On the construction of a family of transversal subspaces over finite fields

Alexander Chistov* Hervé Fournier† Pascal Koiran‡ Sylvain Perifel‡

December 11, 2006

Abstract

Let k be a field. We are interested in the families of r-dimensional subspaces of k^n with the following transversality property: any linear subspace of k^n of dimension $n-r$ is transversal to at least one element of the family. While it is known how to build such families in polynomial time over infinite fields k, no such technique is known for finite fields. However, transversal families in dimension n can be built when the field k is large enough with respect n. We improve here on how large k needs to be with respect to the considered dimension n.

1 Introduction

Let K be a field and $\mathcal{F}$ a family of r-dimensional linear subspaces of K^n. We say that $\mathcal{F}$ has property $\mathcal{P}_{n,r}(K)$ if for every $(n-r)$-dimensional subspace $E \subset K^n$ there exists an element F of $\mathcal{F}$ which is transversal to E – i.e. such that $E \cap F = \{0\}$. Over infinite fields, it was shown in [3] that families with "small coefficients" having this property and as small as $r(n-r)+1$ do exist. There the question of efficient algorithms to build transversal families was raised in relationship with the complexity of computing the rank of a matrix. This transversality property has also been used recently for instance in computational algebraic geometry [8] over un an infinite field, and in complexity theory [1] over finite fields.

In the case of an infinite field K, explicit constructions of families of size $n^{O(1)}$ with property $\mathcal{P}_{n,r}(K)$ were given in [4]. In this paper, we address the same problem over finite fields. Although no polynomial time algorithm is known to solve this problem, the previoulsly mentionned algorithm allows to build in polynomial time transversal families over K^n when $|K|$ is large enough with respect to n. The main results we present here are polynomial-time algorithms that work on fields of size linear in the dimension n instead of quadratic as was previously known.

*St.-Petersburg Department of Steklov Mathematical Institute of the Academy of Sciences of Russia, Fontanka 27, St.-Petersburg 191023, Russia. Email: alch@pdmi.ras.ru

†Laboratoire PRiSM, Université de Versailles Saint-Quentin en Yvelines, 45 avenue des États-Unis, 78035 Versailles Cedex, France. Email: herve.fournier@prism.uvsq.fr

‡LIP, École Normale Supŕieure de Lyon, 46, Allée d'Italie 69364 Lyon Cedex 07 - France. Email: [pascal.koiran,sylvain.perifel]@ens-lyon.fr

Let us now generalize the notion of family of transversal subspaces. Let $k \subset K$ be two fields. An r-dimensional subspace V of k^n defines in the natural way the subspace that consists in the vector space of K^n spanned by V; we shall denote it $\hat{V}$ when the big field K is clear from the context. Let $\mathcal{F}$ be a finite family of r-dimensional linear subspaces of k^n. We shall say that $\mathcal{F}$ has property $\mathcal{P}_{n,r}(k, K)$ if and only if for every $(n-r)$-dimensional subspace $W \subset K^n$ there exists an element V of $\mathcal{F}$ such that the linear subspaces $\hat{V}$ and W are transversal. For a field K the property $\mathcal{P}_{n,r}(K, K)$ is the property $\mathcal{P}_{n,r}(K)$ defined above. We shall also say that a family of full rank $n \times r$ matrices over k has property $\mathcal{P}_{n,r}(k, K)$ if the family of linear subspaces of k^n spanned by the columns of each of these matrices has this property – note that it does not depend on the chosen basis of k^n.

Constructions of transversal families in [4] are given for infinite fields (of any characacteristic) but allow to build families with the $\mathcal{P}_{n,r}(K)$ property as long as the field K is large enough with regard to n. More precisely, we have the following. Consider the n-dimensional space $\mathbb{F}_q^n$ over the field $\mathbb{F}_q$ and its linear subspaces. By [4], given $0 \leqslant r \leqslant n$ and $q = p^{\nu_0}$ (where p is prime), if $q > r(n-r)+1$ then one can construct a family $\mathcal{F}$ satisfying property $\mathcal{P}_{n,r}(\mathbb{F}_q)$ and of size $|\mathcal{F}| = r(n-r)+1$. The working time of this algorithm is polynomial in n, p and ν_0. In fact, this family even has property $\mathcal{P}_{n,r}(\mathbb{F}_q, \overline{\mathbb{F}_q})$ where $\overline{\mathbb{F}_q}$ is the algebraic closure of $\mathbb{F}_q$ – and we know that the size of the family is optimal with respect to this property. Let us define $\tau(n, r) = r(n-r) + 1$.

In the present paper we improve the inequality $q > r(n-r)+1$. Namely, in section 3 we show that for $q \geqslant \lfloor n/2 \rfloor$ we can build a family with property $\mathcal{P}_{n,r}(\mathbb{F}_q)$ but with $|\mathcal{F}| \leqslant \tau(n, r)^3$. Note that the size $|\mathcal{F}|$ is bigger (still polynomial in n, though) but now q is linear in n, i.e. less than in [4] where it had to be quadratic. The proof uses techniques of traces in extensions of finite fields. This leads to the construction of families of size $n^{O(1/\varepsilon)}$ with property $\mathcal{P}_{n,r}(\mathbb{F}_q)$ for $q \geqslant \varepsilon n$. In section 4 using another approach of differentiations we get similar results but for the property $\mathcal{P}_{n,r}(\mathbb{F}_q, \overline{\mathbb{F}_q})$. Although this result is stronger than the one of section 3 we decided to leave the construction of section 3 in this paper since its proof is simple and instructive. Of course, we would like to have, for any prime power q, an algorithm that, given n and r, would build a family $\mathcal{F}$ satisfying property $\mathcal{P}_{n,r}(\mathbb{F}_q)$ – or even the stronger property $\mathcal{P}_{n,r}(\mathbb{F}_q, \overline{\mathbb{F}_q})$) – in time $n^{O(1)}$; this would of course imply that $|\mathcal{F}| = n^{O(1)}$.

Indeed, we do know that such small families with property $\mathcal{P}_{n,r}(\mathbb{F}_q, \overline{\mathbb{F}_q})$ exist: this is proved by a probabilistic argument using known bounds on the number of zero-patterns of a set of polynomials in section 5, where related questions are raised.

2 Elementary properties

For vectors $a, b \in \mathbb{F}_q^n$, $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$, let $ab = a_1 b_1 + \ldots + a_n b_n \in \mathbb{F}_q$. For an arbitrary $(n-r)$-dimensional subspace W of $\mathbb{F}_q^n$ let

$$W^{\perp} = \left\{ a \in \mathbb{F}_q^n \ : \ ab = 0 \quad \forall b \in W \right\}.$$

The set $W^{\perp}$ is an r-dimensional linear subspace of $\mathbb{F}_q^n$. Let us state two simple lemmas related to duality.

