On Proper Secrets, (t, k)-Bases and Linear Codes

Tamir Tassa * Jorge L. Villar †

Abstract

This paper contains three parts where each part triggered and motivated the subsequent one. In the first part (*Proper Secrets*) we study the Shamir's "k-out-of-n" threshold secret sharing scheme. In that scheme, the dealer generates a random polynomial of degree $k-1$ whose free coefficient is the secret and the private shares are point values of that polynomial. We show that the secret may, equivalently, be chosen as any other point value of the polynomial (including the point at infinity), but, on the other hand, setting the secret to be any other linear combination of the polynomial coefficients may result in an imperfect scheme. In the second part (*(t, k)-Bases*) we define, for every pair of integers t and k such that $1 \leq t \leq k-1$, the concepts of (t, k)-spanning sets, (t, k)-independent sets and (t, k)-bases as generalizations of the usual concepts of spanning sets, independent sets and bases in a finite-dimensional vector space. We study the relations between those notions and derive upper and lower bounds for the size of such sets. In the third part (*Linear Codes*) we show the relations between those notions and linear codes. Our main notion of a (t, k)-base bridges between two well-known structures: $(1, k)$-bases are just projective geometries, while $(k-1, k)$-bases correspond to maximal MDS-codes. We show how the properties of (t, k)-independence and (t, k)-spanning relate to the notions of minimum distance and covering radius of linear codes and how our results regarding the size of such sets relate to known bounds in coding theory. We conclude by comparing between the notions that we introduce here and some well known objects from projective geometry.

Keywords. Threshold Secret Sharing, Discrete Linear Algebra, Linear Independence, Spanning Sets, Linear Codes, Projective Geometry.

1 Introduction

In his seminal work on secret sharing, [28], Shamir introduced the concept of threshold secret sharing. Given a set $\mathcal{U} = \{u_1, \ldots, u_n\}$ of n participants, he showed how to share a secret S among those participants by giving each one of them a share, such that two properties hold:

- Correctness. Any subset of k shares may be used to recover the secret unequivocally.
- Perfect Security. Any subset of $k-1$ shares reveals no information about the secret.

In his scheme, the secret and the shares all take values in a finite field $\mathbb{F}_q$ whose size is at least $n+1$. The dealer generates a random polynomial of degree $k-1$ over that field, $P(x) =$

*Department of Mathematics and Computer Science, The Open University, Ra'anana, Israel. tamirta@openu.ac.il

†Department of Applied Mathematics IV, Universitat Politècnica de Catalunya, Barcelona, Spain. jvillar@ma4.upc.edu

$\sum_{i=0}^{k-1} a_i x^i$, so that the secret S is the free coefficient of that polynomial, $S = a_0$. Then, the dealer identifies each participant with a unique public identity in the field, $u_i \leftarrow x_i \in \mathbb{F}_q \setminus \{0\}$, $1 \leq i \leq n$, and gives that participant the private share $P(x_i)$. Qualified subsets, namely, subsets of size at least k, may recover the entire polynomial by means of interpolation and then deduce the value of the secret, $S = a_0 = P(0)$. Non-qualified subsets, on the other hand, may reveal no information about the secret from the shares that they hold.

It is clear that any value of the form $P(x_0)$ is also a suitable choice for the secret, provided that there is no participant in $\mathcal{U}$ whose identity equals x_0. Such a modification of the Shamir's scheme is obviously also correct and perfect. In addition to that, also the value of a_{k-1} may serve as the secret [19, Theorem 2.1].

The coefficient a_{k-1} may be viewed as the value of P "at infinity", since the vector $(0, \ldots, 0, 1)$, that does not equal $(1, x, x^2, \ldots, x^{k-1})$ for any $x \in \mathbb{F}_q$, is the "point at infinity" in the corresponding projective geometry $\mathrm{PG}(k-1, q)$.[1] (Another way of associating the leading coefficient to the value of the polynomial at infinity is by looking at the polynomial as if it was a polynomial over the reals and then taking the limit $\lim_{x\to\infty} P(x)/x^{k-1} = a_{k-1}$.) Hence, any (generalized) point value of the polynomial P is a suitable choice of the secret in Shamir's scheme.

All those point values are linear combinations of the coefficients of the secret generating polynomial P. Any qualified subset may recover all of the polynomial coefficients, and, consequently, may also compute all linear combinations of those coefficients. Therefore, a natural question arises: can any linear combination of the polynomial coefficients serve as the secret? In Section 2 we prove that the answer to this question is negative.

The discussion in Section 2 motivates the one that follows in Section 3. The section begins with definitions of novel notions in discrete linear algebra. For every pair of integers t and k such that $1 \leq t \leq k-1$, we define a set of vectors in a k-dimensional vector space over a finite field to be (t, k)-spanning if any vector in the space is a linear combination of at most t vectors from that set. A minimal (t, k)-spanning set is a (t, k)-spanning set that has no proper subset that is still (t, k)-spanning. We proceed to define the related notion of a (t, k)-independent set: A set of vectors in a k-dimensional vector space is (t, k)-independent if no vector in that set is a linear combination of up to t other vectors from that set. A maximal (t, k)-independent set is a (t, k)-independent set that has no proper superset having the same property. Such a set is called a (t, k)-base.[2] Those notions generalize the usual concepts of spanning sets, independent sets and bases in a finite-dimensional vector space. We discuss the relations between those notions, exemplify them, and derive upper and lower bounds for the size of (t, k)-bases and minimal (t, k)-spanning sets.

In Section 3.2 we discuss the relations between our (t, k)-notions and linear codes. The notion of (t, k)-bases coincides with projective geometries when $t = 1$, while, on the other hand, it corresponds to Maximum Distance Separable (MDS) codes when $t = k - 1$. Hence, the notion of (t, k)-bases, $1 \leq t \leq k - 1$, "interpolates" between the concepts of projective geometries and MDS codes, that, to the best of our knowledge, were previously unrelated. We then show how every spanning set of n vectors $V \subset \mathbb{F}_q^k$ defines a $[n, k]$ code $\mathcal{C}_V$ and a corresponding dual $[n, n-k]$ code $\mathcal{C}_V^*$. Namely, the vectors are just the rows of a generating matrix for $\mathcal{C}_V$ and hence they are the rows of a parity check matrix for $\mathcal{C}_V^*$. Then, the (t, k)-independence of V is related to the minimum distance of $\mathcal{C}_V^*$, while its (t, k)-spanning property is related to the covering radius of $\mathcal{C}_V^*$. Moreover, the bounds that we derived in Section 3 on the size of (t, k)-independent and (t, k)-spanning sets are related to the well known Hamming

[1] The projective geometry $\mathrm{PG}(d, q)$ is the collection of all $\sum_{i=0}^{d} q^i$ one-dimensional subspaces of $\mathbb{F}_q^{d+1}$.

[2] After the completion of this work, the authors were notified that Y. Dodis defined the notion of (t, k)-spanning sets in his master thesis [10]. In addition, we found out that Damelin et. al. introduced recently the notion of (t, k)-independence in [9, 8]. We describe herein their results.

and Gilbert-Varshamov bounds for linear codes.

In Section 4 we discuss the relation of our notions of (t,k)-independence and (t,k)-bases to well-known structures in projective geometry. Finally we conclude in Section 5, where we propose some interesting open problems.

2 Proper secrets in the Shamir's secret sharing scheme

In this section we address the question that we posed in the introduction about the Shamir's secret sharing scheme. Namely, can the secret in that scheme be any linear combination of the coefficients of the secret generating polynomial P, other than the linear combinations that correspond to (generalized) point values of the polynomial?

A counterexample immediately emerges. Consider the case $k = 3$ and assume that $\mathrm{char}(\mathbb{F}_q) \geq 3$. In that case $P(x) = a_0 + a_1 x + a_2 x^2$. $S = a_0 = P(0)$ and $S = a_2 = P(\infty)$ are both proper choices of the secret. However, $S = a_1$ is an improper choice, since then any non-qualified subset $\{u_i, u_j\}$ with identities x_i, x_j that satisfy $x_i = -x_j \neq 0$ will be able to recover the secret. Indeed, the share of u_i in this case is $a_0 + a_1 x_i + a_2 x_i^2$, while the share of u_j is $a_0 - a_1 x_i + a_2 x_i^2$. The difference of these two shares equals $2a_1 x_i$, and it discloses the value of the secret $S = a_1$. A similar failure occurs for any value of k if we select the secret to equal one of the intermediate coefficients of the polynomial (namely, one of the coefficients a_i for $1 \leq i \leq k-2$).

It should be noted that even if we select the secret to equal one of the intermediate coefficients of the polynomial, the resulting scheme might still be perfect, for some selections of the participant identities in the field. For instance, in the above example of $k = 3$ and $S = a_1$, if the set of participant identities does not include pairs x_i and x_j such that $x_i = -x_j \neq 0$, then everything works just fine. Other choices of linear combinations to represent the secret may result in other conditions on the participant identities that might be significantly harder to verify. In view of this, we introduce the concept of *proper secrets* in Shamir's scheme.

Definition 2.1 *Let $\mathbb{F}_q$ be the underlying field in Shamir's secret sharing scheme, and let $P(x) = \sum_{i=0}^{k-1} a_i x^i$ be the secret generating polynomial. Then a linear combination of the coefficients of the polynomial $P(x)$ is a proper choice for the secret if there exists $x_0 \in \mathbb{F}_q$ such that the resulting scheme is perfect for any choice of participant identities in $\mathbb{F}_q$.*

In view of the above, all polynomial point values are proper secrets. Our main result here is the following theorem.

Theorem 2.1 *All point values of the polynomial $P(x)$, namely,*

$$P(x_0) = \sum_{i=0}^{k-1} a_i x_0^i \quad x_0 \in \mathbb{F}_q, \quad \textit{and} \quad P(\infty) := a_{k-1}\,, \tag{1}$$

are proper secrets in Shamir's scheme. If

$$q \geq (k-1)^2 \quad \textit{and} \quad k \leq \mathit{char}(\mathbb{F}_q)\,, \tag{2}$$

then any linear combination of the coefficients of $P(x)$ that is not a point value of $cP(x)$ for some $c \neq 0$ is improper.

We begin with some definitions of basic terminology.

Definition 2.2 *A vector $\mathbf{v} \in \mathbb{F}_q^k$, $k \geq 2$, is called a regular Vandermonde vector if it takes the form $\mathbf{v} = \mathbf{v}(x) := (1, x, x^2, \ldots, x^{k-1})$ for some $x \in \mathbb{F}_q$. A vector $\mathbf{v} \in \mathbb{F}_q^k$ is called a*

Vandermonde vector if it is a regular Vandermonde vector or if $\mathbf{v} = (0, \ldots, 0, 1)$. *The set of all* $(q+1)*(q-1)$ *Vandermonde vectors in* $\mathbb{F}_q^k$ *and their nontrivial scalar multiples is denoted by* $\boldsymbol{V}_k$ *(or simply* $\boldsymbol{V}$*).*

The set $\mathbf{V}$, when interpreted as a set of points in the projective geometry $\mathrm{PG}(k-1, q)$, is called a normal rational curve. We are now ready to state the key ingredient in the proof of Theorem 2.1.

Proposition 2.2 *Let* $\mathbb{F}_q$ *be a field of cardinality at least* k. *Then:*

1. *All nonzero vectors in* $\mathbb{F}_q^k \setminus \boldsymbol{V}$ *may be expressed as a linear combination of* $k-1$ *regular Vandermonde vectors, provided that (2) holds.*
2. *For* $k \geq 3$, *there exist nonzero vectors in* $\mathbb{F}_q^k \setminus \boldsymbol{V}$ *that cannot be expressed as a linear combination of* $k-2$ *Vandermonde vectors.*
3. *No vector in* $\boldsymbol{V}$ *may be expressed as a linear combination of* $k-1$ *other Vandermonde vectors.*

The proof of Proposition 2.2 is given in Section 2.1. Note that the lower bound on the size of the field in Proposition 2.2 is implied by the lower bound on the field size in Shamir's scheme. Indeed, as Shamir's scheme requires that $q \geq n+1$ and $n \geq k$, fields that are suitable for the secret sharing scheme always satisfy the condition in Proposition 2.2.

