

COMPLEXITY OF OUTPUT FEEDBACK STABILIZATION

AMIR ALI AHMADI*, ABRAAR CHAUDHRY†, IJAY NARANG‡, AND YUKAI TANG*

ABSTRACT. We show that unless $P = NP$, there cannot be a polynomial-time (or even pseudo-polynomial-time) algorithm for output feedback stabilization of a linear dynamical system with a linear controller. This settles one of the best-known open problems in control theory. The result holds in both continuous and discrete time. We also present a family of stabilizable linear dynamical systems for which no polynomial-time algorithm can write down a stabilizing controller in its standard representation.

AI Declaration: On August 2, 2026, the authors realized that ChatGPT 5.6 could produce a one-shot proof of NP-hardness of output feedback stabilization. However, this proof and its initial variants were long and hard to verify, relied on techniques unfamiliar to us, and offered little intuition. We have since worked hand in hand with this tool to simplify the proof, make it more interpretable, and base it on tools familiar to most control theorists. This involved proposing plausible proof techniques, checking the resulting arguments, and replacing some with our own. The current proof gives a reduction directly from 3SAT, making the combinatorial source of the hardness clear. It also relies on nothing but basic matrix analysis and linear systems theory. The same general approach was applied to all results in this paper and the authors assume responsibility for all content. We believe that, given the remarkable pace of AI’s progress in automated theorem proving, an emerging role for mathematicians is to teach AI which proofs come closer to being, as Erdős put it, from “The Book.”

1. INTRODUCTION

A real matrix is *Hurwitz* if all its eigenvalues have negative real parts, and *Schur* if all its eigenvalues lie in the open unit disk in the complex plane. For matrices $A \in \mathbb{Q}^{N \times N}$, $B \in \mathbb{Q}^{N \times p}$, and $C \in \mathbb{Q}^{q \times N}$, the *output feedback stabilization* problem in continuous time (resp. discrete time) asks whether there exists some $K \in \mathbb{R}^{p \times q}$ that makes $A + BKC$ Hurwitz (resp. Schur). This amounts to asymptotically stabilizing the linear dynamical system $\dot{x} = Ax + Bu$, $y = Cx$, or its discrete-time analogue, using a static linear control law $u = Ky$ that maps the observed output y of the system to the control u . When the answer to this question is positive, one often also hopes to find a stabilizing “feedback gain” matrix K .

In their 1995 survey, Blondel, Gevers, and Lindquist [1] described output feedback stabilization as “the most often mentioned specific open problem” in systems and control theory. When C is the identity matrix, the problem reduces to *state feedback stabilization* and admits an efficient test based on the stabilizability of the pair (A, B) [8], or a polynomial-size semidefinite programming formulation that can also recover the feedback gain matrix [3, Section 7.2.1]. In general, one can reformulate the output feedback stabilization problem as the problem of testing the feasibility of a system of polynomial inequalities¹ and hence the problem admits exponential-time algorithms; see,

*Princeton University, Department of Operations Research and Financial Engineering. Partially supported by the Princeton AI Lab Seed Grant, the Princeton SEAS Innovation Grant, and a Research Gift in Mathematical Optimization. Email: aaa@princeton.edu, yt3846@princeton.edu.

†University of Colorado Boulder, Department of Applied Math. Email: abraar.chaudhry@colorado.edu.

‡Georgia Institute of Technology, School of Computer Science. Email: inarang3@gatech.edu.

¹Such a formulation can be obtained, for example, by jointly searching for the controller matrix K and a quadratic Lyapunov function for the closed-loop system, and then invoking Sylvester’s criterion for matrix positive definiteness.

e.g., [6]. However, no polynomial-time algorithm is known for output feedback stabilization. Blondel and Tsitsiklis [2] proved NP-hardness when the entries of K are constrained to prescribed intervals, but left the complexity of the unrestricted problem open. Chaudhry [4] proved strong NP-hardness of the more general problem of deciding whether an affine subspace of matrices contains a Hurwitz (or a Schur) matrix. The affine subspaces in that reduction, however, do not have the specific form $\{A + BKC : K \in \mathbb{R}^{p \times q}\}$ required by output feedback stabilization.

In this paper, we prove that output feedback stabilization is strongly NP-hard. This result is established both in continuous time (Section 2) and in discrete time (Section 3). The implication of this result is that unless $P=NP$, there is no polynomial-time (or even pseudo-polynomial-time) algorithm for output feedback stabilization. In Section 4, we also establish, in both continuous and discrete time, a representation obstruction to polynomial-time algorithms that is independent of any complexity-theoretic assumption: even when the system is stabilizable, a polynomial-time algorithm cannot, in general, write down a stabilizing feedback gain matrix in its natural representation.

All results in this paper are in the Turing model of computation, where the input consists of the rational entries of the matrices A, B, C . Each entry is represented as a/b , where a is a signed integer and b is a positive integer. The input size L is the total number of bits needed to encode these numerators and denominators in binary, including the signs. Let M be the maximum of $|a|$ and b over all entries of A, B, C . An algorithm is polynomial-time if its running time is bounded by a polynomial in L , and pseudo-polynomial-time if its running time is bounded by a polynomial in M and the dimensions of A, B, C . In particular, every polynomial-time algorithm is also pseudo-polynomial-time, though the converse is not true as pseudo-polynomial time algorithms can take exponential time in L . Our reductions establish NP-hardness even when M is polynomially bounded in the matrix dimensions. On these instances, any pseudo-polynomial-time bound becomes a polynomial-time bound. Thus, our NP-hardness results are in the strong sense and rule out pseudo-polynomial-time algorithms unless $P = NP$. See [5] for more details on these notions.

2. CONTINUOUS-TIME HARDNESS

In this section, we prove the following theorem.

Theorem 1. *Given matrices $A \in \mathbb{Z}^{N \times N}$, $B \in \mathbb{Z}^{N \times p}$, and $C \in \mathbb{Z}^{1 \times N}$, deciding if there exists a matrix $K \in \mathbb{R}^{p \times 1}$ that makes $A + BKC$ Hurwitz is strongly NP-hard.*

Note that the theorem establishes strong NP-hardness of output feedback stabilization even when the system has a single output. The result trivially extends to systems with any fixed number of outputs. The proof will further show the claim even when C is binary, every entry of A has absolute value at most $256N^2$, and every entry of B has absolute value at most 6.

We shall prove Theorem 1 by a reduction from 3SAT which proceeds in two steps. In Step 1, which is the easier step, we reduce 3SAT to the problem of simultaneous output feedback stabilization of multiple dynamical systems by a common controller. In Step 2, which is more involved, we reduce these simultaneous-stabilization instances to output feedback stabilization of a single system. Since the closed-loop system in all cases is linear, its asymptotic stability can be shown with algebraic certificates involving quadratic forms. This allows Step 2 to be carried out by relating the algebraic certificates for the two stabilization problems. We note that (weak) NP-hardness of simultaneous output feedback stabilization, corresponding to Step 1, was previously shown by Blondel and Tsitsiklis [2]. However, we need a different reduction both to establish strong NP-hardness, and because the construction used in Step 2 is closely intertwined with the particular simultaneous-stabilization instances produced in Step 1.

To present the proof formally, we begin by introducing some notation and establishing three technical lemmas.² For a real matrix E , we write its transpose as $E^\top$ and $\text{sym}(E) = (E + E^\top)/2$.

²The proof of Step 1 relies on Lemma 2 and Lemma 4, while Step 2 relies on Lemma 2, Lemma 3, and Lemma 4.

We denote its kernel by $\ker E$. We use the notation Diag for block-diagonal assembly, I_n for the $n \times n$ identity matrix, and $\|\cdot\|$ for the Euclidean vector norm or its induced matrix norm. For a symmetric matrix X , the notation $X \succeq 0$ (resp. $X \succ 0$) denotes that X is positive semidefinite (resp. positive definite); i.e., it has nonnegative (resp. positive) eigenvalues. For a positive integer m , denote the set $\{1, \dots, m\}$ by $[m]$. For a complex number $z \in \mathbb{C}$, we denote its real part by $\text{Re}(z)$ and its conjugate by $\bar{z}$. For a complex matrix E , we denote its conjugate transpose by E^* . We use the notation $\vee$ for Boolean OR and $\wedge$ for Boolean AND.