Lemma 1 *Let $\mathcal{F}$ be a family with the $\mathcal{P}_{n,r}(k,K)$ property. Then $\mathcal{F}^\perp = \{V^\perp,\ V \in \mathcal{F}\}$ has the $\mathcal{P}_{n,n-r}(k,K)$ property.*

Proof. Let V be a linear subspace of K^n of dimension r. Then there exists $W \in \mathcal{F}$ transversal to $V^\perp$. Thus $W^\perp \in \mathcal{F}^\perp$ is transversal to V. $\square$

Remark moreover that if $\mathcal{F}$ is given by matrices, $\mathcal{F}^\perp$ can be computed from $\mathcal{F}$ in a polynomial number of operations over the field k.

Lemma 2 *Let $\mathcal{F}$ be a family of matrices of size $n \times r$ over k. This family has the $\mathcal{P}_{n,r}(k,K)$ property if and only if for all full rank matrix A of size $r \times n$ over K, there exists $F \in \mathcal{F}$ such that* $\det(AF) \neq 0$.

Proof. Remember that the family $\mathcal{F}$ has property $\mathcal{P}_{n,r}(k,K)$ if and only if for all $n \times (n-r)$ full rank matrix V over K, there exists $F \in \mathcal{F}$ such that $\det(F|V) \neq 0$.

For the "if" part, take an $n \times (n-r)$ full rank matrix V over K. Then there exists an $r \times n$ full rank matrix A over K such that $AV = 0$ (take for the rows of A a basis of $\mathrm{Span}(V)^\perp$) as well as an $(n-r) \times n$ matrix B over K such that $BV = I$. Furthermore, by hypothesis there exists $F \in \mathcal{F}$ such that AF has full rank. Since $\begin{pmatrix} A \\ B \end{pmatrix} \begin{pmatrix} F \,|\, V \end{pmatrix} = \begin{pmatrix} AF & 0 \\ BF & I \end{pmatrix}$, this implies that $(F|V)$ has full rank.

For the converse, take an $r \times n$ full rank matrix A over K. As before, take an $n \times (n-r)$ full rank matrix V over K such that $AV = 0$ and an $(n-r) \times n$ matrix B over K such that $BV = I$. Remark that $\binom{A}{B}$ has full rank. Now, as above, if $F \in \mathcal{F}$ is such that $(F|V)$ has full rank, then AF also has full rank. $\square$

Given $\mathcal{F}$ and $\mathcal{G}$ two families of linear subspaces of the same vector space, let us define

$$\mathcal{F} \cdot \mathcal{G} = \{F + G \,:\, F \cap G = \{0\},\ F \in \mathcal{F},\ G \in \mathcal{G}\}.$$

Lemma 3 *Let $\mathcal{F}$ be a family with property $\mathcal{P}_{n,r}(k,K)$ and $\mathcal{G}$ be a family with property $\mathcal{P}_{n,s}(k,K)$, with $r + s \leqslant n$. Then $\mathcal{F} \cdot \mathcal{G}$ has property $\mathcal{P}_{n,r+s}(k,K)$.*

Proof. Let V be a subspace of dimension $n-(r+s)$. There exists $F \in \mathcal{F}$ such that $V \cap F = \{0\}$. Now, $V + F$ has dimension $n - s$ therefore there exists $G \in \mathcal{G}$ transversal to $V + F$. The subspace $F + G \in \mathcal{F} \cdot \mathcal{G}$ is then transversal to V. $\square$

We shall note $\mathcal{F}^n$ for $\mathcal{F} \cdot \mathcal{F} \cdot \ldots \cdot \mathcal{F}$ (n times).

Lemma 4 *Let $\mathcal{F} = \{A_i \mid i \in I\}$ be a family of $n \times r$ matrices with property $\mathcal{P}_{n,r}(k,K)$. Let $m < n$ and A'_i be the submatrix of A_i composed of its first m rows. Then $\mathcal{F}' = \{A'_i \mid i \in I\ \}$ has property $\mathcal{P}_{m,r}(k,K)$.*

Proof. Let B be a full rank matrix of size $m \times (m-r)$ over K. Now let $C = \begin{pmatrix} 0 & B \\ I_{n-m} & 0 \end{pmatrix}$ where I_{n-m} is the $(n-m) \times (n-m)$ identity matrix. As C has full rank, there exists $i \in I$ such that $\det(C \mid A_i) \neq 0$. But $\det(C \mid A_i) = \det(B \mid A'_i)$. $\square$

3 Construction based on the trace

Let $\nu \geqslant 1$ be an integer and $\mathbb{F}_{q^\nu}$ be the field with q^ν elements. Then the $\mathbb{F}_q$-linear mapping of the trace

$$\mathrm{tr} : \mathbb{F}_{q^\nu} \longrightarrow \mathbb{F}_q, \quad \mathrm{tr}(a) = \sum_{0 \leqslant i \leqslant \nu-1} a^{q^i},$$

is defined. It is known that $\mathrm{tr}(\mathbb{F}_{q^\nu}) = \mathbb{F}_q$, i.e., the mapping of trace is nonzero. For an arbitrary matrix $B = (b_{i,j})$ with coefficients from $\mathbb{F}_{q^\nu}$ we shall denote by $\mathrm{tr}(B) = (\mathrm{tr}(b_{i,j}))$ the matrix consisting of traces of coefficients of B. So $\mathrm{tr}(B)$ is a matrix of the same size and with coefficients from $\mathbb{F}_q$.

Lemma 5 *Let $A = (a_{i,j})$ be a square nondegenerate matrix of size $s \geqslant 1$ with coefficients $a_{i,j} \in \mathbb{F}_{q^\nu}$ (so $\det(A) \neq 0$). Assume that $q \geqslant s$. Then there exists an element $t \in \mathbb{F}_{q^\nu}$ such that the matrix $\mathrm{tr}(tA)$ is nondegenerate, i.e., $\det(\mathrm{tr}(tA)) \neq 0$.*

Proof. If $s = 1$ the assertion holds since the trace mapping is nonzero. So we shall suppose without loss of generality that $s > 1$ and $\nu > 1$. Let X be a variable and let $f = \det(\mathrm{tr}(XA))$. Then $f \in \mathbb{F}_{q^\nu}[X]$ is a polynomial of degree $\deg f \leqslant sq^{\nu-1} \leqslant q^\nu$. Let us write $f = \sum_{0 \leqslant i \leqslant q^\nu} f_i X^i$, where all the f_i are in $\mathbb{F}_{q^\nu}$. Obviously $f_s = \det(A) \neq 0$. Set $g = f + f_{q^\nu}(X - X^{q^\nu}) \in \mathbb{F}_{q^\nu}[X]$. Then $\deg g \leqslant q^\nu - 1$. The coefficient of X^s in the polynomial g is f_s since $s > 1$ and $\nu \geqslant 1$. Hence $g \neq 0$. Further, the polynomial $X - X^{q^\nu}$ vanishes on $\mathbb{F}_{q^\nu}$. Therefore, $g(t) = f(t)$ for every $t \in \mathbb{F}_{q^\nu}$. The polynomial g does not vanish on $\mathbb{F}_{q^\nu}$ since $g \neq 0$, the degree $\deg g \leqslant q^\nu - 1$ and the number of elements of the field is $|\mathbb{F}_{q^\nu}| = q^\nu$. Thus, there exists $t \in \mathbb{F}_{q^\nu}$ such that $g(t) \neq 0$. Now $\det(\mathrm{tr}(tA)) \neq 0$. $\square$

