Fault Tolerant Control: A Simultaneous Stabilization Result

Stoustrup, Jakob; Blondel, V.D.

Published in:
IEEE Transactions on Automatic Control

DOI (link to publication from Publisher):
10.1109/TAC.2003.822999

Publication date:
2004

Document Version
Tidlig version også kaldet pre-print

[2] ——, "A generalized entropy criterion for Nevanlinna–Pick interpolation with degree constraint," *IEEE Trans. Automat. Contr.*, vol. 46, pp. 822–839, June 2001.
[3] J. C. Doyle, B. A. Francis, and A. R. Tannenbaum, *Feedback Control Theory*. New York: Macmillan, 1992.
[4] B. A. Francis, *A Course in $\boldsymbol{H}_\infty$ Control Theory*. New York: Springer-Verlag, 1987, Lecture Notes in Control and Information Sciences.
[5] J. W. Helton and O. Marino, *Classical Control Using $\boldsymbol{H}^\infty$ Methods*. Philadelphia, PA: SIAM, 1998.
[6] H. Kwakernaak, "Robust control and $\boldsymbol{H}_\infty$-optimization-Tutorial paper," *Automatica*, vol. 29, no. 2, pp. 255–273, 1993.
[7] D. J. N. Limebeer and B. D. O. Anderson, "An interpolation theory approach to $\boldsymbol{H}^\infty$ controller degree bounds," *Linear Alg. Applicat.*, vol. 98, pp. 347–386, 1988.
[8] R. Nagamune, "A shaping limitation of rational sensitivity functions with a degree constraint," *IEEE Trans. Automat. Contr.*, vol. 49, pp. 296–300, Feb. 2004.
[9] ——, "Robust control with complexity constraint: A Nevanlinna–Pick interpolation approach," Ph.D. dissertation, Dept. Math., Royal Inst. Technol., Stockholm, Sweden, 2002.
[10] ——, "A robust solver using a continuation method for Nevanlinna–Pick interpolation with degree constraint," *IEEE Trans. Automat. Control*, vol. 48, pp. 113–117, Jan. 2003.
[11] J. L. Walsh, *Interpolation and Approximation by Rational Functions in the Complex Domain*. Providence, RI: AMS, 1956, vol. 20.
[12] K. Zhou, *Essential of Robust Control*. Upper Saddle River, NJ: Prentice-Hall, 1998.

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 of 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 accomodate 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, $\mathcal{RP}^{p\times m}$ shall denote the set of proper, real-rational functions taking values in $\mathcal{C}^{p\times m}$, and $\mathcal{RSP}^{p\times m}$ shall denote the set of strictly proper, real-rational functions taking values in $\mathcal{C}^{p\times m}$. $\mathcal{RH}_\infty^{p\times m}$ shall denote the set of stable, proper, real-rational functions taking values in $\mathcal{C}^{p\times m}$. The notation $\{s \in \mathcal{R}_{+\infty} : B(s) = 0\}$ will 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

$$G(s) = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$$

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

$$\begin{aligned} \dot{x} &= Ax + Bu \\ y_1 &= C_1 x \\ &\vdots \\ y_p &= C_p x \end{aligned} \tag{1}$$

where $x \in \mathcal{R}^n, u \in \mathcal{R}^m, y_i \in \mathcal{R}, i = 1\ldots, p$ and $A, B, C_i, i = 1\ldots, p$ are matrices of compatible dimensions. Each of the p measure-

Manuscript received May 9, 2003; revised September 26, 2003. Recommended by Associate Editor F. M. Callier.

J. Stoustrup is with the Department of Control Engineering, Institute of Electronic Systems, Aalborg University, DK-9220 Aalborg, Denmark (e-mail: jakob@control.auc.dk).

V. D. Blondel is with the Department of Mathematical Engineering, Université Catholique de Louvain, B-1348 Louvain-la-Neuve, Belgium (e-mail: blondel@inma.ucl.ac.be).

