A Rank Theorem for Vandermonde Matrices

Pascal Koiran, Natacha Portier and Gilles Villard*

Laboratoire LIP, École Normale Supérieure de Lyon

46, Allée d'Italie, 69364 Lyon Cedex 07, France

March 12, 2002

Abstract

We show that certain matrices built from Vandermonde matrices are of full rank. This result plays a key role in the construction of the "limit theory of generic polynomials".

1 Introduction

Let $V = V_d(x_1, \ldots, x_n)$ denote the $n \times (d+1)$ Vandermonde matrix built from the complex numbers $x_1, \ldots, x_n$ (that is, $V_{ij} = x_i^{j-1}$). The main purpose of this note is to prove the following result.

Theorem 1.1 *Let n, r and d be three positive integers. Let A be a $r \times (d+1)$ matrix with entries in an algebraically closed field $\mathsf{K} \subset \mathbb{C}$. Let $x = (x_1, ..., x_n)$ be a vector of n distinct elements of $\mathbb{C} \setminus \mathsf{K}$.*

If A has rank r then the $(n+r) \times (d+1)$ matrix

$$V(x, A) = \begin{bmatrix} V_d(x_1, \ldots, x_n) \\ A \end{bmatrix}$$

has rank $n + r$ as soon as $d + 1 \geq n(r + 1)$.

One may of course assume without loss of generality that K is the algebraic closure of the extension of $\mathbb{Q}$ generated by the entries of A.

This theorem and Theorem 1.2 below (a kind of nonlinear version of Theorem 1.1) play a key role in the construction of the "limit theory of generic polynomials". Just as in the case of generic curves [1, 3] this construction yields undefinability results. For instance, the parity of the degree of complex polynomials turns out to be undefinable. This means that there is no first-order sentence F in the language of fields expanded with a unary predicate f such that:

(i) F is true in $\mathbb{C}$ whenever f is interpreted by a polynomial of even degree.

(ii) F is false in $\mathbb{C}$ whenever f is interpreted by a polynomial of odd degree.

A proof of this result and of Theorem 1.2 will appear in [2]. Note that the parity of the degree of *real* polynomials is definable. This follows immediately from the fact that a real polynomial is of odd degree if and only if it has different limits at $\pm\infty$.

*{Pascal.Koiran,Natacha.Portier,Gilles.Villard}@ens-lyon.fr

Theorem 1.2 *There exists a function $\phi : \mathbb{N}^2 \to \mathbb{N}$ such that the following property holds for any $r \geq 1$, any $n \geq 1$ and any $D \geq \phi(r,n)$.*

Let V be an algebraic subset of $\mathbb{C}^D$ of codimension r, defined over an algebraically closed subfield $\mathsf{K} \subseteq \mathbb{C}$. Given two sequences $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ of complex numbers, denote by $W(x,y)$ the affine subspace of $\mathbb{C}^D$ defined by the system of equations $\sum_{j=1}^{D} x_i^j \alpha_j = y_i$ $(i = 1, \ldots, n)$. Then $V \cap W(x,y) \neq \emptyset$ if x and y satisfy the following two conditions:

(i) The x_i's are pairwise distinct and all lie outside K.

(ii) There exists $u_1 \in \{x_1, y_1\}, \ldots, u_n \in \{x_n, y_n\}$ such that $(u_1, \ldots, u_n)$ is of transcendence degree n over K.

An equivalent formulation of condition (ii) (the "marriage condition") can be found in [1]. Theorem 1.1 implies that one may take $\phi(r,n) = n(r+1)$ if we restrict our attention to algebraic subsets V which are affine subspaces (set $d = D-1$). Moreover, there is no need for condition (ii) in this case. As pointed out in section 1.1, this condition is nevertheless necessary in the general case.

The remainder of this note is organized as follows. Section 2 is devoted to some special cases. In particular we show that Theorem 1.1 is tight for all values of n and r. As explained in Section 1.1 below, this implies that the function ϕ in Theorem 1.2 must satisfy the condition $\phi(r,n) \geq n(r+1)$. We then propose two different proofs of Theorem 1.1. The first one in Section 3 relies on dimension arguments. An alternative proof in Section 4 is based on methods from the theory of linear recurrences.

