Vandermonde Matrices, NP-Completeness, and Transversal Subspaces

Alexander Chistov, Hervé Fournier, Leonid Gurvits, Pascal Koiran

Laboratoire de l'Informatique du Parallélisme

École Normale Supérieure de Lyon
Unité Mixte de Recherche CNRS-INRIA-ENS LYON n° 5668

Vandermonde Matrices, NP-Completeness, and Transversal Subspaces

Alexander Chistov, Hervé Fournier,
Leonid Gurvits and Pascal Koiran

September 2002

Research Report N° 2002-31

École Normale Supérieure de Lyon
46 Allée d'Italie, 69364 Lyon Cedex 07, France
Téléphone : +33(0)4.72.72.80.37
Télécopieur : +33(0)4.72.72.80.80
Adresse électronique : lip@ens-lyon.fr

Vandermonde Matrices, NP-Completeness, and Transversal Subspaces

Alexander Chistov, Hervé Fournier,
Leonid Gurvits and Pascal Koiran

September 2002

Abstract

Let $\mathbb{K}$ be an infinite field. We give polynomial time constructions of families of r-dimensional subspaces of $\mathbb{K}^n$ with the following transversality property: any linear subspace of $\mathbb{K}^n$ of dimension $n-r$ is transversal to at least one element of the family. We also give a new NP-completeness proof for the following problem: given two integers n and m with $n \leqslant m$ and a $n \times m$ matrix A with entries in $\mathbb{Z}$, decide whether there exists a $n \times n$ sub-determinant of A which is equal to zero.

Keywords: linear algebra, transversality, derandomization, NP-completeness.

Résumé

Soit $\mathbb{K}$ un corps infini. Nous construisons en temps polynomial des familles de sous-espaces de dimension r de $\mathbb{K}^n$ satisfaisant la propriété suivante: tout sous-espace de dimension $n-r$ de $\mathbb{K}^n$ est supplémentaire à au moins l'un des membres de la famille. Nous donnons également une nouvelle preuve de NP-complétude pour le problème suivant: étant donnés deux entiers n et m tels que $n \leqslant m$, et une matrice A de taille $n \times m$ à coefficients entiers, décider s'il existe un sous-déterminant $n \times n$ de A qui est égal à zéro.

Mots-clés: algèbre linéaire, transversalité, dérandomisation, NP-complétude.

Vandermonde Matrices, NP-Completeness, and Transversal Subspaces

Alexander Chistov[*], Hervé Fournier[†], Leonid Gurvits[‡] and Pascal Koiran[§]

20th September 2002

Abstract

Let $\mathbb{K}$ be an infinite field. We give polynomial time constructions of families of r-dimensional subspaces of $\mathbb{K}^n$ with the following transversality property: any linear subspace of $\mathbb{K}^n$ of dimension $n-r$ is transversal to at least one element of the family. We also give a new NP-completeness proof for the following problem: given two integers n and m with $n \leqslant m$ and a $n \times m$ matrix A with entries in $\mathbb{Z}$, decide whether there exists a $n \times n$ sub-determinant of A which is equal to zero.

Keywords: linear algebra, transversality, derandomization, NP-completeness.

1 Introduction

Let $\mathbb{K}$ be an infinite field and let $\mathcal{F}$ be a finite family of r-dimensional linear subspaces of $\mathbb{K}^n$. We say that $\mathcal{F}$ has property $\mathcal{P}_{n,r}(\mathbb{K})$ if for every $(n-r)$-dimensional subspace $E \subseteq \mathbb{K}^n$ there exists an element of $\mathcal{F}$ which is transversal to E. It is not difficult to see that such families do exist. Given a basis of $\mathbb{K}^n$, consider for instance the family of subspaces spanned by r basis vectors. This particular family is of cardinality $\binom{n}{r}$. It was shown in [5] that families of cardinality as small as $1 + r(n-r)$ exist. Moreover, it was shown in the same paper that in most cases of interest (including in particular all fields of characteristic 0 and all algebraically closed fields) the basis vectors of the elements of such a family can be chosen of polynomial bit size. Due to the non-constructive nature of the proof of this transversality lemma, the parallel algorithm of [5] for computing the rank of matrices is non-uniform. A uniform parallel algorithm was published soon afterwards by Mulmuley [13], but the problem of a constructive proof of the transversality lemma had remained open. In this note we give such a constructive proof. More recently, the transversality lemma has also been used in computational algebraic geometry [14] and in complexity theory in the study of sparse sets [2].

