Thresholds in the Lattice of Subspaces of $\mathbb{F}_q^n$

Benjamin Rossman

Duke University, Durham NC 27708, USA
benjamin.rossman@duke.edu

Abstract. Let Q be an ideal (downward-closed set) in the lattice of linear subspaces of $\mathbb{F}_q^n$, ordered by inclusion. For $0 \leqslant k \leqslant n$, let $\mu_k(Q)$ denote the fraction of k-dimensional subspaces that belong to Q. We show that these densities satisfy

$$\mu_k(Q) = \frac{1}{1+z} \quad \Longrightarrow \quad \mu_{k+1}(Q) \leqslant \frac{1}{1+qz}.$$

This implies a sharp threshold theorem: if $\mu_k(Q) \leqslant 1-\varepsilon$, then $\mu_\ell(Q) \leqslant \varepsilon$ for $\ell = k + O(\log_q(1/\varepsilon))$.

1 Introduction

Let $\mathcal{L}_q(n)$ be the lattice of linear subspaces of $\mathbb{F}_q^n$, ordered by inclusion. Let Q be a nontrivial ideal in $\mathcal{L}_q(n)$ (that is, a nonempty proper subset of $\mathcal{L}_q(n)$ such that $A \in Q$ implies $B \in Q$ for all $B \subset A$). For $0 \leqslant k \leqslant n$, let $\mu_k(Q)$ denote the fraction of k-dimensional subspaces that belong to Q. Densities $\mu_k(Q)$ are known to be non-increasing: thus,

$$1 = \mu_0(Q) \geqslant \cdots \geqslant \mu_{t-1}(Q) \geqslant 1/2 > \mu_t(Q) \geqslant \cdots \geqslant \mu_n(Q) = 0$$

for a unique t. This paper addresses the question: How quickly must $\mu_k(Q)$ transition from $1-o(1)$ to $o(1)$?

It follows from known results (described in §2) that

$$\mu_{\lfloor (t-1)/c \rfloor}(Q) \geqslant 2^{-1/c} \quad \text{and} \quad \mu_{\lceil ct \rceil}(Q) \leqslant 2^{-c}$$

for all $c \geqslant 1$. This is the q-analog of the Bollobás-Thomason Theorem [3], which speaks of ideals in the boolean lattice $\mathcal{P}(n)$ of subsets of $\{1, \ldots, n\}$.

On the one hand, $\mathcal{L}_q(n)$ is the q-analog of $\mathcal{P}(n)$; on the other hand, it is a sub-lattice of $\mathcal{P}(q^n)$. This raises the question: Do k-subspace densities of ideals in $\mathcal{L}_q(n)$ scale like k-subset densities in $\mathcal{P}(n)$ or like q^k-subset densities in $\mathcal{P}(q^n)$? Quantitatively, the latter suggests we should expect that

$$\mu_{t-1-c}(Q) \geqslant 1 - q^{-c} \quad \text{and} \quad \mu_{t+c}(Q) \leqslant q^{-c}.$$

for all integers $c \geqslant 1$. This is precisely what we show.

Our main result actually concerns shadows in the subspace lattice. Let $\mathcal{L}_q(n,k)$ denote the set of k-dimensional subspaces of $\mathbb{F}_q^n$. For $1 \leqslant k \leqslant n$ and $S \subseteq \mathcal{L}_q(n,k)$, the *shadow* of S is the set $\triangle S \subseteq \mathcal{L}_q(n,k-1)$ defined by $\triangle S := \{B \in L_{n,k-1} : \exists A \in S,\ A \subset B\}$. We show:

Theorem 1 *For all $1 \leqslant k \leqslant n$ and $S \subseteq \mathcal{L}_q(n,k)$, if $\mu_k(S) = (1+z)^{-1}$ where $z \in \mathbb{R}_{\geqslant 0}$, then*

$$\mu_{k-1}(\triangle S) \geqslant \left(1 + \frac{q(q^{k-1}-1)(q^{n-k}-1)}{(q^k-1)(q^{n-k+1}-1)} \cdot z\right)^{-1} \geqslant \left(1 + \frac{z}{q}\right)^{-1}.$$

The first inequality in Theorem 1 is tight in two cases:

- when S is the set of k-dimensional subspaces of a fixed $n-1$-dimensional space ($z = \frac{q^n - q^{n-k}}{q^{n-k}-1}$), as well as
- when S is the set of k-dimensional subspaces not containing a fixed 1-dimensional space ($z = \frac{q^k-1}{q^n-q^k}$).

For values of z between $\frac{q^k-1}{q^n-q^k}$ and $\frac{q^n-q^{n-k}}{q^{n-k}-1}$, Theorem 2 improves the lower bound on $\mu_{k-1}(\triangle S)$ given by a q-analog of the Kruskal-Katona Theorem due to Chowdhury and Patkós [5].

A sharp threshold theorem for $\mathcal{L}_q(n)$ follows immediately from Theorem 1 and the observation that $\triangle(Q \cap \mathcal{L}_q(n,k)) \subseteq Q \cap \mathcal{L}_q(n,k-1)$ for ideals Q.

Theorem 2 *For every ideal Q in $\mathcal{L}_q(n)$ and $1 \leqslant k \leqslant n-1$, if $\mu_k(Q) = (1+z)^{-1}$, then $\mu_{k-1}(Q) \geqslant (1+(z/q))^{-1}$ and $\mu_{k+1}(Q) \leqslant (1+qz)^{-1}$. As a consequence, if $\mu_k(Q) \leqslant 1-\varepsilon$, then $\mu_\ell(Q) \leqslant \varepsilon$ for $\ell = k + O(\log_q(1/\varepsilon))$.*

The rest of the paper is organized as follows. In §2 we describe the previous q-analogs of the Kruskal-Katona and Bollobás-Thomason Theorems and their dual versions. In §3 we prove Theorem 1 using well-known tools (the Expander Mixing Lemma and bounds on the eigenvalues of Grassmann graphs). In §4 we discuss the tightness of the results. Finally, in §5 we give an application of Theorem 2 to a problem in query complexity.

