A q-analog of Approximate Inclusion-Exclusion

Marios Mavronicolas*
Department of Computer Science
University of Cyprus
Nicosia CY-1678, Cyprus

March 1997

*Part of this work was performed while the author was at Aiken Computation Laboratory, Harvard University, supported by ONR contract N00014-91-J-1981, at Department of Computer Science, University of Crete, and at Institute of Computer Science, Foundation for Research and Technology – Hellas, Greece. E-mail: mavronic@turing.cs.ucy.ac.cy

Abstract

We consider the lattice of subspaces of an n-dimensional vector space V_q^n over a finite field $GF(q)$ and represent a family of such subspaces by elements of a set X. The q-analog of the principle of inclusion-exclusion expresses the size of the union of elements of X representing subspaces of V_q^n in terms of the sizes of subsets of X whose intersection contains a given subspace of V_q^n. We study the problem of approximating the size of this union when intersection sizes are known only for some subspaces of V_q^n.

In particular, we consider the case where intersection sizes are given for subsets of X whose intersection contains a subspace of V_q^n of dimension at most k. We extend methods of Linial and Nisan (*Combinatorica,* Vol. 10, No. 4, pp. 349–365, 1990), drawn from approximation theory, to show that the quality of approximation changes in a significant way around $\sqrt{q^{n-1}}$: if $k \leq O(\sqrt{q^{n-1}})$, then any approximation may err by a factor of $\Theta(\sqrt{q^{n-1}}/k)$, while if $k \geq \Omega(\sqrt{q^{n-1}})$, the size of the union may be approximated to within a multiplicative factor of $1 + e^{-\Omega(k/\sqrt{q^{n-1}})}$.

Our result, the first q-analog of a computational property of the lattice of subsets of a finite set, answers in the affirmative a question posed by Linial and Nisan.

1 Introduction

The triality principle in combinatorics, commonly attributed to Rota, asserts that to any theorem holding on the lattice of subsets of a finite set, there corresponds a *q-analog,* i.e., a matching theorem holding on the lattice of subspaces of a finite-dimensional vector space and a *partition analog,* i.e., a matching theorem holding on the lattice of partitions of a finite set. (See, e.g., [7] for a discussion of the triality principle.) Although this principle has attracted a lot of attention and has been successfully verified in a variety of combinatorial situations (see, e.g., [3, 4, 5, 6, 8, 10, 11, 16, 19]), the exact mathematical nature of these theorem correspondences remains as yet unexplained.

In this paper, we initiate a study of the triality principle in algorithmic combinatorics by presenting a q-analog of a computational property of the lattice of subsets of a finite set. In particular, we address a q-analog of a result of Linial and Nisan [14] concerning the quality of approximating the size of the union of a family of sets in terms of the sizes of intersections of subsets, when intersection sizes are known for only some of the subsets. (The problem of exactly computing the size of this union is known to be at least as hard as computing the number of satisfying assignments to a Boolean formula in disjunctive normal form, which is a $\#\mathcal{P}$-complete problem [21].)

Linial and Nisan [14] have been the first to look at the approximability of "hard" counting problems from the point of view of a corresponding *Möbius inversion* problem. Their starting point was the classical inclusion-exclusion formula and their main result was that a good approximation may be obtained if and only if sufficiently many terms from the inclusion-exclusion formula are taken, more precisely, terms that express the size of intersections of up to $\sqrt{n}$ subsets. The elegant methods of Linial and Nisan were drawn from approximation theory, in particular, from the theory of Chebyshev polynomials [17].

Following Linial and Nisan [14], we present a corresponding result for a counting problem over the lattice of subspaces of a finite-dimensional vector space. In particular, we consider an n-dimensional vector space V_q^n over a finite field $GF(q)$ and a family of subspaces of it represented by the elements of a set X. We consider a q-analog of the principle of inclusion-exclusion due to Chen and Rota [5] expressing the size of the union of elements of X representing subspaces of V_q^n in terms of the sizes of subsets of X whose intersection contains a given subspace of V_q^n. We address the problem of approximating the size of the union when intersection sizes are known only for some subspaces of V_q^n.

More specifically, we consider the case where intersection sizes are given for subsets of

X whose intersection contains a subspace of V_q^n of dimension at most k for some integer k, $1 \leq k \leq n$. We extend the methods of Linial and Nisan to apply to the lattice of subspaces of an n-dimensional vector space; we show that the quality of approximation changes in a significant way around $\sqrt{q^{n-1}}$: if $k \leq O(\sqrt{q^{n-1}})$, then any approximation may err by a factor of $\Theta(\sqrt{q^{n-1}}/k)$, while if $k \geq \Omega(\sqrt{q^{n-1}})$, the size of the union may be approximated to within a multiplicative factor of $1 + e^{-\Omega(k/\sqrt{q^{n-1}})}$.

Our result, the first q-analog of a computational property of the lattice of subsets of a finite set, answers in the affirmative a question posed by Linial and Nisan [14, Section 6, Open Problem 2]:

> "The inclusion-exclusion formula is the Möbius inversion formula for the full Boolean lattice. Are there results similar to the present ones for other lattices?"

The rest of this paper is organized as follows. Section 2 presents the lattice of subspaces of an n-dimensional vector space over a finite field $GF(q)$, describes Möbius inversion for this lattice, and introduces some notation. Section 3 includes a brief introduction to Chebyshev polynomials, highlighting several properties of them. In Section 4, we present our upper and lower bounds on approximability. We conclude, in Section 5, with a discussion of the results and some open problems.

2 The Lattice of Subspaces of an n-dimensional Vector Space over a Finite Field $GF(q)$

Our presentation combines elements from [5] and [14]. More precisely, we adopt the q-analog of the principle of inclusion-exclusion presented in [5], and use it to generalize definitions and properties of the lattice of subsets of a finite set given in [14] to the lattice of subspaces of a finite-dimensional vector space.

2.1 Basic Definitions and Facts

Let V_q^n be an n-dimensional vector space over a finite field $GF(q)$ with q elements, and consider the set $\mathcal{L}(n, q)$ of all subspaces of V_q^n ordered by inclusion. It is known that $\mathcal{L}(n, q)$ is an indecomposable, modular, self-dual and complemented lattice (see, e.g., [1, Chapter 2] or [15, Chapter 24]).

For subspaces T_1 and T_2 of V_q^n, we write $T_1 \sqsubseteq T_2$ whenever T_1 is a subspace of T_2, and we write $T_1 \sqsubset T_2$ whenever T_1 is a *proper* subspace of T_2, i.e., $T_1 \sqsubseteq T_2$ but $T_1 \neq T_2$. Clearly, $T_1 \sqsubseteq T_2$ only if $\dim(T_1) \leq \dim(T_2)$, where $\dim(T)$ denotes the *dimension* of a vector space T. Let $\emptyset$ denote the *empty* vector space; clearly, $\dim(\emptyset) = 0$. Henceforth, we will use the term *j-subspace* as a short form of j-dimensional subspace.