Proof of Theorem 2.1. First, we prove that all point values of P, (1), are proper secrets. This claim is obviously true for regular point values, $P(x_0)$, for some $x_0 \in \mathbb{F}_q$. As for the point value $P(\infty) = a_{k-1}$, we include herein, for the sake of completeness, the proof of [19, Theorem 2.1]. Let $\mathcal{V} \subset \mathcal{U}$ be an arbitrary maximal non-qualified subset. We aim at showing that the information that the members of $\mathcal{V}$ hold does not reveal any information about the secret a_{k-1}. To show that, we need to prove that the $k-1$ linear equalities in the unknowns $(a_0, \ldots, a_{k-1})$ that are implied by the shares possessed by the members of $\mathcal{V}$ do not pose any restriction on the value of a_{k-1}. This is equivalent to the statement that the vector $(0, \ldots, 0, 1) \in \mathbb{F}_q^k$ is not spanned by the rows of the matrix

$$\begin{pmatrix} 1 & x_1 & \cdots & x_1^{k-2} & x_1^{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{k-1} & \cdots & x_{k-1}^{k-2} & x_{k-1}^{k-1} \end{pmatrix},$$

where $x_1, \ldots, x_{k-1}$ are the distinct identities of the participants in $\mathcal{V}$. This is indeed the case since

$$\det \begin{pmatrix} 1 & x_1 & \cdots & x_1^{k-2} & x_1^{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{k-1} & \cdots & x_{k-1}^{k-2} & x_{k-1}^{k-1} \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} = \prod_{1 \leq i < j \leq k-1} (x_j - x_i) \neq 0 \ .$$

After establishing the positive part of the theorem, we turn to prove its negative part. Given a linear combination of the coefficients of $P(x) = \sum_{i=0}^{k-1} a_i x^i$, say $\sum_{i=0}^{k-1} v_i a_i$, we refer to the vector $(v_0, \ldots, v_{k-1})$ as the vector of the linear combination. Each point value of the polynomial $P(x) = \sum_{i=0}^{k-1} a_i x^i$ is a linear combination of $(a_0, \ldots, a_{k-1})$ where the corresponding vector is a Vandermonde vector. More specifically, the point value $P(x_0)$ is a linear combination with the vector $(1, x_0, x_0^2, \ldots, x_0^{k-1})$ while the point value $P(\infty) := a_{k-1}$ is a linear combination with the vector $(0, \ldots, 0, 1)$. In view of the above, all of those point values, that are linear combinations of the coefficients with a Vandermonde vector, are proper values for the secret. All linear combinations of the polynomial coefficients that are not point values of

$cP(x)$ for some $c \neq 0$ correspond to nonzero vectors in $\mathbb{F}_q^k \setminus \mathbf{V}$. In view of Proposition 2.2, such vectors may be expressed as linear combinations of $k-1$ regular Vandermonde vectors, say $\mathbf{v}(x_1), \ldots, \mathbf{v}(x_{k-1})$. Hence, if $\mathcal{U}$ includes participants with identities $x_1, \ldots, x_{k-1}$, their coalition, whose size is less than k, may recover such a linear combination. Namely, such secrets that correspond to linear combinations of the polynomial coefficients whose vector is not a Vandermonde vector (or a nonzero multiple of such a vector) are improper. □

Before moving on to the main part of proving Proposition 2.2, we note in passing that while the original Shamir scheme imposes the following lower bound on the size of the field, $q \geq n+1$, the modified Shamir scheme with the secret being the most significant polynomial coefficient, $S = a_{k-1}$, relaxes that demand to $q \geq n$. The reason is that with this choice of the secret, we identify the dealer with the point at infinity, which is not a field element (while in the original Shamir scheme the dealer was identified with the point $x_0 = 0$); that way, we "free" all of the field elements to be suitable candidates for participant identities.

2.1 Proof of Proposition 2.2

The third part of the proposition is obvious since any selection of k Vandermonde vectors is linearly independent (provided that $q \geq k$). The second part is also straightforward: All vectors of the form $(0, \ldots, 0, 1, v_k)$ are in $\mathbb{F}_q^k \setminus \mathbf{V}$ and they cannot be expressed as a linear combination of $k-2$ Vandermonde vectors since then, by projecting such a linear dependence onto $\mathbb{F}_q^{k-2}$, we would get $k-2$ Vandermonde vectors in $\mathbb{F}_q^{k-2}$ that are linearly dependent.

Hence, we concentrate on the first part of the proposition, but only for $k \geq 3$ (since $\mathbb{F}_q^2 \setminus \mathbf{V} = \{\mathbf{0}\}$). We prove that if $\mathbf{v} = (a_0, a_1, \ldots, a_{k-1}) \in \mathbb{F}_q^k \setminus \mathbf{V}$ is nonzero then the polynomial

$$G_{\mathbf{V}}(x_1, \ldots, x_{k-1}) := \begin{vmatrix} a_0 & a_1 & \cdots & a_{k-2} & a_{k-1} \\ 1 & x_1 & \cdots & x_1^{k-2} & x_1^{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{k-1} & \cdots & x_{k-1}^{k-2} & x_{k-1}^{k-1} \end{vmatrix} \tag{3}$$

has a zero $(x_1, \ldots, x_{k-1}) \in \mathbb{F}_q^{k-1}$ for which $x_i \neq x_j$ for all $1 \leq i < j \leq k-1$. This will imply that the rows of the matrix in (3) are linearly dependent for that choice of $x_1, \ldots, x_{k-1}$, whence the vector $\mathbf{v}$ is a linear combination of the corresponding $k-1$ regular Vandermonde vectors.

Expanding the determinant in (3) by the first row, we get that

$$G_{\mathbf{V}}(x_1, \ldots, x_{k-1}) = \sum_{j=0}^{k-1} (-1)^j a_j \cdot V_j(x_1, ..., x_{k-1}) \tag{4}$$

where

$$V_j(x_1, ..., x_{k-1}) = \begin{vmatrix} 1 & x_1 & \cdots & x_1^{j-1} & x_1^{j+1} & \cdots & x_1^{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ 1 & x_{k-1} & \cdots & x_{k-1}^{j-1} & x_{k-1}^{j+1} & \cdots & x_{k-1}^{k-1} \end{vmatrix}. \tag{5}$$

In order to evaluate the determinants in (5) we review the basic definitions and results regarding generalized Vandermonde determinants. Given a monotonic non-decreasing sequence of integer offsets, $d_0 \leq \cdots \leq d_{n-1}$, the corresponding generalized Vandermonde determinant is

$$V_{(d_0,\ldots,d_{n-1})}(x_1, \ldots, x_n) = \begin{vmatrix} x_1^{d_0} & x_1^{d_1+1} & \cdots & x_1^{d_{n-2}+n-2} & x_1^{d_{n-1}+n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_n^{d_0} & x_n^{d_1+1} & \cdots & x_n^{d_{n-2}+n-2} & x_n^{d_{n-1}+n-1} \end{vmatrix}.$$

It is given by

$$V_{(d_0,\ldots,d_{n-1})}(x_1,\ldots,x_n) = S_{(d_0,\ldots,d_{n-1})}(x_1,\ldots,x_n)\cdot V_{(0,\ldots,0)}(x_1,\ldots,x_n) \tag{6}$$

where

$$V_{(0,\ldots,0)}(x_1,\ldots,x_n) = \prod_{1\le i<j\le n}(x_j - x_i) \tag{7}$$

is the regular Vandermonde determinant and $S_{(d_0,\ldots,d_{n-1})}(x_1,\ldots,x_n)$ is the Schur polynomial which is symmetric and homogenous of degree $d = d_0 + \cdots + d_{n-1}$ [20]. The determinant in (5) is the general Vandermonde determinant that corresponds to the offset vector $\mathbf{d}_j := (0,\ldots,0,1,\ldots,1)$ that has $k-1$ components and j leading zeros. It may be shown that the Schur polynomial in this case is given by

$$S_{\mathbf{d}_j}(x_1,\ldots,x_{k-1}) = \sum_{1\le i_1<i_2<\cdots<i_{k-1-j}\le k-1} x_{i_1}\cdot x_{i_2}\cdots x_{i_{k-1-j}}\,. \tag{8}$$

Namely, $S_{(0,\ldots,0,1)} = \sum_{1\le\ell\le k-1} x_\ell$, $S_{(0,\ldots,0,1,1)} = \sum_{1\le\ell<m\le k-1} x_\ell x_m$, and so forth up to $S_{(1,\ldots,1)} = \prod_{1\le\ell\le k-1} x_\ell$. It should be noted that $S_{(0,\ldots,0,0)} = 1$ (and not zero, as given by the right hand side of (8) in the case $j = k-1$).

Combining (4) through (8) we infer that

$$\frac{G_{\mathbf{v}}(x_1,\ldots,x_{k-1})}{\prod_{1\le i<j\le k-1}(x_j-x_i)} = \sum_{j=0}^{k-1}(-1)^j a_j\cdot\left\{\sum_{1\le i_1<i_2<\cdots<i_{k-1-j}\le k-1} x_{i_1}\cdot x_{i_2}\cdots x_{i_{k-1-j}}\right\}. \tag{9}$$

Denoting the polynomial on the right hand side of (9) by $H(x_1,\ldots,x_{k-1})$, we have

$$\begin{aligned} H(x_1,\ldots,x_{k-1}) \;=\; & a_0\cdot x_1x_2\cdots x_{k-1} \\ & -a_1\cdot\textstyle\sum_{1\le i\le k-1}\frac{x_1x_2\cdots x_{k-1}}{x_i} \\ & \pm\cdots \\ & +(-1)^{k-2}a_{k-2}\cdot(x_1+\cdots+x_{k-1}) \\ & +(-1)^{k-1}a_{k-1}\,. \end{aligned} \tag{10}$$

We proceed to prove that $H(x_1,\ldots,x_{k-1})$ has a zero $(x_1,\ldots,x_{k-1})\in\mathbb{F}_q^{k-1}$ for which $x_i\neq x_j$ for all $1\le i<j\le k-1$.

Assume that the first component of the vector $\mathbf{v} = (a_0,\ldots,a_{k-1})$ that is nonzero is a_ℓ, where $0\le\ell\le k-2$ (note that $\ell < k-1$ since otherwise the vector $\mathbf{v}$ would be a multiple of a Vandermonde vector). Then $H(x_1,\ldots,x_{k-1})$ is of degree $k-1-\ell$. Let $b_1,\ldots,b_{k-2}\in\mathbb{F}_q$ be any selection of $k-2$ distinct field elements, and consider the bivariate polynomial $\hat{H}(y,z) := H(y+b_1,\ldots,y+b_{k-2},z)$. Then, in view of (10) and the above discussion, $\hat{H}(y,z) = z*P(y)+Q(y)$ where $P(y)$ is of degree $k-2-\ell$ and $Q(y)$ is of degree $k-1-\ell$ (unless $\ell=0$ in which case $Q(y)$ is of degree $k-2$).

The leading monomial in $P(y)$ is $\binom{k-2}{\ell}y^{k-2-\ell}$. The second part of assumption (2) implies that $\binom{k-2}{\ell}\neq 0$ in $\mathbb{F}_q$, whence P is not the zero polynomial. Therefore, it has at most $k-2$ zeros. Let y be any value in the field that is different from each of the roots of P. Then we set $z = -Q(y)\cdot P(y)^{-1}$. By doing so, we found a zero (y,z) for $\hat{H}$ which translates to a zero $(y+b_1,\ldots,y+b_{k-2},z)$ of H. However, while the first $k-2$ components of the latter zero are obviously distinct from each other, we still need to show that z may be selected so that it differs from all of those $k-2$ components. Hence, we need to guarantee that

$$-Q(y)\cdot P(y)^{-1}\notin\{y+b_1,\ldots,y+b_{k-2}\}\,.$$

Namely, y must not be a zero of any of the polynomial equations

$$Q(y) + P(y) \cdot (y + b_j) = 0\,, \quad 1 \le j \le k-2\,. \tag{11}$$

The polynomials on the left hand side of (11) are of degree $k-1-\ell$. Their leading monomial equals the leading monomial of $Q(y) + P(y) * y = \hat{H}(y, y) := H(y + b_1, \ldots, y + b_{k-2}, y)$, which is $\binom{k-1}{\ell} y^{k-1-\ell}$. As the second part of assumption (2) implies that $\binom{k-1}{\ell} \neq 0$ in $\mathbb{F}_q$, we infer that each of the $k-2$ polynomials on the left hand side of (11) is a nonzero polynomial of degree $k-1$ at the most. Consequently, each of those polynomials has at most $k-1$ roots. Therefore, there are at most $(k-2)*(k-1)$ bad selections of y that may lead to an inequality between z and one of the other components. Together with the previous $k-2$ bad selections of y (the roots of P), we conclude that there are at most $(k-2)*k$ bad selections of y. Any other selection of y guarantees that z is well defined and, in addition, that its value is different from from each of the values in $\{y + b_1, \ldots, y + b_{k-2}\}$. Therefore, since we assumed that the size of the field is at least $(k-2)*k+1$ (the first part of assumption (2)), we can find distinct $x_1, \ldots, x_{k-1}$ for which the determinant is zero. □

3 (t, k)-spanning sets, independent sets and bases

3.1 Definitions and basic results

The discussion in the previous section motivates the following definition.

Definition 3.1 *A family V of vectors in a k-dimensional vector space U is called a (t, k)-spanning set, if any vector $\mathbf{u} \in U$ is a linear combination of t vectors from V. A (t, k)-spanning set is called a minimal (t, k)-spanning set if it does not have a proper subset that is also a (t, k)-spanning set.*

These concepts generalize the usual concepts of a spanning set and a base. Any base of a k-dimensional vector space is a (minimal) (k, k)-spanning set.