2 q-Analogs of Kruskal-Katona and Bollobás-Thomason

For $x \in \mathbb{R}_{\geqslant 0}$, let $[x]_q := \frac{q^x-1}{q-1}$. The (Gaussian) q-binomial coefficient $\begin{bmatrix} x \\ k \end{bmatrix}_q$ is defined by

$$\begin{bmatrix} x \\ k \end{bmatrix}_q := \prod_{i=0}^{k-1} \frac{[x-i]_q}{[k-i]_q}.$$

Note that $[0]_q = 0$ and $[1]_q = 1$ and $|\mathcal{L}_q(n,k)| = \begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q$ for integers $n \geqslant k$.

Chowdhury and Patkós [5] proved a q-analog the Kruskal-Katona Theorem [8, 11], specifically a version due Keevash [10]. (See [15] for an alternative proof.)

Theorem 3 (q-Kruskal-Katona) *For all $1 \leqslant k \leqslant n$ and $S \subseteq \mathcal{L}_q(n,k)$, if $|S| = \begin{bmatrix} x \\ k \end{bmatrix}_q$, then $|\triangle S| \geqslant \begin{bmatrix} x \\ k-1 \end{bmatrix}_q$. Moreover, this bound is tight when S is the set of k-dimensional subspaces of a fixed ℓ-dimensional space where $k \leqslant \ell \leqslant n$.*

Note that the parameter n (the dimension of the ambient vector space) plays no role in this bound, in contrast to Theorem 1. It turns out Theorem 3 is slack when $n-1 < x < n$; this is precisely where Theorem 1 gives an improvement (as we discuss in §4).

Combining Theorem 3 with the inequality $(\begin{bmatrix} x \\ k-1 \end{bmatrix}_q / \begin{bmatrix} n \\ k-1 \end{bmatrix}_q)^k \geqslant (\begin{bmatrix} x \\ k \end{bmatrix}_q / \begin{bmatrix} n \\ k \end{bmatrix}_q)^{k-1}$ for all $k \leqslant x \leqslant n$, we have the following q-analog of the Bollobás-Thomason Theorem [3] for the boolean lattice $\mathcal{P}(n)$.

Theorem 4 (q-Bollobás-Thomason) *For every ideal Q in $\mathcal{L}_q(n)$,*

$$\mu_1(Q) \geqslant \mu_2(Q)^{1/2} \geqslant \mu_3(Q)^{1/3} \geqslant \cdots \geqslant \mu_n(Q)^{1/n}.$$

In particular, if $\mu_{t-1}(Q) \geqslant 1/2 > \mu_t(Q)$, then $\mu_{\lfloor (t-1)/c \rfloor}(Q) \geqslant 2^{-1/c}$ and $\mu_{\lceil ct \rceil}(Q) \leqslant 2^{-c}$ for all $c \geqslant 1$.

If we regard Q as a sequence of ideals in $\mathcal{L}_q(n)$, one for each n, then Theorem 4 implies that every nontrivial Q has a *threshold function* $t(n)$, meaning that $\mu_{k(n)}(Q) = 1 - o(1)$ for all $k(n) = o(t(n))$ and $\mu_{\ell(n)}(Q) = o(1)$ for all $\ell(n) = \omega(t(n))$. In the boolean lattice $\mathcal{P}(n)$, nothing more can be said in general, although certain classes of ideals in $\mathcal{P}(n)$, such as monotone graph properties when $n = \binom{m}{2}$, are known to have *sharp thresholds* such that $\mu_{k(n)}(Q) = 1 - o(1)$ and $\mu_{\ell(n)}(Q) = o(1)$ for some $k(n) = t(n) - o(t(n))$ and $\ell(n) = t(n) + o(t(n))$ (see [6]). In the same sense, Theorem 2 shows that every sequence of nontrivial ideals in $\mathcal{L}_q(n)$ has a sharp threshold.

2.1 Dual versions of Theorems 3 and 4

For a subspace A of $\mathbb{F}_q^n$, the orthogonal complement is defined by

$$A^\perp := \{b \in \mathbb{F}_q^n : \sum_{i=1}^n a_i b_i = 0 \text{ for all } a \in A\}.$$

Note that $\dim(A^\perp) = n - \dim(A)$ and $(A^\perp)^\perp = A$ and $B \subseteq A \Longrightarrow A^\perp \subseteq B^\perp$.

For every ideal Q in $\mathcal{L}_q(n)$, there is a dual ideal $Q^* := \{A \in \mathcal{L}_q(n) : A^\perp \notin Q\}$ satisfying $\mu_k(Q^*) = 1 - \mu_{n-k}(Q)$. Applying Theorem 4 to Q^* yields:

Theorem 5 (Dual q-Bollobás-Thomason) *For every ideal Q in $\mathcal{L}_q(n)$,*

$$1 - \mu_{n-1}(Q) \geqslant (1 - \mu_{n-2}(Q))^{1/2} \geqslant (1 - \mu_{n-3}(Q))^{1/3} \geqslant \cdots \geqslant (1 - \mu_0(Q))^{1/n}.$$

In particular, $\mu_{\lfloor c(t-1)+(1-c)n \rfloor}(Q) \geqslant 1 - 2^{-c}$ and $\mu_{\lceil t/c+(1-1/c)n \rceil}(Q) \leqslant 1 - 2^{-1/c}$ for all $c \geqslant 1$. (This improves Theorem 4 when $t \geqslant n/2$.)

