Probability estimates for reachability of linear systems defined over finite fields

Lieb, Julia ; Jordan, Jens ; Helmke, Uwe

DOI: https://doi.org/10.3934/amc.2016.10.63

Advances in Mathematics of Communications
Volume 10, No. 1, 2016, 63–78
doi:10.3934/amc.2016.10.63

PROBABILITY ESTIMATES FOR REACHABILITY OF LINEAR SYSTEMS DEFINED OVER FINITE FIELDS

Uwe Helmke, Jens Jordan and Julia Lieb

Institute of Mathematics
University of Würzburg
97074 Würzburg, Germany

(Communicated by Paula Rocha)

Abstract. This paper deals with the probability that random linear systems defined over a finite field are reachable. Explicit formulas are derived for the probabilities that a linear input-state system is reachable, that the reachability matrix has a prescribed rank, as well as for the number of cyclic vectors of a cyclic matrix. We also estimate the probability that the parallel connection of finitely many single-input systems is reachable. These results may be viewed as a first step to calculate the probability that a network of linear systems is reachable.

1. Introduction

Linear systems over finite fields play an important role in many mathematical areas, including, e.g., convolutional codes [13, 14], finite state automata and Boolean networks [9], network coding [7], and quantised information dissemination [15]. Since convolutional codes are dual to complete linear behaviors [13], they can be regarded as discrete linear systems over a finite field. Thus, fundamental concepts from control theory such as reachability and observability play a role in convolutional coding theory. In particular, reachability is necessary for the equivalence between non-catastrophicity and observability [14]. Moreover, observability is dual to reachability, so that the non-catastrophicity of a code can be guaranteed by two reachability conditions. Furthermore, it is stated in [14] that reachability and observability are necessary conditions if one tries to find a convolutional code with good distance properties.

In linear systems theory, the role of parallel, series and feedback interconnection has been recognized from early on since these operations constitute the building blocks for designing arbitrary networks of control systems. More recently, the importance of parallel and series interconnections for convolutional coding theory has been observed in, e.g., [1], where sufficient conditions for the minimality and observability of concatenations for two convolutional codes are derived. These concatenations consist of a specific combination of series and parallel connections of associated first order system realizations and thus allow for a system theoretic analysis. Moreover, in [8], so called woven convolutional codes, which are networks of convolutional codes consisting of series and parallel connections, are studied with

2010 *Mathematics Subject Classification:* Primary: 93B05, 93C05, 11T06; Secondary: 93B25, 93C55.

Key words and phrases: Linear systems, finite fields, reachability, Grassmann manifolds, parallel connection.

The first author is affiliated with AIMS.

the aim to achieve encoders with large free distances. This motivates us to investigate reachability problems for networks of linear systems over finite fields.

Further motivation for studying the interaction between systems theory and coding theory is provided from the fact that convolutional network codes as defined in [7] can be viewed as structured linear systems over finite fields. Typically, for network coding with acyclic networks, block codes are used. However, for networks containing cycles, convolutional codes suggest themselves as building blocks. Thus, using convolutional network coding, it becomes possible to extend solvability criteria for linear network coding problems to networks with cycles [7, Theorem 2.7].

In all such applications it becomes important to estimate the probability that randomly chosen interconnections in networks of linear systems entail reachability. A special case in point is the recent work [15], where probability estimates are derived for structural reachability of systems over finite fields. This covers the case where the node dynamics are first order one-dimensional systems. Similar investigations for general networks are unknown.

In this paper we consider parallel connections of N discrete-time linear systems defined over a finite field $\mathbb{F}$. This interconnection structure could be interpreted as a network consisting of several independent blocks of nodes. Our goal is to establish a formula for the probability that such a system is reachable. Two cases of interest are considered, that of $N = 1$ and the parallel connection of single-input systems. Our first result is Theorem 1 that yields an explicit formula for the number of reachable pairs, i.e. covers the case $N = 1$. This extends earlier results by [10], derived for at most two inputs. The proof of Theorem 1 rests on the Hermite cell decomposition of the quotient space of reachable pairs, introduced in [5] and [6]. As a next step, Theorem 1 is extended by calculating the number of state space pairs with a reachability space of fixed dimension. Moreover, in section 2.4, we consider the closely related task of obtaining a formula for the probability that a vector is a cyclic vector of a matrix. Finally, Theorem 7 estimates the probability that the parallel connection of $N \geq 2$ single-input systems is reachable. This is based on a formula for the number of N-tuples of pairwise coprime polynomials over $\mathbb{F}$.

2. Probability of reachable properties

We begin with a brief summary of well-known properties of Grassmannians over a finite field $\mathbb{F}$ with cardinality $|\mathbb{F}|$. Throughout this paper $\mathbb{F}$ is endowed with the uniform probability distribution that assigns to each field element the same probability

$$t = \frac{1}{|\mathbb{F}|}.$$

2.1. Counting points of the Grassmannian.

The **Grassmannian** over a finite field $\mathbb{F}$ is the set $G_k(\mathbb{F}^n)$ of all k-dimensional linear subspaces $V \subset \mathbb{F}^n$ (more precisely, it is the set of $\mathbb{F}$-rational points of the Grassmann variety but this distinction does not play a significant role in this paper). To count the number of elements in $G_k(\mathbb{F}^n)$ one can proceed in at least two different ways. The first approach identifies the Grassmann manifold $G_k(\mathbb{F}^n)$ of k-dimensional linear subspaces of $\mathbb{F}^n$ with the homogeneous space $GL_n(\mathbb{F})/\mathcal{P}$ by the parabolic subgroup

$$\mathcal{P} = \begin{pmatrix} GL_k(\mathbb{F}) & \mathbb{F}^{k\times(n-k)} \\ 0 & GL_{n-k}(\mathbb{F}) \end{pmatrix}$$

of block upper triangular matrices. It is well-known and easily established that the general linear group $GL_n(\mathbb{F})$ of invertible $n \times n$-matrices has exactly

$$|GL_n(\mathbb{F})| = t^{-n^2} \prod_{j=1}^{n} (1 - t^j) \tag{1}$$

elements. Therefore the Grassmannian $G_k(\mathbb{F}^n)$ has exactly

$$|G_k(\mathbb{F}^n)| = \frac{|GL_n(\mathbb{F})|}{|GL_k(\mathbb{F})||GL_{n-k}(\mathbb{F})||\mathbb{F}^{k\times(n-k)}|} = t^{-k(n-k)} \prod_{j=1}^{n-k} \frac{(1 - t^{k+j})}{(1 - t^j)} \tag{2}$$

points. In particular, one obtains the well-known formula $1 + t^{-1} + \cdots + t^{1-n}$ for the cardinality of the projective space $\mathbb{P}^{n-1}(\mathbb{F})$.

Alternatively, one constructs a cell decomposition of the Grassmannian $G_k(\mathbb{F}^n)$

$$G_k(\mathbb{F}^n) = \bigsqcup_{a \in \mathcal{A}_{k,n}} S(a)$$

into finitely many disjoint Euclidean spaces $S(a)$; see e.g. [11]. Recall that a Schubert-cell $S(a) \subset G_k(\mathbb{F}^n)$ is defined for each sequence $a = (a_1, \ldots, a_k)$ of strictly increasing integers $1 \leq a_1 < \ldots < a_k \leq n$. Let $\mathcal{A}_{k,n}$ denote the set of such sequences a. Thus $S(a)$ can be identified with the set of all full row rank $k \times n$ matrices X that are in a-row echelon canonical form, i.e. $X = (x_{ij}) \in \mathbb{F}^{k\times n}$ has the standard basis vectors $e_1, \ldots, e_k$ at columns $a_1, \ldots, a_k$ and satisfies $x_{ij} = 0$ for $j < a_i$.