Remark 1 *The inequality $q \geqslant s$ in the statement of the lemma can not be improved by, e.g., $q \geqslant s - 1$. Indeed, let $\nu > 1$. Then there exist two elements $a, b \in \mathbb{F}_{q^\nu}$ linearly independent over $\mathbb{F}_q$. Let A be a square diagonal matrix of size $q + 1$ with the elements on the diagonal a, $b + \lambda a$, $\lambda \in \mathbb{F}_q$. Then $\det(A) \neq 0$ but $\det(\mathrm{tr}(tA)) = 0$ for every $t \in \mathbb{F}_{q^\nu}$.*

Theorem 1 *Let $q = p^{\nu_0} \geqslant \min\{r, n - r\}$ where $0 \leqslant r \leqslant n$. Then one can construct a family $\mathcal{F}$ satisfying property $\mathcal{P}_{n,r}(\mathbb{F}_q)$ with $|\mathcal{F}| \leqslant \tau(n,r)^3$. The working time of the algorithm for computing $\mathcal{F}$ is polynomial in n, p and ν_0.*

Proof. By [4] we can assume without loss of generality that $q \leqslant \tau(n,r)$. Also in what follows $1 \leqslant r \leqslant n - 1$.

At first suppose that $q \geqslant r$. Let $\nu \geqslant 1$ be the least integer such that $q^\nu > \tau(n,r)$. Since $q \leqslant \tau(n,r)$, of course $q^\nu \leqslant \tau(n,r)^2$. First remark that we can efficiently work in the extension of fields $\mathbb{F}_{q^\nu}$. Indeed, according to [2] and [9], one can construct in time polynomial in ν, ν_0 and p an irreducible polynomial Φ of degree $\nu\nu_0$ over the field $\mathbb{F}_p$. Further, within the same time one can factor Φ over the field $\mathbb{F}_q$ and construct an irreducible polynomial $\varphi \in \mathbb{F}_q[Z]$ of degree $\deg_Z \varphi = \nu$. So one can construct the extension of fields $\mathbb{F}_{q^\nu} = \mathbb{F}_q[Z]/(\varphi) \supset \mathbb{F}_q$.

Now, the algorithm of [4] constructs a family $\mathcal{F}_0$ of matrices of size $n \times r$ satisfying $\mathcal{P}_{n,r}(\mathbb{F}_{q^\nu})$. This family $\mathcal{F}_0$ has size $\tau(n,r)$.

Let $\mathcal{F}_0 = \{B_\alpha\}_{1 \leqslant \alpha \leqslant \tau(n,r)}$. Let

$$\mathcal{F} = \left\{ \operatorname{tr}(tB_\alpha) \,:\, \operatorname{rank}(\operatorname{tr}(tB_\alpha)) = r,\, 1 \leqslant \alpha \leqslant \tau(n,r),\, t \in \mathbb{F}_{q^\nu} \right\}.$$

Obviously one can construct the family $\mathcal{F}$ in time polynomial in n, p and ν_0. The size satisfies $|\mathcal{F}| \leqslant q^\nu |\mathcal{F}_0| \leqslant \tau(n,r)^3$.

Let us show that the family $\mathcal{F}$ satisfies property $\mathcal{P}_{n,r}(\mathbb{F}_q)$. We shall use the characterization of Lemma 2. Let D be a full rank matrix of size $r \times n$ over $\mathbb{F}_q$. There exists α such that $\det(DB_\alpha) \neq 0$. Hence by Lemma 5 there exists $t \in \mathbb{F}_{q^\nu}$ such that $\det(\operatorname{tr}(tDB_\alpha)) \neq 0$. We have $\operatorname{tr}(tDB_\alpha) = D \operatorname{tr}(tB_\alpha)$ since the matrix D has coefficients from $\mathbb{F}_q$ and the mapping of trace is $\mathbb{F}_q$-linear. The theorem is proved for $q \geqslant r$.

Assume that $q < r$. Then $q \geqslant n - r$ since $q \geqslant \min\{r, n-r\}$. By the first part one can construct a family $\mathcal{F}'$ satisfying property $\mathcal{P}_{n,n-r}(\mathbb{F}_q)$. Let $\mathcal{F}' = \{V_\iota\}_{\iota \in I}$. By Lemma 1 the family $\mathcal{F} = \{V_\iota^\perp\}_{\iota \in I}$ satisfies property $\mathcal{P}_{n,r}(\mathbb{F}_q)$. Moreover, it can be computed in polynomial time. $\square$

Corollary 1 *Let $\varepsilon > 0$ be a real number. Let $0 \leqslant r \leqslant n$ be two integers and $q = p^{\nu_0} \geqslant \varepsilon \cdot \min\{r, n-r\}$. Then one can construct a family $\mathcal{F}$ satisfying property $\mathcal{P}_{n,r}(\mathbb{F}_q)$ with $|\mathcal{F}| \leqslant (q(n-q)+1)^{3\lceil r/q \rceil} = n^{O(1/\varepsilon)}$. The working time of the algorithm for computing $\mathcal{F}$ is polynomial in $n^{1/\varepsilon}$, p and ν_0.*

Proof. One can suppose that $q \geqslant \varepsilon r$ (otherwise, apply the following construction to $r' = n - r$ then apply Lemma 1). Now perform the Euclidean division $r = aq + b$. Note that $a \leqslant 1/\varepsilon$. By Theorem 1, one can build $\mathcal{F}_1$ with property $\mathcal{P}_{n,q}(\mathbb{F}_q)$ and $\mathcal{F}_2$ with property $\mathcal{P}_{n,b}(\mathbb{F}_q)$. Now build $\mathcal{F} = (\mathcal{F}_1)^a \cdot \mathcal{F}_2$. By Lemma 3 the family $\mathcal{F}$ has property $\mathcal{P}_{n,r}(\mathbb{F}_q)$. The working time of the algorithm is as announced. $\square$

4 Construction based on differentiation

We now give two constructions of families with the $\mathcal{P}_{n,r}(\mathbb{F}_q, \overline{\mathbb{F}_q})$ property – while the families built in the previous section only had the $\mathcal{P}_{n,r}(\mathbb{F}_q)$ property. The first construction is straightforward. The second is more involved but yields much smaller families.

