Nontrivial $t$-Designs over Finite Fields
Exist for All $t$

Arman Fazeli
University of California San Diego
9500 Gilman Drive, La Jolla, CA 92093
afazelic@ucsd.edu

Shachar Lovett
University of California San Diego
9500 Gilman Drive, La Jolla, CA 92093
slovett@ucsd.edu

Alexander Vardy
University of California San Diego
9500 Gilman Drive, La Jolla, CA 92093
avardy@ucsd.edu

June 11, 2013

Abstract

A $t$-$(n,k,\lambda)$ design over $\mathbb{F}_q$ is a collection of $k$-dimensional subspaces of $\mathbb{F}_q^n$, called blocks, such that each $t$-dimensional subspace of $\mathbb{F}_q^n$ is contained in exactly $\lambda$ blocks. Such $t$-designs over $\mathbb{F}_q$ are the $q$-anlogs of conventional combinatorial designs. Nontrivial $t$-$(n,k,\lambda)$ designs over $\mathbb{F}_q$ are currently known to exist only for $t \leq 3$. Herein, we prove that simple (meaning, without repeated blocks) nontrivial $t$-$(n,k,\lambda)$ designs over $\mathbb{F}_q$ exist for all $t$ and $q$, provided that $k > 12t$ and $n$ is sufficiently large. This may be regarded as a $q$-analog of the celebrated Teirlinck theorem for combinatorial designs.
1. Introduction

Let $X$ be a set with $n$ elements. A $t$-$(n, k, \lambda)$ combinatorial design (or $t$-design, in brief) is a collection of $k$-subsets of $X$, called blocks, such that each $t$-subset of $X$ is contained in exactly $\lambda$ blocks. A $t$-design is said to be simple if there are no repeated blocks — that is, all the $k$-subsets in the collection are distinct. A trivial $t$-design is the set of all $k$-subsets of $X$. The celebrated theorem of Teirlinck [20] establishes the existence of nontrivial simple $t$-designs for all $t$.

It was suggested by Tits [23] in 1957 that combinatorics of sets could be regarded as the limiting case $q \to 1$ of combinatorics of vector spaces over the finite field $\mathbb{F}_q$. Indeed, there is a strong analogy between subsets of a set and subspaces of a vector space, expounded by numerous authors [6, 9, 24]. In particular, the notion of $t$-designs has been extended to vector spaces by Cameron [4, 5] and Delsarte [7] in the early 1970s. Specifically, let $\mathbb{F}_q^n$ be a vector space of dimension $n$ over the finite field $\mathbb{F}_q$. Then a $t$-$(n, k, \lambda)$ design over $\mathbb{F}_q$ is a collection of $k$-dimensional subspaces of $\mathbb{F}_q^n$ (called blocks), such that each $t$-subspace of $\mathbb{F}_q^n$ is contained in exactly $\lambda$ blocks. Such $t$-designs over $\mathbb{F}_q$ are the $q$-analogs of conventional combinatorial designs. As for combinatorial designs, we will say that a $t$-design over $\mathbb{F}_q$ is simple if it does not have repeated blocks, and trivial if it is the set of all $k$-subspaces of $\mathbb{F}_q^n$.

The first examples of simple nontrivial $t$-designs over $\mathbb{F}_q$ with $t \geq 2$ were found by Thomas [21] in 1987. Today, following the work of many authors [3, 11, 15, 16, 18, 19, 22], numerous such examples are known. All these examples have $t = 2$ or $t = 3$. If repeated blocks are allowed, nontrivial $t$-designs over $\mathbb{F}_q$ exist for all $t$, as shown in [16]. However, no simple nontrivial $t$-designs over $\mathbb{F}_q$ are presently known for $t > 3$. Our main result is the following theorem.

**Theorem 1.** Simple nontrivial $t$-$(n, k, \lambda)$ designs over $\mathbb{F}_q$ exist for all $q$ and $t$, and all $k > 12(t+1)$ provided that $n \geq ckt$ for a large enough absolute constant $c$. Moreover, these $t$-$(n, k, \lambda)$ designs have at most $q^{12(t+1)n}$ blocks.