For example, take $k = 2, n = 5$ and $a = (2, 4)$. Then the 3-dimensional Schubert cell $S(a)$ is described by all matrices of the form

$$\begin{pmatrix} 0 & 1 & x_{13} & 0 & x_{15} \\ 0 & 0 & 0 & 1 & x_{25} \end{pmatrix}.$$

A simple counting argument shows that each Schubert cell $S(a)$ is uniquely characterized by exactly

$$\dim S(a) = d(a) := k(n - k) - \sum_{i=1}^{k} (a_i - i) \tag{3}$$

free parameters and therefore consists of $t^{-d(a)}$ elements. This implies that the number of elements of the Grassmannian is given as

$$|G_k(\mathbb{F}^n)| = \sum_{a \in \mathcal{A}_{k,n}} t^{-d(a)}. \tag{4}$$

In particular, we deduce from (2) the identity of power series

$$\sum_{a \in \mathcal{A}_{k,n}} t^{-d(a)} = t^{-k(n-k)} \prod_{j=1}^{k} \frac{(1 - t^{n-k+j})}{(1 - t^j)}. \tag{5}$$

2.2. PROBABILITY OF A SYSTEM TO BE REACHABLE. We consider linear control systems of the form

$$x(\tau + 1) = Ax(\tau) + Bu(\tau), \quad x(0) = 0, \quad \tau = 0, 1, 2, \ldots \tag{6}$$

with system matrices $A \in \mathbb{F}^{n\times n}, B \in \mathbb{F}^{n\times m}$; see [3] for a summary of linear systems theory developed over an arbitrary field.

A linear system (6) is called reachable if for each $\xi \in \mathbb{F}^n$ there exists a finite sequence of inputs $u(0), \ldots, u(\tau_*) \in \mathbb{F}^m$ such that the sequence of states $x(0), x(1), \ldots,$

$x(\tau_* + 1)$ generated by (6) satisfies $x(\tau_* + 1) = \xi$. We then say that ξ is reached from the initial condition $x(0) = 0$ in $\tau_* + 1$ steps. A simple characterization of reachable linear systems is available using the so-called Kalman test. Explicitly, (6) is reachable if and only if the $n \times nm$-reachability matrix satisfies

$$rank(B, AB, \dots, A^{n-1}B) = n. \tag{7}$$

Let $\Sigma^{cr}_{n,m}(\mathbb{F})$ denote the set of all such reachable pairs and let $|\Sigma^{cr}_{n,m}(\mathbb{F})|$ denote its cardinality. We are interested in calculating the number of reachable pairs $(A, B) \in \mathbb{F}^{n\times n} \times \mathbb{F}^{n\times m}$, i.e., in calculating $|\Sigma^{cr}_{n,m}(\mathbb{F})|$. Equivalently, for the equidistribution on $\mathbb{F}^{n\times(n+m)}$, we compute the probability

$$P_{n,m}(t) := \frac{|\Sigma^{cr}_{n,m}(\mathbb{F})|}{|\mathbb{F}^{n\times n} \times \mathbb{F}^{n\times m}|}$$

of a pair $(A, B) \in \mathbb{F}^{n\times n} \times \mathbb{F}^{n\times m}$ to be reachable. Our first theorem generalizes an earlier result by [10], that has been restricted to the case $m \leq 2$.

Theorem 1. *The probability that a pair $(A, B) \in \mathbb{F}^{n\times n} \times \mathbb{F}^{n\times m}$, $n, m \geq 1$, is reachable is equal to*

$$P_{n,m}(t) = \prod_{j=m}^{n+m-1} (1 - t^j) = 1 - t^m + O(t^{m+1}). \tag{8}$$

In particular, one obtains for $n \geq 2$:

$$(1 - t^m)(1 - (n - 1)t^{m+1}) \leq P_{n,m}(t) \leq (1 - t^m)(1 - t^{m+1}). \tag{9}$$

Proof. Clearly, reachability is invariant under the state space similarity transformations $(A, B) \mapsto (TAT^{-1}, TB)$ with $T \in GL_n(\mathbb{F})$. Thus $GL_n(\mathbb{F})$ acts on $\Sigma^{cr}_{n,m}(\mathbb{F})$ via similarity. Denote the corresponding orbit space by $\Sigma_{n,m}(\mathbb{F})$. Since (A, B) is reachable, the similarity action is a free action and therefore the map

$$GL_n(\mathbb{F}) \to GL_n(\mathbb{F}) \cdot (A, B), \quad T \mapsto (TAT^{-1}, TB)$$

from the group to the group orbit is injective. This implies that the cardinalities of $\Sigma^{cr}_{n,m}(\mathbb{F})$ and $\Sigma_{n,m}(\mathbb{F})$ are related as

$$|\Sigma^{cr}_{n,m}(\mathbb{F})| = |GL_n(\mathbb{F})| \cdot |\Sigma_{n,m}(\mathbb{F})|.$$

Thus it amounts to determine the number of $\mathbb{F}$-rational points in the quasi-affine algebraic variety $\Sigma_{n,m}(\mathbb{F})$. This we do following [5], using a cell decomposition of $\Sigma_{n,m}(\mathbb{F})$ that is obtained by fixing the so-called Hermite indices of reachable pairs. This is the main point where our analysis departs from [10], who use the more complicated Kronecker invariants rather the Hermite indices. We refer to [5] and [6] for further details and proofs of the subsequent statements on cell decompositions of $\Sigma_{n,m}(\mathbb{F})$. Specifically, $\Sigma_{n,m}(\mathbb{F})$ admits a disjoint decomposition into finitely many affine spaces

$$\Sigma_{n,m}(\mathbb{F}) = \bigsqcup_{K\in K_{n,m}} Her_K,$$

that is parameterized by the combinations $K = (K_1, \dots, K_m)$ of n into m parts. Here the Hermite cells

$$Her_K = \mathbb{F}^{n(K)}$$

are affine spaces of dimension $n(K) = \sum_{i=1}^{m}(m-i+1)K_i$. In contrast, the Grassmannian $G_{m-1}(\mathbb{F}^{n+m-1})$ has the cell decomposition

$$G_{m-1}(\mathbb{F}^{n+m-1}) = \bigsqcup_{a \in \mathcal{A}_{m-1,n+m-1}} S(a),$$

into finitely many Schubert cells $S(a) = \mathbb{F}^{d(a)}$, where $d(a)$ is given by (3). Clearly, the map $f : K_{n,m} \longrightarrow \mathcal{A}_{m-1,n+m-1}$

$$(K_1, \ldots, K_m) \mapsto a_K := (K_m + 1, K_m + K_{m-1} + 2, \ldots, K_m + \cdots + K_2 + m - 1)$$

is bijective and therefore defines a bijection $Her_K \mapsto S(a_K)$ of Hermite cells and Schubert cells, respectively. Since

$$nm - \sum_{i=1}^{m}(m-i+1)K_i = \sum_{i=1}^{m}\left(n - \sum_{j=1}^{i} K_j\right) = \sum_{i=1}^{m-1}\left(\sum_{j=i+1}^{m} K_j\right),$$

one obtains

$$\begin{aligned} \dim S(a_K) &= n(m-1) + \frac{(m-1)m}{2} - \sum_{i=1}^{m-1}\left(\sum_{j=i+1}^{m} K_j + m - j + 1\right) \\ &= n(m-1) - \sum_{i=1}^{m-1}\left(\sum_{j=i+1}^{m} K_j\right) = \dim Her_K - n, \end{aligned}$$

for all $K \in K_{n,m}$. In particular, both spaces $\Sigma_{n,m}(\mathbb{F})$ and $G_{m-1}(\mathbb{F}^{n+m-1})$ admit cell decompositions that are indexed by the combinations of n into m nonnegative parts. Moreover, the mutual dimensions of the Schubert and Hermite cells differ by n, respectively. Thus, although no direct relation between these very different spaces is known, the cardinalities of their $\mathbb{F}$-rational points can be easily compared. Explicitly, one obtains