Digital Object Identifier 10.1109/TAC.2003.822999

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 $u = K(s)y, K \in \mathcal{RP}^{m\times p}$, with the property, that each of the following feedback laws:

$$\begin{array}{ccccc} u = K(s)y & u = K(s)y_{\mathrm{f},1}, & \cdots, & u = K(s)y_{\mathrm{f},p} \\ y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_p \end{pmatrix} & y_{\mathrm{f},1} = \begin{pmatrix} 0 \\ y_2 \\ \vdots \\ y_p \end{pmatrix}, & \cdots, & y_{\mathrm{f},p} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ 0 \end{pmatrix} \end{array} \tag{2}$$

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 to design a compensator, that works in the nominal situation, but also if any of the actuators would fail.

III. Preliminaries

We remind the reader (see, e.g., [12, Th. 5.9, p. 127]) that a doubly coprime factorization of a strictly proper plant and a stabilizing compensator

$$\begin{aligned} G(s) &= N(s)M^{-1}(s) = \tilde{M}^{-1}(s)\tilde{N}(s) \\ K(s) &= U(s)V^{-1}(s) = \tilde{V}^{-1}(s)\tilde{U}(s) \end{aligned}$$

where

$$\begin{array}{ccc} G \in \mathcal{RSP}^{p\times m} & N \in \mathcal{RH}_\infty^{p\times m} & M \in \mathcal{RH}_\infty^{m\times m} \\ & \tilde{M} \in \mathcal{RH}_\infty^{p\times p} & \tilde{N} \in \mathcal{RH}_\infty^{p\times m} \\ K \in \mathcal{RP}^{m\times p} & U \in \mathcal{RH}_\infty^{m\times p} & V \in \mathcal{RP}_\infty^{p\times p} \\ & \tilde{V} \in \mathcal{RH}_\infty^{m\times m} & \tilde{U} \in \mathcal{RH}_\infty^{m\times p} \end{array}$$

can be found from an observer based controller by the formulas

$$\begin{aligned} \begin{pmatrix} M & U \\ N & V \end{pmatrix} &= \left(\begin{array}{c|cc} A+BF & B & -L \\ \hline F & I & 0 \\ C & 0 & I \end{array}\right) \\ \begin{pmatrix} \tilde{V} & \tilde{U} \\ \tilde{N} & \tilde{M} \end{pmatrix} &= \left(\begin{array}{c|cc} A+LC & B & L \\ \hline -F & I & 0 \\ C & 0 & I \end{array}\right) \end{aligned} \tag{3}$$

where A, B, C are parameters for a (minimal) state space representation for $G(s)$, i.e., matrices of smallest, compatible dimensions such that

$$G(s) = \left(\begin{array}{c|c} A & B \\ \hline C & 0 \end{array}\right)$$

F is an arbitrary stabilizing state feedback gain and L is an arbitrary stabilizing observer gain, i.e., F and L are matrices of compatible dimensions such that both $A + BF$ and $A + LC$ have characteristic polynomials which are Hurwitz.

The eight matrices defined by (3) satisfy the double Bezout identity

$$\begin{pmatrix} M & U \\ N & V \end{pmatrix} \begin{pmatrix} \tilde{V} & -\tilde{U} \\ -\tilde{N} & \tilde{M} \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}.$$

We also remind the reader, that a *unit* is an element of a ring, which has an inverse in that ring. In particular, a unit in the ring of stable proper rational functions, is simply a stable proper function with a stable proper inverse.

We will need the following result (see [13, Th. 5.2, p. 106] or [11, Cor. 6, p. 118]) on the strong stabilization problem, i.e., the problem of finding a stable stabilizing compensator.

Lemma 1: Let $A(s),\ B(s)$ be stable proper transfer functions. Then there exists a stable proper transfer function $Q(s)$ such that the function

$$A(s) + B(s)Q(s)$$

is a unit in the ring of stable proper rational functions, if and only if $A(z_{\mathrm{ip}})$ has constant sign for all $z_{\mathrm{ip}} \in \{s \in \mathcal{R}_{+\infty} : B(s) = 0\}$.

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 precondition 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

$$\begin{aligned} \dot{x} &= Ax + \bar{B}\bar{u} \\ y_1 &= C_1 x \\ &\vdots \\ y_p &= C_p x \end{aligned} \tag{4}$$

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

$$K(s) = (K_1(s) \quad K_2(s)) \tag{5}$$

is a fault tolerant feedback compensator for this system

$$\begin{aligned} \dot{x} &= Ax + Bu \\ y_1 &= C_1 x \\ y_2 &= C_2 x \end{aligned} \tag{6}$$

then

$$K(s) = (K_1(s) \quad K_2(s) \quad 0 \quad \cdots \quad 0) \tag{7}$$

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, $u, y_i \in \mathcal{R}, i = 1, 2$. Thus, it will

be assumed that the transfer functions from u to each of the outputs are scalar.