Lemma 6 *Let $0 \leqslant r \leqslant n$ and $q = p^{\nu_0} > (\nu - 1)r$. Let P be an irreductible polynomial of degree ν over $\mathbb{F}_q$, so that $\mathbb{F}_{q^\nu} = \mathbb{F}_q[X]/(P(X))$. Let $\{B_\alpha(X) \,:\, 1 \leqslant \alpha \leqslant N\}$ be a family of matrices (where coefficients are polynomials of degree at most $\nu - 1$ over $\mathbb{F}_q$) with property $\mathcal{P}_{n,r}(\mathbb{F}_{q^\nu}, \overline{\mathbb{F}_q})$. Let $F \subset \mathbb{F}_q$ with $|F| > (\nu - 1)r$. Then $\{B_\alpha(x) \,:\, x \in F, 1 \leqslant \alpha \leqslant N\}$ has property $\mathcal{P}_{n,r}(\mathbb{F}_q, \overline{\mathbb{F}_q})$.*

Proof. Let D be a full rank matrix of size $(n-r) \times n$ with coefficients in $\overline{\mathbb{F}_q}$. There exists α such that $\det(D, B_\alpha(X)) \notin P \cdot K[X]$. In particular, this is a nonzero polynomial, and its degree is at most $(\nu - 1)r < q$. Thus there exists $x \in F$ which is not a root of this polynomial, and $B_\alpha(x)$ satisfies $\det(D, B_\alpha(x)) \neq 0$. $\square$

Theorem 2 *Let $\varepsilon > 0$ be a real number. Let $q > 2$ be such that $q = p^{\nu_0} \geqslant \varepsilon n$ and let $0 \leqslant r \leqslant n$ be an integer. Then one can construct a family $\mathcal{F}$ satisfying property $\mathcal{P}_{n,r}(\mathbb{F}_q, \overline{\mathbb{F}_q})$ with size $|\mathcal{F}| = O((nq^2/2)^{2r/(q-2)+1}) = n^{O(1/\varepsilon)}$. The working time of the algorithm for computing $\mathcal{F}$ is polynomial in $n^{1/\varepsilon}$, p and ν_0.*

Proof. By [4] one can assume that $q \leqslant \tau(n,r)$. We begin with the case $q \geqslant n$. Then $q^2 \geqslant \tau(n,r)$, thus [4] gives a family $\mathcal{G}$ with property $\mathcal{P}_{n,r}(\mathbb{F}_{q^2}, \overline{\mathbb{F}_q})$. Lemma 6 for $\nu = 2$ and $r \leqslant n/2$ (without loss of generality by Lemma 1) thus yields a family $\mathcal{F}$ with property $\mathcal{P}_{n,r}(\mathbb{F}_q, \overline{\mathbb{F}_q})$ and of size $(r+1)\tau(n,r)$.

If $q < n$, however, one cannot apply this method directly because $\mathbb{F}_q$ must contain more than r elements, which might not be the case. Let us therefore suppose $q < n$ and choose $\nu = 3$. For n big enough, it holds that $q^\nu \geqslant \varepsilon^3 n^3 > \tau(n,r)$, and we will deal with this case. Just remark that we can solve the case where $\varepsilon^3 n^3 \leqslant \tau(n,r)$ (that is, the case where n is small) with the family of all the subspaces of dimension r over $\mathbb{F}_q$, of which there are less than q^{nr}. This does not affect the asymptotic bound on the size of the family since only a finite number of n are concerned. Therefore we now suppose that $q^\nu > \tau(n,r)$. Let $t = \lfloor \frac{q-1}{2} \rfloor$. Let us perform the Euclidean division $r = at + b$. Remark that $a = O(1/\varepsilon)$. Thanks to [4] one can build two families $\mathcal{G}_1$ of size $\tau(n,t)$ with property $\mathcal{P}_{n,t}(\mathbb{F}_{q^\nu}, \overline{\mathbb{F}_q})$ and $\mathcal{G}_2$ of size $\tau(n,b)$ with property $\mathcal{P}_{n,b}(\mathbb{F}_{q^\nu}, \overline{\mathbb{F}_q})$. As $\nu = 3$, one has $q > (\nu-1)t$ and $q > (\nu-1)b$; thus Lemma 6 allows to build $\mathcal{F}_1$ of size $(2t+1)\tau(n,t)$ with property $\mathcal{P}_{n,t}(\mathbb{F}_q, \overline{\mathbb{F}_q})$ and $\mathcal{F}_2$ of size $(2b+1)\tau(n,b)$ with property $\mathcal{P}_{n,b}(\mathbb{F}_q, \overline{\mathbb{F}_q})$. Then we can build $\mathcal{F} = (\mathcal{F}_1)^a \cdot \mathcal{F}_2$. This family has property $\mathcal{P}_{n,r}(\mathbb{F}_q, \overline{\mathbb{F}_q})$ thanks to Lemma 3 and $|\mathcal{F}| = O((nq^2/2)^{2r/(q-2)+1}) = n^{O(1/\varepsilon)}$. Moreover, the time needed to perform this construction is polynomial in $n^{1/\varepsilon}$, p and ν_0. □

This method based on Lemma 6 unfortunately does not work in the case where $q = 2$ because the set F of the lemma must have more than $(\nu-1)r$ elements, that is, more than 2. Theorem 3 however remedies this situation.

Lemma 7 *Let $q = p^{\nu_0}$. Let $n \geqslant 1$ and $1 \leqslant r \leqslant n-1$ be arbitrary integers. Let $\nu \geqslant 1$ be the least integer such that $q^\nu > \tau(n,r)$. Suppose that $\nu \geqslant 2$. Assume that $2q+1 \geqslant \nu - 1$. Let*

$$\lambda = \left\lfloor \frac{2q+1}{\nu-1} \right\rfloor, \qquad \sigma = \left\lceil \frac{r}{\lambda} \right\rceil.$$

Then one can construct a family $\mathcal{F}$ satisfying property $\mathcal{P}_{n,r}(\mathbb{F}_q, \overline{\mathbb{F}_q})$ with size

$$|\mathcal{F}| \leqslant (\,(q+1)(\lambda+1)\,)^\sigma\, \tau(n,r).$$

The working time of the algorithm for computing the family $\mathcal{F}$ is polynomial in n, ν_0, q^σ and λ^σ.

The idea of the proof is the following. Given an $(n-r) \times n$ full rank matrix D, the method of [4] allows to build a transversal family in a sufficiently big extension. This gives a matrix G with coefficients in that extension and such that $\det \binom{G}{D} \neq 0$. We are able to find a sequence of differentiations and substitutions which keeps the determinant nonzero while bringing back the coefficients of the matrix in $\mathbb{F}_q$. Now, this sequence of differentiations of the determinant can be expressed as a big sum of determinants, in which at least one term must be nonzero. It remains to take as our transversal family the set corresponding to all these terms.

Proof. Let us first give a couple of definitions. For $1 \leqslant j \leqslant \sigma$, define the set P_j of polynomials of $\mathbb{F}_q[X_j, Y_j]$ by $P_j = \{\, zY_j + X_j \,:\, z \in \mathbb{F}_q \,\} \cup \{Y_j\}$. For $b \in P_j$ we let $\widetilde{b} = (-z, 1)$ if $b = zY_j + X_j$, and $\widetilde{b} = (1, 0)$ if $b = Y_j$. Define the differentiation $D_{j,b} = \partial/\partial X_j$ if $b \neq Y_j$, and $D_{j,b} = \partial/\partial Y_j$ if $b = Y_j$.