[*]sliss@iias.spb.su. Saint Petersburg Institute for Informatics and Automation.
[†]Herve.Fournier@prism.uvsq.fr. PRISM, Université de Versailles Saint-Quentin.
[‡]gurvits@c3.lanl.gov. Los Alamos National Laboratory.
[§]Pascal.Koiran@ens-lyon.fr. LIP, ENS Lyon.

Our construction hinges on an elementary property of Vandermonde-like matrices, established in Lemma 1. In section 3 we give a second application of this lemma. Let NULLDET be the following problem: given two integers n and m with $n \leqslant m$ and a $n \times m$ matrix A with entries in $\mathbb{Z}$, decide whether there exists a $n \times n$ sub-determinant of A which is equal to zero. We show that this problem is NP-complete for polynomial time many-one reductions. It is not difficult to show that NULLDET is NP-hard for randomized reductions, and our proof can be viewed as a derandomization result. The NP-completeness of NULLDET was proposed as an open problem as early as in 1982 [3] and as late as in 1998 [6]. One motivation comes from computational geometry, where general position assumptions are often made. It is therefore of interest to determine whether such an assumption can be checked efficiently [6]. In fact, when that paper was published the problem had already been solved by Khachiyan [8]. Subsequently, a very elegant proof was published by Erickson [7]. This result is therefore not new, but at least we hope that the proof is new.

2 Transversal Subspaces

Let E and F be two linear subspaces of $\mathbb{K}^n$ such that $\dim E + \dim F \leqslant n$. Recall that E and F are said to be transversal if $\dim(E+F) = \dim E + \dim F$, or equivalently if $E \cap F = \{0\}$.

For $d \in \mathbb{N}$, we denote by $v_d(x)$ the Vandermonde vector $(1, x, \ldots, x^d)$. More generally, given a tuple $\overline{\alpha} = (\alpha_1, \ldots, \alpha_p) \in \mathbb{N}^p$, we denote $v_{\overline{\alpha}}(x) = (x^{\alpha_1}, \ldots, x^{\alpha_p})$. In this section we shall only use the case $\overline{\alpha} = (0, 1, \ldots, n-1)$. The following lemma is a variation on a result of [9].

Lemma 1 *Let E be a subspace of $\mathbb{K}^n$ of dimension p and $\overline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ a strictly increasing sequence of integers. Let $f \in \mathbb{K}[X]$ be a nonconstant polynomial such that $f^k \neq Id$ for $1 \leqslant k \leqslant \alpha_n$, where f^k denotes the k-th iterate of f. If $n \geqslant p + r$ and if x is transcendent over $\mathbb{K}$ then $V_r(x) = \mathrm{Vect}\{v_{\overline{\alpha}}(x), v_{\overline{\alpha}}(f(x)), \ldots, v_{\overline{\alpha}}(f^{r-1}(x))\}$ is transversal to E.*

Proof. By induction on r; we may start from $r = 0$. In this case the result is clear since $V_r(x) = \{0\}$. Assume now by contradiction that $r \geqslant 1$ and that $V_r(x)$ is not transversal to E. By induction hypothesis, E is transversal to $V_{r-1}(x)$. Hence x must satisfy property $\mathcal{Q}(x)$ below:

$$v_{\overline{\alpha}}(f^{r-1}(x)) \in E + V_{r-1}(x).$$

Since this property is algebraic in x and $f^k(x)$ is transcendent over $\mathbb{K}$ for any $k \geqslant 0$, $\mathcal{Q}(f^k(x))$ must in fact hold for all $k \geqslant 0$. This implies that for $k = 0, \ldots, \alpha_n$ the $1 + \alpha_n$ vectors $v_{\overline{\alpha}}(f^k(x))$ all belong to $E + V_{r-1}(x)$. Now build a $(1+\alpha_n) \times n$ matrix A such that $v_{\overline{\alpha}}(f^k(x))$ is the k-th row of A. The columns of A are n distinct columns extracted from a $(1+\alpha_n) \times (1+\alpha_n)$ Vandermonde matrix, hence A is of rank n. This is absurd since $\dim(E + V_{r-1}(x)) = p + r - 1 < n$. □

Proposition 1 *Let $\mathbb{K}$ be a field of characteristic 0. The family $(V_i)_{0 \leqslant i \leqslant r(n-r)}$ where $V_i = \mathrm{Vect}\{v_{n-1}(i), \ldots, v_{n-1}(i+r-1)\}$ has property $\mathcal{P}_{n,r}(\mathbb{K})$.*