For each j, $1 \leq j \leq n$, the *Gaussian coefficient*

$$\begin{bmatrix} n \\ j \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\ldots(q^{n-j+1})}{(q^j-1)(q^{j-1}-1)\ldots(q-1)} \tag{1}$$

represents the number of j-subspaces of V_q^n. (For a general account of properties of Gaussian coefficients, see, e.g., [9, 10], where the foundations for the study of the combinatorial properties of finite-dimensional vector spaces have been laid, or [15, Chapter 24] for a modern account.)

Consider a set X with N elements. Suppose $\mathcal{A}$ is a set of properties on X indexed by elements of V_q^n, that is,

$$\mathcal{A} = \{\mathcal{A}_v \subseteq X \mid v \in V_q^n\}\,. \tag{2}$$

In other words, $\mathcal{A}_v$ is identified with the set of elements in X that satisfy the property $\mathcal{A}_v$. For each element $x \in X$, define the *associated space of x under $\mathcal{A}$*, denoted $V^{\mathcal{A}}(x)$, to be

$$V^{\mathcal{A}}(x) = \{v \in V_q^n \mid x \in \mathcal{A}_v\}\,. \tag{3}$$

We say that the property set $\mathcal{A}$ is *V_q^n-consistent* if for every $x \in X$, $V^{\mathcal{A}}(x)$ is a subspace of V_q^n. Henceforth, $\mathcal{A}$ will be assumed to be V_q^n-consistent.

For each subspace T of V_q^n, we define the quantities $P^{\mathcal{A}}(T)$ and $S^{\mathcal{A}}(T)$, to be later associated with appropriate, vector space-theoretic notions of atoms, unions and intersections:

- $P^{\mathcal{A}}(T)$ is the number of elements x in X such that $T = V^{\mathcal{A}}(x)$;
- $S^{\mathcal{A}}(T)$ is the number of elements x in X such that T is a subspace of $V^{\mathcal{A}}(x)$.

That is,

$$P^{\mathcal{A}}(T) = |\{x \in X \mid T = V^{\mathcal{A}}(x)\}|\,, \tag{4}$$

and

$$S^{\mathcal{A}}(T) = |\{x \in X \mid T \sqsubseteq V^{\mathcal{A}}(x)\}|\,. \tag{5}$$

Clearly, for each subspace L of V_q^n,

$$S^{\mathcal{A}}(L) \;=\; \sum_{T:\; L \sqsubseteq T \sqsubseteq V_q^n} P^{\mathcal{A}}(T)\,. \tag{6}$$

For each j, $1 \le j \le n$, we define a *j-atom of $\mathcal{A}$,* denoted $p_j^{\mathcal{A}}$, to be $P^{\mathcal{A}}(L)$ for some vector space L, $\emptyset \sqsubset L \sqsubseteq V_q^n$, such that $\dim(L) = j$; that is, $p_j^{\mathcal{A}}$ is the cardinality of a subset of X whose elements have each their associated spaces (under $\mathcal{A}$) equal to the same j-subspace L of V_q^n. The *union of j-atoms of $\mathcal{A}$,* denoted $P_j^{\mathcal{A}}$, is the sum of all j-atoms of $\mathcal{A}$, i.e.,

$$P_j^{\mathcal{A}} \;=\; \sum_{\text{all } j\text{-atoms}} p_j^{\mathcal{A}} \;=\; \sum_{T:\; \emptyset \sqsubset T \sqsubseteq V_q^n,\ \dim(T)=j} P^{\mathcal{A}}(T)\,. \tag{7}$$

For each j, $1 \le j \le n$, we define a *j-intersection of $\mathcal{A}$,* denoted $s_j^{\mathcal{A}}$, to be $S^{\mathcal{A}}(L)$ for some vector space L, $\emptyset \sqsubset L \sqsubseteq V_q^n$, such that $\dim(L) = j$; that is, $s_j^{\mathcal{A}}$ is the cardinality of a subset of X whose elements have each their associated spaces (under $\mathcal{A}$) containing the same j-subspace L of V_q^n. Thus,

$$s_j^{\mathcal{A}} \;=\; S^{\mathcal{A}}(L) \;=\; \sum_{T:\; L \sqsubseteq T \sqsubseteq V_q^n} P^{\mathcal{A}}(T) \;=\; \sum_{l=j}^{n} \; \sum_{T:\; L \sqsubseteq T \sqsubseteq V_q^n,\ \dim(T)=l} P^{\mathcal{A}}(T)\,. \tag{8}$$

for any j-subspace L of V_q^n. The *union of j-intersections of $\mathcal{A}$,* denoted $S_j^{\mathcal{A}}$, is the sum of all j-intersections of $\mathcal{A}$, i.e.,

$$S_j^{\mathcal{A}} \;=\; \sum_{\text{all } j\text{-intersections}} s_j^{\mathcal{A}} \;=\; \sum_{T:\; \emptyset \sqsubset T \sqsubseteq V_q^n,\ \dim(T)=j} S^{\mathcal{A}}(T)\,. \tag{9}$$

We remark that our definitions of j-atoms, j-intersections and their unions are all q-analogs of the corresponding ones in [14, Section 2.1].

2.2 Möbius Inversion

In this Section, we review basic facts about Möbius inversion in $\mathcal{L}(n, q)$ and apply them to derive expressions for various quantities of interest.

Let f and g be functions on $\mathcal{L}(n, q)$ taking values in some ring $\mathcal{R}$. Suppose f and g are related by the summation formula

$$f(L) = \sum_{T:\; L \sqsubseteq T \sqsubseteq V_q^n} g(T)\,, \tag{10}$$

for each $L \in \mathcal{L}(n,q)$. One may invert the previous equation to get that

$$g(L) = \sum_{T:\ L \sqsubseteq T \sqsubseteq V_q^n} \mu_{\mathcal{L}(n,q)}(L,T) f(T)\,, \tag{11}$$

where $\mu_{\mathcal{L}(n,q)}(L,T)$ is a unique integer-valued function on $\mathcal{L}(n,q) \times \mathcal{L}(n,q)$, depending only on $\mathcal{L}(n,q)$ (but not on f or g) and assuming nonzero values only when $L \sqsubseteq T$. The function $\mu_{\mathcal{L}(n,q)}$ is called the *Möbius function of* $\mathcal{L}(n,q)$ [18]. (An excellent survey of the theory of Möbius functions appears in [2].) For $L \sqsubseteq T$, the value of $\mu_{\mathcal{L}(n,q)}(L,T)$ is given by the *Möbius inversion formula* for $\mathcal{L}(n,q)$ [10]

$$\mu_{\mathcal{L}(n,q)}(L,T) = (-1)^{\dim(T)-\dim(L)} q^{\binom{\dim(T)-\dim(L)}{2}}\,. \tag{12}$$

Since both $S^{\mathcal{A}}$ and $P^{\mathcal{A}}$ are functions on $\mathcal{L}(n,q)$, we may apply Möbius inversion to Equation (6) to obtain that

$$P^{\mathcal{A}}(L) \ = \sum_{T:\ L \sqsubseteq T \sqsubseteq V_q^n} (-1)^{\dim(T)-\dim(L)} q^{\binom{\dim(T)-\dim(L)}{2}} S^{\mathcal{A}}(T)\,. \tag{13}$$