Let us define $J = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $e = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. For real scalars λ_i and vectors $u_i, v_i \in \mathbb{R}^2$, $i = 1, \dots, m$, we define $D_i = \lambda_i I_2 - J$, and

$$D = \text{Diag}(D_1, \dots, D_m) \in \mathbb{R}^{2m \times 2m}, \quad u = \begin{pmatrix} u_1 \\ \vdots \\ u_m \end{pmatrix}, \quad v = \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix}, \quad c = \begin{pmatrix} e \\ \vdots \\ e \end{pmatrix} \in \mathbb{R}^{2m}. \quad (1)$$

Define $\mathcal{M} \in \mathbb{R}^{4m \times 4m}$ and $\mathcal{C} \in \mathbb{R}^{1 \times 4m}$ by

$$\mathcal{M} = \begin{pmatrix} 0 & -D - uc^\top \\ I_{2m} & -vc^\top \end{pmatrix}, \quad \mathcal{C} = (0_{1 \times 2m}, c^\top). \quad (2)$$

The next lemma relates Hurwitzness of $\mathcal{M}$ to Lyapunov-type positive (semi)definiteness conditions on symmetric matrices.

Lemma 2 (Hurwitzness of $\mathcal{M}$). *Let m be a positive integer, $\lambda_1, \dots, \lambda_m$ be distinct real scalars, and $u_i, v_i \in \mathbb{R}^2$ for $i \in [m]$. Let D, u, v, c be defined as in (1) and $\mathcal{M}$ be defined as in (2). Suppose $X = X^\top \in \mathbb{R}^{2m \times 2m}$ satisfies*

$$Xc = v, \quad DX - XD^\top = vu^\top - uv^\top. \quad (3)$$

Then the following claims hold:

- (i) *If $\mathcal{M}$ is Hurwitz, then $X \succeq 0$.*
- (ii) *If $X \succ 0$ and $\text{sym}(D + uc^\top) \succ 0$, then $\mathcal{M}$ is Hurwitz.*

Proof. We first prove (i). Let $E = D + uc^\top$, $Y = DX + uv^\top$, and $\mathcal{C}$ be defined as in (2). The second equation in (3) gives $Y = Y^\top = EX$. Define $H = \text{Diag}(Y, X)$. Since $Xc = v$, we observe that the matrix

$$\mathcal{M}H + H\mathcal{M}^\top = -2(HC^\top)(HC^\top)^\top$$

is negative semidefinite. Suppose for the sake of contradiction that $X \not\succeq 0$. Since X is a principal submatrix of H , this implies $H \not\succeq 0$. Hence, there exists $z \in \mathbb{R}^{4m}$ and $\epsilon > 0$ such that $z^\top H z \leq -\epsilon$. Along the trajectory of the system $\dot{x} = \mathcal{M}^\top x$ starting at $x(0) = z$, the quadratic form $V(x) = x^\top H x$ satisfies

$$\dot{V}(x) = x^\top (\mathcal{M}H + H\mathcal{M}^\top) x.$$

Since $\mathcal{M}H + H\mathcal{M}^\top$ is negative semidefinite, $\dot{V}(x) \leq 0$. Thus, $V(x(t)) \leq V(z) \leq -\epsilon$ for all $t \geq 0$. However, $\mathcal{M}^\top$ being Hurwitz implies that $x(t) \rightarrow 0$, hence $V(x(t)) \rightarrow 0$, which is a contradiction, proving (i).

We now prove (ii). Assume $X \succ 0$ and $E + E^\top \succ 0$. We first show that $Y \succ 0$. Suppose for the sake of contradiction that $Y \not\succ 0$. Since Y is symmetric, there is a nonzero vector z and $\lambda \leq 0$ such that $Yz = \lambda z$. Then, we have

$$z^\top (X^{-1}Y + YX^{-1})z = 2\lambda z^\top X^{-1}z \leq 0.$$

This is a contradiction since

$$X^{-1}Y + YX^{-1} = E^\top + E \succ 0.$$

Therefore, $Y \succ 0$ and $H = \text{Diag}(Y, X) \succ 0$. We next show that no eigenvector of $\mathcal{M}$ lies in $\ker \mathcal{C}$. Suppose, for contradiction, that there exist $\mu \in \mathbb{C}$ and $(p^\top, q^\top)^\top \in \mathbb{C}^{4m} \setminus \{0\}$ such that

$$\mathcal{M} \begin{pmatrix} p \\ q \end{pmatrix} = \mu \begin{pmatrix} p \\ q \end{pmatrix}, \quad \mathcal{C} \begin{pmatrix} p \\ q \end{pmatrix} = c^\top q = 0.$$

By the definition of $\mathcal{M}$, the eigenvalue equation gives

$$-(D + uc^\top)q = \mu p, \quad p - vc^\top q = \mu q.$$

Since $c^\top q = 0$, these equations reduce to $-Dq = \mu p$, $p = \mu q$, and hence $Dq = -\mu^2 q$. Write $q = (q_1^\top, \dots, q_m^\top)^\top$, with $q_j \in \mathbb{C}^2$. Since $D_j = \lambda_j I_2 - J$, for every $j \in [m]$ we have

$$((\lambda_j + \mu^2)I_2 - J)q_j = 0. \quad (4)$$

If $\lambda_j + \mu^2 \neq 0$, then since J is nilpotent, we have $q_j = 0$. Since the λ_j are distinct, at most one block q_i can be nonzero. Since $(p^\top, q^\top)^\top \neq 0$, there is $i \in [m]$ such that $\lambda_i + \mu^2 = 0$. Equation (4) gives $Jq_i = 0$. As $\ker J = \text{span}\{e\}$, we have $q_i = \alpha e$ for some $\alpha \in \mathbb{C}$. But then

$$0 = c^\top q = e^\top q_i = \alpha,$$

so $q_i = 0$. Thus $q = 0$, and consequently $p = \mu q = 0$, contradicting $(p^\top, q^\top)^\top \neq 0$. Therefore every nonzero eigenvector z of $\mathcal{M}$ satisfies $\mathcal{C}z \neq 0$.

Let $\mu \in \mathbb{C}$ be an eigenvalue of $\mathcal{M}$, and let $z \in \mathbb{C}^{4m} \setminus \{0\}$ be a corresponding eigenvector. We have

$$-2z^* \mathcal{C}^\top \mathcal{C} z = z^* \mathcal{M}^\top H^{-1} z + z^* H^{-1} \mathcal{M} z = \bar{\mu} z^* H^{-1} z + \mu z^* H^{-1} z = 2 \text{Re}(\mu) z^* H^{-1} z,$$

where the second equality follows from the fact that $\mathcal{M}$ is real. Since $H \succ 0$, this gives $\text{Re}(\mu) \leq 0$. If $\text{Re}(\mu) = 0$, then $\mathcal{C}z = 0$, contradicting the fact we showed above. Hence every eigenvalue of $\mathcal{M}$ has strictly negative real part, so $\mathcal{M}$ is Hurwitz. $\square$

For $a = (a_1, a_2)^\top \in \mathbb{R}^2$ and $b = (b_1, b_2)^\top \in \mathbb{R}^2$, let us define the matrix

$$\mathcal{G}(a, b) = \begin{pmatrix} a_2 b_1 - a_1 b_2 & b_1 \\ b_1 & b_2 \end{pmatrix}. \quad (5)$$

To motivate this definition, we note that

$$\mathcal{G}(a, b)e = b, \quad -J\mathcal{G}(a, b) + \mathcal{G}(a, b)J^\top = ba^\top - ab^\top.$$

Thus, $G_i = \mathcal{G}(u_i, v_i)$ is a natural solution of (3) when $m = 1$. We now develop a ‘gluing’ lemma that allows one to combine these one-block solutions to obtain a matrix X satisfying the linear equations in (3). When parameters λ_i are sufficiently separated, X remains close to the block diagonal matrix $G_0 = \text{Diag}(G_1, \dots, G_m)$ while preserving the $(1, 1)$ entry of each diagonal block exactly.