Proposition 3.1 *Assume that $k \ge 3$, $q \ge \max\{k, (k-2)^2\}$, and $k - 1 \le char(\mathbb{F}_q)$. Then the collection V of $q+1$ Vandermonde vectors is a minimal $(k-1, k)$-spanning set in $\mathbb{F}_q^k$, but not $(k-2, k)$-spanning.*

Proof. We begin by showing that under the assumed conditions on the size of the field and its characteristics, the set V is $(k-1, k)$-spanning. Consider an arbitrary vector $\mathbf{u} = (u_1, \ldots, u_k) \in \mathbb{F}_q^k$. By the first part of Proposition 2.2, its restriction to $\mathbb{F}_q^{k-1}$, $\mathbf{u}' = (u_1, \ldots, u_{k-1})$, may be expressed as the linear combination of $k-2$ regular Vandermonde vectors in $\mathbb{F}_q^{k-1}$, say $\mathbf{v}'_i = (1, x_i, \ldots, x_i^{k-2})$, $1 \le i \le k-2$. Recall now that V includes, apart from the q regular Vandermonde vector, also the vector $\mathbf{v} = (0, \ldots, 0, 1)$. Hence, $\mathbf{u}$ may be expressed as the linear combination of the $k-1$ Vandermonde vectors $\{\mathbf{v}, \mathbf{v}_1, \ldots, \mathbf{v}_{k-2}\}$, where $\mathbf{v}_i = (1, x_i, \ldots, x_i^{k-1})$, $1 \le i \le k-2$.

Next, we observe that the set V is in fact a minimal $(k-1, k)$-spanning set. Indeed, since any selection of k vectors from V is independent, then all vectors in V are essential for this property.

Finally, the set V cannot be $(k-2, k)$-spanning, as implied by the second part of Proposition 2.2. □

It is tempting to call a minimal (t, k)-spanning set a (t, k)-base. However, the correct way to define a (t, k)-base starts from the opposite notion of (t, k)-independence.

Definition 3.2 *A family V of vectors in a k-dimensional vector space U is called (t,k)-independent, if none of its vectors is a linear combination of up to t other vectors from V. A (t,k)-independent set is called a maximal (t,k)-independent set, or a (t,k)-base, if it does not have a proper superset that is also (t,k)-independent.*

In view of the above, the collection V of $q+1$ Vandermonde vectors is a $(k-1,k)$-base whenever the conditions of Proposition 3.1 are met. We also note that any base of a k-dimensional space U, say $B=\{\mathbf{v}_1,\ldots,\mathbf{v}_k\}$, is a (k,k)-base. Indeed, no vector in B is a linear combination of up to k other vectors in B, while $B\cup\{\mathbf{u}\}$ is not (k,k)-independent for any $\mathbf{u}\in U\setminus B$ (since $\mathbf{u}$ is a linear combination of the k vectors in B).

Next, we study the relation between the notions of minimal (t,k)-spanning sets and maximal (t,k)-independent sets (namely, (t,k)-bases). To that end, we first introduce some notations that we shall use here and also in subsequent sections.

Definition 3.3 *Let $(k_1,\ldots,k_\ell)$ be a sequence of positive integers and let $k=\sum_{j=1}^{\ell}k_j$. Then the mapping $\varphi_j:\mathbb{F}_q^{k_j}\to\mathbb{F}_q^k$ is defined by $\varphi_j(w_1,\ldots,w_{k_j})=(0,\ldots,0,w_1,\ldots,w_{k_j},0,\ldots,0)$ where the number of leading zeros is $\sum_{i=1}^{j-1}k_i$ and the number of trailing zeros is $\sum_{i=j+1}^{\ell}k_i$. If, in addition, U_j is a family of vectors in $\mathbb{F}_q^{k_j}$, $1\leq j\leq\ell$, then $U_1\biguplus\cdots\biguplus U_\ell=\bigcup_{j=1}^{\ell}\varphi_j(U_j)$.*

Proposition 3.2 *All (t,k)-bases are minimal (t,k)-spanning sets. However, for all $2\leq t\leq k-1$ there exist minimal (t,k)-spanning sets that are not (t,k)-independent.*

Proof. Let V be a (t,k)-base in U. Namely, it is (t,k)-independent, while $V\cup\{\mathbf{u}\}$ is no longer (t,k)-independent for any vector $\mathbf{u}\in U\setminus V$. This implies that all vectors $\mathbf{u}\in U\setminus V$ may be represented as a linear combination of t vectors from V. Hence, V is a (t,k)-spanning set. It is also a minimal (t,k)-spanning set since if there was a vector $\mathbf{v}\in V$ such that $V\setminus\{\mathbf{v}\}$ was still a (t,k)-spanning set, then $\mathbf{v}$ would have been a linear combination of t other vectors in V, thus contradicting our assumption that V is (t,k)-independent. Hence, any (t,k)-base is also a minimal (t,k)-spanning set.

Next, we exemplify the existence of minimal (t,k)-spanning sets that are not (t,k)-independent for all $2\leq t\leq k-1$. Let V_t be the set of all Vandermonde vectors in $\mathbb{F}_q^t$, M_{k-t} be the set of all monic vectors in $\mathbb{F}_q^{k-t}$, and set $B=V_t\biguplus M_{k-t}=\varphi_1(V_t)\bigcup\varphi_2(M_{k-t})$. (Here, $k=t+(k-t)$, $\ell=2$, and then φ_1 and φ_2 are defined as in Definition 3.3.) We claim that B is a minimal (t,k)-spanning set that is not (t,k)-independent.

First, we show that it is (t,k)-spanning. Consider an arbitrary vector $\mathbf{w}=(w_1,\ldots,w_k)\in\mathbb{F}_q^k$. Define $\mathbf{v}=(w_1,\ldots,w_t,0,\ldots,0)$ and $\mathbf{u}=(0,\ldots,0,w_{t+1},\ldots,w_k)$. By Proposition 2.2, $\mathbf{v}$ is a linear combination of $t-1$ vectors from $\varphi_1(V_t)$ (when the underlying field size and characteristic are sufficiently large). On the other hand, $\mathbf{u}$ must be a linear combination of one vector from $\varphi_2(M_{k-t})$. Hence, $\mathbf{w}=\mathbf{v}+\mathbf{u}$ is a linear combination of at most t vectors from B.

Next, B is a minimal (t,k)-spanning set. Indeed, assume that we remove from B a vector $\mathbf{v}\in\varphi_1(V_t)$. Then the vector $\mathbf{v}+\mathbf{e}_{t+1}$ cannot be expressed as a linear combination of t vectors from $B\setminus\{\mathbf{v}\}$ since such a linear combination must involve at least t vectors from $\varphi_1(V_t)\setminus\{\mathbf{v}\}$ and at least one vector from $\varphi_2(M_{k-t})$. If, on the other hand, we remove from B a vector $\mathbf{v}\in\varphi_2(M_{k-t})$, then the vector $\mathbf{v}+\mathbf{e}_{t-1}$ cannot be expressed as a linear combination of t vectors from $B\setminus\{\mathbf{v}\}$. Indeed, such a linear combination must involve at least $t-1$ vectors from $\varphi_1(V_t)$ (as explained in the proof of the second part of Proposition 2.2) as well as at least two vectors from $\varphi_2(M_{k-t})$.

Finally, B is not (t,k)-independent since any $t+1$ vectors from $\varphi_1(V_t)$ are linearly dependent. □

Example. Consider the space $V = \mathbb{F}_2^3$. A $(2,3)$-spanning set in V must be of size at least four, since any set of three vectors in V can $(2,3)$-span at most seven vectors, while $|V| = 8$. Consider the two families

$$B_1 = \{(1,0,0),(0,1,0),(0,0,1),(1,1,1)\} \quad \text{and} \quad B_2 = \{(1,0,0),(0,1,0),(0,0,1),(1,1,0)\}\,.$$

It may be easily seen that both sets are $(2,3)$-spanning. However, while B_1 is also $(2,3)$-independent, the set B_2 is not (the fourth vector in it is the sum of the first two). □

Proposition 3.3 *A family V of vectors in a k-dimensional vector space U is a (t,k)-base if and only if it is (t,k)-independent and (t,k)-spanning.*

Proof. If V is a (t,k)-base, then, by definition, it is (t,k)-independent, and, in view of Proposition 3.2, it is (t,k)-spanning. On the other hand, assume that V is (t,k)-independent. Then if it is also (t,k)-spanning, it means that any vector from $U \setminus V$ is a linear combination of t vectors from V. This implies that V is a maximal (t,k)-independent set, namely, a (t,k)-base. □

The Vandermonde vectors in $\mathbb{F}_q^k$, V_k, constitute a (t,k)-base for the maximal value of $t = k-1$. It is not clear whether there are other $(k-1,k)$-bases that are not obtained from V_k through trivial independence-preserving linear transformations. The other extreme case, however, of $t = 1$, is much simpler. Here, there is only one $(1,k)$-base up to independence-preserving linear transformations.

Definition 3.4 *A vector $\mathbf{v} \in \mathbb{F}_q^k$ is called monic if it takes the form $\mathbf{v} = (0,\ldots,0,1,v_{i+1},\ldots,v_k)$ for some $1 \le i \le k$.*

Proposition 3.4 *The set of all monic vectors in $\mathbb{F}_q^k$ is a $(1,k)$-base.*

Proof. The family of all monic vectors is

$$V = \bigcup_{i=1}^{k} V_i\,, \quad \text{where} \quad V_i = \{(0,\ldots,0,1,v_{i+1},\ldots,v_k) : v_j \in \mathbb{F}_q,\ i+1 \le j \le k\}\,.$$

This is a $(1,k)$-independent set since no vector in V is proportional to another vector in V. It is also a maximal $(1,k)$-independent set since if $\mathbf{u} \in \mathbb{F}_q^k$ is a nonzero vector whose left-most nonzero component is $\mathbf{u}_i$, $1 \le i \le k$, it is proportional to some vector in V_i. Therefore, no vector may be added to V while still respecting its $(1,k)$-independence. We conclude that V is a $(1,k)$-base. □

3.2 (t,k)-bases and linear codes

(t,k)-independent and (t,k)-spanning sets are naturally related to linear codes. Let us recall some basic notions about linear codes.

A *code* $\mathcal{C}$ of length n over $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^n$. It is called a *linear code* of dimension $1 \le k < n$ if there exists a matrix $G \in M_{n\times k}(\mathbb{F}_q)$, of full rank k, such that the code coincides with $\{G\mathbf{u} : \mathbf{u} \in \mathbb{F}_q^k\}$. Namely, looking at all the vectors $\mathbf{u} \in \mathbb{F}_q^k$ as *messages*, the codewords are obtained from those messages by embedding them in $\mathbb{F}_q^n$ through the linear transformation that corresponds to the so-called *generating matrix* G. Such a code is referred to as a $[n,k]$ *code*.

Given two codewords $\mathbf{x}, \mathbf{y} \in \mathcal{C}$, their *Hamming distance*, $\mathrm{dist}(\mathbf{x}, \mathbf{y})$, is defined as the number of entries in which they differ. (The Hamming distance of a given codeword $\mathbf{x}$ to $\mathbf{0}$ is called the *Hamming weight* of $\mathbf{x}$.) The minimal distance of a code $\mathcal{C}$ is defined as

$$d = d(\mathcal{C}) = \min\{\mathrm{dist}(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \mathcal{C},\ \mathbf{x} \neq \mathbf{y}\}\,.$$

A $[n, k]$ code with minimal distance d is referred to as a $[n, k, d]$ code.

Given a linear $[n, k]$ code $\mathcal{C}$, the *dual code* $\mathcal{C}^*$ is the set of vectors in $\mathbb{F}_q^n$ that are orthogonal to all codewords in $\mathcal{C}$. Clearly, $\mathcal{C}^*$ is a $[n, n-k]$ code that coincides with $\{\mathbf{w} \in \mathbb{F}_q^n : \mathbf{w}^t G = \mathbf{0}\}$, where G is a generating matrix of $\mathcal{C}$. A generating matrix for $\mathcal{C}^*$ is called a *parity check matrix* for $\mathcal{C}$, and it plays a significant role in error correction.

Every (t, k)-base V defines a $[n, k]$ code $\mathcal{C}_V$, where $n = |V|$, in a natural way: The corresponding generating matrix G is the $n \times k$ matrix whose rows are the vectors of V. Since V spans all of $\mathbb{F}_q^k$, the matrix G has indeed a full rank k. We note that any set V of n vectors that spans all of $\mathbb{F}_q^k$ defines a $[n, k]$ code $\mathcal{C}_V$ in this manner (namely, V does not need to be (t, k)-independent). Note that G is also a parity check matrix for $\mathcal{C}_V^*$.

There is a well known relation between the rows of a parity check matrix H and the minimum distance d of a $[n, k, d]$ code. Namely $d \geq r$ if and only if any $r-1$ rows of H are linearly independent. This assertion may be restated in terms of (t, k)-independence.

Lemma 3.5 *Let $V \subseteq \mathbb{F}_q^k$ be a set of vectors that spans $\mathbb{F}_q^k$. Then, for any $1 \leq t \leq k-1$, V is a (t, k)-independent set if and only if $d(\mathcal{C}_V^*) \geq t+2$.*

Proof. The codewords in $\mathcal{C}_V^*$ may be viewed as vectors of coefficients of those linear combinations of the vectors in V that equal zero. Hence, the Hamming weight of a given codeword in $\mathcal{C}_V^*$ is the number of vectors in V that appear in the corresponding linear combination. If V is (t, k)-independent, then no nontrivial linear combination of up to $t+1$ vectors in V is zero. This implies that the Hamming weight of any non-null codeword of $\mathcal{C}_V^*$ is at least $t+2$. The converse is shown similarly. □

Consider, as an example, the set V of all monic vectors in $\mathbb{F}_q^k$, that is $(1, k)$-independent but not $(2, k)$-independent. Lemma 3.5 implies that the code $\mathcal{C}_V^*$ is a $[\frac{q^k-1}{q-1}, \frac{q^k-1}{q-1} - k, 3]$ code. Namely, it is the well known Hamming code.