For $L = \emptyset$ so that $\dim(L) = 0$, Equation (13) reduces to

$$\begin{aligned} P^{\mathcal{A}}(\emptyset) &= \sum_{T:\ \emptyset \sqsubseteq T \sqsubseteq V_q^n} (-1)^{\dim(T)} q^{\binom{\dim(T)}{2}} S^{\mathcal{A}}(T) \\ &= (-1)^{\dim(\emptyset)} q^{\binom{\dim(\emptyset)}{2}} S^{\mathcal{A}}(\emptyset) + \sum_{T:\ \emptyset \sqsubset T \sqsubseteq V_q^n} (-1)^{\dim(T)} q^{\binom{\dim(T)}{2}} S^{\mathcal{A}}(T) \\ &= S^{\mathcal{A}}(\emptyset) + \sum_{T:\ \emptyset \sqsubset T \sqsubseteq V_q^n} (-1)^{\dim(T)} q^{\binom{\dim(T)}{2}} S^{\mathcal{A}}(T)\,, \end{aligned}$$

so that

$$P^{\mathcal{A}}(\emptyset) - S^{\mathcal{A}}(\emptyset) \ = \sum_{T:\ \emptyset \sqsubset T \sqsubseteq V_q^n} (-1)^{\dim(T)} q^{\binom{\dim(T)}{2}} S^{\mathcal{A}}(T)\,. \tag{14}$$

Note, however, that, by definitions of $P^{\mathcal{A}}$ and $S^{\mathcal{A}}$, $P^{\mathcal{A}}(\emptyset) - S^{\mathcal{A}}(\emptyset)$ is precisely the negative of the number of elements of X whose associated spaces (under $\mathcal{A}$) are non-null; each of these elements must belong to a certain $\mathcal{A}_v \subseteq X$ for some $v \in V_q^n$. To indicate an analogy with set-theoretic union, we call the set of elements of X with non-null associated spaces (under $\mathcal{A}$), the V_q^n*-consistent vector-space union of* $\mathcal{A}$, denoted $\bigsqcup_{v \in V_q^n} \mathcal{A}_v$, or vector-space union of $\mathcal{A}$ for short. Thus,

$$\left| \bigsqcup_{v \in V_q^n} \mathcal{A}_v \right| \ = \ - \sum_{T:\ \emptyset \sqsubset T \sqsubseteq V_q^n} (-1)^{\dim(T)} q^{\binom{\dim(T)}{2}} S^{\mathcal{A}}(T) \tag{15}$$

Notice also that $|\bigsqcup_{v \in V_q^n} \mathcal{A}_v|$ is uniquely determined once $P^{\mathcal{A}}(T)$ is given for each subspace T of V_q^n: simply,

$$\left| \bigsqcup_{v \in V_q^n} \mathcal{A}_v \right| \; = \sum_{T:\ \emptyset \sqsubset T \sqsubseteq V_q^n} P^{\mathcal{A}}(T) \; . \tag{16}$$

2.3 Uniform Property Sets

We say that the property set $\mathcal{A}$ is *uniform* if for every j, $1 \leq j \leq n$, all j-atoms are equal; that is, for each j, $1 \leq j \leq n$, for each pair of subspaces T_1 and T_2 such that $\dim(T_1) = \dim(T_2) = j$, $P^{\mathcal{A}}(T_1) = P^{\mathcal{A}}(T_2)$.

The next three results provide simplified expressions for $P_j^{\mathcal{A}}$, $s_j^{\mathcal{A}}$ and $S_j^{\mathcal{A}}$ in case $\mathcal{A}$ is a uniform property set. The first of these results is a direct consequence of Equation (7) and the definition of Gaussian coefficients.

Proposition 2.1 *Fix any uniform property set $\mathcal{A}$. Then, for each j, $1 \leq j \leq n$,*

$$P_j^{\mathcal{A}} \; = \; \begin{bmatrix} n \\ j \end{bmatrix}_q P^{\mathcal{A}}(L) \, ,$$

where L is any j-subspace of V_q^n.

We continue to show:

Proposition 2.2 *Fix any uniform property set $\mathcal{A}$. Then, for each j, $1 \leq j \leq n$,*

$$s_j^{\mathcal{A}} \; = \; \sum_{l=j}^{n} \begin{bmatrix} n-j \\ l-j \end{bmatrix}_q P^{\mathcal{A}}(T^l) \, ,$$

where for each l, $j \leq l \leq n$, T^l is any l-subspace of V_q^n.

Proof: We first prove a simple combinatorial fact.

Claim 2.3 *For any integers j and l, $1 \leq j \leq l \leq n$, the number of l-subspaces of V_q^n containing a given j-subspace of V_q^n is* $\begin{bmatrix} n-j \\ l-j \end{bmatrix}_q$.

Proof: By flipping $\mathcal{L}(n,q)$ upside down, this number is equal to the number of $(n-l)$-subspaces of V_q^n contained in a given $(n-j)$-subspace of V_q^n, which, by definition of Gaussian coefficients, is equal to $\begin{bmatrix} n-j \\ n-l \end{bmatrix}_q$, which equals $\begin{bmatrix} n-j \\ l-j \end{bmatrix}_q$, by self-duality of the lattice $\mathcal{L}(n,q)$ (cf. [10]). ■

By Equation (8), symmetry of $\mathcal{A}$ and Claim 2.3,

$$s_j^{\mathcal{A}} = \sum_{l=j}^{n} \sum_{T:\ L \sqsubseteq T_l \sqsubseteq V, \dim(T_l)=l} P^{\mathcal{A}}(T_l) = \sum_{l=j}^{n} \begin{bmatrix} n-j \\ l-j \end{bmatrix}_q P^{\mathcal{A}}(T^l),$$

where for each l, $j \leq l \leq n$, T^l is any l-subspace of V_q^n, as needed. ■

Finally, we show:

Proposition 2.4 *Fix any uniform property set $\mathcal{A}$. Then, for each j, $1 \leq j \leq n$,*

$$S_j^{\mathcal{A}} = \begin{bmatrix} n \\ j \end{bmatrix}_q \sum_{l=j}^{n} \begin{bmatrix} n-j \\ l-j \end{bmatrix}_q P^{\mathcal{A}}(T^l),$$

where for each l, $j \leq l \leq n$, T^l is any l-subspace of V_q^n.

Proof: By Equation (9), the definition of Gaussian coefficients, and Proposition 2.2,

$$S_j^{\mathcal{A}} = \begin{bmatrix} n \\ j \end{bmatrix}_q S^{\mathcal{A}}(L) = \begin{bmatrix} n \\ j \end{bmatrix}_q \sum_{l=j}^{n} \begin{bmatrix} n-j \\ l-j \end{bmatrix}_q P^{\mathcal{A}}(T^l),$$

where T^l is any l-subspace of V_q^n, as needed. ■

2.4 Linear Forms

Fix some integer k, $1 \leq k \leq n$. For each j, $1 \leq j \leq k$, we introduce the linear form

$$E_j^{(q)}(x_1, \ldots, x_n) = \sum_{l=j}^{n} \begin{bmatrix} l \\ j \end{bmatrix}_q x_l . \qquad (17)$$

The next result establishes an important property of these linear forms.