Lemma 3 (Gluing lemma). *Let m be a positive integer, $\lambda_1, \dots, \lambda_m$ be distinct real scalars, and $u_i, v_i \in \mathbb{R}^2$ for $i \in [m]$. Let D, u, v, c be defined as in (1) and $\mathcal{G}(\cdot, \cdot)$ be defined as in (5). Let $G_i = \mathcal{G}(u_i, v_i)$ for $i \in [m]$, and $G_0 = \text{Diag}(G_1, \dots, G_m) \in \mathbb{R}^{2m \times 2m}$. Then, there is a unique symmetric matrix $X \in \mathbb{R}^{2m \times 2m}$ satisfying (3). Furthermore, writing $X = (X_{ij})_{i,j=1}^m$ in 2×2 blocks, we have*

$$(X_{ii})_{11} = (G_i)_{11} \quad (1 \leq i \leq m). \quad (6)$$

Let $\beta = \max_{1 \leq i \leq m} \{\|u_i\|, \|v_i\|\}$. In addition, if $h \geq 4$ and $|\lambda_i - \lambda_j| \geq h$ for all $i \neq j$, then

$$\|X - G_0\| \leq \frac{12m\beta^2}{h}. \quad (7)$$

Proof. We first construct a solution X to (3). Assume $i, j \in [m]$ and $i \neq j$. By expanding the second equation in (3), the (i, j) block X_{ij} in a solution X satisfies

$$(\lambda_i - \lambda_j)X_{ij} - JX_{ij} + X_{ij}J^\top = v_i u_j^\top - u_i v_j^\top. \quad (8)$$

The existence and uniqueness of the solution of equation (8) follow from the distinctness of λ_i and λ_j by, e.g., [9, p.231]. Taking the transpose of (8) and exchanging i and j shows, by uniqueness, that $X_{ji} = X_{ij}^\top$.

It remains to construct the diagonal submatrices X_{ii} . For $z = (z_1, z_2)^\top \in \mathbb{R}^2$, let $\Gamma(z) = \begin{pmatrix} 0 & z_1 \\ z_1 & z_2 \end{pmatrix}$. Set

$$t_i = \sum_{\substack{1 \leq j \leq m \\ j \neq i}} X_{ij} e \in \mathbb{R}^2. \quad (9)$$

We show that $X_{ii} = G_i - \Gamma(t_i)$ will satisfy (3) and (6). For (6), since $\Gamma(z)_{11} = 0$, we have $(X_{ii})_{11} = (G_i)_{11}$. For (3), direct calculation gives

$$G_i e = v_i, \quad -JG_i + G_i J^\top = v_i u_i^\top - u_i v_i^\top, \quad \Gamma(z)e = z, \quad J\Gamma(z) = \Gamma(z)J^\top.$$

Thus (9) enforces $Xc = v$ and $D_i X_{ii} - X_{ii} D_i^\top = v_i u_i^\top - u_i v_i^\top$.

Next we show that the symmetric solution X is unique. Suppose X and $\tilde{X}$ are two symmetric solutions of (3), and let $Z = X - \tilde{X}$. Then, we have

$$Zc = 0, \quad DZ - ZD^\top = 0.$$

The off-diagonal blocks are zero by the uniqueness of the solution to (8). For $i \in [m]$, write the (i, i) block of Z as $Z_{ii} = \begin{pmatrix} a & b \\ b & d \end{pmatrix}$. Then $DZ - ZD^\top = 0$ gives

$$-JZ_{ii} + Z_{ii}J^\top = \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix} = 0,$$

so $a = 0$. Since all off-diagonal blocks of Z are 0, $Zc = 0$ gives $Z_{ii}e = 0$, and hence $b = d = 0$. Thus, $Z_{ii} = 0$ for every i , so $Z = 0$.

We now show that the matrix X constructed above satisfies the bound in (7). Applying the triangle inequality to (8) yields

$$|\lambda_i - \lambda_j| \|X_{ij}\| \leq \|JX_{ij}\| + \|X_{ij}J^\top\| + \|v_i u_j^\top\| + \|u_i v_j^\top\|.$$

By definition of β and the fact that $\|J\| = 1$, we have $(|\lambda_i - \lambda_j| - 2) \|X_{ij}\| \leq 2\beta^2$. Since $|\lambda_i - \lambda_j| \geq h$ and $h \geq 4$, we have $|\lambda_i - \lambda_j| - 2 \geq h/2$, and hence

$$\|X_{ij}\| \leq \frac{4\beta^2}{h}. \quad (10)$$

We then bound $\|X - G_0\|$. First we have

$$\|X_{ii} - G_i\| = \|\Gamma(t_i)\| \leq 2\|t_i\| \leq 2 \sum_{j \neq i} \|X_{ij}\|.$$

Since $X - G_0$ is symmetric, for any block vector $z = (z_1^\top, \dots, z_m^\top)^\top$ we have

$$\begin{aligned} |z^\top (X - G_0) z| &\leq \sum_i \|X_{ii} - G_i\| \|z_i\|^2 + \sum_{i \neq j} \|X_{ij}\| \|z_i\| \|z_j\| \\ &\leq \sum_i \left(\|X_{ii} - G_i\| + \sum_{j \neq i} \|X_{ij}\| \right) \|z_i\|^2, \end{aligned}$$

where the second inequality uses $2\|z_i\|\|z_j\| \leq \|z_i\|^2 + \|z_j\|^2$ and $\|X_{ij}\| = \|X_{ji}\|$. Therefore, using (10), we have

$$\|X - G_0\| \leq \max_i \left(\|X_{ii} - G_i\| + \sum_{j \neq i} \|X_{ij}\| \right) \leq 3 \max_i \sum_{j \neq i} \|X_{ij}\| \leq \frac{12m\beta^2}{h}.$$

□

The proof of Theorem 1 relies on a reduction from 3SAT, which is well known to be (strongly) NP-hard [5]. Recall that 3SAT is a Boolean satisfiability problem in which a formula is expressed as a conjunction of clauses, where each clause consists of exactly three literals connected by logical OR. The problem asks whether there exists an assignment of truth values to the variables that makes every clause true. More specifically, a 3SAT instance Φ with variables $x_1, \dots, x_n$ and clauses $C_1, \dots, C_r$ is of the form

$$\Phi = C_1 \wedge \dots \wedge C_r,$$

the j th clause reads $C_j = \ell_{j1} \vee \ell_{j2} \vee \ell_{j3}$. Here, each ℓ_{jk} is called a literal and is either one of the variables $x_1, \dots, x_n$ or the negation of one of these variables. We identify a Boolean assignment with a vector $x = (x_1, \dots, x_n) \in \{\pm 1\}^n$, where $x_i = 1$ means that the i th variable is True and $x_i = -1$ means that it is False. The 3SAT instance Φ is satisfiable if there exists such an assignment $x \in \{\pm 1\}^n$ under which every clause C_j evaluates to True.

For each clause index $j \in [r]$ and literal position $k \in [3]$, define

$$y_{jk}(x) = \begin{cases} x_i, & \ell_{jk} = x_i, \\ -x_i, & \ell_{jk} = \neg x_i. \end{cases}$$

Then, $y_{jk}(x) = 1$ when ℓ_{jk} is true under the Boolean assignment x , and equals -1 when ℓ_{jk} is false. For $j \in [r]$, we define an affine clause score function

$$L_j(x) = 3 + 2 \sum_{k=1}^3 y_{jk}(x).$$

On Boolean inputs, $L_j(x) = -3$ when clause C_j is false, while $L_j(x) \in \{1, 5, 9\}$ when it is true. For $i \in [n]$, we define

$$u_i(x) = \begin{pmatrix} 1 \\ 3x_i \end{pmatrix}, \quad v_i(x) = \begin{pmatrix} x_i \\ 1 \end{pmatrix}, \quad G_i(x) = \mathcal{G}(u_i(x), v_i(x)) = \begin{pmatrix} 3x_i^2 - 1 & x_i \\ x_i & 1 \end{pmatrix}. \quad (11)$$

For $j \in [r]$, we define

$$u_{n+j}(x) = \begin{pmatrix} -1 \\ 0 \end{pmatrix}, \quad v_{n+j}(x) = \begin{pmatrix} 0 \\ L_j(x) \end{pmatrix}, \quad G_{n+j}(x) = \mathcal{G}(u_{n+j}(x), v_{n+j}(x)) = L_j(x)I_2. \quad (12)$$

Lemma 4 (Properties of the 3SAT encoding). *Suppose Φ is a 3SAT instance with n variables and r clauses. For $i \in [n+r]$ and $x \in \mathbb{R}^n$, let $u_i(x), v_i(x)$ and $G_i(x)$ be defined as in (11) and (12). Then, the following statements hold:*

(i) *If x is a satisfying Boolean assignment to Φ , then*

$$G_i(x) \succeq \frac{1}{3}I_2 \quad (1 \leq i \leq n+r) \quad \text{and} \quad \max_{1 \leq i \leq n+r} \{\|u_i(x)\|, \|v_i(x)\|\} \leq 9.$$

(ii) *If there exists $x \in \mathbb{R}^n$ such that $(G_k(x))_{11} \geq 0$ for all $k \in [n+r]$, then Φ is satisfiable.*

Proof. If x is a satisfying Boolean assignment for Φ , then for $i \in [n]$, $x_i = \pm 1$. Therefore, $G_i(x) = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ or $\begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}$, both satisfy $G_i(x) \succeq \frac{1}{3}I_2$. We have $\|u_i(x)\| = \sqrt{10}$ and $\|v_i(x)\| = \sqrt{2}$. Since x is a satisfying Boolean assignment for Φ , for all $j \in [r]$ we have $L_j(x) \in \{1, 5, 9\}$. Thus, $G_{n+j}(x) \succeq \frac{1}{3}I_2$, $\|u_{n+j}(x)\| = 1$ and $\|v_{n+j}(x)\| \leq 9$. This proves claim (i).