Define $C = \begin{pmatrix} C_1 \\ C_2 \end{pmatrix}$ 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 $M, N, \tilde{V}_0, \tilde{U}_0$

$$G(s) = N(s)M^{-1}(s) = \begin{pmatrix} N_1(s) \\ N_2(s) \end{pmatrix} M^{-1}(s)$$
$$K_0(s) = \tilde{V}_0^{-1}(s)\tilde{U}_0(s) = \tilde{V}_0^{-1}(s)(\tilde{U}_{0,1}(s) \quad \tilde{U}_{0,2}(s))$$

satisfying the Bezout identity

$$\tilde{V}_0 M - \tilde{U}_0 N = \tilde{V}_0 M - \tilde{U}_{0,1}N_1 - \tilde{U}_{0,2}N_2 = 1. \tag{8}$$

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

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

$$(\tilde{V}_0 \quad \tilde{U}_{0,1} \quad \tilde{U}_{0,2}) \quad \text{by} \quad (\tilde{V} \quad \tilde{U}_1 \quad \tilde{U}_2)$$

where

$$\begin{aligned} \tilde{V} &= \tilde{V}_0 - Q_2N_1 - Q_3N_2 \\ \tilde{U}_1 &= \tilde{U}_{0,1} - Q_1N_2 - Q_2M \\ \tilde{U}_2 &= \tilde{U}_{0,2} + Q_1N_1 - Q_3M \end{aligned}$$

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

$$\begin{aligned} &\tilde{V}M - \tilde{U}_1N_1 - \tilde{U}_2N_2 \\ &\quad = (\tilde{V}_0 - Q_2N_1 - Q_3N_2)M - (\tilde{U}_{0,1} - Q_1N_2 - Q_2M)N_1 \\ &\qquad - (\tilde{U}_{0,2} + Q_1N_1 - Q_3M)N_2 \\ &\quad = \tilde{V}_0M - \tilde{U}_{0,1}N_1 - \tilde{U}_{0,2}N_2 = 1. \end{aligned}$$

Consequently, any transfer function of the form

$$\begin{aligned} \tilde{V}^{-1}(\tilde{U}_1 \quad \tilde{U}_2) &= (\tilde{V}_0 - Q_2N_1 - Q_3N_2)^{-1} \\ &\quad \times (\tilde{U}_{0,1} - Q_1N_2 - Q_2M \quad \tilde{U}_{0,2} + Q_1N_1 - Q_3M) \end{aligned} \tag{9}$$

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 $\tilde{V}^{-1}(\tilde{U}_1 \ \tilde{U}_2)$ stabilizes both the nominal and the faulty systems.

If the sensor corresponding to one of the outputs fails, the controller $\tilde{V}^{-1}(\tilde{U}_1 \ \tilde{U}_2)$ 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:

$$\begin{aligned} &(\tilde{V}_0 - Q_2N_1 - Q_3N_2)M \\ &\quad - (\tilde{U}_{0,1} - Q_1N_2 - Q_2M \quad \tilde{U}_{0,2} \\ &\quad + Q_1N_1 - Q_3M)\begin{pmatrix} N_1 \\ 0 \end{pmatrix} \\ &\quad = \tilde{V}_0M - Q_2N_1M - Q_3N_2M \\ &\qquad - \tilde{U}_{0,1}N_1 + Q_1N_2N_1 + Q_2MN_1 \\ &\quad = \tilde{V}_0M - \tilde{U}_{0,1}N_1 + Q_1N_2N_1 - Q_3N_2M = u_1 \end{aligned} \tag{10}$$

and

$$\begin{aligned} &(\tilde{V}_0 - Q_2N_1 - Q_3N_2)M \\ &\quad - (\tilde{U}_{0,1} - Q_1N_2 - Q_2M \quad \tilde{U}_{0,2} \\ &\quad + Q_1N_1 - Q_3M)\begin{pmatrix} 0 \\ N_2 \end{pmatrix} \\ &\quad = \tilde{V}_0M - \tilde{U}_{0,2}N_2 - Q_1N_1N_2 - Q_2N_1M = u_2 \end{aligned} \tag{11}$$

where u_1, u_2 are units in the ring of stable proper rational functions.