Consider now an arbitrary matrix A with rows $a_1, \ldots, a_m$ and with coefficients from the ring $\mathbb{F}_q[X_j, Y_j]$. For an integer $1 \leqslant w \leqslant m$, let us define the matrix $D_{j,b,w}(A)$ as follows. The rows of $D_{j,b,w}(A)$ are $a_1, \ldots, a_{w-1}, D_{j,b}(a_w), a_{w+1}, \ldots, a_m$, i.e., the matrix $D_{j,b,w}(A)$ is obtained from A by the differentiation $D_{j,b}$ of the w-th row of A.

We now describe the construction of the family $\mathcal{F}$. Using the algorithms of [2] or [9], construct a minimal polynomial of a primitive element ξ of the extension $\mathbb{F}_{q^\nu} \supset \mathbb{F}_q$. So $\mathbb{F}_{q^\nu} = \mathbb{F}_q[\xi]$. With the method of [4], build a family $\mathcal{F}_0 = \{\, B_\alpha \,\}_{1 \leqslant \alpha \leqslant N}$ satisfying property $\mathcal{P}_{n,r}(\mathbb{F}_{q^\nu}, \overline{\mathbb{F}_q})$ with $N = \tau(n, r)$, each matrix B_α being of size $r \times n$. Write B_α as

$$B_\alpha = \sum_{0 \leqslant i \leqslant \nu-1} B_{\alpha,i} \xi^i,$$

where all matrices $B_{\alpha,i}$ have coefficients from the field $\mathbb{F}_q$. Further, let

$$B_{\alpha,i} = \begin{pmatrix} B_{\alpha,i,1} \\ B_{\alpha,i,2} \\ \vdots \\ B_{\alpha,i,\sigma} \end{pmatrix},$$

where every matrix $B_{\alpha,i,j}$, $1 \leqslant j \leqslant \sigma - 1$ has λ rows. Hence the number of rows of the matrix $B_{\alpha,i,\sigma}$ is at most λ by the definitions of λ and σ.

Let X_j and Y_j be variables for $1 \leqslant j \leqslant \sigma$. Set

$$G_{\alpha,j} = \sum_{0 \leqslant i \leqslant \nu-1} B_{\alpha,i,j} X_j^i Y_j^{\nu-1-i}, \quad 1 \leqslant \alpha \leqslant N,\ 1 \leqslant j \leqslant \sigma.$$

Hence the coefficients of the matrix $G_{\alpha,j}$ are homogeneous polynomials with respect to X_j, Y_j. Set

$$G_\alpha = \begin{pmatrix} G_{\alpha,1} \\ G_{\alpha,2} \\ \vdots \\ G_{\alpha,\sigma} \end{pmatrix}, \qquad 1 \leqslant \alpha \leqslant N.$$

Hence G_α is a matrix with r rows and n columns and its coefficients are homogeneous polynomials of the ring $\mathbb{F}_q[X_1, Y_1, \ldots, X_\sigma, Y_\sigma]$.

Let $\lambda(j)$ be the number of rows of the matrix $G_{\alpha,j}$. Let $W_j = \{\star, 1, 2, \ldots, \lambda(j)\}$. For $b_j \in P_j$ and $w_j \in W_j$, let us define $G_{\alpha,j,b_j,w_j} = G_{\alpha,j}$ if $w_j = \star$ and $G_{\alpha,j,b_j,w_j} = D_{j,b_j,w_j}(G_{\alpha,j})$

otherwise. Let $P = P_1 \times \ldots \times P_\sigma$ and $W = W_1 \times \ldots \times W_\sigma$. For $b = (b_1, \ldots, b_\sigma) \in P$, $w = (w_1, \ldots, w_\sigma) \in W$ and $1 \leqslant \alpha \leqslant N$, let us define the matrix

$$G_{\alpha,b,w} = \begin{pmatrix} G_{\alpha,1,b_1,w_1} \\ G_{\alpha,2,b_2,w_2} \\ \vdots \\ G_{\alpha,\sigma,b_\sigma,w_\sigma} \end{pmatrix}.$$

Hence $G_{\alpha,b,w}$ is a matrix with r rows and n columns with coefficients from the ring $\mathbb{F}_q[X_1, Y_1, \ldots, X_\sigma, Y_\sigma]$. Let $H_{\alpha,b,w} = G_{\alpha,b,w}|_{\{(X_j,Y_j)=\widetilde{b}_j,\, 1\leqslant j\leqslant\sigma\}}$, i.e., $H_{\alpha,b,w}$ is a matrix of size $r \times n$ with coefficients from $\mathbb{F}_q$ which is obtained by the substitution of (X_j, Y_j) by $\widetilde{b}_j$ in $G_{\alpha,b,w}$ (for $1 \leqslant j \leqslant \sigma$). Let

$$\mathcal{F} = \{\, H_{\alpha,b,w} \,:\, \mathrm{rank}(H_{\alpha,b,w}) = r,\ 1 \leqslant \alpha \leqslant N,\ b \in P,\ w \in W \,\}.$$

Obviously the number of elements satisfies $|\mathcal{F}| \leqslant (\,(q+1)(\lambda+1)\,)^\sigma\, \tau(n,r)$. Moreover the family $\mathcal{F}$ can be constructed in polynomial time in n, ν_0, q^σ and λ^σ.

We claim that $\mathcal{F}$ satisfies property $\mathcal{P}_{n,r}(\mathbb{F}_q, \overline{\mathbb{F}_q})$. Let D be a $(n-r) \times n$ full rank matrix over $\overline{\mathbb{F}_q}$. Then there is $1 \leqslant \alpha \leqslant N$ such that

$$\det \begin{pmatrix} B_\alpha \\ D \end{pmatrix} \neq 0.$$

Since substituting ξ for each X_j and 1 for each Y_j in G_α gives B_α, we deduce that

$$\Delta = \det \begin{pmatrix} G_\alpha \\ D \end{pmatrix} \neq 0.$$

We shall show the existence of some elements $(b_1, \ldots, b_\sigma) \in P$ and $(r_1, \ldots, r_\sigma) \in \{0,1\}^\sigma$ such that

$$(D^{r_\sigma}_{\sigma,b_\sigma} \ldots D^{r_2}_{2,b_2} D^{r_1}_{1,b_1} \Delta)|_{\{(X_a,Y_a)=\widetilde{b}_a,\, 1\leqslant a\leqslant\sigma\}} \neq 0. \tag{1}$$

This allows to conclude as explained now. Let us first recall the following well known fact. Let A be a square matrix of size n with rows $a_1, \ldots, a_n$. Assume that the coefficients of the matrix A are from a ring R and that D is a differentiation of R. Then

$$D\,(\det(A)) = \det \begin{pmatrix} D(a_1) \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \det \begin{pmatrix} a_1 \\ D(a_2) \\ \vdots \\ a_n \end{pmatrix} + \ldots + \det \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ D(a_n) \end{pmatrix}. \tag{2}$$