(10)
$$|\Sigma_{n,m}(\mathbb{F})| = \sum_{K \in K_{n,m}} t^{-n(K)} = t^{-n} \sum_{a \in \mathcal{A}_{m-1,n+m-1}} t^{-d(a)} = t^{-n}|G_{m-1}(\mathbb{F}^{n+m-1})|.$$

By (2), the Grassmannian $G_{m-1}(\mathbb{F}^{n+m-1})$ has exactly

$$t^{-n(m-1)} \prod_{j=1}^{n} \frac{(1-t^{m+j-1})}{(1-t^j)}$$

elements. Thus the cardinality of $\Sigma^{cr}_{n,m}(\mathbb{F})$ is equal to

$$|\Sigma^{cr}_{n,m}(\mathbb{F})| = |GL_n(\mathbb{F})||\Sigma_{n,m}(\mathbb{F})| = t^{-n(m+n)} \cdot \prod_{j=m}^{n+m-1}(1-t^j),$$

which completes the proof of (8). □

2.3. SYSTEMS WITH r-DIMENSIONAL REACHABILITY SUBSPACE. One can extend Theorem 1 in a rather straightforward way to determine the number of pairs (A, B) with r-dimensional reachability subspace. Consider, for $r = 0, \ldots, n$, the set

$$S^r_{n,m}(\mathbb{F}) := \{(A, B) \in \mathbb{F}^{n\times n} \times \mathbb{F}^{n\times m} \mid rank(B, AB, \cdots, A^{n-1}B) = r\}.$$

In particular, $\Sigma^{cr}_{n,m}(\mathbb{F}) = S^n_{n,m}(\mathbb{F})$. To compute the cardinality of $S^r_{n,m}(\mathbb{F})$, consider the set S_r of all systems of the form

$$A = \begin{pmatrix} A_1 & A_2 \\ 0 & A_3 \end{pmatrix}, \quad B = \begin{pmatrix} B_1 \\ 0 \end{pmatrix},$$

where $(A_1, B_1) \in \Sigma^{cr}_{r,m}(\mathbb{F})$ and $A_2 \in \mathbb{F}^{(r\times(n-r))}$ and $A_3 \in \mathbb{F}^{((n-r)\times(n-r))}$ are arbitrary. This space has cardinality

$$|S_r| = t^{-n(n-r)}|\Sigma^{cr}_{r,m}(\mathbb{F})| = t^{-n^2+r(n-m)} \prod_{j=m}^{r+m-1}(1-t^j).$$

Theorem 2. *The cardinality of $S^r_{n,m}(\mathbb{F})$ is equal to*

$$|S^r_{n,m}(\mathbb{F})| = t^{-n^2-rm} \frac{\prod_{j=r+1}^{n}(1-t^j)\prod_{j=m}^{r+m-1}(1-t^j)}{\prod_{j=1}^{n-r}(1-t^j)}. \tag{11}$$

Proof. Let $\mathcal{P} \subset GL_n(\mathbb{F})$ denote the parabolic subgroup of all block upper triangular matrices of the form

$$p \in \mathcal{P} = \begin{pmatrix} GL_r(\mathbb{F}) & \mathbb{F}^{r\times(n-r)} \\ 0 & GL_{n-r}(\mathbb{F}) \end{pmatrix}$$

which acts on the product space $GL_n(\mathbb{F}) \times S_r$ via

$$(g, (A, B)) \mapsto (gp^{-1}, (pAp^{-1}, pB)). \tag{12}$$

Let $GL_n(\mathbb{F}) \times_{\mathcal{P}} S_r$ denote the quotient space with respect to this free group action. This yields the well-defined map $\phi : GL_n(\mathbb{F}) \times_{\mathcal{P}} S_r \longrightarrow S^r_{n,m}(\mathbb{F})$ that sends each orbit $[g, (A, B)]$ of (12) to the element (gAg^{-1}, gB). This map is a bijection and induces a $G_r(\mathbb{F}^n)$-bundle on S_r. Therefore one obtains the equality of cardinalities $|GL_n(\mathbb{F})\times_{\mathcal{P}} S_r| = |S^r_{n,m}(\mathbb{F})|$. Moreover, the cardinality of the orbit space $GL_n(\mathbb{F})\times_{\mathcal{P}} S_r$ is equal to

$$\frac{|GL_n(\mathbb{F})||S_r|}{|\mathcal{P}|} = |G_r(\mathbb{F}^n)||S_r|.$$

Using Theorem 1, this implies

$$\begin{aligned} |S^r_{n,m}(\mathbb{F})| &= t^{r^2-n^2} \frac{\prod_{j=r+1}^{n}(1-t^j)}{\prod_{j=1}^{n-r}(1-t^j)} |\Sigma^{cr}_{r,m}(\mathbb{F})| \\ &= t^{-n^2-rm} \frac{\prod_{j=r+1}^{n}(1-t^j)\prod_{j=m}^{r+m-1}(1-t^j)}{\prod_{j=1}^{n-r}(1-t^j)}. \end{aligned}$$

This completes the proof. □

2.4. PROBABILITY OF CYCLIC VECTORS. Motivated by the fact that a pair (A, b) is reachable if and only if b is a cyclic vector of A, we consider the following question: Given an arbitrary cyclic matrix $A \in \mathbb{F}^{n\times n}$, what is the probability that a vector $b \in \mathbb{F}^n$ is cyclic?

Thus define

$$N_1(A) := |\{b \in \mathbb{F}^n \mid (A, b) \text{ is reachable}\}|$$

and let

$$q(z) = q_1(z)^{\nu_1} \cdots q_r(z)^{\nu_r}$$

denote the decomposition in irreducible factors $q_1(z), \ldots, q_r(z)$ of the characteristic polynomial $q(z) = \det(zI - A)$. Then the probability of cyclic vectors is given as the fraction

$$\frac{N_1(A)}{|\mathbb{F}|^n}.$$

The next result gives an explicit formula for the probability that a vector is cyclic.

Theorem 3. *The probability of $b \in \mathbb{F}^n$ to be a cyclic vector of A is equal to*

$$(1 - t^{n_1}) \cdots (1 - t^{n_r}), \tag{13}$$

where $n_1, \ldots, n_r$ are the degrees of the distinct irreducible factors $q_1(z), \ldots, q_r(z)$ in the prime decomposition of $\det(zI - A)$.

