} \]
\[ (\tilde{U}_{0,1} \quad \tilde{U}_{0,2}) = -F(sI - A - LC)^{-1}L = \frac{1}{20}(-3s - 6 \quad 2s + 4). \]

It is easy to verify, that the aforementioned six functions satisfy the Bezout identity
\[ \tilde{V}_0 M - \tilde{U}_{0,1} N_1 - \tilde{U}_{0,2} N_2 = 1. \]
Next, we would like to select $Q_1$ satisfying (12), i.e., such that
\[ Q_1(z_{ip}) N_1(z_{ip}) N_2(z_{ip}) - \tilde{U}_{0,1}(z_{ip}) N_1(z_{ip}) = \frac{1}{2} \]
whenever $M(z_{ip}) = 0$ on the positive real half-line, which in our case means $z_{ip} = 3$. Since we have only one interpolation point, a possible choice of $Q_1(s)$ is a constant
\[ Q_1(s) = \frac{1 + 2\tilde{U}_{0,1}(z_{ip}) N_1(z_{ip})}{2N_1(z_{ip}) N_2(z_{ip})} = -200. \]
The remaining two steps are to solve the two (independent) strong stabilization problems (10) and (11). First, we should find $Q_3$ satisfying (10) where $u_1$ is a stable proper function with a stable proper inverse. The interpolation points are the positive real zeros (including $\infty$) of $N_2$ and of $M$ which are $z_{i=2} = \{2, \infty\}$, $z_{i=3} = 3$, for which we have
\[ V_0(2)M(2) - \tilde{U}_{0,1}(2)N_1(2) + Q_1(2)N_1(2)N_2(2) = 1 \]
\[ V_0(3)M(3) - \tilde{U}_{0,1}(3)N_1(3) + Q_1(3)N_1(3)N_2(3) = \frac{1}{2} \]
\[ V_0(\infty)M(\infty) - \tilde{U}_{0,1}(\infty)N_1(\infty) + Q_1(\infty)N_1(\infty)N_2(\infty) = 1. \]
A possible $u_1$ that interpolates $(2, 3, \infty)$ to $(1, (1/2), 1)$ can be found from the Routh–Hurwitz conditions:
\[ u_1 = \frac{s^3 + 24s^2 + 74s + 1766}{s^3 + 480s^2 + 25s + 40}. \]
Thus, $Q_3$ can be computed from (15) as
\[ Q_3(s) = \frac{\tilde{V}_0 M - \tilde{U}_{0,1} N_1 + Q_1 N_2 - u_1}{N_2 M} = \frac{456 s^4 + 4807 s^3 - 50993 s^2 - 5088 s - 4884}{s^4 + 481 s^3 + 503 s^2 + 65 s + 40}. \]

For the second strong stabilization problem
\[ \tilde{V}_0 M - \tilde{U}_{0,2} N_2 - Q_1 N_1 - Q_2 N_1 M = u_2 \]
the interpolation points are: $z_{i=1} = \{1, \infty\}$, $z_{i=3} = 3$ A possible $u_2$ that interpolates $(1, 3, \infty)$ to $(1, (1/2), 1)$ can be found from the Routh–Hurwitz conditions
\[ u_2 = \frac{s^2 + 2s + 21}{s^2 + 20s + 3} \]
which enables us to compute $Q_2$ from (18) as
\[ Q_2(s) = \frac{\tilde{V}_0 M - \tilde{U}_{0,2} N_2 - Q_1 N_1 N_2 - u_2}{N_1 M} = \frac{18s^3 + 302s^2 + 3420s + 496}{s^4 + 21s^2 + 23s + 3}. \]

Now, we are ready to compute a fault tolerant controller as
\[ K = \left( \begin{pmatrix} \tilde{V}_0 - Q_2 N_1 - Q_3 N_2 \end{pmatrix} \right)^{-1} \]
\[ \times \begin{pmatrix} \tilde{U}_{0,1} - Q_1 N_2 - Q_3 M \end{pmatrix} \tilde{U}_{0,2} + Q_1 N_1 - Q_3 M \]
\[ = \frac{1}{s^4 + 29s^3 - 7978s^2 - 124426s - 2006} \times \begin{pmatrix} 18s^4 + 8658s^3 + 9090s^2 + 1170s + 720 \\ 456s^4 + 10439s^3 + 28611s^2 + 21217s^1 + 2589 \end{pmatrix} \]