If there exists $x \in \mathbb{R}^n$ such that $(G_k(x))_{11} \geq 0$ for all $k \in [n+r]$, then $3x_i^2 - 1 \geq 0$ for all $i \in [n]$ and $L_j(x) \geq 0$ for all $j \in [r]$. For every index $i \in [n]$, we construct $\hat{x}_i = \text{sign}(x_i)$. We prove that $\hat{x}$ is a satisfying assignment to Φ . Suppose for the sake of contradiction that there exists $j \in [r]$ such that $L_j(\hat{x}) < 0$. Then we know that

$$y_{j1}(\hat{x}) = -1, y_{j2}(\hat{x}) = -1, y_{j3}(\hat{x}) = -1.$$

Since $|x_i| \geq \frac{1}{\sqrt{3}} > \frac{1}{2}$, we have

$$y_{j1}(x) < -\frac{1}{2}, y_{j2}(x) < -\frac{1}{2}, y_{j3}(x) < -\frac{1}{2}.$$

However, this gives $L_j(x) < 0$, a contradiction. Thus, $L_j(\hat{x}) \geq 0$ for all $j \in [r]$, which indicates that C_j is true under assignment $\hat{x}$ for all $j \in [r]$. This proves claim (ii). $\square$

We can now present the proof of Theorem 1.

Proof of Theorem 1. Step 1: Simultaneous stabilization.

Given a 3SAT instance Φ with n variables and r clauses, let $m = n + r$. Define $h = 4096m$ and for $i \in [m]$ define $\lambda_i = ih$ and $D_i = \lambda_i I_2 - J$. Let $u_i(x), v_i(x)$, and $G_i(x)$ be defined as in (11) and (12). For notational convenience, for $i \in [n+r]$, we write $u_i(x) = u_i^0 + U_i x$ and $v_i(x) = v_i^0 + V_i x$, where $u_i^0, v_i^0 \in \mathbb{Z}^2$ and $U_i, V_i \in \mathbb{Z}^{2 \times n}$. Construct the following matrices $A_i \in \mathbb{Z}^{4 \times 4}$, $B_i \in \mathbb{Z}^{4 \times n}$, and $C_i \in \mathbb{Z}^{1 \times 4}$:

$$A_i = \begin{pmatrix} 0 & -D_i - u_i^0 e^\top \\ I_2 & -v_i^0 e^\top \end{pmatrix}, \quad B_i = -\begin{pmatrix} U_i \\ V_i \end{pmatrix}, \quad C_i = (0, 0, 0, 1).$$

We show that Φ is satisfiable if and only if there exists $x \in \mathbb{R}^n$ such that $A_i + B_i x C_i$ is Hurwitz for all $i \in [m]$.

If Φ is satisfiable, let x be a satisfying Boolean assignment. We claim that for every $i \in [m]$, $A_i + B_i x C_i$ is Hurwitz. A straightforward calculation gives

$$A_i + B_i x C_i = \begin{pmatrix} 0 & -D_i - u_i(x) e^\top \\ I_2 & -v_i(x) e^\top \end{pmatrix}.$$

One can verify that for all $i \in [m]$, we have $D_i G_i(x) - G_i(x) D_i^\top = v_i(x) u_i(x)^\top - u_i(x) v_i(x)^\top$ and $G_i(x) e = v_i(x)$. By Lemma 4(i), $G_i(x) \succ 0$ and $\|u_i(x)\| \leq 9$ for all i . Therefore,

$$\text{sym}(D_i + u_i(x) e^\top) \succeq (\lambda_i - 1 - \|u_i(x)\|) I_2 \succeq (h - 10) I_2 \succ 0.$$

Then, applying Lemma 2(ii) with $\lambda_i, u_i(x), v_i(x), D_i$ shows that $A_i + B_i x C_i$ is Hurwitz for all $i \in [m]$.

Conversely, suppose there exists $x \in \mathbb{R}^n$ such that $A_i + B_i x C_i$ is Hurwitz for all $i \in [m]$. Lemma 2(i) shows that $G_i(x) \succeq 0$ for all $i \in [m]$. Thus, $(G_i(x))_{11} \geq 0$ for all $i \in [m]$. Applying Lemma 4(ii) gives that Φ is satisfiable.

Step 2: Output feedback stabilization.

We now combine the matrices constructed in Step 1 in a specific way to conclude the proof. We define

$$u^0 := \begin{pmatrix} u_1^0 \\ \vdots \\ u_m^0 \end{pmatrix} \in \mathbb{Z}^{2m}, \quad v^0 := \begin{pmatrix} v_1^0 \\ \vdots \\ v_m^0 \end{pmatrix} \in \mathbb{Z}^{2m}, \quad U := \begin{pmatrix} U_1 \\ \vdots \\ U_m \end{pmatrix} \in \mathbb{Z}^{2m \times n}, \quad V := \begin{pmatrix} V_1 \\ \vdots \\ V_m \end{pmatrix} \in \mathbb{Z}^{2m \times n}.$$

For every $x \in \mathbb{R}^n$, we write $u(x) = u^0 + Ux$ and $v(x) = v^0 + Vx$. Let D, c be defined as in (1) and $N = 4m$. Let

$$A = \begin{pmatrix} 0 & -D - u^0 c^\top \\ I_{2m} & -v^0 c^\top \end{pmatrix} \in \mathbb{Z}^{N \times N}, \quad B = -\begin{pmatrix} U \\ V \end{pmatrix} \in \mathbb{Z}^{N \times n}, \quad C = (0_{1 \times 2m}, c^\top) \in \mathbb{Z}^{1 \times N}.$$

We claim that Φ is satisfiable if and only if there exists $x \in \mathbb{R}^n$ such that $A + BxC$ is Hurwitz. By definition of A, B , and C , we have

$$A + BxC = \begin{pmatrix} 0 & -D - u(x)c^\top \\ I_{2m} & -v(x)c^\top \end{pmatrix}.$$

By Lemma 3, for every $x \in \mathbb{R}^n$ there is a symmetric matrix $X(x) \in \mathbb{R}^{2m \times 2m}$ such that

$$X(x)c = v(x), \quad DX(x) - X(x)D^\top = v(x)u(x)^\top - u(x)v(x)^\top.$$

Writing $X(x) = (X_{ij}(x))_{i,j=1}^m$ in 2×2 blocks, we have $(X_{ii}(x))_{11} = (G_i(x))_{11}$ for all $i \in [m]$.

Suppose Φ has a satisfying Boolean assignment $x \in \{\pm 1\}^n$. By Lemma 4(i),

$$\max_{1 \leq i \leq m} \{\|u_i(x)\|, \|v_i(x)\|\} \leq 9.$$

Together with Lemma 3, we have

$$\|X(x) - \text{Diag}(G_1(x), \dots, G_m(x))\| \leq \frac{12m \cdot 9^2}{4096m} = \frac{243}{1024} < \frac{1}{4}. \quad (13)$$

Also from Lemma 4(i), we know that $G_i(x) \succeq \frac{1}{3}I_2$ for all $i \in [m]$. Combining with (13) gives $X(x) \succ \frac{1}{12}I_{2m}$. Since $\|u(x)\| \leq 9\sqrt{m}$ and $\|c\| = \sqrt{m}$, we have

$$\text{sym}(D + u(x)c^\top) \succeq (h - 1 - \|u(x)\| \|c\|)I_{2m} \succeq (h - 1 - 9m)I_{2m} \succ 0.$$

Then applying Lemma 2(ii) gives that $A + BxC$ is Hurwitz.