Similarly, there is a dual version of Theorem 3. It may be helpful to include the proof, since we will use a similar argument in §3.

Theorem 6 (Dual q-Kruskal-Katona) *For all $1 \leqslant k \leqslant n$ and $n - k + 1 \leqslant y \leqslant n$ and $S \subseteq \mathcal{L}_q(n,k)$, if $|S| = \begin{bmatrix} n \\ k \end{bmatrix}_q - \begin{bmatrix} y \\ n-k \end{bmatrix}_q$, then $|\triangle S| \geqslant \begin{bmatrix} n \\ k-1 \end{bmatrix}_q - \begin{bmatrix} y \\ n-k+1 \end{bmatrix}_q$.*

Proof. We will assume $|\triangle S| < \begin{bmatrix} n \\ k-1 \end{bmatrix}_q - \begin{bmatrix} y \\ n-k+1 \end{bmatrix}_q$ and prove that $|S| < \begin{bmatrix} n \\ k \end{bmatrix}_q - \begin{bmatrix} y \\ n-k \end{bmatrix}_q$. Define $T \subseteq \mathcal{L}_q(n, n-k+1)$ by

$$T := \{B^\perp : B \in \mathcal{L}_q(n, k-1) \setminus \triangle S\}.$$

Note that $|T| = \begin{bmatrix} n \\ k-1 \end{bmatrix}_q - |\triangle S| = \begin{bmatrix} y \\ n-k+1 \end{bmatrix}_q$. Therefore, Theorem 3 implies $|\triangle T| > \begin{bmatrix} y \\ n-k \end{bmatrix}_q$.

For all $A \in \mathcal{L}_q(n,k)$, observe that

$$\begin{aligned} A^\perp \in \triangle T &\Longleftrightarrow \exists B \in \mathcal{L}_q(n,k-1) \setminus \triangle S,\ A^\perp \subset B^\perp \\ &\Longleftrightarrow \exists B \in \mathcal{L}_q(n,k-1) \setminus \triangle S,\ B \subset A \\ &\Longrightarrow A \notin S. \end{aligned}$$

Therefore, $S \subseteq \{A \in \mathcal{L}_q(n,k) : A^\perp \notin \triangle T\}$. We conclude that $|S| = \begin{bmatrix} n \\ k \end{bmatrix}_q - |\triangle T| < \begin{bmatrix} n \\ k \end{bmatrix}_q - \begin{bmatrix} y \\ n-k \end{bmatrix}_q$, as required.

3 Proof of Theorem 1

The proof of Theorem 1 involves bounding the edge-expansion of sets in the Grassmann graph $J_q(n,k)$. We state the required definitions and lemmas below. (See [12] for a much deeper study of expansion of Grassman graphs.)

Definition 7 *For a d-regular graph $G=(V,E)$ and $S \subseteq V$, the* edge-expansion *of S is defined by*

$$\Phi_G(S) := \frac{|E(S,\overline{S})|}{d|S|}$$

where $E(S,\overline{S})$ is the set of edges between S and $\overline{S} = V \setminus S$.

Lemma 8 (Expander Mixing Lemma [1]) *Let $G=(V,E)$ be a d-regular graph and suppose the second largest eigenvalue (in absolute value) of the adjacency matrix of G is at most λ. Then for all $S \subseteq V$,*

$$\left(1-\frac{\lambda}{d}\right)\left(1-\frac{|S|}{|V|}\right) \leqslant \Phi_G(S) \leqslant \left(1+\frac{\lambda}{d}\right)\left(1-\frac{|S|}{|V|}\right).$$

Definition 9 *For $1 \leqslant k \leqslant n$, the* Grassmann graph $J_q(n,k)$ *is the $q[k]_q[n-k]_q$-regular graph with vertex set $\mathcal{L}_q(n,k)$ and edge set*

$$E_{J_q(n,k)} := \{(A_1,A_2) \in \mathcal{L}_q(n,k) \times \mathcal{L}_q(n,k) : \dim(A_1 \cap A_2) = k-1\}.$$

Lemma 10 (Spectrum of $J_q(n,k)$ [4]) *The adjacency matrix of $J_q(n,k)$ has eigenvalue $q^{i+1}[k-i]_q[n-k-i]_q - [i]_q$ with multiplicity $\begin{bmatrix} n \\ i \end{bmatrix}_q - \begin{bmatrix} n \\ i-1 \end{bmatrix}_q$ for each $0 \leqslant i \leqslant \min(k, n-k)$. In particular, the second largest eigenvalue (in absolute value) equals 1 if $k \in \{1, n-1\}$ and equals $q^2[k-1]_q[n-k-1]_q - 1$ if $2 \leqslant k \leqslant n-2$.*

Lemmas 8 and 10 give the following lower bound on $\Phi_{J_q(n,k)}(S)$.

Lemma 11 *For all $2 \leqslant k \leqslant n-2$ and $S \subseteq \mathcal{L}_q(n,k)$,*

$$\Phi_{J_q(n,k)}(S) \geqslant \frac{[n]_q}{q[k]_q[n-k]_q}(1-\mu_k(S)).$$

Proof. Lemma 8 implies the lower bound

$$\Phi_{J_q(n,k)}(S) \geqslant \left(1 - \frac{q^2[k-1]_q[n-k-1]_q - 1}{[k]_q[n-k]_q}\right)(1-\mu_k(S)).$$

By a straightforward calculation,

$$1 - \frac{q^2[k-1]_q[n-k-1]_q - 1}{q[k]_q[n-k]_q} = \frac{q^{n+1}-q^n-q+1}{q^{n+1}-q^{k+1}-q^{n-k+1}+q} = \frac{[n]_q}{q[k]_q[n-k]_q}.$$

We next show an upper bound on $\Phi_{J_q(n,k)}(S)$ in terms of the ratio $\mu_k(S)/\mu_{k-1}(\triangle S)$.