1.1 Remarks on Theorem 1.2

We have seen that one may take $\phi(r,n) = n(r+1)$ for affine subspaces, which yields the bound $D \geq 4$ for $n = 2$ and $r = 1$. Without condition (ii) this bound is not valid for arbitrary algebraic subsets of codimension 1. Indeed, let $D = 4$ and let V be the hypersurface $\alpha_1\alpha_4 - \alpha_2\alpha_3 = 1$. Let x_1 be a transcendent number (in fact it would be enough to have $x_1 \neq 0$). Set $x_2 = -x_1$ and $y_1 = y_2 = 0$. One can check that $V \cap W(x,y) = \emptyset$.

We now generalize this construction to higher values of D. This shows that Theorem 1.2 would not be true without condition (ii). We keep $y_1 = y_2 = 0$ and $x_2 = -x_1$. Let $P_\alpha(X)$ and $Q_\alpha(X)$ be the two polynomials $\sum_{i=1}^{D} \alpha_i X^{i-1}$ and $\sum_{i=1}^{D} \alpha_i (-X)^{i-1}$. Their resultant $R(\alpha_1, \ldots, \alpha_D)$ is a nonzero polynomial in $\alpha_1, \ldots, \alpha_D$ since $R(1,1,0,\ldots,0) \neq 0$. Let V be defined by the equation $R(\alpha_1, \ldots, \alpha_D) = 1$. We claim that $V \cap W(x,y) = \emptyset$. Indeed, for any $\alpha \in W(x,y)$ we have $P_\alpha(x_1) = Q_\alpha(x_1) = 0$ since $x_1 \neq 0$. Since P_α and Q_α have a common root one must have $R(\alpha) = 0$, hence $\alpha \not\in V$.

Let $d = n(r+1) - 2$. In Proposition 2.4 we show that there exists a vector $x_1, \ldots, x_n$ of distinct transcendent numbers and a $r \times (d+1)$ matrix A of rank r with rational (even boolean) entries such that $V(x,A)$ has rank $n + r - 1$. This implies that Theorem 1.2 fails for $D = n(r+1) - 1$. Indeed, let $(y_1, \ldots, y_{n+r})$ be a vector of complex numbers which are algebraically independent over $\mathbb{Q}(x_1, \ldots, x_n)$. Let K be the algebraic closure of $\mathbb{Q}(y_{n+1}, \ldots, y_{n+r})$ and let V be the affine subspace of $\mathbb{C}^D$ defined by the system of equations $A\alpha = {}^t(y_{n+1}, \ldots, y_{n+r})$. The sequences $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ satisfy conditions (i) and (ii), but still $V \cap W = \emptyset$. To see this note that $\alpha \in V \cap W$ is equivalent to the satisfaction of a system of equations of the form $V'\alpha = {}^t(y_1, \ldots, y_{n+r})$ where V' has its entries in $\mathbb{Q}(x_1, \ldots, x_n)$ and same rank as $V(x,A)$. This system is not satisfiable since the transcendence degree of $(y_1, \ldots, y_{n+r})$ over $\mathbb{Q}(x_1, \ldots, x_n)$ is higher than the rank of V'.

2 Some Special Cases

In the case of algebraically independent x_i's we can prove the main theorem with an improved (and optimal) bound: $d \geq n+r-1$. We need a very simple but crucial lemma.

Lemma 2.1 *Given $x \in \mathbb{C}$, denote by $v_d(x)$ the vector $(1, x, x^2, \ldots, x^d)$ of $\mathbb{C}^{d+1}$. For any proper linear subspace $E \subset \mathbb{C}^{d+1}$, $v_d(x) \in E$ for at most d values of x. Moreover, if E is defined over a field $k \subset \mathbb{C}$ these values of x are in the algebraic closure of k.*

Proof. We may assume without loss of generality that E is a hyperplane. The condition $v_d(x) \in E$ is equivalent to $P(x) = 0$, where $P \in k[X]$ is a nonzero polynomial of degree at most d. □

Theorem 2.2 *If $x_1, \ldots, x_n$ are algebraically independent over K, $V(x, A)$ has rank $n+r$ as soon as $d \geq n+r-1$.*

Proof. By induction on n. For $n = 1$, since A is of rank r, $V(x_1, A)$ can fail to be of rank $r+1$ only if $v_d(x_1)$ belongs to the subspace of $\mathbb{C}^{d+1}$ spanned by the rows of A. By Lemma 2.1, this would imply $x_1 \in \mathsf{K}$.