This theorem can be regarded as a $q$-analog of Teirlinck’s theorem [20] for combinatorial designs. Our proof of Theorem 1 is based on a new probabilistic technique introduced by Kuperberg, Lovett, and Peled in [12] to prove the existence of certain regular combinatorial structures. We note that this proof technique is purely existential: there is no known efficient algorithm which can produce $t$-$(n, k, \lambda)$ design over $\mathbb{F}_q$ for $t > 3$. Hence, we pose the following as an open problem:

**Design an efficient algorithm to produce simple nontrivial $t$-$(n, k, \lambda)$ designs for large $t$**  \(\ast\)

The rest of this paper is organized as follows. We begin with some preliminary definitions in the next section. We present the Kuperberg-Lovett-Peled (KLP) theorem of [12] in Section 3. In Section 4, we apply this theorem to prove the existence of simple $t$-designs over $\mathbb{F}_q$ for all $q$ and $t$. Detailed proofs of some of the technical lemmas are deferred to Section 5.
2. Preliminaries

Let $\mathbb{F}_q$ denote the finite field with $q$ elements, and let $\mathbb{F}_q^n$ be a vector space of dimension $n$ over $\mathbb{F}_q$. We recall some basic facts that relate to counting subspaces of $\mathbb{F}_q^n$. The number of distinct $k$-subspaces of $\mathbb{F}_q^n$ is given by the $q$-binomial (a.k.a. Gaussian) coefficient

$$\binom{n}{k}_q \equiv \frac{[n]_q!}{[k]_q! [n-k]_q!}$$

(1)

where $[n]_q!$ is the $q$-factorial defined by

$$[n]_q! \equiv [1]_q [2]_q \cdots [n]_q = (1+q)(1+q+q^2)\cdots(1+q+q^2+\cdots+q^n)$$

(2)

Observe the similarities between (1) and (2) and the conventional binomial coefficients and factorials, respectively. Many more similarities between the combinatorics of sets and combinatorics of vector spaces are known; see [10], for example. Here, all we need are upper and lower bounds on $q$-binomial coefficients, established in the following lemma.

Lemma 2.

$$q^k(n-k) \leq \binom{n}{k}_q \leq q^k(n-k)$$

Proof. We use the following identity from [10, p. 19],

$$\binom{n}{k}_q = \sum_{1 \leq s_1 < s_2 < \cdots < s_k \leq n} q^{(s_1+s_2+\cdots+s_k)-(k+1)/2}$$

(3)

The largest term in the sum of (3) is $q^{k(n-k)}$, which corresponds to $s_i = n-k+i$ for all $i$. The number of terms in the sum is $\binom{n}{k}$, and the lemma follows.

3. The KLP theorem

Kuperberg, Lovett, and Peled [12] developed a powerful probabilistic method to prove the existence of certain regular combinatorial structures, such as orthogonal arrays, combinatorial designs, and $t$-wise permutations. In this section, we describe their main theorem.

Let $M$ be a $|B| \times |A|$ matrix with integer entries, where $A$ and $B$ are the set of columns and the set of rows of $M$, respectively. We think of the elements of $A$, respectively $B$, as vectors in $\mathbb{Z}^B$, respectively in $\mathbb{Z}^A$. We are interested in those matrices $M$ that satisfy the five properties below.
1. **Constant vector.** There exists a rational linear combination of the columns of $M$ that produces the vector $(1, 1, \ldots, 1)^T$.

2. **Divisibility.** Let $\overline{b}$ denote the average of the rows of $M$, namely $\overline{b} = \frac{1}{|B|} \sum_{b \in B} b$. There is an integer $c_1 < |B|$ such that the vector $c_1 \overline{b}$ can be produced as an integer linear combination of the rows of $M$. The smallest such $c_1$ is called the divisibility parameter.

3. **Boundedness.** The absolute value of all the entries in $M$ is bounded by an integer $c_2$, which is called the boundedness parameter.

4. **Local decodability.** There exist a positive integer $m$ and an integer $c_3 \geq m$ such that, for every column $a \in A$, there is a vector of coefficients $\gamma^a = (\gamma_1^a, \gamma_2^a, \ldots, \gamma_{|B|}^a) \in \mathbb{Z}^B$ satisfying $\|\gamma^a\|_1 \leq c_3$ and $\sum_{b \in B} \gamma_b^a b = m e_a$, where $e_a \in \{0, 1\}^A$ is the vector with 1 in coordinate $a$ and 0 in all other coordinates. The parameter $c_3$ is called the local decodability parameter.