This property is useful in order to conclude as follows. Let $W[r] = \{(w_1, \ldots, w_\sigma) \in W \mid w_j = \star \text{ iff } r_j = 0\}$. Applying (2) several times we get

$$D^{r_\sigma}_{\sigma,b_\sigma} \ldots D^{r_2}_{2,b_2} D^{r_1}_{1,b_1} \Delta = \sum_{w \in W[r]} \det \begin{pmatrix} G_{\alpha,b,w} \\ D \end{pmatrix}. \tag{3}$$

If we substitute (X_j, Y_j) by $\widetilde{b}_j$ in (3) (for $1 \leqslant j \leqslant \sigma$), we get

$$(D^{r_\sigma}_{\sigma,b_\sigma} \dots D^{r_2}_{2,b_2} D^{r_1}_{1,b_1} \Delta)|_{\{(X_a,Y_a)=\widetilde{b}_a,\, 1\leqslant a\leqslant\sigma\}} = \sum_{w\in W[r]} \det \begin{pmatrix} H_{\alpha,b,w} \\ D \end{pmatrix}. \tag{4}$$

Since by (1) the left part of (4) is a nonzero element of $\overline{\mathbb{F}_q}$, at least one of the determinants in the right part of (4) is nonzero. This implies immediately that the family $\mathcal{F}$ satisfies property $\mathcal{P}_{n,r}(\mathbb{F}_q, \overline{\mathbb{F}_q})$.

It remains to show the existence of $(b_1, \dots, b_\sigma)$ **and** $(r_1, \dots, r_\sigma)$ **satisfying equation (1).** Let $\Delta^{(0)} = \Delta$. We shall show by induction on j the existence of $r_j \in \{0, 1\}$ and $b_j \in P_j$ such that, if we define

$$\Delta^{(j)} = (D^{r_j}_{j,b_j} \dots D^{r_2}_{2,b_2} D^{r_1}_{1,b_1} \Delta)|_{\{(X_a,Y_a)=\widetilde{b}_a,\, 1\leqslant a\leqslant j\}},$$

the polynomial $\Delta^{(j)}$ in $\overline{\mathbb{F}_q}[X_{j+1}, Y_{j+1}, \dots, X_\sigma, Y_\sigma]$ is nonzero. This condition is obviously satisfied at the starting step (for $j = 0$). Assume that $b_1, \dots, b_j$ and $r_1, \dots, r_j$ have been built. First remark that $\Delta^{(j)}$ is homogeneous with respect to X_a, Y_a and that its degree $\deg_{X_a,Y_a} \Delta^{(j)}$ in X_a, Y_a is equal to $\deg_{X_a,Y_a} \Delta = d_a$ for every $j + 1 \leqslant a \leqslant \sigma$ (indeed differentiations and substitutions only occur on variables of index smaller than $j + 1$). Let $b \in P_{j+1}$ be such that b^2 does not divide $\Delta^{(j)}$: such an element exists because $d_{j+1} \leqslant (\nu - 1)\lambda < 2(q + 1)$ (since $\lambda \leqslant (2q+1)/(\nu-1)$). We set $b_{j+1} = b$ and take $b' \in \mathbb{F}_q[X_{j+1}, Y_{j+1}]$ linearly independent with b. Let

$$r_{j+1} = \begin{cases} 1 & \text{if } b \text{ divides } \Delta^{(j)} \\ 0 & \text{otherwise.} \end{cases}$$

Since $\Delta^{(j)}$ is homogeneous in X_{j+1}, Y_{j+1}, it can be uniquely written as

$$\Delta^{(j)} = (b')^{d_{j+1}-r_{j+1}} b^{r_{j+1}} \Phi + b^{r_{j+1}+1} \Psi$$

where $0 \neq \Phi \in \overline{\mathbb{F}_q}[X_{j+2}, Y_{j+2}, \dots, X_\sigma, Y_\sigma]$ and $\Psi \in \overline{\mathbb{F}_q}[X_{j+1}, Y_{j+1}, \dots, X_\sigma, Y_\sigma]$. Remark now that due to the definition of $\widetilde{b}$, r_{j+1} and $\Delta^{(j+1)}$, there exists $0 \neq \mu \in \overline{\mathbb{F}_q}$ such that $\Delta^{(j+1)} = \mu\Phi$. Hence $\Delta^{(j+1)} \neq 0$. $\square$

Theorem 3 *Let $\varepsilon > 0$ be a fixed real number. Let $0 \leqslant r \leqslant n$ be two integers and $q = p^{\nu_0} \geqslant \varepsilon n$. One can construct a family $\mathcal{F}$ satisfying property $\mathcal{P}_{n,r}(\mathbb{F}_q, \overline{\mathbb{F}_q})$ with size $|\mathcal{F}| = O(q^{2\lceil r/q\rceil}\tau(n, r)) = n^{O(1/\varepsilon)}$. The working time of the algorithm for computing $\mathcal{F}$ is polynomial in $n^{1/\varepsilon}$, p and ν_0.*

Proof. Similarly to the proof of Theorem 1 we can suppose without loss of generality that $q \leqslant \tau(n, r)$ and hence $\nu \geqslant 2$. When n large enough then $q^3 \geqslant \varepsilon^3 n^3 > \tau(n, r)$, thus one can suppose that $\nu \leqslant 3$. Therefore Let us suppose $q^3 > \tau(n, r)$. Of course $2q + 1 \geqslant \nu$ and one can apply lemma 7 to build a family $\mathcal{F}$ with property $\mathcal{P}_{n,s}(\mathbb{F}_q, \overline{\mathbb{F}_q})$. The size of this family is $((q + 1)(\lambda + 1))^\sigma \tau(n, r)$. As $\nu \in \{2, 3\}$ (when n large enough), $\lambda \leqslant 2q + 1$ and $\sigma \leqslant \lceil r/q\rceil$. Thus $|\mathcal{F}| = O(q^{2\lceil r/q\rceil}\tau(n, r))$. The time needed to build this family is as announced. $\square$

5 Existence of small transversal families over finite fields

A probabilistic argument shows that there exists a family of size $O(\tau(n,r))$ that has property $\mathcal{P}_{n,r}(\mathbb{F}_q)$, where the constant in the big O is independent of q. In the following we show a similar result for the stronger $\mathcal{P}_{n,r}(\mathbb{F}_q,\overline{\mathbb{F}_q})$ property.