It may be shown that for $[n, k, d]$ codes, $d \leq n-k+1$ [21, Chapter 1, Theorem 11]. Codes with $d = n-k+1$ are called *Maximum Distance Separable (MDS) codes*. The dual of an MDS code is also MDS. An example of MDS codes are the Reed-Solomon codes. An example of the Reed-Solomon codes is the $[q, k, q-k+1]$ code whose generating matrix consists of all regular Vandermonde vectors in $\mathbb{F}_q^k$ as its rows.

A $[n, k]$ code over $\mathbb{F}_q$ is MDS if and only if every k rows of the generating matrix G are linearly independent [21, Chapter 11, Corollary 3]. Namely, a $[n, k]$ code over $\mathbb{F}_q$ is MDS if and only if the rows of its generating matrix are $(k-1, k)$-independent. Hence, the notion of (t, k)-independence extends the notion of MDS codes.

The *covering radius* $\rho(\mathcal{C})$ of a code $\mathcal{C}$ is the maximum Hamming distance between a vector $\mathbf{w} \in \mathbb{F}_q^n \setminus \mathcal{C}$ and the code. That is,

$$\rho(\mathcal{C}) = \max_{\mathbf{w} \in \mathbb{F}_q^n \setminus \mathcal{C}} (\mathrm{dist}(\mathbf{w}, \mathcal{C})) = \max_{\mathbf{w} \in \mathbb{F}_q^n \setminus \mathcal{C}} \left(\min_{\mathbf{w}' \in \mathcal{C}} \mathrm{dist}(\mathbf{w}, \mathbf{w}') \right).$$

While Lemma 3.5 established a relation between (t, k)-independence of V and the minimal distance of the corresponding dual code, $\mathcal{C}_V^*$, the next lemma establishes a similar relation between the (t, k)-spanning property of V and the covering radius of $\mathcal{C}_V^*$.

Lemma 3.6 *Let $V \subseteq \mathbb{F}_q^k$ be a set of vectors that spans $\mathbb{F}_q^k$. Then, for any $1 \leq t \leq k-1$, V is a (t,k)-spanning set if and only if $\rho(\mathcal{C}_V^*) \leq t$.*

Proof. Let $n = |V|$ and let G be the $n \times k$ matrix whose rows are the vectors in V. Consider the following mapping from $\mathbb{F}_q^n$ to $\mathbb{F}_q^k$: $\mathbf{u}^t \mapsto \mathbf{v}^t = \mathbf{u}^t G$. Since V spans $\mathbb{F}_q^k$, this mapping is a surjective. Indeed, every vector $\mathbf{v} \in \mathbb{F}_q^k$ can be written as a linear combination of some vectors in V. Letting $\mathbf{u} \in \mathbb{F}_q^n$ be the vector of the coefficients in such a linear combination, we have $\mathbf{v}^t = \mathbf{u}^t G$. Conversely, every $\mathbf{u} \in \mathbb{F}_q^n$ defines a vector $\mathbf{v} \in \mathbb{F}_q^k$ as the corresponding linear combination of the vectors in V. As before, the number of vectors of V that are involved in that linear combination is exactly the Hamming weight of $\mathbf{u}$.

Let $\mathbf{v}$ be an arbitrary vector in $\mathbb{F}_q^k$ and let $\mathbf{u} \in \mathbb{F}_q^n$ be such that $\mathbf{v}^t = \mathbf{u}^t G$. By the definition of the covering radius, there exists a codeword $\mathbf{w} \in \mathcal{C}_V^*$ such that $\mathrm{dist}(\mathbf{u}, \mathbf{w}) \leq \rho(\mathcal{C}_V^*)$. Hence, the Hamming weight of $\mathbf{u} - \mathbf{w}$ is at most $\rho(\mathcal{C}_V^*)$. But as $(\mathbf{u}-\mathbf{w})^t G = \mathbf{u}^t G - \mathbf{w}^t G = \mathbf{v}^t - \mathbf{0} = \mathbf{v}^t$, we conclude that there exists a linear combination of at most $\rho(\mathcal{C}_V^*)$ vectors in V that equals $\mathbf{v}$. This implies that V is a $(\rho(\mathcal{C}_V^*), k)$-spanning set.

Conversely, if V is a (t,k)-spanning set then for every $\mathbf{u} \in \mathbb{F}_q^n$ there exists a vector $\hat{\mathbf{u}} \in \mathbb{F}_q^n$ with Hamming weight at most t such that $\mathbf{u}^t G = \hat{\mathbf{u}}^t G$. Thus, $\mathbf{w} = \mathbf{u} - \hat{\mathbf{u}} \in \mathcal{C}_V^*$ and $\mathrm{dist}(\mathbf{u}, \mathcal{C}_V^*) \leq \mathrm{dist}(\mathbf{u}, \mathbf{w}) \leq t$. This concludes the proof since then $\rho(\mathcal{C}_V^*) \leq t$. □

Invoking Proposition 3.3, we may summarize Lemmas 3.5 and 3.6 as follows:

Proposition 3.7 *Let $V \subseteq \mathbb{F}_q^k$ be a set of vectors that spans $\mathbb{F}_q^k$. Then, for any $1 \leq t \leq k-1$, V is a (t,k)-base if and only if $\rho(\mathcal{C}_V^*) \leq t \leq d(\mathcal{C}_V^*) - 2$.*

3.3 On the size of (t,k)-bases

In this subsection we address the question of the size of (t,k)-bases over some finite field $\mathbb{F}_q$. To this end, we first recall the definition of a matroid.

Matroids are a combinatorial structure that generalizes both linear spaces and the set of circuits in an undirected graph. They are a useful tool in several fields of theoretical computer science, e.g., optimization algorithms. A matroid $\mathcal{M} = \langle V, \mathcal{I} \rangle$ is a finite set V and a collection $\mathcal{I}$ of subsets of V that satisfy the following three axioms:

(I1) $\emptyset \in \mathcal{I}$.

(I2) If $X \in \mathcal{I}$ and $Y \subseteq X$ then $Y \in \mathcal{I}$.

(I3) If X and Y are members of $\mathcal{I}$ with $|X| = |Y| + 1$ then there exists an element $x \in X \setminus Y$ such that $Y \cup \{x\} \in \mathcal{I}$.

The elements of V are called the *points* of the matroid and the sets in $\mathcal{I}$ are called the *independent* sets of the matroid. Axiom (I1) assures that there is at least one independent set in $\mathcal{I}$. Axiom (I2) asserts that the collection $\mathcal{I}$ is closed under containment. Finally, Axiom (I3) enables the expansion of every small independent set in $\mathcal{I}$. A *dependent set* of the matroid is any subset of V that is not independent.

As a consequence of Axiom (I3), all maximal independent sets in a matroid have the same size, which is called the *rank* of the matroid. Those maximal independent sets are called *bases*. The family of all bases of a matroid $\mathcal{M}$ determines the matroid.

Definition 3.5 *Let k and t be integers such that $1 \leq t \leq k-1$. Then $\mathcal{I}_{t,k;q}$ (or $\mathcal{I}_{t,k}$ for simplicity) denotes the collection of all (t,k)-independent sets in $U = \mathbb{F}_q^k$. In addition, $\mathcal{I}_{t,k;q}^0$ denotes the subfamily of maximal sets in $\mathcal{I}_{t,k;q}$.*

We note that $\mathcal{I}_{t,k}$ is nontrivial since if V is any set of independent vectors in U then it is (t,k)-independent.

A natural question that arises is whether $\mathcal{I}_{t,k}$ is a matroid.

Theorem 3.8 *$\mathcal{I}_{t,k}$ is a matroid if and only if $t = 1$.*

Proof. As Axioms (I1) and (I2) are obviously satisfied by $\mathcal{I}_{t,k}$, we concentrate on Axiom (I3). Let us begin with the case $t = 1$. $\mathcal{I}_{1,k}$ is the collection of all subsets $V \subset U$, such that V does not include vectors that have the same direction. Assume that $X, Y \in \mathcal{I}_{1,k}$ and that $|X| = |Y| + 1$. Given $\mathbf{x} \in X \setminus Y$, the augmented set $Y \cup \{\mathbf{x}\}$ is not $(1,k)$-independent if and only if $\mathbf{x}$ is in the same direction as some vector in Y. As X and Y are both $(1,k)$-independent, it means that X has vectors in $|X|$ different directions and Y has vectors in $|Y|$ different directions. Since $|X| = |Y|+1$, the set X must include a vector, $\mathbf{x}$, whose direction is not the direction of any vector in Y. For that vector, $Y \cup \{\mathbf{x}\}$ must be still $(1,k)$-independent. Therefore, $\mathcal{I}_{1,k}$ satisfies also the third matroid axiom, (I3), whence it is a matroid.

Assume next that $t > 1$. We proceed to show that $\mathcal{I}_{t,k}$ fails to satisfy Axiom (I3). Letting $\mathbf{e}_i$, $1 \le i \le k$ denote the standard basis vectors in $\mathbb{F}_q^k$, we define

$$Y = \{\mathbf{e}_1, \ldots, \mathbf{e}_k\}, \quad \text{and} \quad X = \{\mathbf{e}_1, \mathbf{e}_1 + \mathbf{e}_2, \mathbf{e}_2 + \mathbf{e}_3, \ldots, \mathbf{e}_{k-1} + \mathbf{e}_k, \mathbf{e}_k\}.$$

We claim, and show later, that $X, Y \in \mathcal{I}_{t,k}$. Since each vector in X is a linear combination of at most two vectors from Y, and $t \ge 2$, we infer that $Y \cup \{\mathbf{x}\} \notin \mathcal{I}_{t,k}$ for all $\mathbf{x} \in X$. As $|X| = |Y| + 1$, this contradicts Axiom (I3).

It remains to show that X and Y are (t,k)-independent. This is equivalent to showing that every $t+1$ vectors from each of those sets are independent. As $t + 1 \le k$, we proceed to show a stronger claim - every k vectors from each of those sets are independent. This clearly holds for Y. Let us prove the claim for X.

The k vectors in $X \setminus \{\mathbf{e}_1\}$ are independent since if we write them in the rows of a square matrix we get an upper-triangular matrix with determinant 1. Similarly, the k vectors in $X \setminus \{\mathbf{e}_k\}$ are also independent (here we get a lower-triangular matrix with determinant 1). Consider now the k vectors in $X \setminus \{\mathbf{e}_j + \mathbf{e}_{j+1}\}$, where $1 \le j \le k-1$. The corresponding matrix here is not triangular. However, by applying the elementary row operations $\mathbf{R}_i \leftarrow \mathbf{R}_i - \mathbf{R}_1$, $2 \le i \le j$, we arrive at an upper-triangular matrix with determinant 1. Therefore, all subsets of X of size k are independent subsets. This implies that $X \in \mathcal{I}_{k-1,k}$. As $t \le k-1$, we infer that $X \in \mathcal{I}_{k-1,k} \subset \mathcal{I}_{t,k}$. The proof is thus complete. □

Since $\mathcal{I}_{1,k;q}$ is a matroid, then all $(1,k)$-bases in $\mathcal{I}^0_{1,k;q}$ have the same size. By Proposition 3.4, the set of all monic vectors in $\mathbb{F}_q^k$ is a $(1,k)$-base, and its size is $\frac{q^k-1}{q-1} = \sum_{j=0}^{k-1} q^j$. We note that the collection of all monic vectors in $\mathbb{F}_q^k$ coincides with the projective geometry $\mathrm{PG}(k-1,q)$ (e.g. [21, Appendix B]).

Next, we address the question of the size of (t,k)-bases, namely, the size of the maximal sets in $\mathcal{I}_{t,k}$. As $I_{t,k}$ is not a matroid, for $2 \le t \le k-1$, (t,k)-bases may have different sizes. The following examples show that this is indeed the case.