Proof. Since A is cyclic, one can assume that A is in companion canonical form. Thus, without loss of generality, we can assume that $A = S_q$ is the shift operator on the polynomial model $X_q := \mathbb{F}[z]/q(z)\mathbb{F}[z]$ and b can be identified with an arbitrary element $p(z)$ with $\deg(p) < \deg(q)$. Therefore the question is equivalent to that of determing the probability that a polynomial $p(z)$ of degree $< n$ is coprime with $q(z)$. Now $p(z)$ is coprime with $q(z)$ if and only if $p(z)$ is a unit of the ring X_q. By the Chinese Remainder Theorem and using the primary decomposition of $q(z)$, the ring X_q is isomorphic to the direct product of rings

$$X_q \simeq X_{q_1^{\nu_1}} \times \ldots \times X_{q_r^{\nu_r}}.$$

Via this representation, the units of X_q are seen to be in bijective correspondence with the r-tuples of units in $X_{q_1^{\nu_1}}, \ldots, X_{q_r^{\nu_r}}$, respectively. On the other hand the number of units of $X_{q_i^{\nu_i}}$ is equal to $|\mathbb{F}^{n_i\nu_i}| - |\mathbb{F}^{n_i(\nu_i-1)}|$, where $n_i := \deg q_i$. Thus the number of units of X_q is equal to

$$\prod_{i=1}^{r} \left(t^{-n_i\nu_i} - t^{-n_i(\nu_i-1)} \right) = t^{-n} \prod_{i=1}^{r} (1 - t^{n_i}).$$

The result follows. □

3. Parallel connection of single-input systems

The aim of this section is to compute the probability that the parallel connected system

$$\begin{aligned} x_1(\tau + 1) &= A_1 x_1(\tau) + b_1 u(\tau) \\ &\vdots \\ x_N(\tau + 1) &= A_N x_N(\tau) + b_N u(\tau) \end{aligned} \tag{14}$$

with state vectors $x_i \in \mathbb{F}^{n_i}$ for $i = 1, \ldots, N$ and input $u \in \mathbb{F}$ is reachable. In the first part we present explicit formulas for the probability of (14) to be reachable. For $N > 2$ the formula becomes very complex and difficult to evaluate. However, in part 2 of the section we derive asymptotic estimations.

3.1. PROBABILITY OF REACHABILITY: EXPLICIT EXPRESSIONS. Throughout this section, let gcd and lcm denote the **monic** greatest common divisor and least common multiple, respectively. For $(A,b) \in \mathbb{F}^{n\times n} \times \mathbb{F}^n$ let

$$(zI-A)^{-1}b = (p_1(z),\dots,p_n(z))^\top \cdot d(z)^{-1}$$

be a (not necessarily coprime) factorization of the transfer function by polynomials $p_1,\dots,p_n,d \in \mathbb{F}[z]$, $d \not\equiv 0$. The next characterization of reachability is well-known; the proof is inserted for convenience of the reader.

Lemma 1. *A single-input system (A,b) is reachable if and only if the polynomials $p_1,\dots,p_n$ are linearly independent over $\mathbb{F}$.*

Proof. By the Kalman test (7) system (A,b) is reachable if and only if $c=0$ is the only solution of $cA^ib=0$ for $0\le i\le n-1$ with $c^\top \in \mathbb{F}^n$. Note that $cA^ib=0$ for $0\le i\le n-1$ implies $cA^ib=0$ for $i\ge 0$ by the theorem of Cayley-Hamilton. Since $(zI-A)^{-1} = \sum_{i=0}^{\infty} \frac{A^i}{z^{i+1}}$, reachability is equivalent to the fact that $c=0$ is the only solution of $c(zI-A)^{-1}b \equiv 0$ with $c^\top \in \mathbb{F}^n$. This means that $c(p_1(z),\dots,p_n(z))^\top \equiv 0$ for some $c^\top \in \mathbb{F}^n$ implies $c=0$, i.e. $p_1,\dots,p_n$ are linearly independent over $\mathbb{F}$. □

Moreover, we need the following lemma:

Lemma 2. *If $p_1,\dots,p_n \in \mathbb{F}[z]$, with $\deg(p_i) \le n-1$ for $i=1,...,n$, are linearly independent over $\mathbb{F}$, then $\gcd(p_1,\dots,p_n)=1$.*

Proof. Suppose $\gcd(p_1,\dots,p_n)=g\neq 1$, i.e. $\deg(g)\ge 1$. Consequently, there exist $\bar{p}_i$ with $p_i = g\bar{p}_i$ and $\deg(\bar{p}_i)\le n-2$. Then $a_1\bar{p}_1+\cdots+a_n\bar{p}_n=0$ with $a_1,\dots,a_n\in\mathbb{F}$ implies $a_1p_1+\cdots+a_np_n=0$ and therefore $a_1=\cdots=a_n=0$ since $p_1,\dots,p_n$ are linearly independent. Hence $\bar{p}_1,\dots,\bar{p}_n$ are linearly independent, which is a contradiction to $\deg(\bar{p}_i)\le n-2$. □

Now we compute the probability that a parallel connection of two linear systems is reachable, i.e. we solve the problem for $N=2$:

Theorem 4. *For $i=1,2$ and randomly chosen matrices $A_i \in \mathbb{F}^{n_i\times n_i}$ and vectors $b_i \in \mathbb{F}^{n_i}$ the probability that the parallel connected system*

$$\begin{aligned} x_1(\tau+1) &= A_1x_1(\tau)+b_1u(\tau) \\ x_2(\tau+1) &= A_2x_2(\tau)+b_2u(\tau) \end{aligned} \tag{15}$$

with state vectors $x_i \in \mathbb{F}^{n_i}$ and input $u\in\mathbb{F}$ is reachable is equal to the number of tuples (d_1,d_2) of monic pairwise coprime polynomials of degrees n_1 and n_2 times $|GL_{n_1}(\mathbb{F})|\cdot|GL_{n_2}(\mathbb{F})|$; in particular, this probability is equal to

$$(1-t)\prod_{j=1}^{n_1}(1-t^j)\prod_{j=1}^{n_2}(1-t^j). \tag{16}$$

Proof. For $i=1,2$ assume that (A_i,b_i) are reachable and consider factorizations

$$(zI-A_i)^{-1}b_i = P_i(z)d_i(z)^{-1},\ P_i(z) := \operatorname{adj}(zI-A_i)b_i,\ d_i(z) := \det(zI-A_i),$$

i.e. $d_i\in\mathbb{F}[z]$ monic, $P_i\in\mathbb{F}^{n_i}[z]$ with $\deg(P_i)<\deg(d_i)=n_i$.

From Lemma 1 it follows that the entries of P_i are linearly independent, and consequently P_i and d_i are coprime (see Lemma 2). Since d_i is scalar, these coprime factorizations are unique up to multiplying each factor with a nonzero constant. This constant must be one because d_i is monic. Thus one can map each reachable pair (A_i,b_i) to a unique element (P_i,d_i), where d_i monic, $\deg(P_i)<\deg(d_i)=n_i$

and the entries of P_i are linearly independent. This map is denoted by f_i and is injective because the realization of a transfer function is unique in the case of single input systems.