Proposition 1 *There exists a family of size $O(n(n-r)r^2)$ that has property $\mathcal{P}_{n,r}(\mathbb{F}_q,\overline{\mathbb{F}_q})$, where the hidden constant is independent of q.*

Proof. Let X be the set of all $\mathbb{F}_q$-linear subspaces of dimension r of $\mathbb{F}_q^n$. An element $x \in X$ defines a $\overline{\mathbb{F}_q}$-linear subspace $\hat{x}$ of $\overline{\mathbb{F}_q}^n$. Let Y be the set of $\overline{\mathbb{F}_q}$-linear subspaces of dimension $n-r$ of $\overline{\mathbb{F}_q}^n$. For $y \in Y$, let us define $T_y = \{x \in X, \hat{x} \cap y = \{0\}\}$. Let $\mathcal{F} = \{T_y, y \in Y\}$. A subset $T \subseteq X$ is said to be transversal is it intersects all elements of $\mathcal{F}$. The transversal number of $(X,\mathcal{F})$ is the minimum cardinal of a transversal subset; it is written $\tau(\mathcal{F})$ – see chapter 10 of [6] about set systems and transversality. Of course the size of a minimal family with $\mathcal{P}_{n,r}(\mathbb{F}_q,\overline{\mathbb{F}_q})$ property is given by $\tau(\mathcal{F})$. We shall now upper bound on $\tau(\mathcal{F})$.

The number of linear subspaces of dimension r of $\mathbb{F}_q^n$ is

$$|X| = N_{n,r} = \prod_{i=0}^{r-1} \frac{q^n - q^i}{q^r - q^i} = \prod_{i=0}^{r-1} \frac{q^{n-i}-1}{q^{i+1}-1} \leqslant \prod_{i=1}^{r} \frac{q^{n-r+i}}{q^i - 1} = q^{r(n-r)} \prod_{i=1}^{r} \frac{1}{1-q^{-i}}.$$

Moreover, any $F \in \mathcal{F}$ satisfies

$$|F| \geqslant T_{n,r} = \prod_{i=0}^{r-1} \frac{q^n - q^{n-r+i}}{q^r - q^i} = q^{r(n-r)}.$$

Indeed, for all $\overline{\mathbb{F}_q}$-linear subspace y of dimension k of $\overline{\mathbb{F}_q}^n$, $y' = y \cap \mathbb{F}_q^n$ is a $\mathbb{F}_q$-linear subspace of dimension at most k of $\mathbb{F}_q^n$, and any $e \in \mathbb{F}_q^n \setminus y'$ is transversal to y.

Thus for any $F \in \mathcal{F}$

$$\frac{|F|}{|X|} \geqslant \frac{T_{n,r}}{N_{n,r}} \geqslant \prod_{i=1}^{r}(1-q^{-i}) \geqslant \prod_{i=1}^{\infty}(1-q^{-i}) \geqslant 2^{-2/(q-1)} =: \theta(q).$$

Given a family of polynomials $\{P_i(\bar{X}), i \in I\}$ in n variables over the field $\mathbb{F}$, we call a zero-pattern of this family an element of $\bar{s} \in \{0,\star\}^I$ such that there exists $\bar{x}_0 \in \mathbb{F}^n$ with $P_i(\bar{x}_0)$ of sign s_i – ie $P_i(\bar{x}_0) = 0$ iff $s_i = 0$.

For $x \in X$ let M_x be a $r \times n$ matrix whose lines are a basis of the linear subspace x (in the canonical basis). Let U be a $n \times r$ matrix filled with indeterminates. By lemma 2, the size of $\mathcal{F}$ is bounded by the number of zero-patterns over the field $\overline{\mathbb{F}_q}^n$ of the set of polynomials $\{\det(M_x U),\ x \in X\}$. This family is made of $|X|$ polynomials of degree r in the nr variables of U. Applying the bounds given in [7] we obtain

$$|\mathcal{F}| \leqslant \left(\frac{e \cdot |X|}{n}\right)^{rn}.$$

Thus $\log|\mathcal{F}| = O(rn\log|X|) = n(n-r)r^2O(\log q)$.

Using a probabilistic argument, we shall now upper bound $\tau(\mathcal{F})$. Let $X_1,\dots,X_t$ be independent random variables with uniform distribution over X. The probability that $F \in \mathcal{F}$ is not covered by $\{X_1,\dots,X_t\}$ is upper bounded by $(1-\theta(q))^t$. By the union bound, the family $\{X_1,\dots,X_t\}$ is not transversal with probability bounded above by $|\mathcal{F}|(1-\theta(q))^t$. Therefore, any t such that $|\mathcal{F}|(1-\theta(q))^t < 1$ yields the existence of a transversal family of size t. Thus

$$\tau(\mathcal{F}) \leqslant \left\lceil \frac{\log|\mathcal{F}|}{-\log(1-\theta(q))} \right\rceil = O(n(n-r)r^2)$$

(where the hidden constant is independent of q), ie that there exists a family of size $O(n(n-r)r^2)$ with property $\mathcal{P}_{n,r}(\mathbb{F}_q,\overline{\mathbb{F}_q})$. □

An intriguing question is the optimal size of families with $\mathcal{P}_{n,r}(\mathbb{F}_q,\overline{\mathbb{F}_q})$ or even $\mathcal{P}_{n,r}(\mathbb{F}_q)$ property. Of course a family with $\mathcal{P}_{n,r}(\mathbb{F}_q,\overline{\mathbb{F}_q})$ property has the property $\mathcal{P}_{n,r}(\overline{\mathbb{F}_q})$ so its size is $\Omega(\tau(n,r))$. On the other hand, we are not aware of any nontrivial lower bound on the size of a family with $\mathcal{P}_{n,r}(\mathbb{F}_q)$ property.. Note however that the size of a family with $\mathcal{P}_{n,r}(\mathbb{F}_q)$ property can be smaller than $\tau(n,r)$ – the optimal size on algebraically closed fields – as shows the following.

Remark 2 *Over any finite field k, the optimal size of a family with property $\mathcal{P}_{4,2}(k)$ is* 4.

Proof. Let k be a finite field and let $P(X) = X^2+\alpha X+\beta$ be an irreducible polynomial of degree 2 over k – such a polynomial exists [5]. Consider the following family $\mathcal{F}$ of 4×2 matrices over k

$$\begin{pmatrix} I \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ I \end{pmatrix}, \begin{pmatrix} I \\ I \end{pmatrix}, \begin{pmatrix} T \\ I \end{pmatrix}$$

where I is the 2×2 identity matrix and $T = \left(\begin{smallmatrix} \alpha & \beta \\ -1 & 0 \end{smallmatrix}\right)$. This family has property $\mathcal{P}_{4,2}(k)$. Indeed, any 2-dimensional subspace of k^4 which has a non-trivial intersection with the first two elements of $\mathcal{F}$ must be of the form $V = \mathrm{Span}\{\binom{x}{0},\binom{0}{y}\}$. A subspace of this form can intersect non-trivially at most one of the remaining two elements of $\mathcal{F}$. More precisely, if x and y are colinear then the intersection with the last subspace is $\{0\}$, and if x and y are not colinear then the intersection with the third subspace is $\{0\}$.