Induction step: assume that $n \geq 2$ and that the result is true for $n-1$. It follows from the induction hypothesis that the $n-1+r$ last rows form a minor of $V(x, A)$ of rank $n-1+r$. Hence $V(x, A)$ can fail to be of rank $n+r$ only if $v_d(x_1)$ belongs to the subspace of $\mathbb{C}^{d+1}$ generated by the last $n-1+r$ rows. By Lemma 2.1, this would imply that x_1 belongs to the algebraic closure of $\mathsf{K}(x_2, \ldots, x_n)$. □

A variation on this argument gives the same bound in a few other cases. For instance, we have the following result.

Proposition 2.3 *Let $P \in \mathsf{K}[X]$ be a polynomial of degree at least two. If $x_1 \notin \mathsf{K}$, $V((x_1, P(x_1)), A)$ has rank $r+2$ as soon as $d \geq r+1$.*

Proof. Consider the sequence $(x_k)_{k \geq 1}$ generated by the iteration $x_{k+1} = P(x_k)$. Since $x_1 \notin \mathsf{K}$ the same is true of all the elements of this sequence. This implies in particular that these elements are pairwise distinct since P has degree at least 2. Note also that the case $n = 1$ of Theorem 2.2 implies that $V(x_1, A)$ has rank $r+1$.

Assume by contradiction that x_1 is a counterexample. This implies that $v_d(x_2)$ belongs to the linear space E spanned by $v_d(x_1)$ and the rows of A. More generally, since (x_k, x_{k+1}) has same type over K as (x_1, x_2), for any $k \geq 1$ $v_d(x_{k+1})$ belongs to the linear space spanned by $v_d(x_k)$ and the rows of A. We conclude by an immediate induction on k that the vectors $v_d(x_k)$ all belong to E. This is in contradiction with Lemma 2.1. □

The conclusion of Proposition 2.3 does not hold for the degree one polynomial $P(x_1) = -x_1$ and for several other functions f satisfying $f \circ f = id$. The following matrices have rank 2, for instance if a and c are algebraic numbers:

$$\begin{bmatrix} 1 & x_1 & x_1^2 \\ 1 & \frac{a}{x_1} & \frac{a^2}{x_1^2} \\ -1 & 0 & a \end{bmatrix}, \quad \begin{bmatrix} 1 & x_1 & x_1^2 \\ 1 & \frac{ax_1}{cx_1-a} & \left(\frac{ax_1}{cx_1-a}\right)^2 \\ c & a & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & x_1 & x_1^2 \\ 1 & a-x_1 & (a-x_1)^2 \\ 0 & 1 & a \end{bmatrix}.$$

Our proof of the optimality of Theorem 1.1 is based on a generalization of the example with $P(x_1) = -x_1$.

Proposition 2.4 *Let n and r be two positive integers, $d = n(r+1)-2$ and let $\mathsf{K} \subset \mathbb{C}$ be an algebraically closed field. Then there is a vector $x = (x_1, ..., x_n)$ of n distinct elements of $\mathbb{C} \setminus \mathsf{K}$ and a $r \times (d+1)$ matrix A of rank r with entries in K such that the $(n+r) \times (d+1)$ matrix $V(x, A)$ has rank $n+r-1$.*

Proof of Proposition 2.4. If $n = 1$ and if a $(1 + r, d + 1)$ matrix has rank $1 + r$ then of course $d + 1 \geq 1 + r$. Suppose now that $n \geq 2$ and let $d = n(r + 1) - 2$. Let x_1 be transcendent over K and $b = \exp(2i\pi/n)$. Let $x = (x_1, bx_1, b^2x_1, ..., b^{n-1}x_1)$. Note that we use the function $f(x) = bx$ which satisfies $f \circ \ldots \circ f = f^{(n)} = id$. The $(r, d+1)$ matrix A is defined as follows: for every integer i between 1 and r the (i, ni) entry is 1 and others entries are 0. Its rank is clearly r. Let $C_0, \ldots, C_d$ denote the columns of $V(x, A)$:

$$V(x,A) = \begin{array}{c} \begin{array}{ccccccccccc} \mathbf{C_0} & \mathbf{C_1} & \ldots & \mathbf{C_{n-1}} & \mathbf{C_n} & \ldots & \mathbf{C_{nr-1}} & \mathbf{C_{nr}} & \ldots & \mathbf{C_d} \end{array} \\ \begin{bmatrix} 1 & x_1 & \ldots & x_1^{n-1} & x_1^n & \cdots & x_1^{nr-1} & x_1^{nr} & \cdots & x_1^d \\ 1 & bx_1 & \ldots & b^{n-1}x_1^{n-1} & x_1^n & \cdots & b^{n-1}x_1^{nr-1} & x_1^{nr} & \cdots & b^{n-2}x_1^d \\ \vdots & & & & \vdots & & & \vdots & & \\ 1 & b^{n-1}x_1 & \ldots & bx_1^{n-1} & x_1^n & \cdots & bx_1^{nr-1} & x_1^{nr} & \cdots & b^2x_1^d \\ & & & 1 & & & & & & \\ & & & & \ldots & \ldots & & & & \\ & & & & & & 1 & & & \end{bmatrix} \end{array}$$