Proposition 2.5 *Fix any uniform property set $\mathcal{A}$. Then, for each j, $1 \leq j \leq k$,*

$$S_j^{\mathcal{A}} \;=\; E_j^{(q)}(P_1^{\mathcal{A}}, \ldots, P_n^{\mathcal{A}})\,.$$

Proof: From the definition of linear forms and Proposition 2.1,

$$E_j^{(q)}(P_1^{\mathcal{A}}, \ldots, P_n^{\mathcal{A}}) \;=\; \sum_{l=j}^{n} \begin{bmatrix} l \\ j \end{bmatrix}_q P_l^{\mathcal{A}} \;=\; \sum_{l=j}^{n} \begin{bmatrix} l \\ j \end{bmatrix}_q \begin{bmatrix} n \\ l \end{bmatrix}_q P^{\mathcal{A}}(T^l)\,,$$

where for each l, $j \leq l \leq n$, T^l is any l-subspace of V_q^n. Since

$$\begin{bmatrix} l \\ j \end{bmatrix}_q \begin{bmatrix} n \\ l \end{bmatrix}_q \;=\; \begin{bmatrix} n \\ j \end{bmatrix}_q \begin{bmatrix} n-j \\ l-j \end{bmatrix}_q ,$$

it follows that

$$\begin{aligned} E_j^{(q)}(P_1^{\mathcal{A}}, \ldots, P_n^{\mathcal{A}}) \;&=\; \sum_{l=j}^{n} \begin{bmatrix} n \\ j \end{bmatrix}_q \begin{bmatrix} n-j \\ l-j \end{bmatrix}_q P^{\mathcal{A}}(T^l) \\ &=\; \begin{bmatrix} n \\ j \end{bmatrix}_q \sum_{l=j}^{n} \begin{bmatrix} n-j \\ l-j \end{bmatrix}_q P^{\mathcal{A}}(T^l) \\ &=\; S_j^{\mathcal{A}}\,, \end{aligned}$$

by Proposition 2.4, as needed. ■

3 Chebyshev Polynomials

In this Section, we introduce Chebyshev polynomials and present several properties of them. The reader may prefer to skip this Section for now, returning to it later when its results are required.

The *Chebyshev polynomial of order k*, denoted $T_k(x)$, is a polynomial of degree k given by

$$T_k(x) \;=\; \frac{(x+\sqrt{x^2-1})^k + (x-\sqrt{x^2-1})^k}{2}\,.$$

We list below some representative properties of Chebyshev polynomials which will be used in the sequel.

Proposition 3.1 *The following properties hold on $T_k(x)$:*

(1) *for every point x in the interval $[-1,1]$, $|T_k(x)| \leq 1$;*

(2) *there are exactly $k+1$ distinct points x in the interval $[-1,1]$ such that $|T_k(x)| = 1$, and the sign of $T_k(x)$ alternates between any two consecutive such points;*

(3) *for every point x in the interval $[-1,1]$, $|T'_k(x)| \leq k^2$.*

We continue to show a simple algebraic identity involving Chebyshev polynomials.

Lemma 3.2 *For every real number $x \neq 1$,*

$$2T_k\left(-\frac{x+1}{x-1}\right) = \left(\frac{\sqrt{x}-1}{\sqrt{x}+1}\right)^k + \left(\frac{\sqrt{x}+1}{\sqrt{x}-1}\right)^k .$$

Proof: By definition of $T_k(x)$,

$$\begin{aligned}
&2T_k\left(-\frac{x+1}{x-1}\right)\\
= &\left(-\frac{x+1}{x-1} + \sqrt{\left(-\frac{x+1}{x-1}\right)^2 - 1}\right)^k + \left(-\frac{x+1}{x-1} - \sqrt{\left(-\frac{x+1}{x-1}\right)^2 - 1}\right)^k\\
= &\left(-\frac{x+1}{x-1} + \frac{1}{x-1}\sqrt{(x+1)^2-(x-1)^2}\right)^k + \left(-\frac{x+1}{x-1} - \frac{1}{x-1}\sqrt{(x+1)^2-(x-1)^2}\right)^k\\
= &\frac{1}{(x-1)^k}\left((-(x+1)+2\sqrt{x})^k + (-(x+1)-2\sqrt{x})^k\right)\\
= &\frac{1}{(x-1)^k}\left((\sqrt{x}-1)^{2k} + (\sqrt{x}+1)^{2k}\right)\\
= &\left(\frac{\sqrt{x}-1}{\sqrt{x}+1}\right)^k + \left(\frac{\sqrt{x}+1}{\sqrt{x}-1}\right)^k ,
\end{aligned}$$

as needed. ■

We refer the reader to the recent monograph [17] for an extensive survey on Chebyshev polynomials.

4 Main Result

Consider an n-dimensional vector space V_q^n and let $\mathcal{A}$ and $\mathcal{B}$ be two V_q^n-consistent property sets on a set X. We address the question:

Assume that for each subspace T of V_q^n such that $\dim(T) \leq k$, $S^{\mathcal{A}}(T) = S^{\mathcal{B}}(T)$. How different can $|\bigsqcup_{v \in V_q^n} \mathcal{A}_v|$ and $|\bigsqcup_{v \in V_q^n} \mathcal{B}_v|$ be?

Clearly, this question is scalable; that is, multiplying each size by a constant will change every answer by the same constant. Hence, it is without loss of generality that we restrict our attention to events in a probability space and assume that all values of interest are in the interval $[0,1]$. We proceed to define:

Definition 4.1

$$E^{(q)}(k,n) \;=\; \sup \left(\left| \bigsqcup_{v \in V_q^n} \mathcal{A}_v \right| - \left| \bigsqcup_{v \in V_q^n} \mathcal{B}_v \right| \right),$$

where the supremum ranges over all families of events, in all probability spaces, that satisfy $S^{\mathcal{A}}(T) = S^{\mathcal{B}}(T)$ *for every subspace* T *of* V_q^n *such that* $\dim(T) \leq k$.

Our aim is to derive bounds on $E^{(q)}(k,n)$. We start by showing that there is no loss of generality in assuming uniformity.

Proposition 4.1 $E^{(q)}(k,n)$ *remains unchanged when* $\mathcal{A}$ *and* $\mathcal{B}$ *are restricted to be uniform.*

Proof: Given non-uniform $\mathcal{A}'$ and $\mathcal{B}'$ realizing $E^{(q)}(k,n)$, we construct uniform property sets $\mathcal{A}$ and $\mathcal{B}$ with the same probabilities of their vector-space unions and, therefore, the same difference between those probabilities. For each j, $1 \leq j \leq n$, the probability of each j-atom in $\mathcal{A}$ is set to the average of the probabilities of all j-atoms in $\mathcal{A}'$, and similarly for $\mathcal{B}$. ■

Henceforth, $\mathcal{A}$ and $\mathcal{B}$ will always be assumed to be uniform. We continue with a key observation that $E^{(q)}(k,n)$ can be expressed as the optimum of a certain linear program.