Now let K be an arbitrary field. Let us show that no family of three elements has the property $\mathcal{P}_{4,2}(K)$. Indeed let us suppose that $\mathcal{F} = \{V_1,V_2,V_3\}$ has this property. Let us first assume that $V_1\cap V_2 \neq \{0\}$. Let $a \in V_1\cap V_2$ with $a\neq 0$ and then let $b\in V_3$ with $b\notin \mathrm{Span}\{a\}$. No element of $\mathcal{F}$ is transversal to $\mathrm{Span}\{a,b\}$. Thus we can assume that $V_i\cap V_j = \{0\}$ for $i\neq j$. Let $v_3 \in V_3\setminus\{0\}$. It can be written $v_3 = v_1+v_2$ with $v_i\in V_i$ for $i\in\{1,2\}$. Of course $V = \mathrm{Span}\{v_1,v_2\}$ is of dimension 2 ($v_i\neq 0$ because $V_i\cap V_3 = \{0\}$). Once again no element of $\mathcal{F}$ is transversal to V. □

Although they do exist, we don't know how to build in polynomial time families of polynomial size with property $\mathcal{P}_{n,r}(K)$ for a finite field K. In what follows we slightly improve the trivial bound $O(n^2)$ in the case $r=2$ on an arbitrary field (e.g. $\mathbb{F}_2$).

Proposition 2 *A family $\mathcal{F}_n$ with the following properties can be built in polynomial time:*

- *the elements of $\mathcal{F}_n$ are $\{0,1\}$-matrices;*
- *the size of $\mathcal{F}_n$ is $O(n^{\log_2 3})$;*
- *the family $\mathcal{F}_n$ has property $\mathcal{P}_{n,2}(K)$ for any field K.*

Proof. By Lemma 4, it is enough to build this family for n of the form 2^m. The process is recursive. For the base case $n = 4$, let $\mathcal{F}_4$ be the family of the $\binom{4}{2}$ full rank 4×2 matrices with coefficients in $\{0,1\}$ built by putting $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ on a principal minor and 0 elsewhere. We now build $\mathcal{F}_{2^{m+1}}$ from $\mathcal{F}_{2^m}$. If u is a vector of K of size 2^m (i.e. $u \in K^{2^m}$), we denote by $u0$ the vector of size 2^{m+1} whose 2^m first components are those of u, and whose 2^m last components are 0. Similarly for $0u$. More generally, uv is the concatenation of u and v. We will also write them in column as in ${}^t(uv)$. Let e_i denote the i-th vector of the canonical basis of K^{2^m}. Then $\mathcal{F}_{2^{m+1}}$ is the family of $2^{m+1} \times 2$ matrices with coefficients in $\{0,1\}$ defined by

$$\mathcal{F}_{2^{m+1}} = \{\left(\begin{smallmatrix}u0\\v0\end{smallmatrix}\right)/\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right) \in \mathcal{F}_{2^m}\} \cup \{\left(\begin{smallmatrix}0u\\0v\end{smallmatrix}\right)/\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right) \in \mathcal{F}_{2^m}\} \cup$$

$$\{\left(\begin{smallmatrix}uu\\vv\end{smallmatrix}\right)/\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right) \in \mathcal{F}_{2^m}\} \cup \{\left(\begin{smallmatrix}e_i0\\0e_i\end{smallmatrix}\right)/1 \le i \le 2^m\}.$$

We now prove that this family is transversal. Let aa' and bb' be two independent vectors of $K^{2^{m+1}}$, where $a, a', b, b' \in K^{2^m}$. If $\mathrm{rank}(a,b) = 2$ there exists $\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right) \in \mathcal{F}_{2^m}$ such that $\left(\begin{smallmatrix}a\\b\end{smallmatrix}\right)({}^tu|{}^tv)$ is of rank 2. Then $\left(\begin{smallmatrix}aa'\\bb'\end{smallmatrix}\right)({}^t(u0)|{}^t(v0)) = \left(\begin{smallmatrix}a\\b\end{smallmatrix}\right)({}^tu|{}^tv)$ is also of rank 2, hence $\left(\begin{smallmatrix}u0\\v0\end{smallmatrix}\right) \in \mathcal{F}_{2^{m+1}}$ is suitable for $\left(\begin{smallmatrix}aa'\\bb'\end{smallmatrix}\right)$. The case where $\mathrm{rank}(a',b') = 2$ is dealt with identically thanks to the matrix $\left(\begin{smallmatrix}0u\\0v\end{smallmatrix}\right) \in \mathcal{F}_{2^{m+1}}$. At last, the case where $\mathrm{rank}(a+a', b+b') = 2$ is dealt with a matrix of the form $\left(\begin{smallmatrix}uu\\vv\end{smallmatrix}\right)$.

It remains the case where $\mathrm{rank}(a,a') = \mathrm{rank}(b,b') = \mathrm{rank}(a+a', b+b') = 1$. We can furthermore suppose that one of the a, a', b, b' is zero, say $a' = 0$: indeed, the subspace spanned by aa' and bb' is equal to the subspace spanned by $(a - \alpha b)0$ and bb' provided that $a' = \alpha b'$. Performing a second linear combination, we can in fact assume that the matrix is of the form $\left(\begin{smallmatrix}a0\\0b'\end{smallmatrix}\right)$. As $\mathrm{rank}(a+a', b+b') = 1$, this means that $a \neq 0$ and $b' = \mu a$ with $\mu \neq 0$. Then $\left(\begin{smallmatrix}e_i0\\0e_i\end{smallmatrix}\right) \in \mathcal{F}_{2^{m+1}}$ is suitable as soon as $e_i.a \neq 0$.

Finally, we have to prove the claim on the size u_m of the family $\mathcal{F}_{2^m}$. It satisfies the relation $u_{m+1} = 3u_m + 2^m$, hence $u_m = O(3^m)$. It follows that the size of $\mathcal{F}_n$ is $O(n^{\log_2 3})$, that is $O(n^{1.59})$. $\square$

Many *existence vs. construction* open problems are raised in [7]. It would be interesting to relate one of these problems to the construction of transversal families over finite fields.

References

[1] Jin-yi Cai, Ashish V. Naik, and D. Sivakumar. On the existence of hard sparse sets under weak reductions. In *Proc. STACS'96*, volume 1046 of *Lecture Notes in Computer Science*, pages 307–318. Springer-Verlag, 1996.

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

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

[4] Alexander Chistov, Hervé Fournier, Leonid Gurvits, and Pascal Koiran. Vandermonde matrices, NP-completeness and transversal subspaces. *Foundations of Computational Mathematics*, 3(4):421–427, 2003.

[5] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 2nd edition, 1997.

[6] Jiří Matoušek. *Lectures on Discrete Geometry*, volume 212 of *Graduate Texts in Mathematics*. Springer, 2002.

[7] Lajos Rónyai, László Babai, and Murali K. Ganapathy. On the number of zero-patterns of a sequence of polynomials. *Journal of the American Mathematical Society*, 14(3):717–735, 2001.

[8] Marie-Françoise Roy and Nicolai Vorobjov. The complexification and degree of a semi-algebraic set. *Mathematische Zeitschrift*, 239(1):131–142, 2002.

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