For every integer $j \in [0, n-2]$ we have

$$x_1^{nr} C_j = x_1^{n(r-1)} C_{j+n} = x_1^{n(r-2)} C_{j+2n} = ... = x_1^n C_{j+(r-1)n} = C_{j+rn}.$$

Thus it is easy to check that a basis of the space spanned by the columns is $C_0, C_1..., C_{n-1}, C_{2n-1}, C_{3n-1}, ..., C_{rn-1}$ and that the rank of $V(x, A)$ is $n + r - 1$. □

3 First proof of the main theorem

Let $D(n, r) = n(r + 1) - 1$ be the bound in the statement of Theorem 1.1. Call $\mathcal{A}(n, r, d)$ the assertion which is to be established for $d \geq D(n, r)$. The case $n = 1$ was taken care of in Theorem 2.2. Note also that the theorem still makes sense for $r = 0$: in this case $V(x, A)$ is just a $n \times n$ Vandermonde matrix. We therefore fix two integers n, r such that $n \geq 2$ and $r \geq 1$. Our induction hypothesis is that $\mathcal{A}(n', r', d')$ holds for all triples (n', r', d') such that $n' + r' < n + r$ and $d' \geq D(n', r')$. Our first goal is to show that $\mathcal{A}(n, r, d)$ holds for $d = D(n, r)$.

Assume by contradiction that $V(x, A)$ is a counterexample, i.e., has rank at most $n + r - 1$. Assume also without loss of generality that K is the algebraic closure of the extension of $\mathbb{Q}$ generated by the entries of A. Since $D(n, r) \geq D(n - 1, r)$, by induction hypothesis the last $n + r - 1$ rows of $V(x, A)$ form a minor of rank $n + r - 1$. The first row $v_d(x_1)$ of $V(x, A)$ thus belongs to the linear space spanned by the last $n + r - 1$ rows. We consider now r "copies" $y^1, \ldots, y^r$ of x which are independent over K. More precisely, we assume the following two properties:

(i) $y^j = (y_1^j, \ldots, y_n^j)$ has same type over K as $x = (x_1, \ldots, x_n)$.

In field-theoretic terminology, this means that there is an isomorphism of fields from $\mathsf{K}(x_1, \ldots, x_n)$ to $\mathsf{K}(y_1^j, \ldots, y_n^j)$ which leaves K invariant and maps $x_1, \ldots, x_n$ to $y_1^j, \ldots, y_n^j$. Since $x_1, \ldots, x_n$ are distinct, this implies in particular that $y_1^j, \ldots, y_n^j$ are distinct.

(ii) The $n(r + 1)$ components of x and its copies are pairwise distinct.

It follows from (i) that the first row $v_d(y_1^j)$ of $V(y^j, A)$ belongs to the linear space spanned by the last $n + r - 1$ rows, since the corresponding property is true of x. Let E

be the linear space spanned by the $r+n-1$ last rows of $V(x,A)$ and the corresponding rows in the matrices $V(y^j,A)$ as j ranges from 1 to r. This space has dimension at most $r+(r+1)(n-1) < d+1$ since $d+1 = n(r+1)$. We have just shown that $v_d(z) \in E$, where z is any component of x or of its r copies. There are $n(r+1) > d$ such components, and they are pairwise distinct. This is in contradiction with Lemma 2.1, and the proof of $\mathcal{A}(n,r,d)$ for $d = D(n,r)$ is thus complete. To finish off the proof of the theorem, we show by a second induction (on d) that $\mathcal{A}(n,r,d)$ also holds for $d > D(n,r)$. Assume therefore that $\mathcal{A}(n,r,d-1)$ holds. In order to show that $V(x,A)$ has rank $n+r$ under the hypotheses of Theorem 1.1, we distinguish two cases.

First case: the first d columns of A have rank r. We conclude from our second induction hypothesis that the first d columns of $V(x,A)$ have rank $n+r$, and this must also be the rank of the whole matrix.