Lemma 12 *For all $1 \leqslant k \leqslant n$ and $\emptyset \subset S \subseteq \mathcal{L}_q(n,k)$,*

$$\Phi_{J_q(n,k)}(S) \leqslant \frac{[n-k+1]_q}{q[n-k]_q}\left(1 - \frac{\mu_k(S)}{\mu_{k-1}(\triangle S)}\right).$$

Proof. For $B \in \triangle S$, let $S_B := \{A \in S : B \subset A\}$. We have $\sum_{B\in\triangle S} |S_B| = [k]_q|S|$ and, by the Cauchy-Schwarz inequality,

$$\sum_{B\in\triangle S} |S_B|^2 \geqslant \frac{(\sum_{B\in\triangle S} |S_B|)^2}{|\triangle S|} = \frac{([k]_q|S|)^2}{|\triangle S|}.$$

Therefore,

$$\begin{aligned}|E_{J_q(n,k)}(S,\overline{S})| = \sum_{B\in\triangle S} |S_B \times \overline{S}_B| &= \sum_{B\in\triangle S} |S_B|\left([n-k+1]_q - |S_B|\right)\\ &\leqslant [k]_q|S|\left([n-k+1]_q - \frac{[k]_q|S|}{|\triangle S|}\right).\end{aligned}$$

We now have

$$\Phi_{J_q(n,k)}(S) = \frac{|E_{J_q(n,k)}(S,\overline{S})|}{q[k]_q[n-k]_q|S|} \leqslant \frac{[n-k+1]_q}{q[n-k]_q} - \frac{[k]_q}{q[n-k]_q}\cdot\frac{|S|}{|\triangle S|}.$$

The lemma now follows from the equality

$$\frac{[k]_q}{q[n-k]_q}\cdot\frac{|S|}{|\triangle S|} = \frac{[k]_q\begin{bmatrix}n\\k\end{bmatrix}_q}{q[n-k]_q\begin{bmatrix}n\\k-1\end{bmatrix}_q}\cdot\frac{\mu_k(S)}{\mu_{k-1}(\triangle S)} = \frac{[n-k+1]_q}{q[n-k]_q}\cdot\frac{\mu_k(S)}{\mu_{k-1}(\triangle S)}.$$

We are ready to prove:

Theorem 1 (restated) *For all $1 \leqslant k \leqslant n$ and $S \subseteq \mathcal{L}_q(n,k)$, if $\mu_k(S) = (1+z)^{-1}$ where $z \in \mathbb{R}_{\geqslant 0}$, then*

$$\mu_{k-1}(\triangle S) \geqslant \left(1 + \frac{q(q^{k-1}-1)(q^{n-k}-1)}{(q^k-1)(q^{n-k+1}-1)}\cdot z\right)^{-1} \geqslant \left(1+\frac{z}{q}\right)^{-1}.$$

Proof. The second inequality is by a straightforward calculation:

$$\frac{q(q^{k-1}-1)(q^{n-k}-1)}{(q^k-1)(q^{n-k+1}-1)} = \frac{1}{q}\left(1 - \frac{(q-1)(q^{n-k+1}+q^k-q-1)}{(q^k-1)(q^{n-k+1}-1)}\right) \leqslant \frac{1}{q}.$$

For the first inequality, consider the case that $k \in \{1,n\}$. In both cases, we have $\mu_{k-1}(\triangle S) = 1$ for every nonempty $S \subseteq \mathcal{L}_q(n,k)$. Therefore, the inequality holds (moreover, with equality since $[k-1]_q[n-k]_q = 0$).

Next, consider the case that $2 \leqslant k \leqslant n-2$. In this case, Lemmas 11 and 12 imply

$$\frac{[n]_q}{q[k]_q[n-k]_q}(1-\mu_k(S)) \leqslant \Phi_{J_q(n,k)}(S) \leqslant \frac{[n-k+1]_q}{q[n-k]_q}\left(1 - \frac{\mu_k(S)}{\mu_{k-1}(\triangle S)}\right).$$

Therefore,

$$\frac{[n]_q}{[k]_q[n-k+1]_q}(1-\mu_k(S)) \leqslant 1 - \frac{\mu_k(S)}{\mu_{k-1}(\triangle S)}.$$

Substituting $(1+z)^{-1}$ for $\mu_k(S)$, this rearranges to

$$\begin{aligned}\mu_{k-1}(\triangle S) &\geqslant \left(1 + \left(1 - \frac{[n]_q}{[k]_q[n-k+1]_q}\right) z\right)^{-1} \\ &= \left(1 + \frac{q(q^{k-1}-1)(q^{n-k}-1)}{(q^k-1)(q^{n-k+1}-1)} \cdot z\right)^{-1}.\end{aligned}$$