Example 1. Consider the case $q = 2$, $t = 2$ and $k = 4$. Then the following two sets are $(2,4)$-bases in $\mathbb{F}_2^4$. The first one has eight vectors (written in columns) and the second has five vectors:

$$\left\{ \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} \right\} \qquad \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \right\}$$

Example 2. Consider the case $q = 5$, $t = 2$ and $k = 4$. The following two sets, of sizes 16 and 26 respectively, are $(2, 4)$-bases in $\mathbb{F}_5^4$:

$$\left\{\begin{array}{cccccccccccccccc} 1&0&1&1&1&1&1&1&1&1&0&0&1&0&1&0\\ 0&0&1&2&3&4&1&2&3&2&1&0&0&1&4&1\\ 0&0&1&4&4&1&2&2&0&0&3&1&1&4&2&0\\ 0&1&1&3&2&4&3&1&3&1&1&4&3&2&0&0 \end{array}\right\}$$

$$\left\{\begin{array}{cccccccccccccccccccccccc} 1&0&1&1&1&1&1&1&0&1&1&1&1&1&1&0&1&1&0&1&1&0&1&1&1&0\\ 0&0&1&2&3&4&2&2&1&4&3&1&0&3&3&1&2&0&1&1&4&1&0&4&1&0\\ 0&0&1&4&4&1&2&1&3&0&3&4&4&1&0&1&3&3&0&2&2&4&2&3&0&1\\ 0&1&1&3&2&4&1&1&0&0&2&2&3&4&4&2&3&2&2&0&4&0&0&3&1&3 \end{array}\right\}$$

In view of the above, the notion of dimension does not have a natural parallel of (t, k)-dimension. Instead, we introduce the notions of minimal and maximal $(t, k; q)$-dimensions:

Definition 3.6 *Let $\mathbb{F}_q$ be a finite field of size q and let $\mathcal{I}^0_{t,k;q}$ be the family of (t, k)-bases in $\mathbb{F}_q^k$. Then the minimal $(t, k; q)$-dimension, $d(t, k; q)$, and the maximal $(t, k; q)$-dimension, $D(t, k; q)$, are:*

$$d(t,k;q) = \min\left\{|A| : A \in \mathcal{I}^0_{t,k;q}\right\}, \qquad D(t,k;q) = \max\left\{|A| : A \in \mathcal{I}^0_{t,k;q}\right\}.$$

A natural question is to obtain lower and upper bounds on those minimal and maximal $(t, k; q)$-dimensions.

3.3.1 The size of $(2, k)$-bases over $\mathbb{F}_2$

We begin by identifying the value of $D(2, k; 2)$ and later on we determine $d(2, k; 2)$.

Proposition 3.9 $D(2, k; 2) = 2^{k-1}$.

Proof. Let $V \in \mathcal{I}^0_{2,k;2}$ be a $(2, k)$-base in $\mathbb{F}_2^k$ and let $n = |V|$. Let us identify the vectors of V with the vertices of the complete graph K_n and consider the following edge-coloring of that graph:

$$c(\{\mathbf{u}, \mathbf{v}\}) = \mathbf{u} + \mathbf{v}, \quad \forall \mathbf{u}, \mathbf{v} \in V.$$

This is a legal coloring in the sense that any two adjacent edges must have a different color. Hence, the size of the palette of colors must be at least the edge-chromatic number of K_n which is either $n - 1$ or n. The palette of colors is exactly $\mathbb{F}_2^k \setminus (V \cup \{\mathbf{0}\})$, because every nonzero vector in $\mathbb{F}_2^k$ may be expressed as a linear combination of two vectors from V, while, owing to the $(2, k)$-independence of V, no vector from $V \cup \{\mathbf{0}\}$ can. This implies that $2^k - n - 1 \geq n - 1$, whence $n \leq 2^{k-1}$. To conclude the proof, we show that $\mathcal{I}^0_{t,k;q}$ always includes a set of size 2^{k-1}. Indeed, the collection

$$V = \{(a_1, \ldots, a_{k-1}, 1) : a_1, \ldots, a_{k-1} \in \mathbb{F}_2\}$$

is clearly a $(2, k)$-independent set (the sum of any two vectors in V is no longer in V), it is maximal (since any vector $(a_1, \ldots, a_{k-1}, 0) \in \mathbb{F}_2^k \setminus V$ is the sum of the two vectors $(a_1, \ldots, a_{k-1}, 1)$ and $(0, \ldots, 0, 1)$, both of which are in V), and its size is 2^{k-1}. □

The last proof is constructive in the sense that it describes a specific $(2, k)$-base V of maximal size. From a geometric point of view, V is a complement of a particular hyperplane in $\mathbb{F}_2^k$. In the next proposition we show that the same holds for any hyperplane.

Proposition 3.10 *If H is a hyperplane in $\mathbb{F}_2^k$ then $V = \mathbb{F}_2^k \setminus H$ is a $(2,k)$-base of maximal size. Conversely, if V is a $(2,k)$-base of $\mathbb{F}_2^k$ and $|V| = D(2,k;2)$ then $\mathbb{F}_2^k \setminus V$ is a hyperplane in $\mathbb{F}_2^k$.*

Proof. Let H be a hyperplane in $\mathbb{F}_2^k$ and $V = \mathbb{F}_2^k \setminus H$. Proving that V is a $(2,k)$-base is straightforward when considering the quotient vector space $\mathbb{F}_2^k/H \cong \mathbb{F}_2$: All vectors in H correspond to the scalar 0 while all those in V correspond to 1. Hence, the sum of two vectors in V cannot be in V (i.e., V is $(2,k)$-independent), whence it must be in H (i.e., V is $(2,k)$-spanning).

Now, let us assume that V is a $(2,k)$-base of $\mathbb{F}_2^k$ and $|V| = D(2,k;2) = 2^{k-1}$. Then $|\mathbb{F}_2^k \setminus V| = |V|$. For any $\mathbf{v} \in V$, we have $|\mathbf{v}+V| = |\{\mathbf{v}+\mathbf{v}' \mid \mathbf{v}' \in V\}| = |V|$. But $\mathbf{v}+V \cap V = \emptyset$, since V is a $(2,k)$-independent set. Thus, $\mathbf{v}+V = \mathbb{F}_2^k \setminus V$ for all $\mathbf{v} \in V$. This implies that given $\mathbf{w}_1, \mathbf{w}_2 \in \mathbb{F}_2^k \setminus V$ and $\mathbf{v} \in V$, there exist $\mathbf{v}_1, \mathbf{v}_2 \in V$ such that $\mathbf{w}_1 = \mathbf{v}+\mathbf{v}_1$ and $\mathbf{w}_2 = \mathbf{v}+\mathbf{v}_2$. Hence, $\mathbf{w}_1 + \mathbf{w}_2 = \mathbf{v}_1 + \mathbf{v}_2 \in \mathbb{F}_2^k \setminus V$. Therefore, $\mathbb{F}_2^k \setminus V$ is a vector subspace. Since $|\mathbb{F}_2^k \setminus V| = 2^{k-1}$, it is a hyperplane in $\mathbb{F}_2^k$. □

In order to determine $d(2,k;2)$ we first introduce some notation. For any proper subset V of $\mathbb{F}_2^k$ we define $S(V) = (V+V) \setminus \{\mathbf{0}\} = \{\mathbf{v}_1 + \mathbf{v}_2 \mid \mathbf{v}_1, \mathbf{v}_2 \in V, \mathbf{v}_1 \neq \mathbf{v}_2\}$. Then we claim the following:

Proposition 3.11 $d(2,k;2) \geq \alpha(k) := \sqrt{2^{k+1} - \frac{7}{4}} - \frac{1}{2}$.

Proof. Let V be a $(2,k)$-base of $\mathbb{F}_2^k$ of size n. As V is a $(2,k)$-spanning set, $|\mathbb{F}_2^k| = 2^k \leq 1 + |V| + |S(V)| \leq 1 + n + \binom{n}{2}$. But $2^k \leq 1 + n + \binom{n}{2}$ is equivalent to $n \geq \sqrt{2^{k+1} - \frac{7}{4}} - \frac{1}{2}$. □

If V is a $(2,k)$-base of $\mathbb{F}_2^k$ of size n then $|S(V)| \leq \binom{n}{2}$. In the following lemma we characterize the cases where $S(V)$ is of maximal size.

Lemma 3.12 *Let V be a $(2,k)$-independent set of $\mathbb{F}_2^k$. Then $|S(V)| = \binom{|V|}{2}$ if and only if V is also a $(3,k)$-independent set.*

Proof. A $(2,k)$-independent set V is also $(3,k)$-independent if and only if no vector $\mathbf{v} \in V$ can be expressed as a sum $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3$, where $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ are three distinct vectors in $V \setminus \{\mathbf{v}\}$. But $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3$ if and only if $\mathbf{v} + \mathbf{v}_1 = \mathbf{v}_2 + \mathbf{v}_3$. Namely, V is also $(3,k)$-independent if and only if there do not exist four vectors $\mathbf{v}, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ in V such that $\mathbf{v} + \mathbf{v}_1 = \mathbf{v}_2 + \mathbf{v}_3$. As the latter condition is equivalent to $|S(V)| = \binom{|V|}{2}$, that completes the proof. □

As a consequence, every $(2,k)$-base of $\mathbb{F}_2^k$ with cardinality $\alpha(k)$ (if one exists) is also a $(3,k)$-base. That is, $d(2,k;2) = \alpha(k)$ implies $D(3,k;2) \geq \alpha(k)$. However, this situation can rarely happen since $\alpha(k)$ must be an integer and, additionally, there must exist a $(2,k)$-base with that number of vectors.

Lemma 3.13 *$\alpha(k)$ is an integer exactly for $k = 1, 2, 4$ and 12.*

Proof. $\alpha(k) = \dfrac{\sqrt{2^{k+3} - 7} - 1}{2}$ can be an integer if only if $2^{k+3} - 7 = x^2$ for some odd integer x. The diophantine equation $2^m - 7 = x^2$, known as the Ramanujan-Nagell equation [30], has only a finite number of integral solutions. Those solutions correspond to $m = 3, 4, 5, 7$ and 15. Since k must be positive, the only possible values for k are 1,2,4 and 12. □

For $k = 1, 2$ every (normal) base is in particular a $(2, k)$-base with cardinality $\alpha(k)$. An example of a $(2, 4)$-base with $\alpha(4) = 5$ vectors was given in Example 1. As for the last case, $k = 12$, we do not know whether a $(2, 12)$-base of size $\alpha(12) = 90$ exists.

3.3.2 The size of (t, k)-bases over a general field

Here, we obtain upper and lower bounds on the size of (t, k)-bases over a general field. To that end, we introduce the useful notation $V_q(n, e) = \sum_{\ell=0}^{e} \binom{n}{\ell}(q-1)^\ell$, where $0 \le e \le n$.

Lemma 3.14 *Let V be a (t, k)-independent set in $\mathbb{F}_q^k$ and let $n = |V|$. Then*

$$q^k \ge V_q(n, \lfloor \tfrac{t+1}{2} \rfloor) \,. \tag{12}$$

Proof. Although the lemma can be proven directly, we prefer to relate it to the well known Hamming upper bound on the size of a code. According to that bound, the maximal size $A_q(n, d)$ of a code $\mathcal{C} \subseteq \mathbb{F}_q^n$ with minimum distance d is upper-bounded by

$$A_q(n, d) \le \frac{q^n}{V_q(n, \lfloor \frac{d-1}{2} \rfloor)} \,.$$

Applying this bound to the code $\mathcal{C}_V^*$, that is a $[n, n-k, d^*]$ code, we infer that

$$q^{n-k} \le \frac{q^n}{V_q(n, \lfloor \frac{d^*-1}{2} \rfloor)} \,.$$

By Lemma 3.5, the (t, k)-independence of V implies that $d^* \ge t + 2$. Therefore, $q^k \ge V_q(n, \lfloor \frac{t+1}{2} \rfloor)$. □

Neglecting all terms, excluding the last one, in the sum on the right hand side of (12), and using the simple lower bound on the binomial coefficient, $\binom{n}{s} \ge \left(\frac{n}{s}\right)^s$, we obtain the following explicit upper bound on $D(t, k; q)$.

Corollary 3.15 *$D(t, k; q) \le \frac{s}{q-1} \cdot q^{k/s}$ where $s = \lfloor \frac{t+1}{2} \rfloor$.*

The following recursive estimate bounds the rate in which $D(t, k; q)$ increases with respect to t and k.

Theorem 3.16 *$D(t, k; q) \le D(t-1, k-1; q) + 1$ for all $t \le k - 1$.*

Proof. Assume that $D(t, k; q) = n$ and that $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \subset \mathbb{F}_q^k$ is a (t, k)-base. Without loss of generality we assume that $\mathbf{v}_n = \mathbf{e}_k = (0, \ldots, 0, 1)$ since, if it is not the case, there exists an invertible matrix $A \in M_k(\mathbb{F}_q)$ such that $A\mathbf{v}_n = \mathbf{e}_k$ and then we may consider the (t, k)-base $\{A\mathbf{v}_1, \ldots, A\mathbf{v}_n\}$.