Proposition 4.2 $E^{(q)}(k,n)$ *is the optimum of the following linear program:*

$$\textit{Maximize} \sum_{i=1}^{n} x_i,$$

subject to the constraints:

(1) *for each* j, $1 \leq j \leq k$, $E_j^{(q)}(x_1, \ldots, x_n) = 0$;

(2) *for each S, $S \subseteq [n]$, $-1 \leq \sum_{i \in S} x_i \leq 1$.*

Proof: Let $\mathcal{A}$ and $\mathcal{B}$ be uniform V_q^n-consistent property sets that realize $E^{(q)}(k,n)$. We show that the optimum of the linear program is at least $E^{(q)}(k,n)$.

We define real numbers $x_1, x_2, \ldots, x_n$ such that constraints (1) and (2) are satisfied and $\sum_{i=1}^n x_i = E^{(q)}(k,n)$.

For each i, $1 \leq i \leq n$, let $x_i = u_i^{\mathcal{A}} - u_i^{\mathcal{B}}$. By Proposition 4.1 and the assumption that $S^{\mathcal{A}}(T) = S^{\mathcal{B}}(T)$ for every subspace T of V_q^n such that $\dim(T) \leq k$, we have that for each j, $1 \leq j \leq k$,

$$\begin{aligned} E_j^{(q)}(x_1, \ldots, x_n) &= E_j^{(q)}(u_1^{\mathcal{A}}, \ldots, u_n^{\mathcal{A}}) - E_j^{(q)}(u_1^{\mathcal{B}}, \ldots, u_n^{\mathcal{B}}) \\ &= r_j^{\mathcal{A}} - r_j^{\mathcal{B}} \\ &= \begin{bmatrix} n \\ j \end{bmatrix}_q (S^{\mathcal{A}}(T) - S^{\mathcal{B}}(T)) \\ &= 0\,. \end{aligned}$$

Thus, constraint (1) is satisfied. For constraint (2), consider any $S \subseteq [n]$, and note that, since for each $i, i' \in [n], i \neq i'$, the events $u_i^{\mathcal{A}}$ and $u_{i'}^{\mathcal{A}}$ (resp., $u_i^{\mathcal{B}}$ and $u_{i'}^{\mathcal{B}}$) are disjoint, it follows that $0 \leq \sum_{i \in S} u_i^{\mathcal{A}} \leq 1$ and $0 \leq \sum_{i \in S} u_i^{\mathcal{B}} \leq 1$. This implies that $|\sum_{i \in S} x_i| = |\sum_{i \in S} u_i^{\mathcal{A}} - \sum_{i \in S} u_i^{\mathcal{B}}| \leq 1$, and constraints of type (2) are also satisfied. Finally, note that

$$\begin{aligned} \left|\bigsqcup_{v \in V_q^n} \mathcal{A}_v\right| - \left|\bigsqcup_{v \in V_q^n} \mathcal{B}_v\right| &= \sum_{\emptyset \sqsubset L \sqsubseteq V} P^{\mathcal{A}}(L) - \sum_{\emptyset \sqsubset L \sqsubseteq V} P^{\mathcal{B}}(L) \\ &= \sum_{i=1}^n \sum_{\dim(L)=i} P^{\mathcal{A}}(L) - \sum_{i=1}^n \sum_{\dim(L)=i} P^{\mathcal{B}}(L) \\ &= \sum_{i=1}^n u_i^{\mathcal{A}} - \sum_{i=1}^n u_i^{\mathcal{B}} \\ &= \sum_{i=1}^n (u_i^{\mathcal{A}} - u_i^{\mathcal{B}}) \\ &= \sum_{i=1}^n x_i\,, \end{aligned}$$

as needed.

In the other direction, let $x_1, x_2, \ldots, x_n$ be real numbers realizing the optimum of the linear program. We show that $E^{(q)}(k,n)$ is at least the optimum of the linear program by constructing uniform, V_q^n-consistent property sets $\mathcal{A}$ and $\mathcal{B}$ such that $|\bigsqcup_{v\in V_q^n}\mathcal{A}_v| - |\bigsqcup_{v\in V_q^n}\mathcal{B}_v| = \sum_{i=1}^n x_i$, and $S^{\mathcal{A}}(T) = S^{\mathcal{B}}(T)$ for each subspace T of V_q^n such that $\dim(T) \leq k$.

For each i, $1 \leq i \leq n$, define $u_i^{\mathcal{A}}$ to be x_i if $x_i > 0$ and 0 otherwise, and define $u_i^{\mathcal{B}}$ to be $-x_i$ if $x_i < 0$ and 0 otherwise. Consider uniform, V_q^n-consistent property sets $\mathcal{A}$ and $\mathcal{B}$ such that the probability of each j-atom in $\mathcal{A}$ (resp., $\mathcal{B}$) is $u_i^{\mathcal{A}}/\begin{bmatrix} n \\ i \end{bmatrix}_q$ (resp., $u_i^{\mathcal{B}}/\begin{bmatrix} n \\ i \end{bmatrix}_q$). Such a collection exists because $u_i^{\mathcal{A}}$'s (resp., $u_i^{\mathcal{B}}$'s) are all non-negative and sum to one. Notice that

$$\begin{aligned}
\left|\bigsqcup_{v\in V_q^n}\mathcal{A}_v\right| - \left|\bigsqcup_{v\in V_q^n}\mathcal{B}_v\right| &= \sum_{i=1}^n \sum_{\dim(L)=i} P^{\mathcal{A}}(L) - \sum_{i=1}^n \sum_{\dim(L)=i} P^{\mathcal{B}}(L) \\
&= \sum_{i=1}^n \begin{bmatrix} n \\ i \end{bmatrix}_q \frac{u_i^{\mathcal{A}}}{\begin{bmatrix} n \\ i \end{bmatrix}_q} - \sum_{i=1}^n \begin{bmatrix} n \\ i \end{bmatrix}_q \frac{u_i^{\mathcal{B}}}{\begin{bmatrix} n \\ i \end{bmatrix}_q} \\
&= \sum_{i=1}^n u_i^{\mathcal{A}} - \sum_{i=1}^n u_i^{\mathcal{B}} \\
&= \sum_{i\in[n]:x_i>0} x_i - \sum_{i\in[n]:x_i<0} (-x_i) \\
&= \sum_{i=1}^n x_i\,.
\end{aligned}$$

Note also that for each j, $1 \leq j \leq k$, for each j-subspace T of V_q^n,

$$S^{\mathcal{A}}(T) - S^{\mathcal{B}}(B) = \frac{E_j^{(q)}(x_1,\ldots,x_n)}{\begin{bmatrix} n \\ j \end{bmatrix}_q} = 0\,,$$

by constraint (2), as needed. ■

To gain more insight, we pass to the dual of the linear program in Proposition 4.2. We observe that the proof of [14, Lemma 4], expressing the optimum of the corresponding linear program as the optimum of its dual, is independent of the particular form of the linear forms E_j, $1 \leq j \leq k$; hence, this result directly applies in our case to yield:

Proposition 4.3 *$E^{(q)}(k,n)$ is given by the optimum of the following linear program:*

$$\textit{Minimize } \max_{i\in[n]}(1 - f_i)\,,$$

over all linear forms $f = \sum_{i=1}^{n} f_i x_i$ that are linear combinations of the linear forms E_j, $1 \leq j \leq k$, and satisfy $f_i \leq 1$ for every i, $1 \leq i \leq n$.