5. **Symmetry.** A symmetry of the matrix $M$ is a permutation of rows $\pi \in S_B$ for which there exists an invertible linear map $\ell : \mathbb{Q}^A \to \mathbb{Q}^A$ such that applying the permutation on rows and the linear map on columns does not change the matrix, namely $\ell(\pi(M)) = M$. The group of symmetries of $M$ is denoted by $\text{Sym}(M)$. It is required that this group acts transitively on $B$. That is, for all $b_1, b_2 \in B$ there exists a permutation $\pi \in \text{Sym}(M)$ satisfying $\pi(b_1) = b_2$.

The following theorem has been proved by Kuperberg, Lovett, and Peled in [12]. In fact, the results of Theorem 2.4 and Claim 3.2 of [12] are more general than Theorem 3 below. However, Theorem 3 will suffice for our purposes.

**Theorem 3.** Let $M$ be a $|B| \times |A|$ integer matrix satisfying the five properties above. Let $N$ be an integer divisible by $c_1$ such that

$$c_1 |A|^{52/5} c_2 c_3^{12/5} \log(\frac{|A|}{c_2})^8 \leq N < |B|$$

where $c > 0$ is a sufficiently large absolute constant. Then there exists a set of rows $T \subset B$ of size $|T| = N$ such that the average of the rows in $T$ is equal to the average of all the rows in $M$, namely

$$\frac{1}{N} \sum_{b \in T} b = \frac{1}{|B|} \sum_{b \in B} b = \overline{b}$$

4. **Proof of the main result**

We will apply Theorem 3 to prove existence of designs over finite fields. We first introduce the appropriate matrix $M$, which is the incidence matrix of $t$-subspaces and $k$-subspaces.
Let $M$ be a $|B| \times |A|$ matrix, whose columns $A$ and rows $B$ correspond to the $t$-subspaces and the $k$-subspaces of $\mathbb{F}_q^n$, respectively. Thus $|A| = \binom{n}{t} q$ and $|B| = \binom{n}{k} q$. The entries of $M$ are defined by $M_{b,a} = 1_{a \subset b}$. It is easy to see that a simple $t$-$(n,k,\lambda)$ design over $\mathbb{F}_q$ corresponds to a set of rows $b_1, b_2, \ldots, b_N$ of $M$ such that

$$b_1 + b_2 + \cdots + b_N = (\lambda, \lambda, \ldots, \lambda) \quad \text{for some } \lambda \in \mathbb{N}$$

(6)

Note that this implies $\lambda \frac{n}{t} q = N \frac{k}{t} q$, because each row $b \in B$ has Hamming weight $\frac{k}{t} q$. In order to relate (6) to Theorem 3, we need the following simple lemma. The lemma is well known; we include a brief proof for completeness.

**Lemma 4.** Let $V$ be a $t$-subspace of $\mathbb{F}_q^n$. The number of $k$-subspaces $U$ such that $V \subset U \subset \mathbb{F}_q^n$ is given by $\binom{n-t}{k-t} q$.

**Proof.** Fix a basis $\{v_1, v_2, \ldots, v_t\}$ for $V$. We extend this basis to a basis $\{v_1, v_2, \ldots, v_k\}$ for $U$. The number of ways to do so is $(q^n - q^t)(q^n - q^{t+1}) \cdots (q^n - q^{k-1})$. However, each subspace $U$ that contains $V$ is counted $(q^k - q^t)(q^k - q^{t+1}) \cdots (q^k - q^{k-1})$ times in the above expression.

It follows from Lemma 4 that

$$\bar{b} = \frac{1}{|B|} \sum_{b \in B} b = \frac{\binom{n-t}{k-t}}{\binom{n}{k} q} (1,1,\ldots,1) = \frac{\binom{k}{t} q}{\binom{n}{t} q} (1,1,\ldots,1)$$

(7)

Therefore, a simple nontrivial $t$-$(n,k,\lambda)$ design over $\mathbb{F}_q$ is a set of $N < |B|$ rows of $M$ satisfying

$$b_1 + b_2 + \cdots + b_N = N \bar{b}$$

But this is precisely the guarantee provided by Theorem 3 in (5). Note that the corresponding value of $\lambda = N \frac{k}{t} q / \binom{n}{t} q$ would be generally quite large.