Conversely, suppose there is $x \in \mathbb{R}^n$ such that $A + BxC$ is Hurwitz. By Lemma 2 (i), $X(x)$ is positive semidefinite. By Lemma 3, for $i \in [m]$, $(G_i(x))_{11} = (X_{ii}(x))_{11} \geq 0$. Then applying Lemma 4(ii) shows that Φ is satisfiable.

The reduction uses only polynomially bounded integers. We have $N = 4m$, $h = 4096m$, and

$$\lambda_i = ih \leq \lambda_m = 4096m^2 = 256N^2.$$

It is not difficult to verify that every entry of A has absolute value at most $256N^2$, every entry of B has absolute value at most 6, and C is binary. Therefore, the reduction can be carried out in polynomial time and establishes strong NP-hardness. $\square$

3. DISCRETE-TIME HARDNESS

In this section, we establish the discrete-time analogue of Theorem 1:

Theorem 5. *Given matrices $A_d \in \mathbb{Q}^{N \times N}$, $B_d \in \mathbb{Q}^{N \times p}$, and $C_d \in \mathbb{Q}^{1 \times N}$, deciding if there exists a matrix $K_d \in \mathbb{R}^{p \times 1}$ that makes $A_d + B_d K_d C_d$ Schur is strongly NP-hard.*

The key idea of the proof (modulo an important technical problem that we shall address) is to utilize the Cayley transform to transfer the reduction from the continuous-time case. The Cayley transform is a well-studied tool for passing between continuous and discrete time systems (see, for example, [7]).

Lemma 6 (Cayley transform). *Let $A \in \mathbb{Q}^{N \times N}$, $B \in \mathbb{Q}^{N \times p}$, and $C \in \mathbb{Q}^{1 \times N}$. Choose $\beta \in \mathbb{Q}$, $\beta > 0$, such that $\beta I - A$ is invertible, and denote*

$$R_\beta = (\beta I - A)^{-1}, \quad \hat{D} = CR_\beta B, \quad A_d = 2\beta R_\beta - I, \quad B_d = R_\beta B, \quad C_d = 2\beta CR_\beta. \quad (14)$$

Let $\mathcal{K}_c$ denote the set of all stabilizing controllers of the system (A, B, C) in continuous time and $\mathcal{K}_d$ the set of all stabilizing controllers of the system (A_d, B_d, C_d) in discrete time. Then, the maps

$$\begin{aligned}\Psi_{c \rightarrow d} : \mathcal{K}_c &\longrightarrow \mathcal{K}_d, & \Psi_{c \rightarrow d}(K_c) &= \frac{K_c}{1 - \widehat{D}K_c}, \\ \Psi_{d \rightarrow c} : \mathcal{K}_d &\longrightarrow \mathcal{K}_c, & \Psi_{d \rightarrow c}(K_d) &= \frac{K_d}{1 + \widehat{D}K_d},\end{aligned}\tag{15}$$

are inverses and provide a bijection between the rational stabilizing controllers.

Proof. Let $F_c = A + BK_cC$ and $F_d = A_d + B_dK_dC_d$. Since $R_\beta = (\beta I - A)^{-1}$, the matrix determinant lemma gives that

$$\begin{aligned}\det(\beta I - F_c) &= \det(\beta I - A - BK_cC) = \det(\beta I - A)(1 - CR_\beta BK_c) \\ &= \det(\beta I - A)(1 - \widehat{D}K_c), \\ \det(I + F_d) &= \det(2\beta R_\beta + 2\beta R_\beta B K_d C R_\beta) = (2\beta)^N \det(R_\beta) \det(I + B K_d C R_\beta) \\ &= (2\beta)^N \det(R_\beta)(1 + \widehat{D}K_d).\end{aligned}$$

If K_c is stabilizing, then F_c must be Hurwitz and thus β is not an eigenvalue of F_c . Therefore, $1 - \widehat{D}K_c \neq 0$. Similarly, if K_d is stabilizing, then F_d must be Schur, and thus -1 is not an eigenvalue of F_d , implying that $1 + \widehat{D}K_d \neq 0$. It follows that $\Psi_{c \rightarrow d}$ is well-defined for every $K_c \in \mathcal{K}_c$, and that $\Psi_{d \rightarrow c}$ is well-defined for every $K_d \in \mathcal{K}_d$. We next show that these mappings preserve stability.

We begin by applying the Sherman–Morrison formula to $\beta I - F_c = (\beta I - A) - BK_cC$. This gives us

$$(\beta I - F_c)^{-1} = R_\beta + \frac{R_\beta B K_c C R_\beta}{1 - \widehat{D}K_c}.\tag{16}$$

Using (14), (15), and (16), we have

$$\begin{aligned}F_d &= 2\beta R_\beta - I + 2\beta R_\beta B K_d C R_\beta \\ &= 2\beta \left(R_\beta + \frac{R_\beta B K_c C R_\beta}{1 - \widehat{D}K_c} \right) - I \\ &= 2\beta(\beta I - F_c)^{-1} - I = (\beta I - F_c)^{-1}(\beta I + F_c).\end{aligned}\tag{17}$$

Now, let s be an eigenvalue of F_c . Equation (17) shows that the corresponding eigenvalue of F_d is $z = \frac{\beta+s}{\beta-s}$. Conversely, every eigenvalue of F_d is obtained from an eigenvalue of F_c through this transformation. Since

$$|\beta + s|^2 - |\beta - s|^2 = 4\beta \operatorname{Re} s,$$

and $\beta > 0$, we have

$$|z| < 1 \iff |\beta + s| < |\beta - s| \iff \operatorname{Re} s < 0.$$

Therefore, F_c is Hurwitz if and only if F_d is Schur. The fact that $\Psi_{c \rightarrow d}$ and $\Psi_{d \rightarrow c}$ are mutual inverses follows from a direct computation:

$$\begin{aligned}\Psi_{d \rightarrow c}(\Psi_{c \rightarrow d}(K_c)) &= \frac{\frac{K_c}{1 - \widehat{D}K_c}}{1 + \widehat{D}\frac{K_c}{1 - \widehat{D}K_c}} = \frac{K_c}{1 - \widehat{D}K_c + \widehat{D}K_c} = K_c, \\ \Psi_{c \rightarrow d}(\Psi_{d \rightarrow c}(K_d)) &= \frac{\frac{K_d}{1 + \widehat{D}K_d}}{1 - \widehat{D}\frac{K_d}{1 + \widehat{D}K_d}} = \frac{K_d}{1 + \widehat{D}K_d - \widehat{D}K_d} = K_d.\end{aligned}$$

Finally, since $\beta I - A$ is an invertible rational matrix, $R_\beta = (\beta I - A)^{-1}$ and $\widehat{D} = CR_\beta B$ are rational. Hence (15) shows that both transformations preserve rationality. $\square$

Since the inverse of a rational matrix can be computed in polynomial time, a direct application of Lemma 6 gives NP-hardness of output feedback stabilization in discrete time. For strong NP-hardness, however, this is not enough: the numerators and denominators of the transformed data must themselves have polynomial magnitude and this can in general fail under matrix inversion.

To control these denominators, we modify the parameters λ_i used in the continuous-time construction. With the original choice $\lambda_i = ih$, the blocks $(I_2 + D_i)^{-1}$ involve denominators $(1 + ih)^2$ that vary with i . Although each denominator has polynomial magnitude, this alone does not control the denominators arising when the blocks are combined through the Sherman–Morrison formula. We therefore choose parameters for which these blocks share a common denominator of polynomial magnitude.

Proof of Theorem 5. Let Φ be a 3SAT formula with $n \geq 1$ variables and r clauses, and set $m = n + r$ and $N = 4m$. Let $u_i(x)$ and $v_i(x)$ be the vectors defined in (11) and (12). Collect these vectors into

$$u(x) = \begin{pmatrix} u_1(x) \\ \vdots \\ u_m(x) \end{pmatrix} = u^0 + Ux, \quad v(x) = \begin{pmatrix} v_1(x) \\ \vdots \\ v_m(x) \end{pmatrix} = v^0 + Vx.$$

Here $u^0, v^0 \in \mathbb{Z}^{2m}$ contain the constant terms, and $U, V \in \mathbb{Z}^{2m \times n}$ contain the coefficients of x . By (11) and (12), every entry of u^0, v^0 has absolute value at most 3, and every entry of U, V has absolute value at most 6.