Thus, 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 stable proper function Q_1, such that:

$$Q_1(s)N_1(s)N_2(s) - \tilde{U}_{0,1}(s)N_1(s)|_{s=z_{\rm ip}} = \frac{1}{2} \tag{12}$$

for every value of $z_{\rm ip} \in \{z \in \mathcal{R}_{+\infty} : M(z) = 0\}$, since $N_1(z_{\rm ip})N_2(z_{\rm ip})$ can not be zero for $M(z_{\rm ip}) = 0$ 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

$$\tilde{V}_0M - \tilde{U}_{0,1}N_1 + Q_1N_2N_1|_{s=z_{\rm ip}}$$

has constant sign for every value of

$$z_{\rm ip} \in \{z \in \mathcal{R}_{+\infty} : M(z) = 0 \quad \text{or} \quad N_2(z) = 0\}.$$

For $M(z_{\rm ip}) = 0$, we obtain

$$\begin{aligned} &\tilde{V}_0(s)M(s) - \tilde{U}_{0,1}(s)N_1(s) + Q_1(s)N_2(s)N_1(s)|_{s=z_{\rm ip}} \\ &\qquad = -\tilde{U}_{0,1}(s)N_1(s) + Q_1(s)N_2(s)N_1(s)|_{s=z_{\rm ip}} = \frac{1}{2} \end{aligned} \tag{13}$$

from (12). For $N_2(z_{\rm ip}) = 0$, we get

$$\begin{aligned} &\tilde{V}_0(s)M(s) - \tilde{U}_{0,1}(s)N_1(s) + Q_1(s)N_2(s)N_1(s)|_{s=z_{\rm ip}} \\ &\qquad = \tilde{V}_0(s)M(s) - \tilde{U}_{0,1}(s)N_1(s)|_{s=z_{\rm ip}} = 1 \end{aligned} \tag{14}$$

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

$$Q_3 = \frac{\tilde{V}_0M - \tilde{U}_{0,1}N_1 + Q_1N_2N_1 - u_1}{N_2M}. \tag{15}$$

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 $M(z_{\rm ip}) = 0$ amounts to

$$\begin{aligned} &\tilde{V}_0(s)M(s) - \tilde{U}_{0,2}(s)N_2(s) - Q_1(s)N_1(s)N_2(s)|_{s=z_{\rm ip}} \\ &\quad = -\tilde{U}_{0,2}(s)N_2(s) - Q_1(s)N_1(s)N_2(s)|_{s=z_{\rm ip}} \\ &\quad = 1 - \tilde{V}_0(s)M(s) + \tilde{U}_{0,1}(s)N_1(s) \\ &\qquad - Q_1(s)N_1(s)N_2(s)|_{s=z_{\rm ip}} \\ &\quad = 1 - \frac{1}{2} = \frac{1}{2} \end{aligned} \tag{16}$$

where (8) and (12) has been exploited. For $N_1(z_{\rm ip}) = 0$, we obtain the constraints

$$\begin{aligned} \tilde{V}_0(s)M(s) - \tilde{U}_{0,2}(s)N_2(s)|_{s=z_{\rm ip}} &= \tilde{V}_0(s)M(s) \\ &\quad - \tilde{U}_{0,2}(s)N_2(s) - Q_1(s)N_1(s)N_2(s)|_{s=z_{\rm ip}} = 1 \end{aligned} \tag{17}$$

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

$$Q_2 = \frac{\tilde{V}_0M - \tilde{U}_{0,2}N_2 - Q_1N_1N_2 - u_2}{N_1M}. \tag{18}$$

Thus, one possible fault tolerant compensator is

$$K = (\tilde{V}_0 - Q_2 N_1 - Q_3 N_2)^{-1} \times (\tilde{U}_{0,1} - Q_1 N_2 - Q_2 M \quad \tilde{U}_{0,2} + Q_1 N_1 - Q_3 M) \tag{19}$$