Second case: the first d columns of A have rank $r-1$. Since $d-1 \geq D(n,r) \geq D(n,r-1)$, we conclude from our first induction hypothesis that the first d columns of $V(x,A)$ have rank $n+r-1$. But the last column of $V(x,A)$ does not belong to the span of the first d columns since the same is true of A itself. The rank of $V(x,A)$ is therefore equal to $1+(n+r-1) = n+r$.

4 A proof based on linear recurring sequences

This alternative proof will also give a slightly more precise result for $r=1$ (see Lemma 4.3 below). We rely on the following generalization of linear recurring sequences.

Definition 4.1 *A sequence $(A_i)_{i\geq 0}$ of vectors in K^r is a* linear pseudo-recurrent *sequence of order n if one can find a polynomial $f(X) = f_0 + f_1X + \ldots + f_nX^n \in \mathbb{C}[X]$ and a nonzero vector $q \in \mathbb{C}^r$ such that*

$$q^T \cdot (A_i f_0 + A_{i+1} f_1 + \ldots + A_{i+n} f_n) = 0, \ i \geq 0. \tag{1}$$

For a given n, any vector $q \neq 0$ satisfying (1) for some f is called an admissible vector.

For $r=1$ or for any fixed admissible q, the set of the generating polynomials f is an ideal that can be determined from the $2n$ first terms of the sequence (see for instance [4] or Corollary 5.6.3 of [5]). For $r \geq 2$, the set of all the possible f in (1) contains an ideal that can be determined from the $n(r+1)$ first terms:

Lemma 4.2 *Let $(A_i)_{i\geq 0}$ be a linear pseudo-recurrent sequence of order $n \geq 1$ in $\mathbb{C}^r$, where n is as small as possible. There exists a polynomial c of degree $m \in [n, nr]$ such that*

$$q^T.(A_i c_0 + A_{i+1} c_1 + \cdots + A_{i+m} c_m) = 0, \ i \geq 0,$$

for any admissible vector q. Such a polynomial can be computed from the first $n(r+1)$ terms $A_0, \ldots, A_{n(r+1)-1}$ of the vector sequence. If the entries of these vectors lie in a subfield $\mathsf{K} \subset \mathbb{C}$ then one may take c in $\mathsf{K}[X]$.

Proof. The construction of c is the computation of a simultaneous generating polynomial of degree lower than nr for the r component sequences of $(A_i)_{i\geq 0}$. This polynomial may be seen as a common multiple of at most r polynomials of degree n in (1). It is therefore natural to introduce nr shifts of the sequence and to work with the $(r \times 1)$-block Hankel matrix

$$\mathcal{H}_{n,r} = \begin{bmatrix} A_0 & A_1 & \ldots & A_{nr-1} & A_{nr} \\ A_1 & A_2 & \ldots & A_{nr} & A_{nr+1} \\ \vdots & \vdots & & \vdots & \vdots \\ A_{n-2} & A_{n-1} & \ldots & A_{n(r+1)-3} & A_{n(r+1)-2} \\ A_{n-1} & A_n & \ldots & A_{n(r+1)-2} & A_{n(r+1)-1} \end{bmatrix} \in \mathsf{K}^{nr\times(nr+1)}.$$

This matrix is constructed from the $n(r+1)$ first terms of $(A_i)_{i\geq 0}$. We claim that one can find the coefficients of c from a vector in its kernel. We first notice that the first n columns of $\mathcal{H}_{n,r}$ are linearly independent. Otherwise, the Hankel matrix

$$H_q(n,n) = \begin{bmatrix} q^TA_0 & q^TA_1 & \dots & q^TA_{n-1} \\ q^TA_1 & q^TA_2 & \dots & q^TA_n \\ \vdots & \vdots & & \vdots \\ q^TA_{n-1} & q^TA_n & \dots & q^TA_{2n-2} \end{bmatrix} \in \mathsf{K}^{n\times n}$$

would be singular for any q in K^r, therefore using (1) the infinite Hankel matrix $H_q(n,\infty)$ would have rank less than n for any q and n would not be minimal as assumed. Now, let $c = [c_0, c_1, \dots, c_m, 0, \dots, 0]^T \in K^{nr+1}$ be a nonzero vector in the kernel of $\mathcal{H}_{n,r}$ ($n \leq m \leq nr$). Such a vector exists since $\mathcal{H}_{n,r}$ has a greater number of columns than of rows. The same vector c is in the kernel of $H_q(n, m+1) \in \mathsf{K}^{n\times(m+1)}$ for any q. The corresponding polynomial $c \in \mathsf{K}[X]$ is thus a generating polynomial for any admissible vector q. □