As in [14], the main observation for our solution is made in the next result, where $E^{(q)}(k,n)$ is expressed as the infimum, over a class of polynomials, of the maximum value of a function of these polynomials over the integer set $\{1, 2, \ldots, n\}$. Our next result links our problem with the theory of approximation by polynomials.

Proposition 4.4

$$E^{(q)}(k,n) \;=\; \inf_p \{ \max_{m=1,2,\ldots,n} \{1 - p(q^m)\}\},$$

where the infimum is taken over all polynomials p of degree at most k that have zero constant term and satisfy $p(q^m) \leq 1$ for all integers m, $1 \leq m \leq n$.

Proof: It follows from Lemma 4.3 that for each i, $1 \leq i \leq n$, the coefficient f_i of x_i in f is equal to $\sum_{j=1}^{\min\{i,k\}} \lambda_j \begin{bmatrix} i \\ j \end{bmatrix}_q$, for some real number λ_j. Equation (1) implies that $\begin{bmatrix} i \\ j \end{bmatrix}_q$ is a polynomial of degree j in q^i with zero constant term. Hence, f_i is a polynomial with zero constant term of degree at most $\min\{i,k\} \leq k$ in q^i, as needed. ■

We proceed to estimate $E^{(q)}(k,n)$ in terms of a related quantity, also used in [14].

Definition 4.2

$$D^{(q)}(k,n) \;=\; \inf_p \{ \max_{m \in [n]} \{|p(q^m) - 1|\}\},$$

where the infimum ranges over all polynomials p of degree at most k that have zero constant term.

We continue to show:

Proposition 4.5

$$E^{(q)}(k,n) \;=\; \frac{2D^{(q)}(k,n)}{1 + D^{(q)}(k,n)}$$

Proof: Let r be a polynomial achieving $D^{(q)}(k,n)$ and consider $r' = r/(1+D^{(q)}(k,n))$. We have:

$$\begin{aligned} 1 + D^{(q)}(k,n) &= 1 + \inf_p\{\max_{m\in[n]}\{|p(q^m) - 1|\}\} \\ &= 1 + \max_{m\in[n]}\{|r(q^m) - 1|\} \\ &\geq 1 + |r(q^m) - 1| \\ &\geq r(q^m)\,, \end{aligned}$$

for any $m \in [n]$. This implies that for any $m \in [n]$, $r'(q^m) \leq 1$. Note also that for any $m \in [n]$,

$$1 - r(q^m) \;=\; |r(q^m) - 1| \;\leq\; \max_{m\in[n]}\{|r(q^m) - 1|\} \;=\; D^{(q)}(k,n)\,.$$

This implies that

$$\frac{1 - D^{(q)}(k,n)}{1 + D^{(q)}(k,n)} \;\leq\; \frac{r(q^m)}{1 + D^{(q)}(k,n)} \;=\; r'(q^m)\,,$$

for any $m \in [n]$. This inequality can be written as

$$\frac{2D^{(q)}(k,n)}{1 - D^{(q)}(k,n)} \;\geq\; 1 - r'(q^m)\,,$$

for any $m \in [n]$, which implies, in particular, that

$$\frac{2D^{(q)}(k,n)}{1 - D^{(q)}(k,n)} \;\geq\; \max_{m\in[n]}\{1 - r'(q^m)\} \;\geq\; \inf_p\{1 - p(q^m)\} \;=\; E^{(q)}(k,n)\,.$$

Conversely, let r' be a polynomial achieving $E^{(q)}(k,n)$, and consider $r = 2r'/(2 - E^{(q)}(k,n)$. It similarly follows that

$$\frac{2D^{(q)}(k,n)}{1 - D^{(q)}(k,n)} \;\leq\; E^{(q)}(k,n)\,,$$

as needed. ■

As in [14], the continuous version of the discrete optimization problem of Proposition 4.4 resembles standard questions in approximation theory, a prototype of which asks for a polynomial of a given degree, with leading coefficient one, whose maximum of the absolute value in the interval $[-1,1]$ is minimal over all such polynomials. This prototypical question is answered in terms of Chebyshev polynomials introduced in Section 3. Chebyshev polynomials will play an important role in the present article, as well, as they did in [14].

For the purposes of our analysis, we find it convenient to restate the definition of $D^{(q)}(k,n)$ as follows:

Definition 4.3

$$D^{(q)}(k,n) \;=\; \inf_p\{\max_{m\in\{q,q^2,\ldots,q^n\}}\{|p(m)-1|\}\}\,,$$

where the infimum ranges over all polynomials of degree at most k that have zero constant term.

The next result is shown using properties of Chebyshev polynomials.

Proposition 4.6

$$\frac{1-\frac{k^2}{q^n-q}}{\left|T_k\left(-\frac{q^n+q}{q^n-q}\right)\right|} \;\leq\; D^{(q)}(k,n) \;\leq\; \frac{1}{\left|T_k\left(-\frac{q^n+q}{q^n-q}\right)\right|}$$

Proof: To show the upper bound on $D^{(q)}(k,n)$, consider the polynomial $p_{k,n}$, resulting from the Chebyshev polynomial of order k through a linear transormation,

$$p_{k,n}(x) \;=\; 1-\frac{T_k\left(\frac{2x-(q^n+q)}{q^n-q}\right)}{T_k\left(\frac{-(q^n+q)}{q^n-q}\right)}\;.$$

Note that $p_{k,n}$ has the following properties:

- it is a polynomial of degree k with a zero constant term (it can be readily seen that $p_{k,n}(0)=0$);
- for any $x\in\{q,q^2,\ldots,q^n\}$,

  $$|p_{k,n}(x)-1| \;\leq\; \frac{1}{|T_k(\frac{-(q^n+q)}{q^n-q})|}\,,$$

  since for all such x, $(2x-(q^n+q))/(q^n-q)$ is between -1 and $+1$, implying, by a property of Chebushev polynomials, that $|T_k((2x-(q^n+q))/(q^n-q))|\leq 1$.

It follows that

$$\begin{aligned} D^{(q)}(k,n) \;&=\; \inf_p\{\max_{m\in\{q,q^2,\ldots,q^n\}}\{|p(m)-1|\}\} \\ &\leq\; \max_{m\in\{q,q^2,\ldots,q^m\}}\{|p_{q,n}(m)-1|\} \\ &\leq\; \frac{1}{|T_k(\frac{-(q^n+q)}{q^n-q})|}\,, \end{aligned}$$

as needed.

To show the lower bound on $D^{(q)}(k,n)$, assume, by way of contradiction, that there exists a polynomial $p(x)$, of degree k and with zero constant term, such that

$$\max_{x\in\{q,q^2,\ldots,q^n\}} |p(x)-1| \ < \ \frac{1-\frac{k^2}{q^n-q}}{T_k(-\frac{q^n+q}{q^n-q})},$$

which implies that for all $x \in \{q, q^2, \ldots, q^n\}$,

$$|p(x)-1| \ < \ \frac{1-\frac{k^2}{q^n-q}}{T_k(-\frac{q^n+q}{q^n-q})}.$$

The properties of Chebyshev polynomials mentioned above imply the following properties for $p_{k,n}(x)$:

- There are exactly $k+1$ real points in the interval $[q,q^n]$ such that

  $$|p_{k,n}(x)-1| \ = \ \frac{1}{T_k(\frac{-(q^n+q)}{q^n-q})},$$

  and the sign of $q_{k,n}(x)-1$ alternates between each pair of two such consecutive points. (This follows since for any $x \in [q,q^n]$, $|(2x-(q^n+q))/(q^n-q)| \leq 1$.)