According to Theorem 1 (with $m = 1$) there are $t^{-(n_i^2+n_i)} \prod_{j=1}^{n_i}(1-t^j)$ reachable pairs (A_i, b_i). On the other hand one has t^{-n_i} possibilities for d_i and $|GL_{n_i}(\mathbb{F})| = t^{-n_i^2} \prod_{j=1}^{n_i}(1-t^j)$ possibilities for P_i. Therefore the sets of pairs (A_i, b_i) and (P_i, d_i) have the same cardinality. Thus f_i is a bijection and one can consider the pairs (P_i, d_i) instead of (A_i, b_i).

In [2] Fuhrmann has shown that reachability of (15) is equivalent to the fact that the scalar polynomials d_1 and d_2 are pairwise coprime if the single systems are reachable. The number of coprime pairs of monic polynomials (d_1, d_2) is equal to $t^{-n_1-n_2}(1-t)$; see [4]. By Lemma 1, the pairs (A_i, b_i) are reachable if and only if the entries of the polynomial vectors $P_i(z)$ are linearly independent over $\mathbb{F}$. In particular, reachability of the systems depends only on P_i. Thus the number of systems (A_i, b_i) such that (15) is reachable coincides with the number of tuples (d_1, d_2) of monic pairwise coprime polynomials of degrees n_1 and n_2 times $|GL_{n_1}(\mathbb{F})| \cdot |GL_{n_2}(\mathbb{F})|$. Hence the total number of systems (A_i, b_i) such that (15) is reachable is

$$t^{-(n_1+n_2)}(1-t) \cdot t^{-n_1^2} \prod_{j=1}^{n_1}(1-t^j) \cdot t^{-n_2^2} \prod_{j=1}^{n_2}(1-t^j).$$

Therefore the considered probability is equal to

$$(1-t) \prod_{j=1}^{n_1}(1-t^j) \prod_{j=1}^{n_2}(1-t^j),$$

which proves the theorem. □

We next attempt to extend these arguments to the parallel connection of $N \geq 2$ single-input systems. As in the proof of Theorem 4, consider coprime factorizations of the corresponding transfer functions $(zI - A_i)^{-1}b_i = P_i(z)d_i(z)^{-1}$ for $i = 1, \ldots, N$. Fuhrmann's characterization of reachability of two parallel connected systems is easily extended to more than two node systems. Explicitly, see [3], system (14) is reachable if and only if (A_i, b_i) are reachable for $i = 1, \ldots, N$ and $d_1, \ldots, d_N$ are pairwise coprime. Thus one has to compute the number of N-tuples $(d_1, \ldots, d_N)$ of monic pairwise coprime polynomials of given degrees $n_1, \ldots, n_N$.

To this end we first prove the following theorem, which extends a result by [12] from the ring of integers to the ring of polynomials. Let $n := (n_1, \ldots, n_N) \in \mathbb{N}^N$ and Γ be an undirected graph with set of vertices $\mathcal{V} = \{1, \ldots, N\}$ and set of edges $\mathcal{E}$, having cardinality $E := |\mathcal{E}|$. The edges of Γ are denoted as ij, for suitable $i, j \in \mathcal{V}$ with $i < j$. For every vertex $l \in \mathcal{V}$ let

$$\mathcal{E}_l := \{ij \in \mathcal{E} \mid i = l \text{ or } j = l\}$$

denote the set of edges terminating at l. With each edge ij of Γ we associate a monic, square-free polynomial $k_{ij}(z) \in \mathbb{F}[z]$. We refer to this as a polynomial labeling of the graph and denote it by $\mathbf{k}$. For each polynomial labeling and vertices $l \in \mathcal{V}$ let

$$K_l := \operatorname{lcm}\{k_{ij} \mid ij \in \mathcal{E}_l\}.$$

Then

$$M(n) := \{\mathbf{k} \in \mathbb{F}[z]^E \mid k_{ij} \text{ monic, square-free for } ij \in \mathcal{E},\ \deg(K_l) \leq n_l,\ l \in \mathcal{V}\}$$

is the set of all polynomial labelings $\mathbf{k}$ of Γ satisfying the degree bounds $\deg(K_l) \leq n_l$ for all vertices l. For each monic square-free polynomial p let $\omega(p)$ denote the number of irreducible factors of p.

Theorem 5. *Let* $X(n) := \{(d_1, \ldots, d_N) \mid d_i \in \mathbb{F}[z]$ *monic with* $deg(d_i) = n_i\}$ *and* $\Gamma(n) := \{(d_1, \ldots, d_N) \in X(n) \mid \gcd(d_i, d_j) = 1$ *for* $ij \in \mathcal{E}\}$. *The cardinality of* $\Gamma(n)$ *is*

$$|\Gamma(n)| = t^{-(n_1+\ldots+n_N)} \sum_{\boldsymbol{k} \in M(n)} \prod_{ij \in \mathcal{E}} (-1)^{\omega(k_{ij})} \prod_{l=1}^{N} t^{\deg(K_l)}. \tag{17}$$

Proof. The sets

$$P := \{p \in \mathbb{F}[z] \mid \text{monic, irreducible, } \deg(p) \leq \max_{1 \leq i \leq N} n_i\}$$

and $R := P \times \mathcal{E}$ are finite. For $r = (p, ij) \in R$ define

$$D_r := \{(d_1, ..., d_N) \mid \ p \mid d_i \text{ and } p \mid d_j\}.$$

Thus $\Gamma(n) = X(n) \setminus \bigcup_{r \in R} D_r$. From the well-known inclusion-exclusion principle one obtains

$$|\Gamma(n)| = \sum_{S \subset R} (-1)^{|S|} |D_S|, \tag{18}$$

where $D_\emptyset = X(n)$ and $D_S := \bigcap_{r \in S} D_r$ for $S \neq \emptyset$.

It remains to determine $|S|$ and $|D_S|$. For each edge ij define the monic and square-free polynomial

$$k_{ij}^S := \prod_{(p,ij) \in S} p, \tag{19}$$

while for each vertex $l \in \mathcal{V}$ we consider the monic and square-free polynomials

$$K_l^S := \operatorname{lcm}\{k_{ij}^S \mid ij \in \mathcal{E}_l\}. \tag{20}$$

From the definition of D_S one obtains $(d_1, \ldots, d_N) \in D_S$ if and only if $p \mid \gcd(d_i, d_j)$ is satisfied for all $(p, ij) \in S$. This implies the equivalence:

$$(d_1, ..., d_N) \in D_S \quad \Leftrightarrow \quad k_{ij}^S \mid d_i \text{ and } k_{ij}^S \mid d_j \ \text{ for } \ ij \in \mathcal{E}.$$

Note that $k_{ij}^S \mid \gcd\{d_i, d_j\}$ holds for all $ij \in \mathcal{E}$ if and only if $k_{ij}^S \mid \mathrm{d}_l$ for all $ij \in \mathcal{E}_l$ and $l \in \mathcal{V}$. Since k_{ij}^S are square-free, this in turn yields the characterization

$$(d_1, ..., d_N) \in D_S \quad \Leftrightarrow \quad K_l^S \mid d_l \ \text{ for } l \in \mathcal{V}.$$