Lemma 4.3 *For $d \geq n(r+1)-1$ and any $q \in \mathbb{C}^r$ there exists, under the hypotheses of Theorem 1.1, a submatrix of rank $n+1$ made up of $n+1$ consecutive columns of $V(x, q^TA)$.*

Proof. Assume by contradiction that for some q the determinants of all matrices made up of $n+1$ consecutive columns of $V(x, q^TA)$ are equal to zero. Let us expand the determinant made up of columns i through $i+n$ with respect to its last row. After factoring out $(x_1x_2\cdots x_n)^i$ we obtain the relation

$$V_0q^TA_i + V_1q^Ta_{i+1} + \cdots + V_nq^Ta_{i+n} = 0$$

where $V_0, \dots, V_n$ are cofactors of $V(x, q^TA)$ restricted to its first $n+1$ columns. This relation is nontrivial since $V_n = \det V_{n-1}(x_1, \dots, x_n) \neq 0$. The sequence $(A_i)_{0\leq i\leq d}$ is thus linear pseudo-recurrent of order n with minimal order greater than 1 (A has rank r) and Lemma 4.2 provides a generating polynomial $c \in \mathsf{K}[X]$ for any row combination q^T. This implies that $V_0 + V_1x + \dots V_nx^n$ must be a multiple of a nontrivial divisor of c (for any q the minimal polynomial is non trivial). This yields a contradiction since the roots $x_1, \dots, x_n$ of the first polynomial are all outside K and the roots of the second polynomial must be in K. □

Proof of Theorem 1.1. If rank $V(x,A) < n+r$ there must exist a q such that rank $V(x, q^TA) < n+1$. This is in contradiction with Lemma 4.3. □

For $r=1$, Lemma 4.3 gives a property stronger than Theorem 1.1 but does not generalize to minors of higher dimensions, as shown by the following example with $r=2$. Take $n=1$ and (for instance) $d=100$. Take a_{ij} identically 0 except that $a_{1,1}=1$ and $a_{2,50}=1$. Then no submatrix of $V(x_1, A)$ made up of three consecutive columns has rank 3. Still, this matrix has rank 3 since the minor made of columns 1,2, and 50 has rank 3 for any $x_1 \neq 0$.

To conclude, let us illustrate the optimality of Theorem 1.1 by a construction with linear recurring sequences:

Example 4.4 *For $r=2$, the coefficients $(a_i)_{0\leq i\leq 3n-2}$ and $(b_i)_{0\leq i\leq 3n-2}$ of the expansions at infinity*

$$a(x) = \frac{1}{x^n} = \sum_{i\geq 0} \frac{a_i}{x^{i+1}} \quad \text{and} \quad b(x) = \frac{1}{x^n(x^n-\alpha)} = \frac{1}{x^{2n}} + \frac{\alpha}{x^{3n}} + O(\frac{1}{x^{4n}}) = \sum_{i\geq 0} \frac{b_i}{x^{i+1}}$$

give the two rows of the matrix A in Proposition 2.4. Let the sequence $(A_i)_{i\geq 0}$ be defined by the columns of A. For any α we have $a(x) + \alpha b(x) = 1/(x^n - \alpha)$ thus the minimal polynomial of the sequence $(q^T A_i)_{i\geq 0}$ for $q^T = [1 \quad \alpha]$ is $x^n - \alpha$. This expresses the optimality of Lemma 4.2 since only the $3n$-th term of b fixes the value of α and hence of a generating polynomial. □

References

[1] O. Chapuis, E. Hrushovski, P. Koiran, and B. Poizat. La limite des théories de courbes génériques. To appear in *Journal of Symbolic Logic.*

[2] P. Koiran. The limit theory of generic polynomials. LIP Research Report 2001-35, Ecole Normale Supérieure de Lyon, 2001. To appear in *Proc. Logic Colloquium 2001.*

[3] P. Koiran and N. Portier. Back-and-forth systems for generic curves and a decision algorithm for the limit theory. *Annals of Pure and Applied Logic*, 111:257-275, 2001.

[4] J. L. Massey. Shift-register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, 15(1):122–127, 1969.

[5] E.D. Sontag. *Mathematical Control Theory: Deterministic Finite Dimensional Systems.* Texts in Applied Mathematics. Springer-Verlag, New-York, 1990.