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

$$\begin{aligned} \dot{x} &= Ax + B_1 u_1 + \cdots + B_m u_m \\ y &= Cx \end{aligned} \tag{20}$$

where $x \in \mathcal{R}^n, u_i \in \mathcal{R}, i = 1 \ldots, m, y \in \mathcal{R}^p$ 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

$$u = \begin{pmatrix} 0 \\ u_2 \\ \vdots \\ u_m \end{pmatrix} \quad u = \begin{pmatrix} u_1 \\ 0 \\ \vdots \\ u_m \end{pmatrix}, \quad \cdots, \quad u = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ 0 \end{pmatrix}$$

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 $\varepsilon > 0$

$$G_\varepsilon(s) = \begin{pmatrix} \frac{s-1}{(s-(1+\varepsilon))(s+1)} \\ \frac{s-1}{(s-(1+\varepsilon))(s+1)} \end{pmatrix} \tag{21}$$

with the following coprime factorization:

$$G_\varepsilon(s) = N(s)M(s)^{-1} = \begin{pmatrix} \frac{s-1}{(s+1)^2} \\ \frac{s-1}{(s+1)^2} \end{pmatrix} \left(\frac{s-(1+\varepsilon)}{s+1} \right)^{-1}$$

for which the fault tolerant control problem is equivalent to finding $K(s) = \tilde{V}^{-1}(\tilde{U}_1 \ \tilde{U}_2)$ such that

$$\begin{aligned} \tilde{V}\frac{s-(1+\varepsilon)}{s+1} - \tilde{U}_1 \frac{s-1}{(s+1)^2} - \tilde{U}_2 \frac{s-1}{(s+1)^2} &= u_1 \\ \tilde{V}\frac{s-(1+\varepsilon)}{s+1} - 0 - \tilde{U}_2 \frac{s-1}{(s+1)^2} &= u_2 \\ \tilde{V}\frac{s-(1+\varepsilon)}{s+1} - \tilde{U}_1 \frac{s-1}{(s+1)^2} - 0 &= u_3 \end{aligned} \tag{22}$$

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

$$u_1(1) = u_2(1) = u_3(1) \quad \text{and} \quad u_1(\infty) = u_2(\infty) = u_3(\infty).$$

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

$$\begin{aligned} v_2(1) = v_3(1) = 1 \\ v_2(\infty) = v_3(\infty) = 1 \quad v_2(1+\varepsilon) + v_3(1+\varepsilon) = 1. \end{aligned}$$

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

$$v_2(1) = 1 \quad \gamma := v_2(1+\varepsilon) \leq \frac{1}{2} \quad \text{and} \quad v_2(\infty) = 1.$$

The constraint at infinity, means that we can assume v_2 to be of the form

$$v_2(s) = \frac{s^n + \alpha_1 s^{n-1} + \cdots + \alpha_n}{s^n + \beta_1 s^{n-1} + \cdots + \beta_n} \tag{23}$$

for some n, which leads to the conditions

$$1 + \alpha_1 + \cdots + \alpha_n = 1 + \beta_1 + \cdots + \beta_n \tag{24}$$

and

$$\begin{aligned} &(1+\varepsilon)^n + (1+\varepsilon)^{n-1}\alpha_1 + \cdots + \alpha_n \\ &\quad = \gamma(1+\varepsilon)^n + \gamma(1+\varepsilon)^{n-1}\beta_1 + \cdots + \gamma\beta_n. \end{aligned} \tag{25}$$

Subtracting (24) from (25) gives

$$\begin{aligned} &(1+\varepsilon)^n - 1 \\ &\quad + ((1+\varepsilon)^{n-1} - 1)\alpha_1 + \cdots + ((1+\varepsilon) - 1)\alpha_{n-1} \\ &= (\gamma(1+\varepsilon)^n - 1) + (\gamma(1+\varepsilon)^{n-1} - 1)\beta_1 \\ &\quad + \cdots + (\gamma - 1)\beta_n. \end{aligned} \tag{26}$$

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

$$(1+\varepsilon)^n > \frac{1}{\gamma} \geq 2$$

or, equivalently

$$n > \frac{\log 2}{\log(1+\varepsilon)} \to \infty \quad \text{for} \quad \varepsilon \to 0_+.$$