Proof. We apply Lemma 1 to the polynomial $f(x) = x + 1$. Let E be a linear subspace of $\mathbb{K}^n$ of dimension $n-r$; let $e_1, \ldots, e_{n-r}$ be a basis of E. By Lemma 1, the polynomial

$$Q(x) = \det(e_1, \ldots, e_{n-r}, v_{n-1}(x), v_{n-1}(x+1), \ldots, v_{n-1}(x+r-1))$$

is not identically zero. Obviously, the degree of Q is upper bounded by $\sum_{i=n-r}^{n-1} i = r(2n-r-1)/2$. In order to obtain a better bound, consider the polynomial $R(x_1, \ldots, x_r) = \det(e_1, \ldots, e_{n-r}, v_{n-1}(x_1), v_{n-1}(x_2), \ldots, v_{n-1}(x_r))$. Its degree is upper bounded by $r(2n-r-1)/2$ as well. The point is that R admits a factorization of the form $R = \prod_{1 \leqslant i < j \leqslant r}(x_i - x_j)S(x_1, \ldots, x_r)$. The degree of S is therefore upper bounded by $r(2n-r-1)/2 - \binom{r}{2} = r(n-r)$, and the same is true of Q. Hence there exists an integer $i \in \{0, 1, \ldots, r(n-r)\}$ which is not a root of Q. The corresponding subspace V_i is transversal to E. □

The next proposition takes care of fields of positive characteristic. We denote by order(θ) the order of the multiplicative group generated by θ.

Proposition 2 *Let $\mathbb{K}$ be an infinite field (of arbitrary characteristic). Let $(z_i)_{0 \leqslant i \leqslant r(n-r)}$ be a family of non-zero distinct elements of $\mathbb{K}$. If* order(θ) $\geqslant n$, *the family $(V_i)_{0 \leqslant i \leqslant r(n-r)}$ where*

$$V_i = \mathrm{Vect}\{v_{n-1}(z_i), v_{n-1}(\theta z_i), \ldots, v_{n-1}(\theta^{r-1} z_i)\}$$

has property $\mathcal{P}_{n,r}(\mathbb{K})$.

Proof. We now apply Lemma 1 to the polynomial $f(x) = \theta x$. Let E be a linear subspace of $\mathbb{K}^n$ of dimension $n-r$; let $e_1, \ldots, e_{n-r}$ be a basis of E. By Lemma 1, the polynomial

$$Q(x) = \det(e_1, \ldots, e_{n-r}, v_{n-1}(x), v_{n-1}(\theta x), \ldots, v_{n-1}(\theta^{r-1} x))$$

is not identically 0. Consider the polynomial

$$R(x_1, \ldots, x_r) = \det(e_1, \ldots, e_{n-r}, v_{n-1}(x_1), v_{n-1}(\theta x_2), \ldots, v_{n-1}(\theta^{r-1} x_r)).$$

Now we have a factorization of the form

$$R(x_1, \ldots, x_r) = \prod_{1 \leqslant i < j \leqslant r} (x_j - \theta^{i-j} x_i) S(x_1, \ldots, x_r).$$

Hence Q has at most $r(n-r)$ nonzero roots since this polynomial admits a factorization of the form $Q(x) = x^{\binom{r}{2}} A(x)$. One of the z_i's is not a root of Q, and the corresponding subspace V_i is transversal to E. □

In order to have a completely explicit construction, one should of course explain how to construct an element θ of order at least n. It is natural to represent θ by its minimal polynomial over F_p. Hence we just need to produce an irreducible polynomial of degree at least n. For this purpose we can use the deterministic

algorithms of [4] or [15]. These algorithms produces in time polynomial in n and p a polynomial of degree n which is irreducible over F_p. Alternatively, one may construct an irreducible polynomial of degree m where $p^m > n+1$, and look for an element of order at least n in $GF(p^m)$. Such an element exists since the multiplicative group of a finite field is cyclic.

Here is a slightly different family with the property of transversality.

Proposition 3 *Let $\mathbb{K}$ be an infinite field. Let $a_0, \ldots, a_{n-1}$ be distinct elements of $\mathbb{K}$. For $0 \leqslant i \leqslant r-1$, let us define the column vector $v_i(t) = (a_0^i, a_1^i t, a_2^i t^2, \ldots, a_{n-1}^i t^{n-1})$. Let $(z_i)_{0 \leqslant i \leqslant r(n-r)}$ be a family of non-zero distinct elements of $\mathbb{K}$. The family $(V_i)_{0 \leqslant i \leqslant r(n-r)}$ where $V_i = \mathrm{Vect}\{v_0(z_i), \ldots, v_{r-1}(z_i)\}$ has property $\mathcal{P}_{n,r}(\mathbb{K})$.*