Let $P : \mathbb{F}_q^k \to \mathbb{F}_q^{k-1}$ denote the projection $P(u_1, \ldots, u_k) = (u_1, \ldots, u_{k-1})$. We proceed to show that $\{P\mathbf{v}_1, \ldots, P\mathbf{v}_{n-1}\} \subset \mathbb{F}_q^{k-1}$ is $(t-1, k-1)$-independent, hence proving that $D(t-1, k-1; q) \ge n - 1 = D(t, k; q) - 1$. To that end we need to show that every t vectors from the set $\{P\mathbf{v}_1, \ldots, P\mathbf{v}_{n-1}\}$ are independent. Consider the subset $\{P\mathbf{v}_{i_1}, \ldots, P\mathbf{v}_{i_t}\}$. By the (t, k)-independence of $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, the $t+1$ vectors $\{\mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_t}, \mathbf{v}_n\}$ are independent in $\mathbb{F}_q^k$. Hence, they may be complemented into a base of $\mathbb{F}_q^k$ by additional $k-1-t$ vectors, say $\mathbf{w}_1, \ldots, \mathbf{w}_{k-1-t}$. Consider now the matrix $B \in M_k(\mathbb{F}_q)$ whose rows are $\{\mathbf{w}_1, \ldots, \mathbf{w}_{k-1-t}, \mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_t}, \mathbf{v}_n\}$. As it is an invertible matrix, its determinant is nonzero. But since its last row is $\mathbf{v}_n = \mathbf{e}_k$, the

determinant of B equals the determinant of the upper left $(k-1)\times(k-1)$ minor whose rows are $\{P\mathbf{w}_1,\ldots,P\mathbf{w}_{k-1-t},P\mathbf{v}_{i_1},\ldots,P\mathbf{v}_{i_t}\}$. This implies that the vectors $\{P\mathbf{v}_{i_1},\ldots,P\mathbf{v}_{i_t}\}$ are independent. □

Combining Theorem 3.16 and Proposition 3.9, we infer that $D(t,k;2)\leq 2^{k-t+1}+t-2$. Combining Theorem 3.16 and Corollary 3.15, we arrive at the following conclusion.

Corollary 3.17 $D(t,k;q)\leq \frac{t}{2(q-1)}\cdot q^{2(k-1)/t}+1$.

The original estimate in Corollary 3.15 for even values of t was $D(t,k;q)\leq \frac{t}{2(q-1)}\cdot q^{2k/t}$. Hence, Corollary 3.17 always improves Corollary 3.15 for even values of t. When t is odd, on the other hand, we cannot use Theorem 3.16 in order to improve the estimate provided by Corollary 3.15 since the reduction from t to $t-1$ changes the corresponding value of $s=\lfloor\frac{t+1}{2}\rfloor$.

Next, we derive a lower bound for $d(t,k;q)$.

Lemma 3.18 *Let V be a (t,k)-spanning set in $\mathbb{F}_q^k$ and let $n=|V|$. Then*

$$q^k\leq V_q(n,t)\,. \tag{13}$$

Proof. As V is a (t,k)-spanning set, any vector in $\mathbb{F}_q^k$ must be a linear combination of at most t vectors from V. Therefore,

$$|q^k|\leq \sum_{\substack{E\subset V\\ |E|\leq t}}(q-1)^{|E|}=\sum_{\ell=0}^{t}(q-1)^{\ell}\binom{n}{\ell}\,.$$

□

This lemma is related to the Gilbert-Varshamov lower bound on the maximal size $A_q(n,d)$ of a code $\mathcal{C}\subseteq\mathbb{F}_q^n$ with minimum distance d:

$$A_q(n,d)\geq\frac{q^{n-1}}{V_q(n-1,d-2)}\,.$$

Indeed, consider a (t,k)-base of $\mathbb{F}_q^n$, denoted V. From Lemma 3.18 and the definition of $V_q(n,t)$ we conclude that

$$q^k\leq V_q(n,t)=V_q(n-1,t)+(q-1)V_q(n-1,t-1)\leq qV_q(n-1,t)\,. \tag{14}$$

The corresponding dual code, $\mathcal{C}_V^*$, is of size q^{n-k}. Using (14), we conclude that

$$|\mathcal{C}_V^*|=q^{n-k}\geq\frac{q^{n-1}}{V_q(n-1,t)}\,.$$

But, as Lemma 3.5 implies that $t\leq d^*-2$, we infer that

$$|\mathcal{C}_V^*|\geq\frac{q^{n-1}}{V_q(n-1,d^*-2)}\,.$$

But this is exactly the lower bound that is implied by the Gilbert-Varshamov bound since $\mathcal{C}_V^*$ is a $[n,n-k,d^*]$ code.

Using the simple upper bound on the binomial coefficient, $\binom{n}{s} \leq \frac{n^s}{s!}$, and the fact that $n \geq t$, inequality (13) implies that

$$q^k \leq (t+1)\frac{(q-1)^t n^t}{t!} \leq (t+1)\frac{q^t n^t}{t!}\,.$$

This implies the following explicit lower bound on $d(t,k;q)$.

Corollary 3.19 $d(t,k;q) \geq \left(\frac{t!q^{k-t}}{t+1}\right)^{1/t}$.

Finally, Lemmas 3.14 and 3.18 imply the following result.

Corollary 3.20 *Let V be a (t,k)-independent set and a (t',k)-spanning set in $\mathbb{F}_q^k$. Then $t' \geq \lfloor \frac{t+1}{2} \rfloor$. Moreover, $t' = \lfloor \frac{t+1}{2} \rfloor$ if and only if (12) and (13) hold with equality.*

After the completion of this work we came across two recent papers by Damelin et. al. [9, 8] in which the notion of (t,k)-independence is defined. The first of these papers, [9], concentrated on binary fields and its results may be summarized as follows:

Proposition 3.21 *(Damelin et. al.) The following formulae hold:*

1. $D(2,k;2) = 2^{k-1}$ *for* $k \geq 3$.
2. $D(k-m-1,k;2) = k+1$ *for* $k \geq 3m+2$, $m \geq 0$.
3. $D(k-m-1,k;2) = k+2$ *for* $k = 3m+i$, $i = 0,1$, $m \geq 2$.

The first part of the above proposition is equivalent to our Proposition 3.9. In [8], the size of (t,k)-independent sets is studied over general finite fields and the result that is derived there is as follows.

Proposition 3.22 *(Damelin et. al.)* $D(t,k;q) = k+1$ *if and only if* $\frac{q(k+1)}{q+1} \leq t+1$.

3.3.3 $(k-1,k)$-bases and maximum distance separable codes

A well-known research problem in the theory of error-correcting codes is the following: Given k and q, find the largest value of n for which a $[n,k]$ MDS code exists over $\mathbb{F}_q$ [21, Research Problem (11.1a)]. That value of n is denoted $m(k,q)$. Rephrased in our terms, the problem is to determine the size of the largest $(k-1,k)$-base over $\mathbb{F}_q$, namely, the exact value of $D(k-1,k;q)$. Although MDS codes were first studied by Singleton [29], the problem of determining $m(k,q) = D(k-1,k;q)$ has already been studied as a problem in statistics [6] and as a problem in geometry [25, 26]. This problem is equivalent to several other combinatorial problems, as listed in [21, Chapter 11].

We now review the known results regarding the value of $m(k,q)$ and the conjecture that they suggest. (The reader is referred to [12, 21] for a thorough discussion of those results and relevant references.) When $k \geq q$, it is easy to show that $m(k,q) = D(k-1,k;q) = k+1$. (Note that Proposition 3.22 extends this claim on the value of $D(t = k-1,k;q)$ to all values of t.) The interesting cases are when $2 \leq k < q$.

Conjecture 3.23 *If $2 \leq k < q$ then $m(k,q) = q+1$, unless $q = 2^h$ and $k = 3$ or $k = q-1$, in which case $m(k,q) = q+2$.*

The conjecture has already been shown to be true for $k = 2, 3, 4, 5$ [7, 12, 25]. Using duality arguments, the truth of the conjecture for all $k \leq 5$ implies its truth also for all k in the range $q - 3 \leq k \leq q$, see [32]. The conjecture was also shown in [32] to be true for q odd in the ranges $q > (4k - 9)^2$ and $q - 3 > k > q - \frac{1}{4}\sqrt{q} - \frac{5}{4}$. The conjecture has also been verified by exhaustive search for all $q \leq 11$ and all k [18, 22].

In addition to the above mentioned results, it is known that the conjectured values of $m(k, q)$ are all lower bounds. Namely, for $2 \leq k < q$ we have $m(k, q) \geq q + 1$ (as demonstrated by the $q + 1$ Vandermonde vectors in $\mathbb{F}_q^k$ that are a $(k - 1, k)$-base), and when $q = 2^h$ and $k = 3$ or $k = q - 1$, $m(k, q) \geq q + 2$. Finally, it is known that $m(k + 1, q) \leq m(k, q) + 1$ (we have generalized this result in Theorem 3.16). This, coupled with the truth of the conjecture for $k = 5$, implies the upper bound $m(k, q) \leq q + k - 4$ for all $k \geq 6$.

3.4 On the size of minimal (t, k)-spanning sets

Our main focus in the preceding discussion was (t, k)-bases (i.e., maximal (t, k)-independent sets). A similar discussion may be dedicated to minimal (t, k)-spanning sets. In the spirit of Definition 3.6, we let $\delta(t, k; q)$ and $\Delta(t, k; q)$ denote the minimal and maximal sizes of minimal (t, k)-spanning sets in $\mathbb{F}_q^k$. In view of Proposition 3.2, we have

$$\delta(t, k; q) \leq d(t, k; q) \leq D(t, k; q) \leq \Delta(t, k; q)\,.$$

In addition, by the example given in the proof of Proposition 3.2, it holds that

$$\delta(t, k; q) \leq h_{q,2} + h_{q,k-t} \leq \Delta(t, k; q)\,,$$

where hereinafter $h_{q,m} = \sum_{i=0}^{m-1} q^i$. We proceed to improve the above bounds for $\Delta(t, k; q)$ and $\delta(t, k; q)$.

The idea behind the proof of the second part of Proposition 3.2 is formalized in Lemma 3.24 below.

Lemma 3.24 *Let $(k_1, \ldots, k_\ell)$ and $(t_1, \ldots, t_\ell)$ be sequences of positive integers and let $k = \sum_{j=1}^{\ell} k_j$ and $t = \sum_{j=1}^{\ell} t_j$. Assume that U_j is a (t_j, k_j)-spanning set in $\mathbb{F}_q^{k_j}$, $1 \leq j \leq \ell$. Then $U = \bigcup_{j=1}^{\ell} \varphi_j(U_j)$ is a (t, k)-spanning set in $\mathbb{F}_q^k$. If, in addition, for all $1 \leq j \leq \ell$, U_j is minimal (t_j, k_j)-spanning and it is not (s, k_j)-spanning for any $s < t_j$, then U is a minimal (t, k)-spanning set, and it is not (s, k)-spanning for any $s < t$.*

Proof. Let $\mathbf{w}$ be an arbitrary vector in $\mathbb{F}_q^k$. Then there exist unique vectors $\mathbf{w}_j \in \mathbb{F}_q^{k_j}$, $1 \leq j \leq \ell$, such that $\mathbf{w} = \sum_{j=1}^{\ell} \varphi_j(\mathbf{w}_j)$. Since $\varphi_j(\mathbf{w}_j)$ may be expressed as a linear combination of t_j vectors from $\varphi_j(U_j)$, we infer that $\mathbf{w}$ is a linear combination of t vectors from U.

We turn to prove the second part of the claim. Assume that we remove from U a vector that belongs to $\varphi_j(U_j)$. By the minimality of U_j as a (t_j, k_j)-spanning set, there exists a vector $\mathbf{u}_j \in \mathbb{F}_q^{k_j}$ such that $\varphi_j(\mathbf{u}_j)$ cannot be expressed as a linear combination of t_j vectors from $\varphi_j(U_j)$. Also, by the second assumption that none of the sets U_i is (s, k_i)-spanning for any $s < t_i$, we infer that for all $1 \leq i \leq \ell$ there exists a vector $\mathbf{w}_i \in \mathbb{F}_q^{k_i}$ that cannot be expressed as a linear combination of less than t_i vectors from U_i. Then the vector $\mathbf{u} = \sum_{1 \leq i \neq j \leq \ell} \varphi_i(\mathbf{w}_i) + \varphi_j(\mathbf{u}_j)$ cannot be expressed as a linear combination of t vectors from U. This proves that under the additional assumptions, U is a minimal (t, k)-spanning set in $\mathbb{F}_q^k$. In addition, the vector $\mathbf{w} = \sum_{1 \leq i \leq \ell} \varphi_i(\mathbf{w}_i)$ cannot be expressed as a linear combination of less than t vectors from U. This proves that U it is not (s, k)-spanning for any $s < t$. □

We proceed to use this idea of a superposition of minimal spanning sets to find minimal (t,k)-spanning sets that are smaller or larger than the minimal (t,k)-spanning set that we exemplified in Proposition 3.2. All of our examples rely on Propositions 3.1 and 3.4.

Consider the sequences of length $\ell = t$ where $(k_1,\ldots,k_\ell) = (1,\ldots,1,k-t+1)$ and $(t_1,\ldots,t_\ell) = (1,\ldots,1)$. The corresponding minimal (t_j,k_j)-spanning set, U_j, $1 \le j \le \ell$, consists of all monic vectors in $\mathbb{F}_q^{k_j}$. As $|U_j| = 1$ for all $1 \le j \le t-1$ and $|U_t| = h_{q,k-t+1}$, we have $|U| = t - 1 + h_{q,k-t+1}$. We infer that

$$\Delta(t,k;q) \ge t - 1 + h_{q,k-t+1}\,. \tag{15}$$

Next, we prove the following upper bound on $\delta(t,k;q)$.