- The derivative $p'_{k,n}(x)$ satisfies the inequality

  $$|p'_{k,n}(x)| \ \leq \ \frac{2k^2}{(q^n-q)\left|T_k\left(-\frac{q^n+q}{q^n-q}\right)\right|},$$

  for all $x \in [q,q^n]$.

Consider the $k+1$ extrema of $p_{k,n}$ and let $z_1, z_2, \ldots, z_{k+1}$ be the integer points nearest to them. Each of these points is at most $1/2$ far from an extremum; thus, by the bound on $q_{k,n}(x)$, it follows that

$$|p_{k,n}(z_i)-1| \ \geq \ \frac{1-\frac{k^2}{q^n-q}}{\left|T_k\left(-\frac{q^n+q}{q^n-q}\right)\right|},$$

for any i, $1 \leq i \leq k+1$; moreover, $p_{k,n}(x)-1$ changes sign between any two consecutive z_i's. Consider the polynomial $p(x)-p_{k,n}(x)(=(p(x)-1)-(p_{k,n}(x)-1))$; it follows from the assumed bound on $|p(x)-1|$ that $p(x)-p_{k,n}(x)$ also changes sign between any two consecutive z_i's. Thus, $p(x)-p_{k,n}(x)$ must have at least k roots in the interval $[q,q^n]$. But, $p(x)-p_{k,n}(x)$ is a polynomial of degree at most k that vanishes at 0 as well. A contradiction. ■

Our final bounds are derived in the next result.

Proposition 4.7 *Consider an n-dimensional vector space V_q^n over $GF(q)$, and let $\mathcal{A}$ and $\mathcal{B}$ be uniform, V_q^n-consistent property sets. Assume that for each subspace T of V_q^n of dimension dim T at most k, $S^{\mathcal{A}}(T) = S^{\mathcal{B}}(T)$. Then,*

$$\frac{|\bigsqcup_{v\in V}\mathcal{A}_v|}{|\bigsqcup_{v\in V}\mathcal{B}_v|} \leq \left(\frac{\lambda^k+1}{\lambda^k-1}\right)^2 ,$$

where $\lambda = (\sqrt{q^{n-1}}+1)/(\sqrt{q^{n-1}}-1)$.

Proof: Let $E^{(q)}(k,n) = |\bigsqcup_{v\in V}\mathcal{A}^*_v|/|\bigsqcup_{v\in V}\mathcal{B}^*_v|$; without loss of generality, set $|\bigsqcup_{v\in V}\mathcal{A}^*_v| = 1$, so that

$$\frac{1}{|\bigsqcup_{v\in V}\mathcal{B}^*_v|} = \frac{1}{1-E^{(q)}(k,n)} = \frac{1+D^{(q)}(k,n)}{1-D^{(q)}(k,n)} ,$$

by Lemma 4.5. We have:

$$\begin{aligned}\frac{|\bigsqcup_{v\in V}\mathcal{A}_v|}{|\bigsqcup_{v\in V}\mathcal{B}_v|} &\leq \frac{1}{|\bigsqcup_{v\in V}\mathcal{B}^*_v|}\\ &= \frac{1+D^{(q)}(k,n)}{1-D^{(q)}(k,n)}\\ &\leq \left(1+\frac{1}{\left|T_k\left(-\frac{q^n+q}{q^n-q}\right)\right|}\right) / \left(1-\frac{1}{\left|T_k\left(-\frac{q^n+q}{q^n-q}\right)\right|}\right) .\end{aligned}$$

For $x = q^{n-1}$, Lemma 3.2 implies that

$$\begin{aligned}T_k\left(-\frac{q^{n-1}+1}{q^{n-1}-1}\right) &= \frac{1}{2}\left(\left(\frac{\sqrt{q^{n-1}}-1}{\sqrt{q^{n-1}}+1}+\right)^k + \left(\frac{\sqrt{q^{n-1}}+1}{\sqrt{q^{n-1}}-1}\right)^k\right)\\ &= \frac{1}{2}(\lambda^k+\lambda^{-k}) .\end{aligned}$$

Hence,

$$\frac{|\bigsqcup_{v\in V}\mathcal{A}_v|}{|\bigsqcup_{v\in V}\mathcal{B}_v|} \leq \frac{1+\frac{2}{\lambda^k+\lambda^{-k}}}{1-\frac{2}{\lambda^k+\lambda^{-k}}} = \frac{\lambda^{2k}+2\lambda^k+1}{\lambda^{2k}-2\lambda^k+1} = \left(\frac{\lambda^k+1}{\lambda^k-1}\right)^2 ,$$

as needed. ■

As an immediate consequence of Proposition 4.7, the next Theorem summarizes our results.

Theorem 4.8 *For any integers k and n, $1 \leq k \leq n$, let $\mathcal{A}$ and $\mathcal{B}$ be V_q^n-consistent, uniform property sets on a set X such that*

$$S^{\mathcal{A}}(T) \;=\; S^{\mathcal{B}}(T)\,,$$

for each subspace T of V_q^n of dimension $\dim(T) \leq k$. *Then,*

(1) *for $k \leq O(\sqrt{q^{n-1}})$,*

$$\frac{|\bigsqcup_{v\in V} \mathcal{A}_v|}{|\bigsqcup_{v\in V} \mathcal{B}_v|} \;\leq\; O\left(\frac{\sqrt{q^{n-1}}}{k}\right)\;;$$

(2) *for $k \geq \Omega(\sqrt{q^{n-1}})$,*

$$\frac{|\bigsqcup_{v\in V} \mathcal{A}_v|}{|\bigsqcup_{v\in V} \mathcal{B}_v|} \;\leq\; 1 + e^{-\Omega\left(\frac{k}{\sqrt{q^{n-1}}}\right)}\,.$$

Proof: Assume first that $k \leq \sqrt{q^{n-1}}$. By Proposition 4.7,

$$\begin{aligned}\frac{|\bigsqcup_{v\in V} \mathcal{A}_v|}{|\bigsqcup_{v\in V} \mathcal{B}_v|} &\leq \left(\frac{\lambda^k+1}{\lambda^k-1}\right)^2 \\ &= \frac{(\sqrt{q^{n-1}}+1)^k + (\sqrt{q^{n-1}}-1)^k}{(\sqrt{q^{n-1}}+1)^k - (\sqrt{q^{n-1}}-1)^k}\,.\end{aligned}$$

Notice, however, that

$$(\sqrt{q^{n-1}}+1)^k + (\sqrt{q^{n-1}}-1)^k \;\leq\; O((\sqrt{q^{n-1}})^k)\,,$$

while

$$(\sqrt{q^{n-1}}+1)^k - (\sqrt{q^{n-1}}-1)^k \;\geq\; k(\sqrt{q^{n-1}})^{k-1}\,.$$

It follows that

$$\begin{aligned}\frac{|\bigsqcup_{v\in V} \mathcal{A}_v|}{|\bigsqcup_{v\in V} \mathcal{B}_v|} &\leq \frac{O((\sqrt{q^{n-1}})^k)}{k(\sqrt{q^{n-1}})^{k-1}} \\ &= O(\frac{(\sqrt{q^{n-1}})^k}{k(\sqrt{q^{n-1}})^{k-1}} \\ &= O(\frac{\sqrt{q^{n-1}}}{k})\,,\end{aligned}$$

as needed.