Proof. Let E be a linear subspace of $\mathbb{K}^n$ of dimension $n-r$; let $e_1, \ldots, e_{n-r}$ be a basis of E. By Gaussian elimination, one can assume that $e_i = (e_i^0, e_i^1, \ldots, e_i^{\alpha_i}, 0, \ldots, 0)$ with $e_i^{\alpha_i} \neq 0$ and $\alpha_1 < \alpha_2 < \ldots < \alpha_{n-r}$. Let $P(t) = \det(e_1, \ldots, e_{n-r}, v_0(t), \ldots, v_{r-1}(t))$. We claim that the valuation of P (i.e., the smallest power of t which appears in P with a nonzero coefficient) is $v = \binom{n}{2} - \sum_{j=1}^{n-r} \alpha_j$. Indeed, the basis of E ensures that $\mathrm{val}(P) \geqslant v$ and the coefficient of t^v, up to the sign, equals to $V \cdot \Pi_{i=1}^{n-r} e_i^{\alpha_i}$ where V is the determinant of the $r \times r$ Vandermonde matrix built on $(a_{\alpha_i})_{1 \leqslant i \leqslant r}$. Thus $P(t)$ is not identically zero, and $\mathrm{val}(P) \geqslant \binom{n}{2} - \sum_{j=r}^{n-1} j = \binom{r}{2}$. The argument is now the same as in proposition 2 since $P(t) = t^{\binom{r}{2}} A(t)$ where $A(t)$ is not identically zero and $\deg(A) \leqslant \sum_{j=n-r}^{n-1} j - \binom{r}{2} = r(n-r)$. □

It is a folklore result that no family of cardinality less than $1 + r(n-r)$ can have property $\mathcal{P}_{n,r}(\mathbb{K})$ if $\mathbb{K}$ is algebraically closed (this follows from algebraic geometry: $r(n-r)$ is the dimension of the Grassmanian manifold of r-dimensional subspaces of $\mathbb{K}^n$). Thus our constructions are optimal in this respect. For other fields (for instance $\mathbb{Q}$ or $\mathbb{R}$) it seems that the smallest possible cardinality is unknown. We are not even aware of nontrivial upper or lower bounds. Still the following remark shows that the real case is genuinely different from the complex case.

Remark 1 *Consider the family $\mathcal{F}$ of the 4 two-dimensional subspaces of $\mathbb{R}^4$ spanned by the columns of the following 4×2 matrices:*

$$\begin{pmatrix} I \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ I \end{pmatrix}, \begin{pmatrix} I \\ I \end{pmatrix}, \begin{pmatrix} R_{\pi/2} \\ I \end{pmatrix}.$$

Here I is the identity matrix and $R_{\pi/2}$ the rotation matrix of angle $\pi/2$. This family has property $\mathcal{P}_{4,2}(\mathbb{R})$.

Indeed, any two-dimensional subspace of $\mathbb{R}^4$ which has a non-trivial intersection with the first two elements of $\mathcal{F}$ must be of the form $V = \mathrm{Vect}\{\binom{x}{0}, \binom{0}{y}\}$. A subspace of this form can intersect non-trivially at most one of remaining two elements of $\mathcal{F}$. More precisely, if x and y are colinear the intersection with the last subspace is $\{0\}$, and if they are not colinear the intersection with the third subspace is $\{0\}$.

It is also possible to show that the family in Remark 1 is of cardinality as small as possible.

3 An NP-complete Problem

The problem NULLDET defined in the introduction can be restated in geometric terms as follows: given m points of $\mathbb{Z}^n$, decide if there exists a homogeneous hyperplane which contains at least n of these points. The closely related MAX-FLS problem is known to be NP-complete [1]. In this problem one must decide whether there exist K columns of the input matrix $A \in \mathbb{Z}^{n\times m}$ which form a submatrix of rank $< n$, where $K \geqslant n$ is a part of the input. Geometrically, this means that there exists a homogeneous hyperplane which contains at least K of the m input points.