### 4.1. Parameters for the KLP theorem

Let us now verify that the matrix $M$ satisfies the five conditions in Theorem 3 and estimate the relevant parameters $c_1, c_2, c_3$ in (4).

**Constant vector.** Each $k$-subspace contains exactly $\binom{k}{t} q$ $t$-subspaces, so the sum of all the columns of $M$ is $\binom{k}{t} q (1, \ldots, 1)^T$. Hence $(1,1,\ldots,1)^T$ is a rational linear combination of the columns of $M$. 
Symmetry. An invertible linear transformation $L : \mathbb{F}_q^n \to \mathbb{F}_q^m$ acts on the set of $k$-subspaces by mapping $U = \langle v_1, v_2, \ldots, v_k \rangle$ to $L(U) = \langle L(v_1), L(v_2) \ldots, L(v_k) \rangle$. It acts on the set of $t$-subspaces in the same way. Note that if $U$ is a $k$-subspace and $V$ is a $t$-subspace, then $V \subset U$ if and only if $L(V) \subset L(U)$. Now, let $\pi_L \in S_B$ be the permutation of rows of $M$ induced by $L$, and let $\sigma_L \in S_A$ be the permutation of columns of $M$ induced by $L$. Then $\pi_L(\sigma_L(M)) = M$. Note that $\sigma_L$ acts as an invertible linear map on $Q^A$ by permuting the coordinates. Hence, $\pi_L$ is a symmetry of $M$. The corresponding symmetry group is, in fact, the general linear group $GL(n, q)$. It is well known that $GL(n, q)$ is transitive: for any two $k$-subspaces $U_1, U_2$, we can find an invertible linear transformation $L$ such that $L(U_1) = U_2$, which implies $\pi_L(b_1) = b_2$ for the corresponding rows.

Boundedness. Since all entries of $M$ are either 0 or 1, we can set $c_2 = 1$.

Local decodability. Let $m$ be a positive integer to be determined later. Fix a $t$-subspace $V$ corresponding to a column of $M$. We wish to find a short integer combination of rows of $M$ summing to $m e_V$. In order to do so, we fix an arbitrary $(t + k)$-subspace $W$ that contains $V$. As part of the short integer combination, we will only choose those rows that correspond to the $k$-subspaces contained in $W$. Moreover, the integer coefficient for a $k$-subspace $U \subset W$ will depend only on the dimension $j = \dim(U \cap V)$. We denote this coefficient by $f_{k,t}(j)$.

We need the following conditions to hold. First, by Lemma $4$ there are $\binom{k}{k-t} q$ $k$-subspaces $U$ such that $V \subset U \subset W$. Therefore, we need

$$f_{k,t}(t) \binom{k}{k-t} q = m$$

(8)

Second, for any other $t$-subspace $V' \subset \mathbb{F}_q^m$, we need that

$$\sum_{V' \subset U \subset W} f_{k,t}(\dim(U \cap V)) = 0$$

(9)

where the sum is over all $k$-subspaces $U$ containing $V'$ and contained in $W$. Note that we only need to consider those $t$-subspaces $V'$ that are contained in $W$. For all other $t$-subspaces, our integer combination of rows of $M$ produces zero by construction.

The following lemma counts the number of $k$-subspaces which contain $V'$ and whose intersection with $V$ has a prescribed dimension. Its proof is deferred to Section $5$.

Lemma 5. Let $V_1, V_2$ be two distinct $t$-subspaces of $\mathbb{F}_q^n$ such that $\dim(V_1 \cap V_2) = l$ for some $l$ in $\{0, 1, \ldots, t-1\}$. The number of $k$-subspaces $U \subset \mathbb{F}_q^m$ such that $V_1 \subset U$ and $\dim(U \cap V_2) = j$, for some $j \in \{l, l+1, \ldots, t\}$, is given by

$$q^{(k-t-j+l)(t-j)} \binom{t-l}{j-l} q^{n-2t+l} \binom{k-t-j+l}{j-l} q$$

(10)
With the help of Lemma 5, we can rephrase (9) as the following set of $t$ linear equations:

$$\sum_{j=1}^{t} f_{k,t}(j) \left[ \begin{array}{c} t-l \\ t-j \end{array} \right] q^{(k-t-j+l)(t-j)} = 0 \quad \text{for } l = 0, 1, \ldots, t-1 \quad (11)$$