We derive the remaining case $k = n-1$ from the case $k = 2$ via duality. Letting $S \subseteq \mathcal{L}_q(n, n-1)$, we will assume that

$$\mu_{n-2}(S) < \left(1 + \frac{q(q-1)(q^{n-2}-1)}{(q^2-1)(q^{n-1}-1)} \cdot z\right)^{-1}$$

and show that $\mu_{n-1}(S) < (1+z)^{-1}$. Let $T := \{B^\perp : B \in \mathcal{L}_q(n, n-2) \setminus \triangle S\}$ and note that

$$\begin{aligned}\mu_2(T) = 1 - \mu_{n-2}(\triangle S) &> 1 - \left(1 + \frac{q(q-1)(q^{n-2}-1)}{(q^2-1)(q^{n-1}-1)} \cdot z\right)^{-1} \\ &= \left(1 + \frac{(q^2-1)(q^{n-1}-1)}{z \cdot q(q-1)(q^{n-2}-1)}\right)^{-1}.\end{aligned}$$

From the case $k = 2$, we have

$$\mu_1(\triangle T) \geqslant \left(1 + \frac{q(q-1)(q^{n-2}-1)}{(q^2-1)(q^{n-1}-1)} \cdot (\mu_2(T)^{-1} - 1)\right)^{-1} > \left(1 + \frac{1}{z}\right)^{-1}.$$

Since $S \subseteq \{A \in \mathcal{L}_q(n, n-1) : A^\perp \notin \triangle T\}$ (as in the proof of Theorem 6), it follows that

$$\mu_{n-1}(S) \leqslant 1 - \mu_1(\triangle T) < 1 - \left(1 + \frac{1}{z}\right)^{-1} = (1+z)^{-1},$$

as required.

We remark that Theorem 1 is self-dual: for any $1 \leqslant k \leqslant n$ and $S \subseteq \mathcal{L}_q(n,k)$, we get the same inequality between $\mu_k(S)$ and $\mu_{k-1}(\triangle S)$ as between $1 - \mu_{n-k}(\triangle T)$ and $1 - \mu_{n-k+1}(T)$ where $T := \{B^\perp : B \in \mathcal{L}_q(n, k-1) \setminus \triangle S\}$.

4 Tightness of the result

Fix a flag $V_0 \subset V_1 \subset \cdots \subset V_n = \mathbb{F}_q^n$. (Without loss of generality, we may take $V_k = \{u \in \mathbb{F}_q^n : u_{k+1} = \cdots = u_n = 0\}$.) For $1 \leqslant j \leqslant n$, let $Q_{\widehat{j}}$ be the ideal

$$Q_{\widehat{j}} := \{A \in \mathcal{L}_q(n) : A \cap (V_j - V_{j-1}) = \emptyset\}.$$

In particular, $Q_{\widehat{1}}$ is the set of subspaces of $\mathbb{F}_q^n$ that do not contain V_1, while $Q_{\widehat{n}}$ is the set of subspaces contained in V_{n-1}.

Densities $\mu_k(Q_{\widehat{j}})$ satisfy the following (in)equalities:

(i) $\mu_{n-j}(Q_{\widehat{j}}) > 1/2 > \mu_{n-j+1}(Q_{\widehat{j}})$,

(ii) if $2 \leqslant k \leqslant n-1$ and $\mu_k(Q_{\widehat{j}}) = (1+z)^{-1}$, then

$$\left(1+\frac{z}{q^2}\right)^{-1} \geqslant \mu_{k-1}(Q_{\widehat{j}}) \geqslant \left(1+\frac{z}{q}\right)^{-1},$$

(iii) $\mu_k(Q_{\widehat{n}}) = \dfrac{\begin{bmatrix} n-1 \\ k \end{bmatrix}_q}{\begin{bmatrix} n \\ k \end{bmatrix}_q} = \dfrac{[n-k]_q}{[n]_q} = \left(1+\dfrac{q^{n-k}(q^k-1)}{(q^{n-k}-1)}\right)^{-1}$,

(iv) $\mu_k(Q_{\widehat{1}}) = 1 - \dfrac{\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q}{\begin{bmatrix} n \\ k \end{bmatrix}_q} = 1 - \dfrac{[k]_q}{[n]_q} = \left(1+\dfrac{(q^k-1)}{q^k(q^{n-k}-1)}\right)^{-1}$.

Inequalities (i) and (ii) show that Theorem 2 is essentially tight, no matter where in $\{1,\ldots,n\}$ the threshold for Q occurs. Equations (iii) and (iv) show that the first inequality of Theorem 1 is tight both:

- when S is the set of k-dimensional subspaces of a fixed $n-1$-dimensional space, as well as
- when S is the set of k-dimensional subspaces not containing a fixed 1-dimensional space.

The first example is also tight for q-Kruskal-Katona (Theorem 3), while the second example is tight for the Dual q-Kruskal-Katona (Theorem 6). Taking the maximum of the bounds given by Theorem 1, 3 and 6, we get:

Corollary 13 *For all $1 \leqslant k \leqslant n$ and $\emptyset \subset S \subset \mathcal{L}_q(n,k)$,*

$$|\triangle S| \geqslant \begin{cases} \begin{bmatrix} x \\ k-1 \end{bmatrix}_q & \text{if } |S| = \begin{bmatrix} x \\ k \end{bmatrix}_q,\ k \leqslant x \leqslant n-1, \\ \begin{bmatrix} n \\ k-1 \end{bmatrix}_q \left(1+\dfrac{z\cdot(q^{k-1}-1)}{q^{k-1}(q^{n-k+1}-1)}\right)^{-1} & \\ \qquad\qquad \text{if } |S| = \begin{bmatrix} n \\ k \end{bmatrix}_q \left(1+\dfrac{z\cdot(q^k-1)}{q^k(q^{n-k}-1)}\right)^{-1},\ 1 \leqslant z \leqslant q^n, \\ \begin{bmatrix} n \\ k-1 \end{bmatrix}_q - \begin{bmatrix} y \\ n-k+1 \end{bmatrix}_q & \\ \qquad\qquad \text{if } |S| = \begin{bmatrix} n \\ k \end{bmatrix}_q - \begin{bmatrix} y \\ n-k \end{bmatrix}_q,\ n-k+1 \leqslant y \leqslant n-1. \end{cases}$$