From (22), we obtain

$$\begin{aligned} v_2 = \frac{u_2}{u_1} &= \frac{\tilde{V}\frac{s-(1+\varepsilon)}{s+1} - \tilde{U}_2 \frac{s-1}{(s+1)^2}}{\tilde{V}\frac{s-(1+\varepsilon)}{s+1} - \tilde{U}_1 \frac{s-1}{(s+1)^2} - \tilde{U}_2 \frac{s-1}{(s+1)^2}} \\ &= \frac{(s-(1+\varepsilon))(s+1) - (s-1)\tilde{V}^{-1}\tilde{U}_2}{(s-(1+\varepsilon))(s+1) - (s-1)\tilde{V}^{-1}\tilde{U}_1 - (s-1)\tilde{V}^{-1}\tilde{U}_2}. \end{aligned}$$

Since the order of the left-hand side of this equation tends to infinity as ε tends to zero, clearly also the order either of $\tilde{V}^{-1}\tilde{U}_1$ or of $\tilde{V}^{-1}\tilde{U}_2$ has to tend to infinity.

Thus, the order of the resulting controller can be required to be of arbitrarily high order even for this family of second-order systems.

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

$$\begin{aligned} \dot{x} &= \begin{pmatrix} 3 & 0 \\ -1 & -1 \end{pmatrix} x + \begin{pmatrix} 1 \\ 0 \end{pmatrix} u \\ y_1 &= (1 \quad 2)x \\ y_2 &= (1 \quad 3)x. \end{aligned} \tag{27}$$

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

$$F = (-5 \quad 0).$$

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

$$M(s) = 1 + F(sI - A - BF)^{-1}B = \frac{s-3}{s+2}$$
$$\begin{pmatrix} N_1(s) \\ N_2(s) \end{pmatrix} = C(sI - A - BF)^{-1}B = \begin{pmatrix} \frac{s-1}{s^2+3s+2} \\ \frac{s-2}{s^2+3s+2} \end{pmatrix}.$$

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 satify 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

$$Q_1(z_{\rm ip})N_1(z_{\rm ip})N_2(z_{\rm ip}) - \tilde{U}_{0,1}(z_{\rm ip})N_1(z_{\rm ip}) = \frac{1}{2}$$

whenever $M(z_{\rm ip}) = 0$ on the positive real half-line, which in our case means $z_{\rm ip} = 3$. Since we have only one interpolation point, a possible choice of $Q_1(s)$ is a constant

$$Q_1(s) = \frac{1 + 2\tilde{U}_{0,1}(z_{\rm ip})N_1(z_{\rm ip})}{2N_1(z_{\rm ip})N_2(z_{\rm ip})} = -200.$$

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 ∞) of N_2 and of M which are $z_{N_2} = \{2, \infty\}$, $z_M = 3$, for which we have

$$\tilde{V}_0(2)M(2) - \tilde{U}_{0,1}(2)N_1(2) + Q_1(2)N_1(2)N_2(2) = 1$$
$$\tilde{V}_0(3)M(3) - \tilde{U}_{0,1}(3)N_1(3) + Q_1(3)N_1(3)N_2(3) = \frac{1}{2}$$
$$\tilde{V}_0(\infty)M(\infty) - \tilde{U}_{0,1}(\infty)N_1(\infty) + Q_1(\infty)N_1(\infty)N_2(\infty) = 1.$$

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

$$Q_3(s) = \frac{\tilde{V}_0 M - \tilde{U}_{0,1}N_1 + Q_1N_1N_2 - u_1}{N_2M} = \frac{456s^4 + 4807s^3 - 50\,993s^2 - 5888s - 4884}{s^4 + 481s^3 + 505s^2 + 65s + 40}.$$

For the second strong stabilization problem

$$\tilde{V}_0 M - \tilde{U}_{0,2}N_2 - Q_1N_1N_2 - Q_2N_1M = u_2$$

the interpolation points are: $z_{N_1} = \{1, \infty\}, z_M = 3$ A possible u_2 that interpolates $(1, 3, \infty)$ to $(1, (1/2), 1)$ can be found from the Routh–Hurwitz conditions

$$u2 = \frac{s^2 + 2s + 21}{s^2 + 20s + 3}$$

which enables us to compute Q_2 from (18) as

$$Q_2(s) = \frac{\tilde{V}_0 M - \tilde{U}_{0,2}N_2 - Q_1N_1N_2 - u_2}{N_1M} = \frac{18s^3 + 302s^2 + 3420s + 496}{s^3 + 21s^2 + 23s + 3}.$$