We modify the choice of parameters by setting

$$h = 4096m, \quad \tau = hm(m+1), \quad \lambda_i = \frac{\tau}{i} - 1 \quad (1 \leq i \leq m). \quad (18)$$

As in (1), define

$$D_i = \lambda_i I_2 - J, \quad D = \text{Diag}(D_1, \dots, D_m), \quad c = (e^\top, \dots, e^\top)^\top,$$

and

$$A_0 = \begin{pmatrix} 0 & -D \\ I_{2m} & 0 \end{pmatrix}, \quad b_0 = \begin{pmatrix} u^0 \\ v^0 \end{pmatrix}, \quad B = -\begin{pmatrix} U \\ V \end{pmatrix}, \quad C = (0_{1 \times 2m}, c^\top), \quad A = A_0 - b_0 C.$$

For every $x \in \mathbb{R}^n$, the matrix $A + Bx C$ has the form $\mathcal{M}$ in (2), with $u = u(x)$ and $v = v(x)$. Note that the parameters in (18) satisfy

$$\lambda_i \geq \frac{\tau}{m} - 1 = h(m+1) - 1 \geq h \quad (i \in [m]),$$

and, for $i \neq j$,

$$|\lambda_i - \lambda_j| = \tau \frac{|i-j|}{ij} \geq \frac{\tau}{m^2} = h \frac{m+1}{m} > h.$$

One can verify that the argument in Step 2 of the proof of Theorem 1, using Lemmas 2, 3, and 4, applies whenever $\lambda_i \geq h$ and $|\lambda_i - \lambda_j| \geq h$ for $i \neq j$, with $h = 4096m$. Since the parameters in (18) satisfy these conditions, we obtain

$$\Phi \text{ is satisfiable} \iff \exists x \in \mathbb{R}^n : A + Bx C \text{ is Hurwitz.}$$

Passing to discrete time. We now apply Lemma 6 with $\beta = 1$. First, we verify that $I_N - A$ is invertible. To invert $I_N - A_0$, define

$$S_i := (I_2 + D_i)^{-1} \quad (1 \leq i \leq m), \quad S := \text{Diag}(S_1, \dots, S_m) = (I_{2m} + D)^{-1}.$$

Since $1 + \lambda_i = \tau/i$ and $J^2 = 0$, we have that $S_i = (\frac{\tau}{i}I_2 - J)^{-1} = \frac{i}{\tau}I_2 + \frac{i^2}{\tau^2}J$. Moreover,

$$I_N - A_0 = \begin{pmatrix} I_{2m} & D \\ -I_{2m} & I_{2m} \end{pmatrix},$$

so block inversion gives

$$R_0 := (I_N - A_0)^{-1} = \begin{pmatrix} S & S - I_{2m} \\ S & S \end{pmatrix}.$$

The blocks u_i^0, v_i^0 of the constant vectors u^0, v^0 , obtained from (11) and (12), satisfy

$$u_i^0 = \begin{pmatrix} \epsilon_i \\ 0 \end{pmatrix}, \quad v_i^0 = \begin{pmatrix} 0 \\ \eta_i \end{pmatrix}, \quad (\epsilon_i, \eta_i) = \begin{cases} (1, 1), & 1 \leq i \leq n, \\ (-1, 3), & n < i \leq m. \end{cases}$$

The expressions for R_0, C , and b_0 give

$$CR_0 = (c^\top S, c^\top S), \quad \tau^2 e^\top S_i = (i^2, i\tau).$$

Consequently,

$$1 + CR_0 b_0 = 1 + \frac{1}{\tau^2} \sum_{i=1}^m (\tau \eta_i i + \epsilon_i i^2).$$

For convenience, define

$$T := \tau^2 R_0, \quad q := \tau^2 + \sum_{i=1}^m (\tau \eta_i i + \epsilon_i i^2).$$

Because $\eta_i \geq 1$, $\epsilon_i \geq -1$, and $\tau > m \geq i$, we have that $\tau \eta_i i + \epsilon_i i^2 \geq i(\tau - i) > 0$ and therefore

$$1 + CR_0 b_0 = \frac{q}{\tau^2} > 0.$$

Thus the Sherman–Morrison denominator is nonzero. Since $I_N - A = (I_N - A_0) + b_0 C$, the matrix $I_N - A$ is invertible and the Sherman–Morrison formula gives

$$R := (I_N - A)^{-1} = R_0 - \frac{R_0 b_0 C R_0}{1 + CR_0 b_0}.$$

Set

$$P := qT - T b_0 C T, \quad \Delta := \tau^2 q.$$

Then $R = P/\Delta$. The transformed matrices in Lemma 6, with $\beta = 1$, are

$$A_d = 2R - I_N = \frac{2P - \Delta I_N}{\Delta}, \quad B_d = RB = \frac{PB}{\Delta}, \quad C_d = 2CR = \frac{2CP}{\Delta}.$$

Identifying the continuous-time controller K_c with x , Lemma 6 now gives

$$\begin{aligned} \Phi \text{ is satisfiable} &\iff \exists K_c \in \mathbb{R}^{n \times 1} : A + BK_c C \text{ is Hurwitz} \\ &\iff \exists K_d \in \mathbb{R}^{n \times 1} : A_d + B_d K_d C_d \text{ is Schur.} \end{aligned}$$

It remains to show that these matrices can be computed in polynomial time and that the numerators and denominators of their entries have polynomial magnitude. We establish these properties using the explicit expressions above.

We begin by observing that since τ and J are integral, our expression for S_i gives that $\tau^2 S_i = i\tau I_2 + i^2 J \in \mathbb{Z}^{2 \times 2}$. It then follows from the block expression for R_0 that $T \in \mathbb{Z}^{N \times N}$. Moreover, since τ, ϵ_i , and η_i are integers, q is a positive integer. Thus $P \in \mathbb{Z}^{N \times N}$ and $\Delta \in \mathbb{Z}_{>0}$. Now, since $\tau = O(m^3)$, and $N = 4m$, we have $\tau = N^{O(1)}$. The expressions for S_i and R_0 , together with $\tau > m \geq i$, give

$$|T_{ab}| \leq \tau^2 \quad (1 \leq a, b \leq N).$$

In addition, since every entry of b_0 has absolute value at most 3 and C is binary, we have the bounds $|(Tb_0)_a| \leq 3N\tau^2$, $|(CT)_b| \leq N\tau^2$, and

$$0 < q \leq (1 + 3N^2)\tau^2.$$

Consequently, the absolute value of each entry of the integer matrix $P = qT - Tb_0CT$ is at most $(1 + 6N^2)\tau^4 = N^{O(1)}$ while the common positive denominator Δ is at most $(1 + 3N^2)\tau^4 = N^{O(1)}$.

Finally, every entry of PB and CP is a sum of at most N products. The entries of B have absolute value at most 6, while C is binary. Therefore the integer numerators $2P - \Delta I_N$, PB , and $2CP$ of A_d , B_d , and C_d , respectively, and their common positive denominator Δ all have magnitude $N^{O(1)}$. The displayed expressions can be evaluated using polynomially many arithmetic operations on integers of polynomially bounded magnitude. Reducing the resulting fractions to lowest terms also takes polynomial time and cannot increase these bounds. Hence the reduction is computable in polynomial time and establishes strong NP-hardness. $\square$

4. REPRESENTATION OBSTRUCTION TO POLYNOMIAL-TIME ALGORITHMS

Independently of assumptions such as $P \neq NP$, we show in this section that there is a representation obstruction to polynomial-time controller synthesis: on some stabilizable instances, a polynomial-time algorithm cannot even write down a stabilizing controller (i.e. feedback gain matrix) in its standard representation. This also suggests that output feedback stabilization may not belong to NP, unless there is a polynomial-size certificate of stabilizability that avoids writing down the controller. The problem belongs to PSPACE, however, since we have already argued that it can be reduced to testing the feasibility of polynomial inequalities.

Observe that if a stabilizing controller exists, a rational one exists as well. Indeed, the sets of Hurwitz and Schur matrices are open, and $K \mapsto A + BKC$ is continuous. The set of stabilizing controllers is therefore open, and every nonempty open subset of a finite-dimensional real vector space contains a rational point.

We encode an entry a/b of A , B , or C , with $a \in \mathbb{Z}$, $b \in \mathbb{Z}_{>0}$, and $\gcd(|a|, b) = 1$, by writing its signed numerator and positive denominator explicitly in binary. Dense matrix encoding lists every entry, including zeros, which have constant encoding size. We use the elementary observation that for $a, b \in \mathbb{Z}_{>0}$ and $\varepsilon > 0$,

$$0 < \frac{a}{b} \leq \varepsilon \implies b \geq \varepsilon^{-1}. \quad (19)$$

This follows from $a \geq 1$ and applies after cancellation, so reducing a fraction cannot invalidate this denominator bound.