Equations (8) and (11) together form a set of $t+1$ linear equations, which can be represented in the form of a matrix production:

$$Df = (0, 0, \ldots, 0, m)^T \quad (12)$$

where $f = (f_{k,t}(0), f_{k,t}(1), \ldots, f_{k,t}(t))^T$ and $D$ is an upper-triangular $(t+1) \times (t+1)$ matrix with entries

$$d_{l,j} = \left[ \begin{array}{c} t-l \\ t-j \end{array} \right] q^{(k-t-j+l)(t-j)} \quad \text{for } 0 \leq l \leq j \leq t \quad (13)$$

The condition $t \leq k$ ensures nonzero values on the main diagonal. Therefore, $\det D$ is nonzero and the system of linear equations is solvable. By Cramer’s rule, we have

$$f_{k,t}(j) = \frac{\det D_j}{\det D} m \quad (14)$$

where $D_j$ is the matrix formed by replacing the $j$-th column of $D$ by the vector $(0, 0, \ldots, 1)^T$. Note that $\det D$ is an integer. Thus we set $m = \det D$, so that $f_{k,t}(j) = \det D_j$. This guarantees that the coefficients $f_{k,t}(0), f_{k,t}(1), \ldots, f_{k,t}(t)$ are integers.

We are now in a position to establish a bound on the local decodability parameter $c_3$. First, the following lemma bounds the determinants of $D$ and $D_j$. We defer its proof to Section 5.

**Lemma 6.**

$$|\det D| \leq q^{k(t+1)^2}$$

$$|\det D_j| \leq q^{k(t+1)^2} \quad \text{for } j = 0, 1, \ldots, t$$

The number of $k$-subspaces $U$ contained in $W$ is $\binom{k+t}{k}_q$. We have multiplied the row of $M$ corresponding to each such subspace by a coefficient $f_{k,t}(j)$ which is bounded by $q^{k(t+1)^2}$. Hence

$$c_3 = \max\{m, ||f||_1\} \leq \binom{k+t}{k}_q q^{k(t+1)^2} \leq \binom{k+t}{k} q^{k(t+1)^2} q^{k(t+1)^2} \leq q^{2k(t+1)^2} \quad (15)$$

**Divisibility.** The proof of local decodability also makes it possible to establish a bound on the divisibility parameter $c_1$. We already know that for $m = \det D$, we can represent any element in $mZ^A$ as an integer combination of rows of $M$. By (7), we have $\binom{n}{t}_q \overline{b} = \binom{k}{t}_q (1, 1, \ldots, 1)$. Hence, $m\binom{n}{t}_q \overline{b} \in mZ^A$ can be expressed as an integer combination of rows of $M$. It follows that

$$c_1 \leq m \binom{n}{t}_q \leq q^{k(t+1)^2} \binom{n}{t} q^{t(n-t)} \leq q^{k(t+1)^2+t(n-t)+n} \quad (16)$$
4.2. Putting it all together

We have proved that the incidence matrix $M$ satisfies the five conditions in Theorem 3, and established the following bounds on the parameters:

\begin{align*}
    c_1 &\leq q^{k(t+1)^2 + t(n-t)+n} \\
    c_2 &= 1 \\
    c_3 &\leq q^{2k(t+1)^2}
\end{align*}

By Lemma 2, we also have

\begin{align*}
    |A| &= \left[\begin{array}{c} n \\ t \end{array}\right]_q \leq \left[\begin{array}{c} n \\ t \end{array}\right] q^{t(n-t)} \leq q^{t(n-t)+n} \quad (17) \\
    |B| &= \left[\begin{array}{c} n \\ k \end{array}\right]_q \geq q^{k(n-k)} \quad (18)
\end{align*}

Combining (4) with (17) – (20), we see that the lower bound on $N$ in Theorem 3 is at most

\begin{equation}
    c' |A|^{52/5} c_1^2 c_2 c_3^{12/5} \log(|A| c_2)^8 \leq c q^{(57/5)(t+1)n + ckt^2} n^c \quad (22)
\end{equation}

for some absolute constant $c > 0$. If we fix $t$ and $k$, while making $n$ large enough, then the right-hand side of (22) is bounded by $c q^{12(t+1)n}$. In view of (21), this is strictly less than $|B|$ whenever $k > 12(t+1)$ and $n$ is large enough. It now follows from Theorem 3 that for large enough $n$, there exists a simple $t$-$(n, k, \lambda)$-design over $\mathbb{F}_q$ of size $N \leq c q^{12n(t+1)}$. The reader can verify that this holds whenever $n \geq \tilde{c} kt$ for a large enough constant $\tilde{c} > 0$.