Corollary 13 is known to be tight when x or y are integers (or $z \in \{1, q^n\}$, coinciding with cases $y = n-1$ and $x = n-1$). In other cases, determining the optimal lower bound for $|\triangle S|$ in terms of $|S|$ remains an open problem. In contrast, note that the original Kruskal-Katona Theorem [8, 11] completely solves the shadow minimization problem in the boolean lattice: if S is a family of k-element sets and $|S| = \binom{n_k}{k} + \binom{n_{k-1}}{k-1} + \cdots + \binom{n_j}{j}$ where $n_k > n_{k-1} > \cdots > n_j = j \geqslant 1$, then $|\triangle S| \geqslant \binom{n_k}{k-1} + \binom{n_{k-1}}{k-2} + \cdots + \binom{n_j}{j-1}$ and this bound is tight. Moreover, a family of nested solutions is given by the subsets of $\{1,\ldots,n\}$ in co-lexicographic order. The situation in $\mathcal{L}_q(n)$ appears more complicated, as nested solutions to the shadow minimization problem in $\mathcal{L}_q(n)$ are known not to exist [2, 7, 13].

5 Application to a query problem

In this section, we present an application of Theorem 2 to a problem in query complexity. In this problem, A is a *hidden* nontrivial subspace of $\mathbb{F}_2^n$ and the goal is to learn a nonzero element of A with probability $\geqslant 1/2$ by making m simultaneous (non-adaptive) monotone queries. What is the minimum m for which this is possible? An upper bound of $O(n^2)$ follows from the Valiant-Vazirani isolation technique [14] (see [9]). The following theorem gives a matching lower bound of $\Omega(n^2)$. (We adopt the convention of writing random variables in boldface.)

Theorem 14 *Let $(\mathbf{Q}_1, \ldots, \mathbf{Q}_m)$ be a joint distribution over ideals in the subspace lattice of $\mathbb{F}_2^n$ and let f be a function $\{0,1\}^m \to \mathbb{F}_2^n \setminus \{\overline{0}\}$. Suppose that for every nontrivial subspace A of $\mathbb{F}_2^n$, it holds that*

$$\mathbb{P}[\, f(1_{\{A \in \mathbf{Q}_1\}}, \ldots, 1_{\{A \in \mathbf{Q}_m\}}) \in A \,] \geqslant 1/2$$

where $1_{\{A \in Q_i\}}$ is the indicator function for the event that $A \in \mathbf{Q}_i$. Then $m = \Omega(n^2)$.

This result answers a question of Kawachi, Watanabe and the author [9], who proved the special case of Theorem 14 where ideals $\mathbf{Q}_i$ are restricted to be of the form $\mathbf{Q}_i = \{A \in \mathcal{L}_2(n) : A \cap \mathbf{U}_i = \emptyset\}$ for an arbitrary joint distribution $(\mathbf{U}_1, \ldots, \mathbf{U}_m)$ of subsets $\mathbf{U}_i \subseteq \mathbb{F}_2^n$. In the remainder of this section, we prove Theorem 14 by combining our threshold theorem for $\mathcal{L}_2(n)$ with a few lemmas from the paper [9].

By Yao's principle [16], it suffices to exhibit a *random* nontrivial subspace $\mathbf{A}$ of $\mathbb{F}_2^n$ such that, for all *fixed* ideals $Q_1, \ldots, Q_m$ and every function $f : \{0,1\}^m \to \mathbb{F}_2^n \setminus \{\overline{0}\}$, if

$$\mathbb{P}[\, f(1_{\{\mathbf{A} \in Q_1\}}, \ldots, 1_{\{\mathbf{A} \in Q_m\}}) \in \mathbf{A} \,] \geqslant 1/2,$$

then $m = \Omega(n^2)$. We define $\mathbf{A}$ as follows: first, choose $\mathbf{k} \in \{1, \ldots, \lfloor n/2 \rfloor\}$ uniformly at random; then let $\mathbf{A}$ be a uniform random $\mathbf{k}$-dimensional subspace of $\mathbb{F}_2^n$ (i.e., a uniform random element of $\mathcal{L}_2(n, \mathbf{k})$).

We next state three lemmas (adapted from [9]) concerning the entropy of random variables that depend on $\mathbf{A}$. A reminder of the definition of the (conditional) entropy function: for discrete random variables $\mathbf{X}$ and $\mathbf{Y}$, let

$$\mathbb{H}[\, \mathbf{X} \,] := \sum_{x \in \mathrm{Supp}(\mathbf{X})} \mathbb{P}[\, \mathbf{X} = x \,] \cdot \log(1/\, \mathbb{P}[\, \mathbf{X} = x \,]),$$

$$\mathbb{H}[\, \mathbf{X} \,|\, \mathbf{Y} \,] := \sum_{y \in \mathrm{Supp}(\mathbf{Y})} \mathbb{P}[\, \mathbf{Y} = y \,] \cdot \mathbb{H}[\, \mathbf{X} \,|\, \mathbf{Y} = y \,],$$

where $\log(\cdot)$ is the base-2 logarithm.