Theorem 7 (Continuous time). *For each integer $n \geq 1$, matrices $A \in \mathbb{Z}^{N \times N}$, $B \in \mathbb{Z}^{N \times p}$, and a nonzero row vector $C \in \{0, 1\}^{1 \times N}$ can be constructed in time polynomial in n , with*

$$N = 8n + 12, \quad p = n + 2, \quad \max_{i,j} |A_{ij}| \leq 256N^2, \quad \max_{i,j} |B_{ij}| \leq 6,$$

such that a rational stabilizing controller exists, but every (real) controller $K = (x_0, \dots, x_n, t)^\top$ for which $A + BKC$ is Hurwitz satisfies

$$0 < x_n \leq \frac{2}{3} 2^{-2^n}. \quad (20)$$

In particular, writing $x_n = a/b$ in lowest terms with $b > 0$ for any rational stabilizing controller gives $b \geq \frac{3}{2} 2^{2^n}$; this denominator alone requires more than 2^n bits, while the input size is $L_n = \Theta(n^2)$.

Proof. First, we describe the construction. We will use the definition of J, e , and $\mathcal{G}$ from Section 2. Set $m = 2n + 3$, $h = 4096m$, and, for $i = 1, \dots, m$, set $\lambda_i = ih$ and $D_i = \lambda_i I_2 - J$. Let

$$D = \text{Diag}(D_1, \dots, D_m) \in \mathbb{R}^{2m \times 2m}, \quad c = \begin{pmatrix} e \\ \vdots \\ e \end{pmatrix} \in \mathbb{R}^{2m}.$$

For $K = (x_0, \dots, x_n, t)^\top \in \mathbb{R}^p$, define $u_i(K), v_i(K) \in \mathbb{R}^2$ by

$$\begin{aligned} u_{j+1} &= \begin{pmatrix} -x_j \\ 0 \end{pmatrix}, & v_{j+1} &= \begin{pmatrix} 0 \\ t \end{pmatrix} & (0 \leq j \leq n), \\ u_{n+2+j} &= \begin{pmatrix} x_{j+1} \\ 3x_j \end{pmatrix}, & v_{n+2+j} &= \begin{pmatrix} x_j \\ t \end{pmatrix} & (0 \leq j < n), \\ u_{m-1} &= \begin{pmatrix} 6x_0 - t \\ 0 \end{pmatrix}, & v_{m-1} &= \begin{pmatrix} 0 \\ t \end{pmatrix}, \\ u_m &= \begin{pmatrix} t - 2 \\ 0 \end{pmatrix}, & v_m &= \begin{pmatrix} 0 \\ t \end{pmatrix}. \end{aligned} \tag{21}$$

Stack these vectors vertically as $u = u^0 + UK$ and $v = VK$, with $u^0 \in \mathbb{Z}^{2m}$ and $U, V \in \mathbb{Z}^{2m \times p}$. The only nonzero entry of u^0 is its $(2m - 1)$ st entry, equal to -2 . Define

$$A = \begin{pmatrix} 0 & -D - u^0 c^\top \\ I_{2m} & 0 \end{pmatrix}, \quad B = -\begin{pmatrix} U \\ V \end{pmatrix}, \quad C = (0_{1 \times 2m}, c^\top).$$

Thus $M = A + BKC$ is the matrix $\mathcal{M}$ of Lemma 2. For each controller, let $G_i = \mathcal{G}(u_i, v_i)$ and $G_0 = \text{Diag}(G_1, \dots, G_m)$. Lemma 3 gives a symmetric $X \in \mathbb{R}^{2m \times 2m}$ satisfying

$$Xc = v, \quad DX - XD^\top = vu^\top - uv^\top, \quad (X_{ii})_{11} = (G_i)_{11} \quad (1 \leq i \leq m). \tag{22}$$

Second, we show that any stabilizing controller must satisfy (20). Suppose M is Hurwitz. Since $\text{tr } M = -mt$, we have $t > 0$, and by Lemma 2(i), $X \succeq 0$. Thus X has nonnegative diagonal entries. From (22), we then have that $(G_i)_{11} = (X_{ii})_{11} \geq 0$ for $i = 1, \dots, m$. Substituting the vectors in (21) gives

$$tx_j \geq 0 \quad (0 \leq j \leq n), \quad 3x_j^2 - tx_{j+1} \geq 0 \quad (0 \leq j < n), \quad t(t - 6x_0) \geq 0, \quad t(2 - t) \geq 0.$$

Since $t > 0$, these inequalities yield:

$$\begin{aligned} x_j &\geq 0 \quad (0 \leq j \leq n), & x_0 &\leq t/6, & 0 < t &\leq 2, \\ tx_{j+1} &\leq 3x_j^2 \quad (0 \leq j < n). \end{aligned} \tag{23}$$

Moreover, we claim that $x_n > 0$. Otherwise, the first coordinates of u_{n+1} and v_{n+1} vanish. In the state partition $(\xi, \eta) \in \mathbb{R}^{2m} \times \mathbb{R}^{2m}$, the coordinates with index $q = 2n + 1$ then form the autonomous subsystem

$$\dot{\xi}_q = -\lambda_{n+1}\eta_q, \quad \dot{\eta}_q = \xi_q.$$

Its positive-definite energy $\xi_q^2 + \lambda_{n+1}\eta_q^2$ is conserved, contradicting convergence of every trajectory to zero.

Set $z_j = 3x_j/t$ for $j = 0, \dots, n$. Equations (23) give $0 \leq z_0 \leq 1/2$ and $0 \leq z_{j+1} \leq z_j^2$. Induction therefore gives

$$0 \leq \frac{x_j}{t} \leq \frac{1}{3} 2^{-2^j} \leq \frac{1}{6} \quad (0 \leq j \leq n). \tag{24}$$

Together with $x_n > 0$ and $t \leq 2$, this proves (20). The denominator bound follows from (19).

Third, we show the existence of a rational stabilizing controller. Choose

$$t = 1, \quad x_j = 12^{-2^j} \quad (0 \leq j \leq n). \tag{25}$$

To prove that $X \succ 0$, set $S_i = \text{Diag}(d_i, 1)$ and $S = \text{Diag}(S_1, \dots, S_m)$, where

$$\begin{aligned} d_{j+1} &= \sqrt{x_j} \quad (0 \leq j \leq n), & d_{n+2+j} &= x_j \quad (0 \leq j < n), \\ d_{m-1} &= 1/\sqrt{2}, & d_m &= 1. \end{aligned}$$

Every d_i lies in $(0, 1]$. Direct substitution shows that the matrices $\hat{G}_i = S_i^{-1} G_i S_i^{-1}$ are either I_2 or $F = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$. Since $F \succeq \frac{1}{3} I_2$ and by the definitions of S_i, u_i, v_i , we have

$$\hat{G}_0 := S^{-1} G_0 S^{-1} \succeq \frac{1}{3} I_{2m}, \quad \hat{\beta} := \max_{1 \leq i \leq m} \{ \|S_i^{-1} u_i\|, \|S_i^{-1} v_i\| \} \leq 2.$$

Write $\hat{X} = S^{-1} X S^{-1}$, $\hat{u}_i = S_i^{-1} u_i$, and $\hat{v}_i = S_i^{-1} v_i$. Since $S_i^{-1} J S_i = d_i J$, the off-diagonal block equations are

$$(\lambda_i - \lambda_j) \hat{X}_{ij} - d_i J \hat{X}_{ij} + d_j \hat{X}_{ij} J^\top = \hat{v}_i \hat{u}_j^\top - \hat{u}_i \hat{v}_j^\top \quad (i \neq j).$$

As $d_i, d_j \leq 1$ and $|\lambda_i - \lambda_j| \geq h \geq 4$, the triangle inequality gives $\|\hat{X}_{ij}\| \leq 4\hat{\beta}^2/h$. The diagonal correction also retains its form:

$$\hat{X}_{ii} - \hat{G}_i = -\Gamma \left(\sum_{j \neq i} \hat{X}_{ij} e \right), \quad \Gamma(z) = \begin{pmatrix} 0 & z_1 \\ z_1 & z_2 \end{pmatrix}.$$

Indeed, $S_i e = e$ and $S_i^{-1} \Gamma(S_i z) S_i^{-1} = \Gamma(z)$. Using $\|\Gamma(z)\| \leq 2\|z\|$ and the block-row-sum bound as in Lemma 3, we obtain

$$\|\hat{X} - \hat{G}_0\| \leq 3 \max_{1 \leq i \leq m} \sum_{j \neq i} \|\hat{X}_{ij}\| \leq \frac{12m\hat{\beta}^2}{h} \leq \frac{3}{256} < \frac{1}{3}.$$

Thus $\hat{X} \succ 0$ and $X \succ 0$. Also $\|u\| \leq 2\sqrt{m}$ and $\|c\| = \sqrt{m}$, so

$$\text{sym}(D + uc^\top) \succeq (h - 1 - 2m) I_{2m} \succ 0.$$

Therefore, by Lemma 2(ii), with the above choice of K , M is Hurwitz.