Now, we are ready to compute a fault tolerant controller as

$$K = (\tilde{V}_0 - Q_2N_1 - Q_3N_2)^{-1} \times (\tilde{U}_{0,1} - Q_1N_2 - Q_2M \quad \tilde{U}_{0,2} + Q_1N_1 - Q_3M) = -\frac{1}{s^4 + 29s^3 - 7978s^2 - 12\,426s - 2006} \times \begin{pmatrix} 18s^4 + 8658s^3 + 9090s^2 + 1170s + 720 \\ 456s^4 + 10\,439s^3 + 28\,611s^2 + 21\,217s^1 + 2589 \end{pmatrix}^T.$$

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

[1] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault-Tolerant Control*. New York: Springer-Verlag, 2003.

[2] H. Niemann and J. Stoustrup, "An architecture for fault tolerant controllers," , Jan. 2003.

[3] ——, "Passitive fault tolerant control of an inverted double pendulum—A case study example," in *Proc. IFAC SAFEPROCESS 2003*, Washington, DC, 2003, p. 6.

[4] ——, "Reliable control using the primary and dual Youla parameterization," in *Proc. 41st IEEE Conf. Decision Control*, Las Vegas, NV, 2002, pp. 4353–4358.

[5] J. Stoustrup and H. Niemann, "Fault tolerant feedback control using the youla parameterization," in *Proc. 6th Eur. Control Conf.*, Porto, Portugal, Sept. 2001.

[6] R. Pattern, "Fault tolerant control: The 1997 situation," in *Proc. IFAC Symp. SAFEPROCESS'97*, Hull, U.K., 1997, pp. 1033–1055.

[7] N. Wu, Y. Zhang, and K. Zhou, "Detection, estimation and accommodation of loss of control effectiveness," *Int. J. Adapt. Control, Signal Processing*, vol. 14, pp. 775–795, 2000.

[8] N. Wu, K. Zhou, and G. Salomon, "Control reconfigurability of linear time-invariant systems," *Automatica*, vol. 36, pp. 1767–1771, 2000.

[9] K. Zhou and Z. Ren, "A new controller architecture for high performance robust, and fault-tolerant control," *IEEE Trans. Automat. Contr.*, vol. 46, pp. 1613–1618, Oct. 2001.

[10] A. Alos, "Stabilization of a class of plants with possible loss of outputs or actuator failures," *IEEE Trans. Automat. Contr.*, vol. AC-28, pp. 231–233, Feb. 1983.

[11] M. Vidyasagar, *Control System Synthesis: A Factorization Approach*. Cambridge, MA: MIT Press, 1987.

[12] K. Zhou, J. Doyle, and K. Glover, *Robust and Optimal Control*. Upper Saddle River, NJ: Prentice-Hall, 1996.

[13] V. Blondel, *Simultaneous Stabilization of Linear Systems*, ser. Lecture Notes in Control and Information Sciences. Heidelberg, Germany: Springer-Verlag, 1994.

[14] W. Wonham, *Linear Multivariable Control: A Geometric Approach*. New York: Springer-Verlag, 1979.

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 ρ (cf. Section II) has much better convexity properties. Indeed, the set of $(\rho, u\rho)$ satisfying

$$\nabla \cdot [\rho(f + gu)] > 0 \tag{1}$$

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 $(\rho, u\rho)$ 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.

Manuscript received November 6, 2002; revised August 29, 2003. Recommended by Associate Editor W. Kang. This work was supported by an exchange grant from the Swedish Foundation for International Cooperation in Research and Higher Education. The work of A. Rantzer was supported by the Swedish Research Council.

S. Prajna is with Control and Dynamical Systems, California Institute of Technology, Pasadena, CA 91125, USA (e-mail: prajna@cds.caltech.edu).

P. A. Parrilo is with the Automatic Control Laboratory, ETH Zürich, CH-8092 Zürich, Switzerland (e-mail: parrilo@aut.ee.ethz.ch).

A. Rantzer is with the Department of Automatic Control, Lund Institute of Technology, S-221 00 Lund, Sweden (e-mail: rantzer@control.lth.se).

Digital Object Identifier 10.1109/TAC.2003.823000