Lemma 15 *For every ideal Q in $\mathcal{L}_2(n)$, we have*

$$\mathbb{H}[\, 1_{\{\mathbf{A} \in Q\}} \,|\, \mathbf{k} \,] = O(1/n).$$

Proof. If Q is trivial, then this conditional entropy is 0. So we assume Q in nontrivial and let $t \in \{1, \ldots, n\}$ be the unique threshold such that $\mu_{t-1}(Q) \geqslant 1/2 > \mu_t(Q)$. Let $0 \leqslant y \leqslant 1 < z$ be

the unique real numbers such that $\mu_{t-1}(Q) = (1+y)^{-1}$ and $\mu_t(Q) = (1+z)^{-1}$. By our threshold theorem for ideals in $\mathcal{L}_2(n)$ (Theorem 2), for all $i \in \{1, \ldots, t-1\}$ and $j \in \{1, \ldots, n-t\}$,

$$\begin{aligned}\mu_{t-1-i}(Q) &\geqslant (1+y2^{-i})^{-1} \geqslant (1+2^{-i})^{-1} \geqslant 1-2^{-i},\\ \mu_{t+j}(Q) &\leqslant (1+z2^{j})^{-1} < (1+2^{j})^{-1} \leqslant 2^{-j}.\end{aligned}$$

For $k \in \{0, \ldots, n\}$, let $\mathbf{S}_k$ is a uniform random k-dimensional subspace of $\mathbb{F}_2^n$. It follows that

$$\begin{aligned}\mathbb{H}[\,1_{\{\mathbf{S}_k \in Q\}}\,] &= \mu_k(Q)\log\left(\frac{1}{\mu_k(Q)}\right) + (1-\mu_k(Q))\log\left(\frac{1}{1-\mu_k(Q)}\right)\\ &\leqslant \begin{cases} 1 & \text{if } k \in \{t-1, t\},\\ i2^{-i} + (1-2^{-i})\log(\frac{1}{1-2^{-i}}) & \text{if } k = t-1-i,\\ j2^{-j} + (1-2^{-j})\log(\frac{1}{1-2^{-j}}) & \text{if } k = t+j,\end{cases}\\ &\leqslant \begin{cases} 1 & \text{if } k \in \{t-1, t\},\\ i2^{1-i} & \text{if } k = t-1-i,\\ j2^{1-j} & \text{if } k = t+j.\end{cases}\end{aligned}$$

We now obtain the desired bound as follows:

$$\begin{aligned}\mathbb{H}[\,1_{\{\mathbf{A}\in Q\}}\,|\,\mathbf{k}\,] &= \sum_{k=1}^{\lfloor n/2\rfloor} \mathbb{P}[\,\mathbf{k}=k\,]\cdot\mathbb{H}[\,1_{\{\mathbf{S}_k\in Q\}}\,]\\ &\leqslant \frac{1}{\lfloor n/2\rfloor}\left(2 + \sum_{k=1}^{\min(t-2,\lfloor n/2\rfloor)} \mathbb{H}[\,1_{\{\mathbf{S}_k\in Q\}}\,] + \sum_{k=t+1}^{\lfloor n/2\rfloor} \mathbb{H}[\,1_{\{\mathbf{S}_k\in Q\}}\,]\right)\\ &\leqslant \frac{2}{n+1}\left(2 + 2\sum_{i=1}^{\infty} i2^{1-i}\right)\\ &= \frac{20}{n+1}.\end{aligned}$$

Lemma 16 *Let* $\mathbf{v}$ *be a random vector in* $\mathbb{F}_2^n \setminus \{\overline{0}\}$*, not necessarily independent of* $\mathbf{A}$*. Then*

$$\mathbb{P}[\,\mathbf{v}\in\mathbf{A}\,] \leqslant \frac{4}{n}\,\mathbb{H}[\,\mathbf{v}\,] + \frac{1}{2^{n/4}}.$$

Proof. Let

$$U := \left\{x \in \mathbb{F}_2^n \setminus \{\overline{0}\} : \mathbb{P}[\,\mathbf{v}=x\,] \geqslant 2^{-n/4}\right\}.$$

Note that

$$\mathbb{P}[\,\mathbf{v}\in\mathbf{A}\,] \leqslant \mathbb{P}[\,\mathbf{v}\notin U\,] + \mathbb{P}[\,\mathbf{A}\cap U \neq \emptyset\,].$$

(If $\mathbf{v}\in\mathbf{A}$, then either $\mathbf{v}\notin U$ or $\mathbf{v}\in\mathbf{A}\cap U$.) We bound these two terms separately.

First, we have

$$\begin{aligned}\mathbb{P}[\,\mathbf{v} \notin U\,] = \sum_{x \in (\mathbb{F}_2^n \setminus \{\overline{0}\}) \setminus U} \mathbb{P}[\,\mathbf{v} = x\,] &\leqslant \sum_{x \in (\mathbb{F}_2^n \setminus \{\overline{0}\}) \setminus U} \mathbb{P}[\,\mathbf{v} = x\,] \frac{\log(1/\,\mathbb{P}[\,\mathbf{v} = x\,])}{n/4} \\ &\leqslant \sum_{x \in \mathbb{F}_2^n \setminus \{\overline{0}\}} \mathbb{P}[\,\mathbf{v} = x\,] \frac{\log(1/\,\mathbb{P}[\,\mathbf{v} = x\,])}{n/4} \\ &= \frac{4}{n}\,\mathbb{H}[\,\mathbf{v}\,].\end{aligned}$$

For the second term, observing that $|U| \leqslant 2^{n/4}$ and $\mathbb{P}[\,x \in \mathbf{A}\,] \leqslant \frac{2^{\lfloor n/2 \rfloor}-1}{2^n-1} \leqslant \frac{1}{2^{n/2}}$ for every $x \in \mathbb{F}_2^n \setminus \{\overline{0}\}$, we have

$$\mathbb{P}[\,\mathbf{A} \cap U \neq \emptyset\,] \leqslant \sum_{x \in U} \mathbb{P}[\,x \in \mathbf{A}\,] \leqslant |U| \cdot \frac{1}{2^{n/2}} \leqslant \frac{1}{2^{n/4}}.$$

This complete the proof.