Assume now that $k > \sqrt{q^{n-1}}$. The proof is completed by standard asymptotic arguments. ■

Theorem 4.8 provides an estimation of the quality of an approximation of $|\bigsqcup_{v\in V}\mathcal{A}_v|$, for a V_q^n-consistent property set $\mathcal{A}$ on a finite set X, obtainable from the sizes of subsets of X whose intersection contains a subspace of V of dimension at most k. In fact, it is possible to effectively compute an approximation attaining the bounds of Theorem 4.8.

Theorem 4.9 *For any integers k and n, $1 \le k \le n$, let $\mathcal{A}$ be a V_q^n-consistent, uniform property set on a set X. Then, we can compute constants $\alpha_1(k,n), \alpha_2(k,n), \ldots, \alpha_k(k,n)$ so that the quantity*

$$\sum_{T:\ \emptyset \sqsubset T \sqsubseteq V_q^n,\ dim\ T \le k} \alpha_{dim\ T}(k,n)\, S^{\mathcal{A}}(T)$$

differs from $|\bigsqcup_{v\in V}\mathcal{A}_{v\in V}|$ by at most a factor of

(1) $O(\frac{q^n}{q^{k^2}})$, *if* $k \le O(\sqrt{q^{n-1}})$;

(2) $1 + e^{-\Omega(k/\sqrt{q^{n-1}})}$, *if* $k \ge \Omega(\sqrt{q^{n-1}})$.

5 Discussion and Future Research

We considered a q-analog of the principle of inclusion-exclusion for the lattice of subspaces of an n-dimensional vector space over a finite field $GF(q)$ and demonstrated that the quality of approximating the size of a certain vector space theoretic union is not good below dimension $\sqrt{n}$. Our result provides more evidence that the q-analog of inclusion-exclusion due to Chen Check this
and Rota [5] is the right q-analog of the principle.

Our result is a geometric lattice analog of the one in [14] for the full Boolean lattice, and answers a question of Linial and Nisan. It is conceivable that similar results on good approximations hold for other lattices as well. Good initial candidates to explore are the lattice of partitions of a finite set [6] and the lattice of faces of the n-cube [16].

More ambitiously, can similar results be derived for the *general* Möbius inversion problem? What are minimal lattice properties for such results to be possible? We conjecture that the achievable quality of approximate Möbius inversion in an appropriate lattice depends critically on its Whitney numbers of the second kind.

Such results might potentially explain previous approximate solutions (e.g., [12, 13]) to counting problems that were based on ad-hoc techniques. Much work is also needed in order to understand the relation of such results to analogous complexity-theoretic ones on the approximability of hard counting problems (see, e.g., [20]), which, however, did not make any links with the underlying combinatorial structure of the problems. We believe that there are deep combinatorial reasons determining the quality of such approximability, which should most appropriately be studied in the context of the rich, classical theory of Möbius inversion.

Acknowledgments:

I am grateful to Professor Gian-Carlo Rota for extremely helpful and inspiring discussions. I would also like to thank N. Linial and N. Nisan whose article *"Approximate Inclusion-Exclusion"* [14] has served as a model for this work.

References

[1] M. Aigner, *Combinatorial Theory,* Springer-Verlag, 1979.

[2] M. Barnabei, A. Brini and G.-C. Rota, "The Theory of Möbius Functions," *Russian Mathematical Surveys,* Vol. 41, No. 3, pp. 135–188, 1986.

[3] D. M. Bressoud, "Unimodality of Gaussian Polynomials," *Discrete Mathematics,* Vol. 99, pp. 17–24, 1992.

[4] L. Carlitz, "q-Bernoulli Numbers and Polynomials," *Duke Journal of Mathematics,* Vol. 15, pp. 987–1000, 1948.

[5] W. Chen and G.-C. Rota, "q-Analogs of the Inclusion-Exclusion Principle and Permutations with Restricted Postion," *Discrete Mathematics,* Vol. 104, pp. 7–22, June 1992.

[6] R. Frucht and G.-C. Rota, "The Möbius Function for Partitions of a Set," *Scientia*, No. 122, pp. 111–115, 1963.

[7] C. Greene and D. J. Kleitman, "Proof Techniques in the Theory of Finite Sets," *MAA Survey in Combinatorics,* ed. G.-C. Rota, pp. 22–79, 1981.

[8] I. Gessel, "A q-analog of the Exponential Formula," *Discrete Mathematics,* 1986.

[9] J. Goldman and G.-C. Rota, "The Number of Subspaces of a Vector Space," *Recent Progress of Combinatorics* (W. Tutte, ed.), pp. 75–83, Academic Press, 1969.

[10] J. Goldman and G.-C. Rota, "On the Foundations of Combinatorial Theory IV: Finite Vector Spaces and Eulerian Generating Functions," *Studies in Applied Mathematics,* Vol. 49, pp. 239–258, 1970.

[11] H. W. Gould, "The q-Stirling Numbers of the First and Second Kind," *Duke Journal of Mathematics,* Vol. 28, pp. 281–289, 1961.

[12] D. Grigoriev and M. Karpinski, "An Approximation Algorithm for the Number of Zeros of Arbitrary Polynomials over $GF[q]$," *Proceedings of the 32nd Annual IEEE Symposium on Foundations of Computer Science,* pp. 662–669, October 1991.

[13] M. Karpinski and M. Luby, "Approximating the Number of Solutions of a $GF[2]$ Polynomial," *Proceedings of the 2nd Annual ACM-SIAM Symposium on Discrete Algorithms,* pp. 300–303, January 1991.

[14] N. Linial and N. Nisan, "Approximate Inclusion-Exclusion," *Combinatorica,* Vol. 10, No. 4, pp. 349–365, 1990.

[15] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics,* Cambridge University Press, 1992.

[16] N. Metropolis and G.-C. Rota, "On the Lattice of Faces of the n-Cube," *Bulletin of the American Mathematical Society,* Vol. 84, No. 2, pp. 284–286, March 1978.

[17] T. J. Rivlin, *Chebyshev Polynomials,* Academic Press, 1990.

[18] G.-C. Rota, "On the Foundations of Combinatorial Theory I: Theory of Möbius Inversion," *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete,* Vol. 2, pp. 340–368, 1964.

[19] B. Sagan, "Inductive Proofs of q-log Concavity," *Discrete Mathematics,* Vol. 99, pp. 289–306, 1992.

[20] L. Stockmeyer, "On Approximation Algorithms for $\#\mathcal{P}$," *SIAM J. Computing,* Vol. 14, pp. 849–861, 1985.

[21] L. G. Valiant, "The Complexity of Computing the Permanent," *Theoretical Computer Science,* Vol. 8, pp. 189–201, 1979.