Thus one has to count the number of degree n_l monic multiples of a monic polynomial K_l^S. This number coincides with the number of monic polynomials in $\mathbb{F}[z]$ with degree $n_l - \deg(K_l^S)$ if the last expression is non-negative; otherwise such a polynomial cannot exist. This shows that

$$|D_S| = \prod_{l=1}^{N} t^{\deg(K_l^S) - n_l} \tag{21}$$

if $\deg(K_l^S) \leq n_l$ holds for all $l \in \mathcal{V}$ and $|D_S| = 0$ otherwise. To compute $|S|$, note that $\omega(k_{ij}^S)$ coincides with the number of elements $p \in P$ such that $(p, ij) \in S$. Thus

$$|S| = \sum_{ij \in \mathcal{E}} \omega(k_{ij}^S). \tag{22}$$

Finally, for each non-empty subset $S \subset R$, equation (19) defines a unique polynomial labeling $\mathbf{k}^S \in M(n)$. Conversely, for each $\mathbf{k} \in M(n)$ there exists $S \subset R$ with $\mathbf{k} = \mathbf{k}^S$. In fact, each polynomial labeling $\mathbf{k} = (k_{ij} | ij \in \mathcal{E}) \in M(n)$ admits a unique factorization into primes

$$k_{ij} = \prod_{p_{ij} \in P_{ij}} p_{ij}$$

for subsets $P_{ij} \subset P$. Defining $S = \bigcup_{ij \in \mathcal{E}} P_{ij} \times \{ij\}$ then yields $k_{ij}^S = k_{ij}$ for all edges $ij \in \mathcal{E}$. Thus in (18) one can sum over polynomial labelings $\mathbf{k}$ instead of summing over S. Moreover, the restriction $\mathbf{k} \in M(n)$ in the sum of (17) allows us to use formula (21), i.e. we avoid summing up zeros. This completes the proof. □

In the case that all pairs of vertices of Γ are connected by an edge, one obtains the probability that N monic polynomials are pairwise coprime. Going ahead like in the proof of Theorem 4 and using Theorem 5, one achieves:

Corollary 1. *For $i = 1, \ldots, N$ and randomly chosen $A_i \in \mathbb{F}^{n_i \times n_i}$ and $b_i \in \mathbb{F}_i^n$ the probability that system (14) is reachable is equal to*

$$\prod_{l=1}^{N} \left(\prod_{j=1}^{n_l} (1 - t^j) \right) \sum_{\mathbf{k} \in M(n)} \prod_{ij \in \mathcal{E}} (-1)^{\omega(k_{ij})} \prod_{l=1}^{N} t^{\deg(K_l)},$$

where $\mathcal{E} = \{ij \mid i, j \in \{1, \ldots, N\}, i < j\}$.

Remark 1. For $N = 2$ and $E = 1$ formula (17) has the following form:

$$t^{-n_1-n_2} \sum_{g=0}^{\min(n_1,n_2)} \left(\sum_{\substack{k \text{ monic, square-free} \\ \deg(k)=g}} (-1)^{\omega(k)} \right) t^{2g}$$

$$= t^{-n_1-n_2} \left(1 - t + \sum_{g=2}^{\min(n_1,n_2)} \left(\sum_{\substack{k \text{ monic, square-free} \\ \deg(k)=g}} (-1)^{\omega(k)} \right) t^{2g} \right).$$

Recall that the number of coprime pairs of monic polynomials is $t^{-n_1-n_2}(1-t)$, see [4]. Thus one obtains the combinatorical identity:

$$\sum_{g=2}^{\min(n_1,n_2)} \sum_{\substack{k \text{ monic, square-free} \\ \deg(k)=g}} (-1)^{\omega(k)} t^{2g} = \sum_{g=2}^{\min(n_1,n_2)} (|E(g)| - |U(g)|) t^{2g} = 0,$$

where

$$|E(g)| := \{(p_1, \ldots, p_{2r}) \mid r \in \mathbb{N}, p_i \neq p_j \text{ monic, irreducible, } \sum_{i=1}^{2r} \deg(p_i) = g\}$$

$$|U(g)| := \{(p_1, \ldots, p_{2r-1}) \mid r \in \mathbb{N}, p_i \neq p_j \text{ monic, irreducible, } \sum_{i=1}^{2r-1} \deg(p_i) = g\}$$

are the numbers of monic, square-free polynomials with an even or odd number of irreducible factors, respectively. For $n \geq 2$ it follows:

$$(|E(n)| - |U(n)|)t^{2n} = \sum_{g=2}^{n}(|E(g)| - |U(g)|)t^{2g} - \sum_{g=2}^{n-1}(|E(g)| - |U(g)|)t^{2g} = 0 - 0 = 0,$$

i.e. $|E(n)| = |U(n)|$ for every $n \geq 2$.

For $N > 2$ the formula of Theorem 5 is very difficult to evaluate. If the degree of one of the polynomials is at least as large as the sum of the other degrees, the computation could be reduced to a computation with lower degrees. This fact is explicitely stated in the following corollary:

Corollary 2. *Let $n_1, ..., n_N, h \in \mathbb{N}$. Then:*

$$|\Gamma(n_1, ..., n_N)| = t^{-h}|\Gamma(n_1 - h, n_2, ..., n_N)| \quad \textit{if} \quad n_1 = h + n_2 + ... + n_N.$$

Proof. For $\mathbf{k} \in M(n)$ it holds:

$$\deg(K_1) \leq \sum_{ij \in \mathcal{E}_1} \deg(k_{ij}) \leq \sum_{l=2}^{N} \deg(k_{1l}) \leq \sum_{l=2}^{N} \deg(K_l) \leq \sum_{l=2}^{N} n_l \leq n_1. \tag{23}$$

The first and the third inequality follow because K_l is the least common multiple of the corresponding k_{ij}. The fourth inequality holds since $\mathbf{k} \in M(n)$. Finally, the last inequality holds because of the assumption $n_1 = h + n_2 + ... + n_N$.

From (23) it follows that in the given situation increasing n_1 does not increase the number of elements in $M(n)$, because $\deg(K_l)$ are restricted more strongly by $n_2, ..., n_N$ than by n_1. Thus the only expression in (17) that changes when increasing n_1 is t^{-n_1}, which causes the factor t^{-h}. □

3.2. PROBABILITY OF REACHABILITY: ASYMPTOTIC EXPANSIONS. Now we calculate the asymptotic behaviour when $1/t$ - the size of the field - becomes large.

Theorem 6. *Let $n_1, ..., n_N \in \mathbb{N}$ and let E be the number of edges in a graph Γ. Then:*

$$|\Gamma(n)| = t^{-(n_1+...+n_N)}\left(1 - E \cdot t + O(t^2)\right).$$

Proof. To prove this result, first sort the elements of $M(n)$ with respect to the degrees of the entries of the vector $\mathbf{k} = (k_1, ..., k_E)$.

To this end for each vector of non-negative integers $\mathbf{g} := (g_1, ..., g_E)$ define $M(n, \mathbf{g}) := \{\mathbf{k} \in M(n) \mid \deg(k_m) = g_m \textit{ for } 1 \leq m \leq E\}$. Let A be the set of all $\mathbf{g}$ with $M(n, \mathbf{g}) \neq \emptyset$. Note that the degree bounds for $M(n)$ ensure that A is finite. One achieves:

$$|\Gamma(n)| = t^{-(n_1+...+n_N)} \sum_{\mathbf{g} \in A} \sum_{\mathbf{k} \in M(n,\mathbf{g})} \prod_{ij \in \mathcal{E}} (-1)^{\omega(k_{ij})} \prod_{l=1}^{N} t^{\deg(K_l)}.$$

Starting with small values for the entries of $\mathbf{g}$ the first summands are computed.