Lemma 17 *For every function $f : \{0,1\}^m \to \mathbb{F}_2^n \setminus \{\overline{0}\}$ and ideals $Q_1, \ldots, Q_m \subseteq \mathcal{L}_2(n)$,*

$$\mathbb{P}[\,f(1_{\{\mathbf{A} \in Q_1\}}, \ldots, 1_{\{\mathbf{A} \in Q_m\}}) \in \mathbf{A}\,] \leqslant O\left(\frac{m + n \log n}{n^2}\right).$$

Proof. By standard entropy inequalities and Lemma 15,

$$\begin{aligned}\mathbb{H}[\,f(1_{\{\mathbf{A} \in Q_1\}}, \ldots, 1_{\{\mathbf{A} \in Q_m\}})\,] &\leqslant \mathbb{H}[\,1_{\{\mathbf{A} \in Q_1\}}, \ldots, 1_{\{\mathbf{A} \in Q_m\}}\,] \\ &\leqslant \mathbb{H}[\,1_{\{\mathbf{A} \in Q_1\}}, \ldots, 1_{\{\mathbf{A} \in Q_m\}}, \mathbf{k}\,] \\ &= \mathbb{H}[\,\mathbf{k}\,] + \mathbb{H}[\,1_{\{\mathbf{A} \in Q_1\}}, \ldots, 1_{\{\mathbf{A} \in Q_m\}} \,|\, \mathbf{k}\,] \\ &\leqslant \log(\lfloor n/2 \rfloor) + \sum_{i=1}^{m} \mathbb{H}[\,1_{\{\mathbf{A} \in Q_i\}} \,|\, \mathbf{k}\,] \\ &\leqslant O(\log n) + O(m/n).\end{aligned}$$

Combining the above with Lemma 16, we get the stated bound

$$\begin{aligned}\mathbb{P}[\; f(1_{\{\mathbf{A} \in Q_1\}}, \ldots, 1_{\{\mathbf{A} \in Q_m\}}) \in \mathbf{A}\;] &\leqslant \frac{4}{n}\,\mathbb{H}[\; f(1_{\{\mathbf{A} \in Q_1\}}, \ldots, 1_{\{\mathbf{A} \in Q_m\}})\;] + \frac{1}{2^{n/4}} \\ &\leqslant \frac{4}{n}\Big(O(\log n) + O(m/n)\Big) + \frac{1}{2^{n/4}} \\ &= O\left(\frac{m + n \log n}{n^2}\right).\end{aligned}$$

Theorem 14 follows directly from Lemma 17, as

$$\mathbb{P}[\,f(1_{\{\mathbf{A} \in Q_1\}}, \ldots, 1_{\{\mathbf{A} \in Q_m\}}) \in \mathbf{A}\,] \geqslant 1/2 \implies m = \Omega(n^2).$$

References

1. Alon, N., Chung, F.R.: Explicit construction of linear sized tolerant networks. Discrete Mathematics **72**(1-3), 15–19 (1988)
2. Bezrukov, S., Blokhuis, A.: A Kruskal-Katona type theorem for the linear lattice. European Journal of Combinatorics **20**(2), 123–130 (1999)
3. Bollobás, B., Thomason, A.G.: Threshold functions. Combinatorica **7**(1), 35–38 (1987)
4. Brouwer, A.E., Haemers, W.H.: Distance-regular graphs. In: Spectra of Graphs, pp. 177–185. Springer (2012)
5. Chowdhury, A., Patkós, B.: Shadows and intersections in vector spaces. Journal of Combinatorial Theory, Series A **117**(8), 1095–1106 (2010)
6. Friedgut, E., Kalai, G.: Every monotone graph property has a sharp threshold. Proceedings of the American mathematical Society **124**(10), 2993–3002 (1996)
7. Harper, L., Hergert, F.: The isoperimetric problem in finite projective planes. Congressus Numerantium pp. 225–232 (1994)
8. Katona, G.: A theorem of finite sets. In: Classic Papers in Combinatorics, pp. 381–401. Springer (2009)
9. Kawachi, A., Rossman, B., Watanabe, O.: The query complexity of witness finding. Theory of Computing Systems **61**(2), 305–321 (2017)
10. Keevash, P.: Shadows and intersections: stability and new proofs. Advances in Mathematics **218**(5), 1685–1703 (2008)
11. Kruskal, J.B.: The number of simplices in a complex. Mathematical optimization techniques **10**, 251–278 (1963)
12. Subhash, K., Minzer, D., Safra, M.: Pseudorandom sets in Grassmann graph have near-perfect expansion. In: 59th Annual IEEE Symposium on Foundations of Computer Science (FOCS). pp. 592–601 (2018)
13. Ure, P.K.: A study of $(0, n, n+1)$-sets and other solutions of the isoperimetric problem in finite projective planes. Ph.D. thesis, California Institute of Technology (1996)
14. Valiant, L.G., Vazirani, V.V.: NP is as easy as detecting unique solutions. In: Proc. 17th Annual ACM Symposium on Theory of Computing. pp. 458–463 (1985)
15. Wang, J.: Intersecting antichains and shadows in linear lattices. Journal of Combinatorial Theory, Series A **118**(7), 2092–2101 (2011)
16. Yao, A.C.C.: Probabilistic computations: Toward a unified measure of complexity. In: 18th Annual Symposium on Foundations of Computer Science. pp. 222–227. IEEE (1977)