Lastly, we note the encoding size of the construction. The displayed block assemblies produce integer matrices with $O(n)$ nonzero entries. Their magnitudes are at most $\lambda_m = 4096m^2 = 256N^2$ in A and at most 6 in B . There are $\Theta(n^2)$ entries in the dense input and only $O(n)$ nonzero entries, each with $O(\log(n+1))$ bits. Consequently $L_n = \Theta(n^2)$, and the construction takes polynomial time. $\square$

Theorem 8 (Discrete time). *For each integer $n \geq 1$, matrices $A_d \in \mathbb{Q}^{N \times N}$, $B_d \in \mathbb{Q}^{N \times p}$, and a nonzero row vector $C_d \in \mathbb{Q}^{1 \times N}$ can be constructed in time polynomial in n , with*

$$N = 8n + 12, \quad p = n + 2,$$

and total size $L_{n,d} = \Theta(n^2)$, such that a rational stabilizing controller exists, but every (real) controller $K_d = (y_0, \dots, y_n, s)^\top$ for which $A_d + B_d K_d C_d$ is Schur satisfies

$$0 < y_n \leq \frac{2}{3} 2^{-2^n}.$$

In particular, writing $y_n = a/b$ in lowest terms with $b > 0$ for any rational stabilizing controller gives $b \geq \frac{3}{2} 2^{2^n}$; this denominator alone requires more than 2^n bits.

Proof. First, we describe the construction and use a correspondence between continuous and discrete time. To show that our construction admits a stabilizing controller, we will use the continuous-time

matrices of Theorem 7 and the continuous-to-discrete transformation from Section 3, with parameter one. For $i = 1, \dots, m$, let $a_i = 1 + \lambda_i$ and define

$$\begin{aligned} Q_0 &= \text{Diag}_{1 \leq i \leq m} \left(\frac{I_2}{a_i} + \frac{J}{a_i^2} \right) = (I_{2m} + D)^{-1}, \\ \delta &= 1 + c^\top Q_0 u^0 = 1 - \frac{2}{a_m^2} > 0, \quad Q = Q_0 - \frac{Q_0 u^0 c^\top Q_0}{\delta}. \end{aligned} \quad (26)$$

The Sherman–Morrison formula gives $Q = (I_{2m} + D + u^0 c^\top)^{-1}$. Block multiplication then gives

$$R := (I_N - A)^{-1} = \begin{pmatrix} Q & Q - I_{2m} \\ Q & Q \end{pmatrix}, \quad c^\top Q = \frac{c^\top Q_0}{\delta}.$$

Set

$$A_d = 2R - I_N, \quad B_d = RB, \quad C_d = 2CR, \quad f = CRB \in \mathbb{Q}^{1 \times p}. \quad (27)$$

Note that f is a row vector and thus $fK = CRBK$ is a scalar for each controller $K \in \mathbb{R}^{p \times 1}$.

For $M = A + BKC$ and $M_d = A_d + B_d K_d C_d$, the matrix determinant lemma gives

$$\begin{aligned} \det(I_N - M) &= \det(I_N - A)(1 - fK), \\ \det(I_N + M_d) &= 2^N \det(R)(1 + fK_d). \end{aligned}$$

If M is Hurwitz, then $I_N - M$ is invertible; if M_d is Schur, then $I_N + M_d$ is invertible. Thus the denominators $1 - fK$ and $1 + fK_d$ in the inverse controller maps

$$K_d = \frac{K}{1 - fK}, \quad K = \frac{K_d}{1 + fK_d} \quad (28)$$

do not vanish at stabilizing controllers. The Sherman–Morrison formula yields

$$M_d = 2(I_N - M)^{-1} - I_N = (I_N + M)(I_N - M)^{-1}.$$

For any symmetric matrix $P \in \mathbb{R}^{N \times N}$, we have

$$M_d^\top P M_d - P = 2(I_N - M)^{-\top} (M^\top P + P M) (I_N - M)^{-1}.$$

Lemma 6 shows that (28) is a bijection between stabilizing controllers. It preserves rationality, so the controller (25) gives a rational Schur stabilizer.

Second, we show that the entry y_n of any Schur-stabilizing controller satisfies the claimed bound. For every continuous-time stabilizer, (23) and (24) give $t > 0$ and $0 \leq x_j \leq t/6$. Let $u_i^0 \in \mathbb{R}^2$ be block i of u^0 , and set $w_i = u_i - u_i^0 + v_i$. From the definitions of u_i and v_i in (21) it follows that $(w_i)_1 \geq -t$ and $(w_i)_2 \geq t$ for $1 \leq i \leq m$. Equations (26)–(27) imply

$$fK = -\frac{1}{\delta} \sum_{i=1}^m \left(\frac{(w_i)_1}{a_i^2} + \frac{(w_i)_2}{a_i} \right) < 0,$$

because each summand is at least $t(a_i^{-1} - a_i^{-2}) > 0$. Thus $1 - fK > 1$. Every Schur-stabilizing controller corresponds to such a continuous-time controller, and therefore

$$0 < y_n = \frac{x_n}{1 - fK} \leq x_n \leq \frac{2}{3} 2^{-2^n}.$$

The denominator conclusion follows from (19).

Lastly, we note the encoding size of the construction. Each row and column of Q_0 has at most two nonzero entries, all with $O(\log(n+1))$ bits. Since $Q_0 u^0$ has only two nonzero entries, (26)–(27) show that Q, R, A_d , and C_d also have $O(n)$ nonzero entries, each with $O(\log(n+1))$ bits. For $W = U + V \in \mathbb{Z}^{2m \times p}$, we have

$$B_d = \begin{pmatrix} V - QW \\ -QW \end{pmatrix}, \quad QW = Q_0 W - \frac{(Q_0 u^0)(c^\top Q_0 W)}{\delta}.$$

Every column of W except its last has at most four nonzero entries. Thus B_d has $O(n)$ nonzero entries, each of $O(\log(n+1))$ bits, except possibly four entries in its last column. Those entries involve sums of $O(n)$ rational terms and have $O(n \log(n+1))$ bits. Including all zero entries, the input size is therefore $L_{n,d} = \Theta(n^2)$. $\square$

REFERENCES

- [1] V. Blondel, M. Gevers, and A. Lindquist, Survey on the state of systems and control, *European Journal of Control*, **1**(1) (1995), 5–23.
- [2] V. Blondel and J. N. Tsitsiklis, NP-hardness of some linear control design problems, *SIAM Journal on Control and Optimization*, **35**(6) (1997), 2118–2127.
- [3] S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*, SIAM Studies in Applied Mathematics, vol. 15, Society for Industrial and Applied Mathematics, Philadelphia, 1994.
- [4] A. Chaudhry, *Algebraic Methods in Convex Geometry, Nonlinear Optimization, and Learning Dynamical Systems*, Ph.D. thesis, Princeton University, 2024. <https://dataspace.princeton.edu/handle/88435/dsp01vt150n65n>.
- [5] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W. H. Freeman and Company, San Francisco, 1979.
- [6] D. Yu. Grigor’ev and N. N. Vorobjov, Jr., Solving systems of polynomial inequalities in subexponential time, *Journal of Symbolic Computation*, **5** (1988).
- [7] O. J. Staffans, *Well-Posed Linear Systems*, Encyclopedia of Mathematics and its Applications, vol. 103, Cambridge University Press, Cambridge, 2005.
- [8] W. M. Wonham, *Linear Multivariable Control: A Geometric Approach*, Springer-Verlag, New York, 1979.
- [9] R. Bellman, *Introduction to Matrix Analysis*, McGraw-Hill, New York, 1960.