Proposition 3.25 *Let k and t be integers such that $1 \le t \le k-1$. Let $m = \lfloor \frac{k}{t} \rfloor$ and $r = k - mt$. Then:*

1. *$\delta(t,k;q) \le (t-r)h_{q,m} + rh_{q,m+1}$ when $m \ge 2$.*
2. *$\delta(t,k;q) \le r(1+q)$ when $m = 1$ and $q \ge \frac{k}{r}$.*

Proof. Assume first that $m \ge 2$ (namely, $t \le \frac{k}{2}$). We prove our claim by demonstrating a minimal (t,k)-base of size $(t-r)h_{q,m} + rh_{q,m+1}$. We set $\ell = t$ and consider the following decomposition sequence for k:

$$(k_1,\ldots,k_\ell) \quad \text{where} \quad k_j = \begin{cases} m & 1 \le j \le t-r, \\ m+1 & t-r+1 \le j \le t. \end{cases}$$

The corresponding decomposition sequence for t will be $(t_1,\ldots,t_\ell) = (1,\ldots,1)$. Note that indeed $\sum_{j=1}^{\ell} k_j = m\cdot(t-r) + r\cdot(m+1) = mt + r = k$. The corresponding minimal (t_j,k_j)-spanning set, U_j, $1 \le j \le \ell$, consists of all monic vectors in $\mathbb{F}_q^{k_j}$. As $|U_j| = h_{q,k_j}$ for all $1 \le j \le \ell$, the size of the resulting minimal (t,k)-spanning set is $(t-r)h_{q,m} + rh_{q,m+1}$.

Next, assume that $m = 1$, namely, $t > \frac{k}{2}$. Here, we set $\ell = r = k - t$ and consider the decomposition of k, $(k_1,\ldots,k_r)$, where $k_j \in \{\lfloor \frac{k}{r} \rfloor, \lceil \frac{k}{r} \rceil\}$, $1 \le j \le r$. The corresponding decomposition of t will be $(t_1,\ldots,t_r)$ where $t_j = k_j - 1$, $1 \le j \le r$. (Note that as $t > \frac{k}{2}$, all t_j are well defined since $k_j \ge 2$.) Finally, relying on our assumption on q in this case, the minimal $(k_j - 1, k_j)$-spanning set in $\mathbb{F}_q^{k_j}$ will be the set U_j of all Vandermonde vectors in $\mathbb{F}_q^{k_j}$. Since the size of U_j is $1+q$, our claim is settled in this case as well. □

Y. Dodis derived lower and upper bounds on $\delta(t,k;q)$ in [10]. Our upper bound in Proposition 3.25 is a slightly improved version of his upper bound. (His upper bound assumed that t divides k while ours does not.) In addition to this bound, Dodis derived also the following two additional results:

Proposition 3.26 *(Dodis) Let k and t be integers such that $1 \le t \le k-1$.*

- *If $k - \frac{k}{q} < t < k$ then $\delta(t,k;q) = k+1$.*
- *If $1 \le t \le k - \frac{k}{q}$ then $\delta(t,k;q) \ge tq^{\lfloor k/t \rfloor}/(e(q-1))$.*

Note that the first part of Proposition 3.26 covers the case $t > k/2$ and $q < \frac{k}{k-t}$ that is not covered by Proposition 3.25.

3.5 Applications of (t,k)-independence

3.5.1 An application to network coding

We describe here an application to network coding [1] where the notion of (t,k)-independence arises. A network is a directed graph with a source and a set of terminals (or sinks). Assuming that all edges have a uniform capacity of, say, 1 bit (namely, we can transmit along each edge one bit in a given time unit), then for each terminal we have a maximum data rate that equals the maximum flow from the source to that terminal. The goal in network coding is to increase the maximum data rate by assuming that the nodes can perform computations.

To illustrate the idea of network coding and its relation to our notion of (t,k)-independence we borrow the following example from [17]. Consider the family of three-layered graphs $G_{n,k} = (V,E)$ where the set of nodes is $V = \{s\} \cup U \cup T$, with $U = \{u_1,\ldots,u_n\}$ and $T = \{t_W : W \subseteq U, |W| = k\}$, and the set of edges is $E = \{(s,u) : u \in U\} \cup \{(u,t_W) : t_W \in T, u \in W\}$. Namely, the first layer consists of the source s, the second layer consists of the n intermediate nodes in U, and the third layer consists of the $\binom{n}{k}$ terminals in T. The source is connected to all intermediate nodes in U, while each of those nodes is connected to all terminals that correspond to subsets of U to which that node belongs.

Assume that we wish to broadcast messages $M_1, M_2, \ldots$ from s to all the terminals $t_W \in T$, and that the messages take values in some finite field $\mathbb{F}_q$. If all edges have the same capacity, say $\lceil \log_2 q \rceil$ bits, s may broadcast the message M_i in the ith time unit to all intermediate nodes and from them to all terminals. If $k \leq \lfloor \frac{n+1}{2} \rfloor$, this data rate of 1 may not be improved. Indeed, even if s attempts to send in the same time unit two messages (say, message M_1 to some of the intermediate nodes and M_2 to the remaining ones), at least one terminal will be connected to a subset of the intermediate nodes that got only one of the two messages. (Note that if $k > \lfloor \frac{n+1}{2} \rfloor$ then we may achieve a data rate of 2 by sending M_1 to $\lfloor \frac{n+1}{2} \rfloor$ of the intermediate nodes and M_2 to the others.) However, by assuming that the nodes may perform linear algebraic computations, we may achieve for this network a data rate of k.

Assume that s wishes to transmit the vector $\mathbf{x} \in \mathbb{F}_q^k$ to all terminals. It will select a $(k-1,k)$-independent set of n vectors in $\mathbb{F}_q^k$, $\{\mathbf{a}_1,\ldots,\mathbf{a}_n\}$. Then, it will send to u_i the message $\mathbf{a}_i \cdot \mathbf{x}$. Each node u_i will output the message that it got to all the terminals to which it is connected. Finally, the terminal that corresponds to $\{u_{i_1},\ldots,u_{i_k}\}$ for $1 \leq i_1 < \cdots < i_k \leq n$ will recover $\mathbf{x}$ from $\{\mathbf{a}_{i_j} \cdot \mathbf{x} : 1 \leq j \leq k\}$ by solving the corresponding system of linear equations. Each of those linear systems is solvable since $\{\mathbf{a}_1,\ldots,\mathbf{a}_n\}$ is $(k-1,k)$-independent, whence any selection of k vectors from it is independent.

3.5.2 Multivariate Lagrange interpolation

Consider a k-variate polynomial of degree less than or equal to d over a finite field $\mathbb{F}_q$,

$$P(\mathbf{x}) = \sum_{0 \leq |\mathbf{r}| \leq d} a_{\mathbf{r}} \mathbf{x}^{\mathbf{r}},$$

where $\mathbf{x} = (x_1,\ldots,x_k)$ is a point in $\mathbb{F}_q^k$, $\mathbf{r} = (r_1,\ldots,r_k) \in \mathbb{N}^k$ is a multi-index, $\mathbf{x}^{\mathbf{r}} = \prod_{i=1}^k x_i^{r_i}$, and $|\mathbf{r}| = \sum_{i=1}^k r_i$. The number of coefficients in such a polynomial is $\binom{d+k}{k}$. Hence, interpolation of such a polynomial requires $\binom{d+k}{k}$ point values of the polynomial. Not every $\binom{d+k}{k}$ points give rise to a well-posed system of linear equations. However, if those points are the intersection points of $d+k$ flats in general position in $\mathbb{F}_q^k$, it is guaranteed that the corresponding system of linear equations is well-posed.

Let

$$\{L_i(\mathbf{x}) = \mathbf{a}_i \cdot \mathbf{x} + c_i = 0\}_{1 \leq i \leq d+k} \tag{16}$$

be a collection of $d+k$ flats in $\mathbb{F}_q^k$ in a general position (namely, every k of these flats intersect in a single point, and no two of these points coincide). Let $\mathbf{j} = \{j_1, \ldots, j_k\}$, $1 \leq j_1 < j_2 < \cdots < j_k \leq d+k$, denote a selection of k of these flats, and let $\mathbf{x_j}$ denote the single intersection point of the k selected flats. Assume that we are given the values of the polynomial P at these $\binom{d+k}{k}$ intersection points,

$$P(\mathbf{x_j}) = f_{\mathbf{j}} \quad \text{where} \quad \mathbf{j} = \{j_1, \ldots, j_k\} \ \text{ and } \ 1 \leq j_1 < j_2 < \ldots < j_k \leq d+k \ .$$

Then P is given as follows:

$$P(\mathbf{x}) = \sum_{1 \leq j_1 < j_2 < \ldots < j_k \leq d+k} f_{\mathbf{j}} L_{\mathbf{j}}(\mathbf{x})$$

where

$$L_{\mathbf{j}}(\mathbf{x}) = \prod_{\substack{1 \leq i \leq d+k \\ i \notin \mathbf{j}}} \frac{L_i(\mathbf{x})}{L_i(\mathbf{x_j})} \ .$$

$L_{\mathbf{j}}(\mathbf{x})$ is a product of d linear polynomials, whence it is a polynomial of degree d. It equals 1 in $\mathbf{x_j}$ and it vanishes in every other intersection point, because any other intersection point lies on at least one flat L_i where $i \notin \mathbf{j}$. (For more details on multivariate interpolation see [3].)

A necessary condition for a family of flats (16) to be in a general position is that their corresponding normal vectors, $\mathbf{a}_i$, constitute a $(k-1,k)$-independent set in $\mathbb{F}_q^k$. Hence, in settings where it is necessary to enable a recovery of such a polynomial by means of multivariate Lagrange interpolation, one needs to find a $(k-1,k)$-independent set of vectors of some given cardinality. An application of that sort is described in [2].

4 (t,k)-Bases and Projective Geometry

A structure that is related to (t,k)-bases is defined in projective geometry. Herein we describe that structure and the results that are known regarding that structure that coincide with some of our results. The following summary is based on [13].

Let $\mathrm{PG}(d,q)$ be the projective space of d dimensions over $\mathbb{F}_q$. Namely, $\mathrm{PG}(d,q)$ consists of all $\sum_{i=0}^{d} q^i$ one-dimensional subspaces of $\mathbb{F}_q^{d+1}$. A subspace of dimension ℓ in $\mathrm{PG}(d,q)$ is denoted π_ℓ. A π_0 is a point (that stands for a monic vector, or a subspace of dimension one in the linear space $\mathbb{F}_q^{d+1}$), a π_1 is a line (that stands for a two-dimensional subspace in $\mathbb{F}_q^{d+1}$), and so forth.

Definition 4.1 *A $(k;r,s;d,q)$-set K is a set of k points in $PG(d,q)$ that satisfies two properties:*

1. *There is a π_s that contains r points of K, but no π_s contains $r+1$ points of K.*
2. *There is a π_{s+1} that contains $r+2$ points of K.*

A $(k;r,r-1;d,q)$-set is called a k-set of kind r.

In a k-set of kind r there are at most r points in any π_{r-1}, but there exist $r+2$ points in a π_r. Phrased in linear algebraic terms, a k-set, K, of kind r is a set of k monic vectors in $\mathbb{F}_q^{d+1}$ for which:

1. All $r+1$ vectors from K are linearly independent.
2. There exist $r+2$ vectors from K that are linearly dependent.

Hence, in our terminology, a k-set of kind r in $\mathrm{PG}(d,q)$ is a $(r,d+1)$-independent set of size k in $\mathbb{F}_q^{d+1}$ where r is maximal. It is important to note the difference between this notion and our notion of a $(r,d+1)$-base (of size k). While the latter is a $(r,d+1)$-independent set that is maximal with respect to set-inclusion (namely, it cannot be augmented by additional vectors without violating the property of $(r,d+1)$-independence), a k-set of kind r is a $(r,d+1)$-independent set that is maximal with respect to r (i.e., it is not $(r',d+1)$-independent for any $r'>r$).

Proposition 4.1 *A set K of k vectors in $\mathbb{F}_q^{d+1}$ is $(r,d+1)$-independent if and only if it is a k-set of kind r' for some $r \le r' \le d$.*

Proof. Let K be a set of k vectors in $\mathbb{F}_q^{d+1}$ that is $(r,d+1)$-independent. Namely, all $r+1$ vectors in K are linearly independent. Let r' be the largest integer for which all $r'+1$ vectors in K are linearly independent. Namely, r' is the largest integer for which K is $(r',d+1)$-independent. Clearly, $r' \ge r$ and $r' \le d$. Then K is a k-set of kind r'. Conversely, let K be a k-set of kind r' for some $r \le r' \le d$. Then K is $(r',d+1)$-independent and, consequently, also $(r,d+1)$-independent. □

Hirshfeld [13] defines a *complete* $(k;r,s;d,q)$-set as one that is maximal with respect to inclusion. Hence, every complete k-set of kind r in $\mathrm{PG}(d,q)$ is a $(r,d+1)$-base in $\mathbb{F}_q^{d+1}$, but it is not clear whether the contrary holds as well.

The maximal size of a k-set of kind r in $\mathrm{PG}(d,q)$ is denoted $M_r(d,q)$. We proceed to prove that although the notion of a $(r,d+1)$-base does not (necessarily) coincide with the notion of a k-set of kind r in $\mathrm{PG}(d,q)$, the maximal size of a $(r,d+1)$-base, $D(r,d+1;q)$, equals $M_r(d,q)$. To that end we state and prove the following basic inequality.