5. Proof of the technical lemmas

In this section, we prove the two technical lemmas (Lemma 5 and Lemma 6) we have used to establish the local decodability property.

5.1. Proof of Lemma 5

Let $V_1, V_2$ be two distinct $t$-subspaces of $\mathbb{F}_q^n$ with $\dim(V_1 \cap V_2) = l$. Let $U$ be a $k$-subspace of $\mathbb{F}_q^n$ such that $V_1 \subset U$ and $\dim(U \cap V_2) = j$. Further, let $X = V_1 \cap V_2$ and $Y = V_1 + V_2$. It is not difficult to show that the following holds:

\begin{align*}
    \dim(X) &= l \\
    \dim(Y) &= 2t - l \\
    \dim(U \cap V_1) &= t \\
    \dim(U \cap V_2) &= j \\
    \dim(U \cap X) &= l \\
    \dim(U \cap Y) &= t + j - l
\end{align*}

(23)
We will proceed in three steps. First, fix a basis \{v_1, v_2, \ldots, v_l\} for \(V_1\). Next, we extend \(V_1\) to the subspace \(Z = U \cap Y\) which has an intersection of dimension \(j\) with \(V_2\). In order to do that, we pick \(j - l\) vectors \(v_{l+1}, v_{l+2}, \ldots, v_{l+j-l}\) from \(Y \setminus V_1\), in such a way that \(v_1, v_2, \ldots, v_{l+j-l}\) are linearly independent. The number of ways to do so is

\[
N_1 = \prod_{i=0}^{j-l-1} \left( q^{2j-l} - q^{l+i} \right)
\]  

(24)

However, each such subspace \(Z\) is counted more than once in (24), since there are many different ordered bases for \(Z\). The appropriate normalizing factor is \(N_2 = \prod_{i=0}^{j-l-1} (q^{i+j-l} - q^{l+i})\). Hence, the total number of different choices for \(Z\) is

\[
\frac{N_1}{N_2} = \prod_{i=0}^{j-l-1} \frac{q^{2j-l} - q^{l+i}}{q^{i+j-l} - q^{l+i}} = \prod_{i=0}^{j-l-1} \frac{q^{l+i} - q^i}{q^{l-i} - q^i} = \left[ \frac{t}{j} \right]_q
\]

(25)

In order to complete \(U\), we need to extend \(Z\) by \(k - (t + j - l)\) linearly independent vectors chosen from \(\mathbb{F}_q^n \setminus Y\). The number of ways to do so is \(N_3 = \prod_{i=0}^{k-(t+j-l)-1} (q^n - q^{2(t-l)+i})\), with normalizing factor \(N_4 = \prod_{i=0}^{k-(t+j-l)-1} (q^i - q^{(t+j-l)+i})\). We have

\[
\frac{N_3}{N_4} = \prod_{i=0}^{k-(t+j-l)-1} \frac{q^{2(t-l)+i}}{q^{(t+j-l)+i}} \cdot \frac{q^n - q^{(2t-l)-i} - 1}{q^{(k-(t+j-l)-i)} - 1} = q^{(k-t-j+l)(t-j)} \left[ \frac{n - 2t + l}{k - (t + j - l)} \right]_q
\]

(26)

Combining (25) and (26), the total number of different choices for the desired subspace \(U\) is given by (10), as claimed.

### 5.2. Proof of Lemma 6

Lemma 6 follows from the following two lemmas. The first bounds the product of the largest elements in each row. The second bounds the number of nonzero generalized diagonals in \(D_j\) — that is, the number of permutations \(\pi \in S_{t+1}\) such that \((D_j)_{i, \pi(i)} \neq 0\) for all \(i \in \{0, 1, \ldots, t\}\).