Proposition 4 NULLDET *is NP-complete for polynomial time many-one reductions.*

Proof. We shall reduce MAX-FLS to NULLDET. Let (A, K) be an instance of this problem, where $A \in \mathbb{Z}^{n\times m}$ and $m \geqslant K \geqslant n$. Let M be the largest absolute value of the entries of A. Let $B(x)$ be the following $K \times m$ matrix.

$$B(x) = \begin{pmatrix} A \\ v_{m-1}(x) \\ \vdots \\ v_{m-1}(x + (K-n) - 1) \end{pmatrix}$$

Let $N = M^n K^{Km} + 1$. We claim that $B(N) \in$ NULLDET if and only if $(A, K) \in$ MAX-FLS. If K columns of A are of rank $< n$ then the same columns of $B(N)$ are of rank $< K$. Conversely, assume now that $A \notin$MAX-FLS. Let $(\alpha_1, \ldots, \alpha_K)$ be a strictly increasing sequence of elements of $\{1, \ldots, m\}$. The rank of the submatrix $A_{\overline{\alpha}}$ is equal to n since $A \notin$MAX-FLS. We need to show that $B(N)_{\overline{\alpha}}$ is of rank K. Let $P(x) = \det(B(x)_{\overline{\alpha}})$. By Lemma 1, this polynomial is not identically zero. Moreover, expanding the determinant shows that the coefficients of P are integers bounded by $N - 1$ in absolute value. By the classical bound on roots of polynomials, N is not a root of B so that $B(N)_{\overline{\alpha}}$ is indeed of rank K. As this is true for any $\overline{\alpha}$, $B(N)$ does no belong to NULLDET. □

Let κ-DET be the following problem: given two integers n and m with $n \leqslant m$ and a $n \times m$ matrix A with entries in $\mathbb{Z}$, decide whether there exists a $n \times n$ sub-determinant of A which is equal to κ. It was shown by Dyer, Gritzmann and Hufnagel [6] that κ-DET is NP-complete for $\kappa \neq 0$. However, as pointed out by these authors, their proof does not apply to the case $\kappa = 0$ and therefore stops short of proving that NULLDET is NP-complete.

It would also be interesting to understand the complexity of NULLDET in algebraic models of computation. For instance, can this problem be solved by polynomial depth algebraic computation trees (over the ordered field of real numbers, say)? Note that the NP-completeness of this problem needs not be an obstacle: it is well known that some "geometric" NP-complete problems (e.g., KNAPSACK) can be solved in polynomial depth [10, 11, 12].

References

[1] E. Amaldi and V. Kann. The complexity and approximability of finding maximum feasible subsystems of linear relations. *Theoretical Computer Science*, 147:181–210, 1995.

[2] J. Cai, A. Naik and D. Sivakumar. On the existence of hard sparse sets under weak reductions. In *Proc. STACS'96*, volume 1046 of *Lectures Notes in Computer Science*, pages 307-318. Springer-Verlag, 1996.

[3] R. Chandrasekaran, S. N. Kabadi and K. Murty. Some NP-complete problems in linear programming. *Operations Research Letters*, 1:101-103, 1982.

[4] A. Chistov. Constructing a finite field within a polynomial time. In *Proc. 7th Soviet Conference on Mathematical Logic*, Novosibirsk, 1984 (in Russian).

[5] A. Chistov. Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic. In *Proc. 5th International FCT Conference*, volume 199 of *Lectures Notes in Computer Science*, pages 9–13. Springer-Verlag, 1985.

[6] M. Dyer, P. Gritzmann and A. Hufnagel. On the complexity of computing mixed volumes. *SIAM Journal on Computing*, 27(2):356-400, 1998.

[7] J. Erickson. New lower bounds for convex hull problems in odd dimensions. *SIAM Journal on Computing*, 28(4):1198-1214, 1999.

[8] L. Khachiyan. On the complexity of approximating extremal determinants in matrices. *Journal of Complexity*, 11:138-153, 1995.

[9] P. Koiran, N. Portier, and G. Villard. A rank theorem for Vandermonde matrices. LIP Research Report 01-34, 2001.

[10] S. Meiser. Point location in arrangements of hyperplanes. *Information and Computation*, 106(2):286–303, 1993.

[11] F. Meyer auf der Heide. A polynomial linear search algorithm for the n-dimensional knapsack problem. *Journal of the ACM*, 31(3):668–676, 1984.

[12] F. Meyer auf der Heide. Fast algorithms for n-dimensional restrictions of hard problems. *Journal of the ACM*, 35(3):740–747, 1988.

[13] K. Mulmuley. A fast parallel algorithm to compute the rank of a matrix over an arbitrary field. In *Proc. 18th ACM Symposium on Theory of Computing*, pages 338–339, 1986.

[14] M.-F. Roy and N. Vorobjov. The complexification and degree of a semi-algebraic set. *Mathematische Zeitschrift*, 239(1):131–142, 2002.

[15] V. Shoup. New algorithms for finding irreducible polynomials over finite fields. *Mathematics of Computation*, 54:435–447, 1990.