For $\mathbf{g} = (0, ..., 0)$, i.e. $\mathbf{k} = (1, ..., 1)$, one gets the summand 1 because of $\omega(1) = 0$ and $K_l = 1$ for $l = 1, \ldots, N$. If $g_{m_0} = 1$ for exactly one $1 \leq m_0 \leq E$ and $g_m = 0$ for $m \neq m_0$, there are $|\mathbb{F}| = 1/t$ possibilities for the linear polynomial k_{m_0} and E possibilities for the choice of m_0. Moreover, $\omega(k_{m_0}) = 1$, so that these summands have negative sign. As k_{m_0} is relevant for exactly those K_l for which its associated edge is terminating at l, there are exactly two K_l which are of degree 1. Hence the resulting sum of these terms is equal to $-E \cdot \frac{1}{t} \cdot t^2 = -E \cdot t$.

Thus one only has to show that each of the remaining summands behaves asymptotically as $O(t^2)$, which is done by showing

$$R(\mathbf{g}) := \sum_{\mathbf{k}\in M(n,\mathbf{g})} \prod_{l=1}^{N} t^{\deg(K_l)} = O(t^2)$$

for every fixed $\mathbf{g}$ for which the sum of the entries of $\mathbf{g}$ is at least two.

This will be done by induction with respect to E.

For $E = 1$ note that $\mathbf{g}$ and $\mathbf{k} = k_{12}$ are scalar. Moreover $K_1 = K_2 = k_{12}$. Therefore $R(\mathbf{g}) = 0$ if $\mathbf{g} > \min(n_1, n_2)$ and otherwise

$$R(\mathbf{g}) \le \sum_{\mathbf{k} \text{ monic, } \deg(\mathbf{k})=\mathbf{g}} t^{2\deg(\mathbf{k})} = \left(\frac{1}{t}\right)^{\mathbf{g}} \cdot t^{2\mathbf{g}} = t^{\mathbf{g}} = O(t^2) \text{ for } \mathbf{g} \ge 2.$$

This computation starts with an inequality since the condition that $\mathbf{k}$ has to be square-free is dropped. The first equality follows from the fact that there are $(1/t)^{\mathbf{g}}$ monic polynomials of degree $\mathbf{g}$.

Next we take the step from $E-1$ to E.

To this end choose one of the smallest entries of $\mathbf{g}$ and denote it without loss of generality by g_E. Then the edge with which k_E is associated – in the following denoted by ij – is taken away form the original graph and thus a graph with $E-1$ edges is achieved. In the following the index $(E-1)$ above an expression means that it belongs to a graph with $E-1$ edges; in the same way we use the index (E). Similarly, $\mathbf{k}^{(E-1)}$ and $\mathbf{g}^{(E-1)}$ should denote the vectors consisting of the first $E-1$ entries of $\mathbf{k}$ and $\mathbf{g}$, respectively.

The degrees of the K_l can never increase, when taking an edge away. Therefore $\mathbf{k} \in M(n,\mathbf{g})$ implies $\mathbf{k}^{(E-1)} \in M^{(E-1)}(n, \mathbf{g}^{(E-1)})$. Next we set

$$W_i := \gcd(K_i^{(E-1)}, k_E) \quad \text{and} \quad W_j := \gcd(K_j^{(E-1)}, k_E).$$

Moreover let

$$B^{(E-1)}_{v_i,v_j} := \{\mathbf{k}^{(E-1)} \in M^{(E-1)}(n,\mathbf{g}^{(E-1)}) \mid \deg(K_i^{(E-1)}) = v_i,\ \deg(K_j^{(E-1)}) = v_j\},$$
$$B^{(E)}_{v_i,v_j,w_i,w_j} := \{\mathbf{k} \in M^{(E)}(n,\mathbf{g}) \mid \mathbf{k}^{(E-1)} \in B^{(E-1)}_{v_i,v_j},\ \deg(W_i) = w_i,\ \deg(W_j) = w_j\}.$$

It follows

$$R(\mathbf{g}) \le \sum_{v_i,v_j,w_i,w_j \le \max(n_i,n_j)} \ \sum_{\mathbf{k}\in B^{(E)}_{v_i,v_j,w_i,w_j}} \prod_{l=1}^{N} t^{\deg(K_l^{(E)})}.$$

The number of summands in the first sum is finite and thus one only has to show that for any fixed v_i, v_j, w_i, w_j the following is true:

$$\sum_{\mathbf{k}\in B^{(E)}_{v_i,v_j,w_i,w_j}} \prod_{l=1}^{N} t^{\deg(K_l^{(E)})} = O(t^2).$$

To do this one computes

$$K_i^{(E)} = \operatorname{lcm}(K_i^{(E-1)}, k_E) = \frac{K_i^{(E-1)} \cdot k_E}{W_i}.$$

So $\deg(K_i^{(E)}) = \deg(K_i^{(E-1)}) + g_E - w_i$ and $\deg(K_j^{(E)}) = \deg(K_j^{(E-1)}) + g_E - w_j$, analogous. For $l \notin \{i,j\}$ it holds $K_l^{(E)} = K_l^{(E-1)}$ because nothing changes at the

associated vertices. It follows:

$$\sum_{\mathbf{k}\in B^{(E)}_{v_i,v_j,w_i,w_j}} \prod_{l=1}^{N} t^{\deg(K_l^{(E)})} = \sum_{\mathbf{k}\in B^{(E)}_{v_i,v_j,w_i,w_j}} \prod_{l=1}^{N} t^{\deg(K_l^{(E-1)})} \cdot t^{2g_E-w_i-w_j}. \tag{24}$$

Here the product $\prod_{l=1}^{N} t^{\deg(K_l^{(E-1)})}$ is independent of k_E and $t^{2g_E-w_i-w_j}$ is independent of $\mathbf{k}$.

Next for $\mathbf{k}^{(E-1)} \in B^{(E-1)}_{v_i,v_j}$ the number of polynomials k_E such that $\mathbf{k} \in B^{(E)}_{v_i,v_j,w_i,w_j}$ should be determined. $\mathbf{k}^{(E-1)}$ uniquely determines $K_i^{(E-1)}$ and since W_i is a divisor of $K_i^{(E-1)}$ of degree w_i, there are only finitely many possibilities for W_i. Define C as this number of possibilities for W_i. One knows that k_E has to be a multiple of W_i of degree g_E. Thus for every W_i there are at most $t^{w_i-g_E}$ possibilities for k_E.