**Lemma 7.**

\[
\prod_{l=0}^{t} \max_{j} d_{l,j} \leq 2^{k(t+1)+1} q^{(k-t)l(t+1)}
\]

**Proof.** We first argue that for \(l \in \{1, 2, \ldots, t\}\), the largest element in row \(l\) is \(d_{l,l}\). For \(l = 0\), the largest element in the row is either \(d_{0,0}\) or \(d_{0,1}\). To see that, we calculate
\[
\frac{d_{l,j+1}}{d_{l,j}} = \frac{[t-l]_q}{[t-j-1]_q} \cdot \frac{[k-t+l]_q}{[k-t]_q} \cdot q^{(k-t-j+l-1)(t-j)-k-t-j+l(t-j)}
\]

\[
= \frac{[t-j]q^*[j-l]_q!}{[t-j-1]q^*[j-l+1]_q!} \cdot \frac{[j]q^*[k-t+l-j]_q!}{[j+1]q^*[k-t+l-j-1]_q!} \cdot q^{1-(t-j)-(k-t-j+l)}
\]

\[
= \frac{q^{t-j-1}}{q^{t-l+1-1}} \cdot \frac{q^{k-t+j-l-1}}{q^{t+1-1}} \cdot \frac{q}{(q^{j+1-1})(q^{j-l+1-1})}
\]

\[
< \frac{q}{(q^{j+1-1})(q^{j-l+1-1})}
\]

Note that unless \( j = l = 0 \), this implies that \( d_{l,j+1} < d_{l,j} \). The only remaining case is \( d_{0,1}/d_{0,0} < q/(q-1)^2 \). This ratio can be at most 2 for \( q = 2 \), and is below 1 for \( q > 2 \). Hence

\[
\prod_{l=0}^{t} \max_j d_{l,j} \leq 2 \prod_{j=0}^{t} d_{j,j}
\]

We next bound this product:

\[
\prod_{j=0}^{t} d_{j,j} = \prod_{j=0}^{t} \left[ \frac{k-t+j}{j} \right] q^{(k-t)(t-j)} \leq \prod_{j=0}^{t} \left( \frac{k-t+j}{j} \right) q^{(k-t)j+(k-t)(t-j)} \leq 2^{k(t+1)}q^{(k-t)t(t+1)}
\]

Lemma 8. \( D_j \) has at most \( 2^t \) nonzero generalized diagonals.

Proof. Let \( \pi \in S_n \) be such that \( (D_j)_{i,\pi(i)} \neq 0 \) for all \( i \). If \( j > 0 \) then we must have \( \pi(i) = i \) for all \( i < j \), and \( \pi(t) = j \). Letting \( r = t-j \) this reduces to the following problem: let \( R \) be an \( r \times r \) matrix corresponding to rows \( j, \ldots, t-1 \) and columns \( j+1, \ldots, t \) of \( D_j \). This matrix has entries \( r_{i,j} \neq 0 \) only for \( j \geq l-1 \). We lemma that such matrices have at most \( 2^t \) nonzero generalized diagonals. We show this by induction on \( r \). Let us index the rows and columns of \( R \) by \( 1, \ldots, r \). To get a nonzero generalized diagonal we must have \( \pi(r) = r-1 \) or \( \pi(r) = r \). In both cases, if we delete the \( r \)-th row and the \( \pi(r) \)-th column of \( R \), one can verify that we get an \( (r-1) \times (r-1) \) matrix of the same form (e.g. zero values in coordinates \( (l,j) \)) whenever \( j < l-1 \). The lemma now follows by induction.

Proof of Lemma 6. The determinant of \( D \) or \( D_j \) is bounded by the number of nonzero generalized diagonals (which is 1 for \( D \), and at most \( 2^t \) for \( D_j \)), multiplied by the maximal value a product of choosing one element per row can take. Hence, it is bounded by

\[
\max\{|\det D|, |\det D_j|\} \leq 2^t \cdot 2^{k(t+1)+1} q^{(k-t)t(t+1)} \leq q^{t+k(t+1)+1+(k-t)t(t+1)} \leq q^k(t+1)^2
\]
Acknowledgment

We are grateful to Michael Braun and Alfred Wasserman for helpful discussions regarding the history and the current state of knowledge about $t$-designs over finite fields.