Lemma 4.2 $M_{r+1}(d,q) \le M_r(d,q)$.

Proof. As linear independence of vectors is preserved by injective maps, we can inject any (r,d)-independent set V in $\mathbb{F}_q^d$ into a $(r,d+1)$-independent set in $\mathbb{F}_q^{d+1}$ by means of the natural injection φ which maps $(x_1,\ldots,x_d)$ to $(x_1,\ldots,x_d,0)$. Actually, V is (r,d)-independent if and only if $\varphi(V)$ is $(r,d+1)$-independent. Thus, V is a k-set of kind r if and only if $\varphi(V)$ is. Hence,

$$M_r(d-1,q) \le M_r(d,q)\,.$$

On the other hand, if V is a (r,d)-independent set then so is $W = \varphi(V) \cup \{(0,\ldots,0,1)\}$. Moreover, if V is a (r,d)-independent set but not $(r+1,d)$-independent, then W is also a $(r,d+1)$-independent set which is not $(r+1,d+1)$-independent. Therefore,

$$M_r(d-1,q)+1 \le M_r(d,q)\,.$$

Finally, combining this inequality with the following result due to Gulati [11],

$$M_{r+1}(d,q) \le M_r(d-1,q)+1\,,$$

we infer that

$$M_{r+1}(d,q) \le M_r(d,q).$$

□

Proposition 4.3 $M_r(d,q) = D(r,d+1;q)$.

Proof. Let K be a $(r, d+1)$-base in $\mathbb{F}_q^{d+1}$ with a maximal size, $D(r, d+1; q)$. By Lemma 4.2, K is a k-set of kind r' for some $r \leq r' \leq d$, whence is size is bounded by $M_{r'}(d, q)$. But since Lemma 4.2 implies that $M_{r'}(d, q) \leq M_r(d, q)$ we conclude that $D(r, d+1; q) \leq M_r(d, q)$.

Conversely, let K be a k-set of kind r in $\mathbb{F}_q^{d+1}$ with a maximal size, $M_r(d, q)$. Then K is also a $(r, d+1)$-independent set. There exists $K' \supseteq K$ that is a $(r, d+1)$-base. Hence,

$$M_r(d, q) = |K| \leq |K'| \leq D(r, d+1; q)\,.$$

That completes the proof. □

Numerous results have been proved regarding the value of $M_r(d, q)$. Some of those results coincide with the results that we proved here:

- Proposition 3.9 was proven in [4] for k-sets of kind 2 in $\mathrm{PG}(d, 2)$. (A k-set of kind 2 is called a k-cap.) Namely, $M_2(d, 2) = 2^d$.
- Lemma 3.14 was proven for k-sets of kind r in [4, 5, 24]. Namely, if $m = M_r(d, q)$ then $q^{d+1} \geq V_q(m, \lfloor \frac{r+1}{2} \rfloor)$.
- Theorem 3.16 was proven for k-sets of kind r in [11]. Namely, $M_{r+1}(d+1, q) \leq 1 + M_r(d, q)$.

We proceed to review other interesting results about values of $M_r(d, q)$. The reader is referred to [13, 14, 15] for a more thorough review of known results.

Tallini [31] showed that $M_r(d, q) = d + 2$ for $q \leq \frac{r+1}{d+1-r}$, a result that coincides with Proposition 3.22, due to Damelin et. al.

Bose [4], Seiden [27] and Qvist [23] proved that $M_2(3, q) = D(2, 4; q) = q^2 + 1$ for all $q > 2$. We note that for $q = 2$ we have $M_2(d, 2) = D(2, d+1; 2) = 2^d$ (Proposition 3.9 and [4]).

Examples of other known values of $M_r(d, q)$ are (the reader is referred to [13] for the relevant references):

- $D(2, 5; 3) = M_2(4, 3) = 20$
- $D(2, 6; 3) = M_2(5, 3) = 56$
- $D(3, 5; 2) = M_3(4, 2) = 6$
- $D(3, 6; 2) = M_3(5, 2) = 8$
- $D(3, 7; 2) = M_3(6, 2) = 11$
- $D(3, 8; 2) = M_3(7, 2) = 17$
- $D(3, 5; 3) = M_3(4, 3) = 11$
- $D(3, 6; 3) = M_3(5, 3) = 13$
- $D(4, 7; 2) = M_4(6, 2) = 9$
- $D(4, 6; 3) = M_4(5, 3) = 13$

Finally, some authors give explicit constructions of (t, k)-bases for small values of t, k and q.

5 Conclusion and open questions

The discussion in Section 2 motivated our definitions and discussion in the subsequent sections. Considering the vector space $\mathbb{F}_q^k$ and letting t be a parameter in the range $1 \leq t \leq k-1$, we defined the notions of (t, k)-spanning, minimal (t, k)-spanning, (t, k)-independent and maximal

(t,k)-independent sets (or (t,k)-bases). We discussed the relations between those notions and exemplified them. Then we turned our attention to discussing the size of (t,k)-bases. We showed that such (t,k)-bases over $\mathbb{F}_q$ may have different sizes (unless $t=1$) and continued to derive lower and upper bounds on the size of such bases. To that end, we defined $d(t,k;q)$ and $D(t,k;q)$ to be the minimal and maximal size of a (t,k)-base over $\mathbb{F}_q$.

The two extreme cases — $t=1$ and $t=k-1$ — relate to two well-known structures:

- $(1,k)$-bases in $\mathbb{F}_q^k$ coincide with the projective geometry $\mathrm{PG}(k-1,q)$.
- $(k-1,k)$-independent sets correspond to MDS codes.

Hence, the notion of (t,k)-bases, $1 \leq t \leq k-1$, "interpolates" between the concepts of projective geometries and MDS codes, that, to the best of our knowledge, were previously unrelated.

The first question that we raise here is triggered by the above mentioned two extreme cases. The only examples that we have for (t,k)-bases over a general field are for the cases $t=1$ (all monic vectors, Proposition 3.2) and $t=k-1$ (all Vandermonde vectors). The sizes of those bases are $\sum_{i=0}^{k-t} q^i$. This suggests the following conjecture.

Conjecture 5.1 *For all $1 \leq t < k$ it holds that $d(t,k;q) \leq \sum_{i=0}^{k-t} q^i \leq D(t,k;q)$.*

If $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ is a (t,k)-base, then so is $B' = \{c_1 A\mathbf{v}_1, \ldots, c_m A\mathbf{v}_m\}$, where $c_i \in \mathbb{F}_q^*$, $1 \leq i \leq m$, and $A \in M_k(\mathbb{F}_q)$ is a nonsingular matrix. We refer to bases that relate to each other this way as being *equivalent*. A natural question that arises is the following:

Question 5.2 *How many non-equivalent (t,k)-bases exist in $\mathbb{F}_q^k$?*

For example, the set of all monic vectors in $\mathbb{F}_q^k$ is clearly the only $(1,k)$-base, up to equivalence. But, assuming that Conjecture 3.23 is true and $D(k-1,k;q) = q+1$ for all $2 \leq k \leq q$, is the Vandermonde base the only $(k-1,k)$-base, up to equivalence? (A similar question appears in [25]; a review of known results appears in [16].)

Finally, we raise the following two questions, the first of which was triggered by Lemma 3.24.

Question 5.3 *Can a minimal (t,k)-spanning set be (s,k)-spanning for $s < t$?*

Question 5.4 *Can a maximal (t,k)-independent set be (s,k)-independent for $s > t$?*

Using the terminology given in Section 4, we may rephrase Question 5.4 as follows: Is it true that given a $(r,d+1)$-base of k vectors in $\mathbb{F}_q^{d+1}$ then it is a k-set of kind r? In view of Proposition 4.1, all we can say at the moment is that such a $(r,d+1)$-base is a k-set of kind r' for some $r \leq r' \leq d$.

Acknowledgement. We would like to thank the anonymous reviewer for her or his devoted reading of our manuscript and insightful comments.

References

[1] R. Ahlswede, N. Cai, S.Y.R. Li, and R.W. Yeung, Network Information Flow, *IEEE Transactions on Information Theory*, IT-46 (2000), pp. 1204-1216.

[2] J. Ben Yaakov and T. Tassa, Oblivious Evaluation of Multivariate Polynomials, submitted for publication.

[3] C. de Boor, N. Dyn and A. Ron, Polynomial interpolation to data on flats in $\mathbb{R}^d$, *Journal of Approximation Theory*, 105 (2000), pp. 313-343.

[4] R.C. Bose, Mathematical theorey of the symmetrical factorial design, *Sankhyā*, 8 (1947), pp. 107-166.

[5] R.C. Bose, On some connections between the design of experiments and information theory, *Bull. Inst. Inter. Statist.*, 38 (1961), pp. 257-271.

[6] K.A. Bush, Orthogonal arrays of index unity, *Ann. Math. Stat.*, 23 (1952), pp. 426-434.

[7] L.R.A. Casse, A solution to Beniamino Segre's 'Problem $I_{r,q}$' for q even, *Atti. Accad. Naz. Lincei Rend.*, 46 (1969), pp. 13-20.

[8] S.B. Damelin, G. Michalski and G.L. Mullen, The cardinality of sets of k-independent vectors over finite fields, *Monatsh. Math.*, 150 (2007), pp. 289-295.

[9] S.B. Damelin, G. Michalski, G.L. Mullen and D. Stone, The number of linearly independent binary vectors with applications to the construction of hypercubes and orthogonal arrays, pseudo (t, m, s)-nets and linear codes, *Monatsh. Math.*, 141 (2004), pp. 277288.

[10] Y. Dodis, Space-time tradeoffs for graph properties, Master thesis, MIT (1998), http://theory.lcs.mit.edu/ yevgen/ps/thesis.ps .

[11] B.R. Gulati, On maximal (k, t)-sets, *Ann. Inst. Statist. Math.*, 23 (1971), pp. 527-529.

[12] R. Hill, *A First Course in Coding Theory*, Oxford Applied Mathematics and Computing Science Series, Clarendon Press, Oxford, 2002.

[13] J.W.P Hirschfeld, Maximum sets in finite projective spaces, Surveys in Combinatorics 1983, London Mathematical Society Lecture Note Series 82, Cambridge University Press, Cambridge 1983, pp. 55-76.

[14] J.W.P Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces, *J. Statist. Planning Infer.*, 72 (1998), pp. 355-380.

[15] J.W.P Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces: Update 2001, in *Finite Geometries, Developments in Mathematics*, Kluwer, Boston 2001, pp. 201-246.

[16] J.W.P Hirschfeld and T.A. Thas, *General Galois Geometries*, Oxford University Press, Oxford, 1991.

[17] S. Jaggi, P. Sanders, P.A. Chou, M. Effros, S. Egner, K. Jain and L.M.G.M. Tolhuizen, Polynomial time algorithms for multicast network code construction, *IEEE Transactions on Information Theory*, 51 (2005), pp. 1973-1982.

[18] R.R. Jurick, An algorithm for determining the largest maximally independent set of vectors from an r-dimensional space over a Galois field of n elements, *Tech. Rep. ASD-TR-68-40*, Air Force Systems Command, Wright-Patterson Air Force Base, Ohio.

[19] N. Kogan and T. Tassa, Improved efficiency for revocation schemes via Newton interpolation, *ACM Transactions on Information and System Security*, 9 (2006), pp. 461-486.

[20] I.G. Macdonald, *Symmetric functions and Hall polynomials*, Oxford, 1995.

[21] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library, Vol. 16, 1977.

[22] C. Maneri and R. Silverman, A vector space packing problem, *J. of Algebra*, 4 (1966), pp. 321-330.

[23] B. Qvist, Some remarks concerning curves of the second degree in a finite plane, *Ann. Acad. Sci. Fenn. Ser. A*, no. 134.

[24] C.R. Rao, Factorial experiments derivable from combinatorial arrangements of arrays, *J. Roy. Statis. Soc.*, Suppl. 9 (1947), pp. 128-139.

[25] B. Segre, Curve razionali normali e k-archi negli spazi finiti, *Ann. Mat. Pura Appl.*, 39 (1955), pp. 357-379.

[26] B. Segre, *Lectures on modern geometry*. Cremonese, Rome, 1961.

[27] E. Seiden, A theorem in finite projective geometry and an application to statistics, *Proc. Amer. Math. Soc.*, 1 (1950), pp. 282-286.

[28] A. Shamir, How to share a secret, *Communications of the ACM*, 22 (1979), pp. 612-613.

[29] R.C. Singleton, Maximum distance q-ary codes, *IEEE Trans. Info. Theory*, 10 (1964), pp. 116-118.

[30] I.N. Stewart and D.O. Tall, *Algebraic Number Theory, Second edition*, Chapman and Hall, New York (1987), pp. 104-107.

[31] G. Tallini, Le geometrie di Galois e le loro applicazioni alla statistica e alla teoria delle informazioni, *Rend. Mat. e Appl.*, 19 (1960), pp. 379-400.

[32] J.A. Thas, Normal rational curves and k-arcs in Galois spaces, *Rend. Mat.*, 1 (1968), pp. 331-334.