Using this and the fact that the product in (24) is independent of k_E, it follows for the expression in (24):

$$\begin{aligned}\sum_{\mathbf{k}\in B^{(E)}_{v_i,v_j,w_i,w_j}} \prod_{l=1}^{N} t^{\deg(K_l^{(E)})} &\le t^{2g_E-w_i-w_j} \cdot C \cdot t^{w_i-g_E} \sum_{\mathbf{k}^{(E-1)}\in B^{(E-1)}_{v_i,v_j}} \prod_{l=1}^{N} t^{\deg(K_l^{(E-1)})} \\ &= Ct^{g_E-w_j} \sum_{\mathbf{k}^{(E-1)}\in B^{(E-1)}_{v_i,v_j}} \prod_{l=1}^{N} t^{\deg(K_l^{(E-1)})} \\ &\le C \cdot R(\mathbf{g}^{(E-1)})\end{aligned}$$

because $w_j \le g_E$ since $W_j \mid k_E$. Now we distinguish three cases:

1. The sum of the entries of $\mathbf{g}^{(E-1)}$ is at least two. Then $R(\mathbf{g}^{(E-1)})$ is $O(t^2)$ per induction and we are done.
2. $\mathbf{g}^{(E-1)}$ has a component that is equal to zero. Here g_E must be zero since it was choosen to be one of the smallest entries. But then the sum of the entries of $\mathbf{g}^{(E-1)}$ is equal to the sum of the entries of $\mathbf{g}^{(E)}$ and thus in particular at least two. Consequently, we are done, too.
3. $E = 2$ and $\mathbf{g}^{(E-1)} = g_1 = 1$. Then $g_E = g_2 \le 1$. If $g_2 = 0$, we argue as before. If $g_2 = 1$ and the two edges of the graph meet at a vertex, one gets

$$\begin{aligned}R(\mathbf{g}) = R(1,1) &\le \sum_{\substack{k_1,\,k_2 \text{ monic} \\ \deg(k_m)=1}} t^{2+\deg(\operatorname{lcm}(k_1,k_2))} \\ &= \sum_{\substack{k_1=k_2 \text{ monic} \\ \deg(k_m)=1}} t^3 + \sum_{\substack{k_1\ne k_2 \text{ monic} \\ \deg(k_m)=1}} t^4 \\ &= \frac{1}{t}\cdot t^3 + \frac{1}{t}\cdot\left(\frac{1}{t}-1\right)\cdot t^4 = O(t^2).\end{aligned}$$

   If $g_2 = 1$ and the two edges of the graph are isolated, one gets

$$R(\mathbf{g}) = R(1,1) \le \sum_{\substack{k_1,\,k_2 \text{ monic} \\ \deg(k_m)=1}} t^4 = t^2$$

   since there are two K_l that coincide with k_1 and k_2, respectively. Moreover, there are t^{-2} pairs of monic polynomials of degree one.

   Thus this case is done as well and our proof is complete. □

Now we come to the situation of parallel connected systems again. Recall that here all pairs of vertices of $\Gamma(n)$ are connected by an edge, i.e. it holds $E = \frac{N(N-1)}{2}$. The following result is an easy consequence of Theorem 6:

Corollary 3. *For $n := (n_1, \ldots, n_N) \in \mathbb{N}^N$ the set $G(n)$ of N-tuples $(d_1, \ldots, d_N)$ of monic pairwise coprime polynomials $d_i \in \mathbb{F}[z]$ with $\deg(d_i) = n_i$ for $i = 1, \ldots, N$ has the following cardinality:*

$$|G(n)| = t^{-(n_1+\ldots+n_N)} \left(1 - \frac{N(N-1)}{2} \cdot t + O(t^2)\right).$$

Therefore the probability that $d_1, \ldots, d_N$ are pairwise coprime is equal to

$$1 - \frac{N(N-1)}{2} \cdot t + O(t^2).$$

Using the preceding corollary, it is possible to estimate the probabilty that the parallel connection of N linear single-input systems is reachable.

Theorem 7. *For $i = 1, \ldots, N$ and randomly chosen $A_i \in \mathbb{F}^{n_i \times n_i}$ and $b_i \in \mathbb{F}_i^n$ the probability that system (14) is reachable is equal to*

$$\left(1 - \frac{N(N-1)}{2} t + O(t^2)\right) \prod_{l=1}^{N} \left(\prod_{j=1}^{n_l} (1 - t^j)\right) = 1 - \frac{N(N+1)}{2} t + O(t^2).$$

Proof. Going ahead like in the proof of Theorem 4 and using Corollary 3, one achieves the expression

$$\begin{aligned}
&\left(1 - \frac{N(N-1)}{2} t + O(t^2)\right) \prod_{j=1}^{n_1} (1 - t^j) \cdots \prod_{j=1}^{n_N} (1 - t^j) \\
&= 1 - \frac{N(N-1)}{2} t - N \cdot t + O(t^2) \\
&= 1 - \frac{N(N+1)}{2} t + O(t^2)
\end{aligned}$$

for the considered probability. □

4. Conclusions

We compare cell decompositions of the moduli space of reachable linear systems with the Grassmannian to derive an explicit formula for the probability that a linear system is reachable. The formula is extended to count the number of reachable linear systems with r-dimensional reachability subspace. We calculate the probability that finitely many monic polynomials of given degrees are pairwise coprime. This allows us to estimate the probability that the parallel connection of finitely many linear single-input systems is reachable. Future research will concern the extension to the parallel connection of finitely many multivariable systems and to general networks of systems.

Acknowledgments

We would like to thank the referees very much for their valuable comments and suggestions. This research has been partially supported by the grant DFG 1858/13-1 from the German Research Foundation.

REFERENCES

[1] J.-J. Climent, V. Herranz and C. Perea, A first approximation of concatenated convolutional codes from linear systems theory viewpoint, *Linear Alg. Appl.*, **425** (2007), 673–699.

[2] P. A. Fuhrmann, On controllability and observability of systems connected in parallel, *IEEE Trans. Circ. Syst.*, **22** (1975), 57.

[3] P. A. Fuhrmann and U. Helmke, *The Mathematics of Networks of Linear Systems*, Springer, New York, 2015.

[4] M. Garcia-Armas, S. R. Ghorpade and S. Ram, Relatively prime polynomials and nonsingular Hankel matrices over finite fields, *J. Combin. Theory Ser. A*, **118** (2011), 819–828.

[5] U. Helmke, Topology of the moduli space for reachable linear dynamical systems: The complex case, *Math. Syst. Theory*, **19** (1986), 155–187.

[6] U. Helmke, The cohomology of moduli spaces for linear dynamical systems, *Regensburger Math. Schriften*, **24** (1993).

[7] T. Ho and D. S. Lun, *Network Coding: An Introduction*, Cambridge Univ. Press, New York, 2008.

[8] S. Höst, Woven convolutional codes I: Encoder properties, *IEEE Trans. Inf. Theory*, **48** (2002), 149–161.

[9] A. S. Jarrah, R. Laubenbacher, B. Stigler and M. Stillman, Reverse–engineering of polynomial dynamical systems, *Adv. Appl. Math.*, **39** (2007), 477–489.

[10] M. Kociecky and K. M. Przyluski, On the number of controllable linear systems over a finite field, *Linear Alg. Appl.*, **122-124** (1989), 115–122.

[11] J. Milnor and J. Stasheff, *Characteristic Classes*, Princeton Univ. Press, 1974.

[12] J. A. De Reyna and R. Heyman, Counting tuples restricted by coprimality conditions, preprint, arXiv:1403.2769v1

[13] J. Rosenthal, J. M. Schumacher and E. V. York, On behaviours and convolutional codes, *IEEE Trans. Inf. Theory*, **42** (1996), 1881–1891.

[14] J. Rosenthal and E. V. York, BCH Convolutional Codes, *IEEE Trans. Inf. Theory*, **45** (1999), 1833–1844.

[15] S. Sundaram and C. Hadjicostis, Structural controllability and observability of linear systems over finite fields with applications to mult–agent systems, *IEEE Trans. Autom. Control*, **58** (2013), 60–73.

Received December 2014; revised July 2015.

E-mail address: helmke@mathematik.uni-wuerzburg.de
E-mail address: jordan@mathematik.uni-wuerzburg.de
E-mail address: julia.lieb@mathematik.uni-wuerzburg.de