References

[1] R. Ahlswede, H.K. Aydinian, and L.H. Khachatrian, On perfect codes and related concepts, Des. Codes Cryptogr. 22 (2001), 221–237.

[2] A. Beutelspacher, Parallelismen in unendlichen projektiven Raumen endlicher Dimension, Geom. Dedicata 7 (1978), 499–506.

[3] M. Braun, A. Kerber, and R. Laue, Systematic construction of $q$-analogs of designs, Des. Codes Cryptogr. 34 (2005), 55–70.

[4] P. Cameron, Generalisation of Fisher’s inequality to fields with more than one element, in T.P. McDonough and V.C. Mavron, Eds., Combinatorics, London Math. Soc. Lecture Note Ser. 13, Cambridge: Cambridge Univ. Press, 1974, pp. 9–13.

[5] P. Cameron, Locally symmetric designs, Geom. Dedicata 3 (1974), 65–76.

[6] H. Cohn, Projective geometry over $\mathbb{F}_1$ and the Gaussian binomial coefficients, Amer. Math. Monthly 111 (2004), 487–495.

[7] Ph. Delsarte, Association schemes and $t$-designs in regular semilattices, J. Combin. Theory Ser. A 20 (1976), 230–243.

[8] T. Etzion and A. Vardy, On $q$-analogs for Steiner systems and covering designs, Adv. Math. Commun. 5 (2011), 161–176.

[9] J.R. Goldman and G.-C. Rota, On the foundations of combinatorial theory IV: Finite vector spaces and Eulerian generating functions, Stud. Appl. Math. 49 (1970), 239–258.

[10] V. Kac and P. Cheung, Quantum Calculus, New York: Springer-Verlag, 2001.

[11] A. Kohnert, P.R.J. Östergård, and A. Wassermann, Designs and partial geometries over finite fields, arXiv:1305.1455v1, May 2013.
[12] G. KUPERBERG, SH. LOVETT, and R. PLED, Probabilistic existence of regular combinatorial structures, arXiv:1302.4295, February 2013, also in Proc. 44-th ACM Symp. Theory of Computing (STOC), New York, May 2012, pp. 1091–1106.

[13] J.H. VAN LINT and R.M. WILSON, A Course in Combinatorics, 2nd ed., Cambridge Univ. Press, Cambridge, 2001.

[14] K. METSCH, Bose-Burton type theorems for finite projective, affine and polar spaces, in J.D. LAMB and D.A. PREECE, Eds., Surveys in Combinatorics, 1999, London Math. Soc. Lecture Note Ser. 267, Cambridge Univ. Press, Cambridge, 1999, pp. 137–166.

[15] M. MIYAKAWA, A. MUNEMASA, and S. YOSHIARA, On a class of small 2-designs over GF(q), J. Combin. Des. 3 (1995), 61–77.

[16] D.K. RAY-CHAUDHURI and N.M. SINGHI, q-analogues of t-designs and their existence, Linear Algebra Appl. 114/115 (1989), 57–68.

[17] M. SCHWARTZ and T. ETZION, Codes and anticodes in the Grassmann graph, J. Combin. Theory Ser. A 97 (2002), 27–42.

[18] H. SUZUKI, 2-designs over GF(2^m), Graphs Combin. 6 (1990), 293–296.

[19] H. SUZUKI, 2-designs over GF(q), Graphs Combin. 8 (1992), 381–389.

[20] L. TEIRLINCK, Non-trivial t-designs without repeated blocks exist for all t, Discrete Math. 65 (1987), 301–311.

[21] S. THOMAS, Designs over finite fields, Geom. Dedicata 21 (1987), 237–242.

[22] S. THOMAS, Large Sets of t-Designs over Finite Fields, Geom. Dedicata 63 (1996), 247–253.

[23] J. TITS, Sur les analogues algébriques des groupes semi-simples complexes, in Colloque d’Algèbre Supérieure, tenu á Bruxelles du 19 au 22 décembre 1956, Centre Belge de Recherches Mathématiques Établissements Ceuterick, Louvain, Paris: Librairie Gauthier-Villars, 1957, pp. 261–289.

[24] J. WANG, Quotient sets and subset-subspace analogy, Adv. Appl. Math. 23 (1999), 333–339.