It can be verified, that this compensator manages to stabilize both the nominal system, as well as the faulty system, in case either of (but of course not both) the two sensors fails. The stability margin is rather poor, but numerical experience suggests that it can only be improved substantially by going to (even) higher order compensators which was not done, as this example just serves as an illustration of the principle.

VI. CONCLUSION

In this note, we have proved the existence for any given system of a fault tolerant compensator, which stabilizes the system during its normal operating conditions, but also in the case that one of the sensors or actuators would fail.

The proof given was constructive, and it was demonstrated for a simple example that carrying out the steps of the proofs can lead to a fault tolerant compensator. It should be stated, however, that the design process is not easy. Also, in practice, the issue of performance
should be addressed, which can, unfortunately, not easily be done in the framework suggested here.

It was also shown that the dynamical order of any fault tolerant compensator for some systems even of order two might have to be considerably large, due to intrinsic properties of the system.

A subject of future research is to clarify whether the same results hold for systems in which several sensors and actuators (but not all of either kind) can fail simultaneously.

ACKNOWLEDGMENT

The authors did the research on which this note is based during a stay at the Institut Mittag–Leffler, Stockholm, Sweden, in the spring of 2003, under a program entitled Mathematical Control and Systems Theory. They would like to thank the organizers of this Mittag–Leffler program for inviting them. The authors would also like to thank the anonymous reviewers for reading the manuscript with extraordinary care.

REFERENCES


Nonlinear Control Synthesis by Convex Optimization

Stephen Prajna, Pablo A. Parrilo, and Anders Rantzer

Abstract—A stability criterion for nonlinear systems, recently derived by the third author, can be viewed as a dual to Lyapunov’s second theorem. The criterion is stated in terms of a function which can be interpreted as the stationary density of a substance that is generated all over the state–space and flows along the system trajectories toward the equilibrium. The new criterion has a remarkable convexity property, which in this note is used for controller synthesis via convex optimization. Recent numerical methods for verification of positivity of multivariate polynomials based on sum of squares decompositions are used.

Index Terms—Density functions, nonlinear control, semidefinite programming relaxation, sum of squares decomposition.

I. INTRODUCTION

Lyapunov functions have long been recognized as one of the most fundamental analytical tools for analysis and synthesis of nonlinear control systems; see, for example, [2]–[4], 6], [7], and [9].

There has also been a strong development of computational tools based on Lyapunov functions. Many such methods are based on convex optimization and solution of matrix inequalities, exploiting the fact that the set of Lyapunov functions for a given system is convex.

A serious obstacle in the problem of controller synthesis is however that the joint search for a controller $u(x)$ and a Lyapunov function $V(x)$ is not convex. Consider the synthesis problem for the system

$$
\dot{x} = f(x) + g(x)u.
$$

The set of $u$ and $V$ satisfying the condition

$$
\frac{\partial V}{\partial x}[f(x) + g(x)u(x)] < 0
$$

is not convex. In fact, for some systems the set of $u$ and $V$ satisfying the inequality is not even connected [14].

Given the difficulties with Lyapunov based controller synthesis, it is most striking to find that the new convergence criterion presented in [15] based on the so-called density function $\rho$ (cf. Section II) has much better convexity properties. Indeed, the set of $(\rho, u_p)$ satisfying

$$
\nabla \cdot [\rho(f + gu)] > 0
$$

is convex. In this note, we will exploit this fact in the computation of stabilizing controllers. For the case of systems with polynomial or rational vector fields, the search for a candidate pair $(\rho, u_p)$ satisfying the inequality (1) can be done using the methods introduced in [12]. In particular, a recently available software SOSTOOLS [13] can be used for this purpose.