Limiting Values of the Variance and the Moments of the Dimension of a Sum or Intersection of Random Vector Subspaces

G. D. DIETZ
Department of Mathematics, University of Dayton
Dayton, OH 45469-2316, U.S.A.

D. E. DOBBS
Department of Mathematics, University of Tennessee
Knoxville, TN 37996-1300, U.S.A.

(Received August 2001; accepted October 2001)

Communicated by T. J. Laffey

Abstract—Let $W$ be an $n$-dimensional vector space over a field $F$; for each positive integer $m$, let the $m$-tuples $(U_1, \ldots, U_m)$ of vector subspaces of $W$ be uniformly distributed; and consider the statistics $X_{m,1} := \dim_F(\bigcup_{i=1}^m U_i)$ and $X_{m,2} := \dim_F(\bigcap_{i=1}^m U_i)$. If $F$ is finite of cardinality $q$, we determine $\lim_{q \to \infty} E(X_{m,1})$ and $\lim_{q \to \infty} E(X_{m,2})$, and hence, $\lim_{q \to \infty} \text{var}(X_{m,1})$ and $\lim_{q \to \infty} \text{var}(X_{m,2})$, for any $k > 0$, where the limits are taken as $q \to \infty$ (for fixed $n$). Further, we determine whether these, and other related, limits are attained monotonically. Analogous issues are also addressed for the case of infinite $F$. © 2002 Elsevier Science Ltd. All rights reserved.

Keywords—Expected value, Variance, Moment, Dimension, Vector subspace, Limit, Field.

1. INTRODUCTION

Let $W$ be an $n$-dimensional vector space over a field $F$, for some positive integer $n$. In [1, Theorem 3.4 and Corollary 2.2], it was shown that if the vector subspaces $U$ of $W$ are uniformly distributed, then the random variable $X := \dim_F(U)$ has expected value $E(X) = n/2$. Moreover, for each positive integer $m$, [1] also studied the statistics $X_{m,1} := \dim_F(\bigcup_{i=1}^m U_i)$ and $X_{m,2} := \dim_F(\bigcap_{i=1}^m U_i)$, where all $m$-tuples $(U_1, \ldots, U_m)$ of vector subspaces of $W$ are deemed "equally likely"; note that $X_{1,1} = X = X_{1,2}$. It was shown in [1, Theorems 4.1 and 5.1 and Corollary 5.2] that if $F$ is finite of cardinality $q$, then $\lim_{q \to \infty} E(X_{m,1})$ and $\lim_{q \to \infty} E(X_{m,2})$ can be determined. The values of these limits depend on the parity of $n$ if $m = 2$ but not if $m \geq 3$. Analogously, in case $F$ is infinite, [1, Proposition 5.3] determined $E(X_{m,1})$ and $E(X_{m,2})$. The present paper continues the work in [1] by studying the variance and moments for the statistics $X$, $X_{m,1}$, and $X_{m,2}$, with particular emphasis on the case $m = 1$; if $F$ is finite, we seek, in particular, limiting values as

Both authors were supported in part by the NSF-funded Research Experience for Undergraduates site at the University of Tennessee, Knoxville in 1999.
Properties of Gaussian coefficients and their limiting behavior are studied. In particular, Sections 2-4 treat the case of finite \( F \) (with cardinality \( q \)). Following [1], we let \( \nu_{i,n} \) (or if no confusion can result, \( \nu_i \)) denote the number of \( i \)-dimensional vector subspaces of \( W \). Lemma 2.1 summarizes what we need about these so-called "\( q \)-binomials." Theorem 2.2 then determines the limit, as \( q \to \infty \), of the probability function associated to the discrete random variable \( X \). As a consequence, Corollary 2.3 determines the limiting moments, \( \lim_{q \to \infty} E(X^k) \), and the limiting variance, \( \lim_{q \to \infty} \text{var}(X) \); both answers depend on the parity of \( n \). By way of contrast, if \( q \) is fixed (that is, if \( F \) is fixed) and \( k > 1 \), then Proposition 2.4 establishes that \( \lim_{n \to \infty} E(X^k) = \infty \).

Section 3 studies the possible monotonicity of the above, and other related, limit processes. Broadly speaking, one can say in summary that the "naturally occurring" limits for \( q \to \infty \) are "eventually" monotonic decreasing (in a sense made precise in Section 3); in this regard, see Theorem 3.1 for \( \lim_{q \to \infty} E(X^k) \) and Proposition 3.3 for \( \lim_{q \to \infty} \text{var}(X) \). On the other hand, Proposition 3.5 establishes that \( \lim_{n \to \infty} (E(X^k)/E(X)) \) is attained in a "pseudo-monotonic" increasing manner (made precise in Section 3); and with the subscript denoting the dimension of the ambient vector space \( W \), Theorem 3.6 shows that \( \lim_{n \to \infty} (E(E(X^k)/E_{k+1}(X^k)) \) may fail even to be attained in a "pseudo-monotonic" manner, depending on whether \( k \geq 2 \).

Section 4 is the analogue for \( m > 1 \) of the studies in Section 2. We treat the relevant limiting moments and variances of \( X_{m,1} \) and \( X_{m,2} \) first in case \( m = 2 \) (see Proposition 4.1) and then for \( m \geq 3 \) (see Proposition 4.2).

Section 5 is devoted to the analogues of the above work in case \( F \) is infinite. Especially noteworthy in Section 5 is the "confidence interval" import of Theorem 5.1(c), namely, that \( \inf \{ k > 0 : \lim_{n \to \infty} \mathbb{P}(|X - \mu| < k\sigma) = 1 \} = \sqrt{3} \) if \( F \) is infinite. It is clear from Corollary 2.3 that finite base fields do not support similar behavior.

In the interest of clarity, we occasionally fine-tune the above notation by using subscripts that specify some or all of the prevailing parameters. Thus, we use notation such as \( E_{q,n} \) and \( \text{var}_q \) without further comment. In addition, if \( F \) is finite, it is convenient to let \( N := N_n = \sum_{i=0}^n \nu_{i,n} \), the number of vector subspaces of \( W \).

## 2. LIMITING MOMENTS AND VARIANCE FOR A SINGLE SUBSPACE OVER A FINITE FIELD

Throughout Sections 2-4, our riding hypothesis is that \( F \) is a finite field of cardinality \( q \) (and that \( W \) is an \( n \)-dimensional \( F \)-space). Sections 2 and 3 focus on the case \( m = 1 \), that is, on the statistic \( X \). In particular, Section 2 determines some relevant limits associated to \( X \). We begin by collecting some useful information about Gaussian coefficients \( \nu_{i,n} \).

**Lemma 2.1.**

(a) \( \nu_{i-1,n} = \nu_{i,n} \) if \( i = 0, 1, \ldots, n \).

(b) For each \( n \geq 1 \) and \( 0 \leq i \leq n \), there exists a monic integral polynomial (independent of \( q \)) such that its degree is \( (n-i)i \), all its coefficients are positive, and its value at \( q \) is \( \nu_{i,n} \) for each (prime-power) \( q \).
(c) Fix \( n \geq 1 \), and let \( i = 0,1, \ldots, n \). Then the degree of the polynomial in (b) is maximized precisely when \( i = n/2 \) if \( n \) is even; and precisely when \( i = (n - 1)/2, (n + 1)/2 \) if \( n \) is odd.

(d) For fixed \( q \) and \( n \), let \( p \) be the probability function associated to the discrete random variable \( X \); that is, \( p(i) = \binom{n}{i} \left( \frac{1}{2^k} \right)^i \left( 1 - \frac{1}{2^k} \right)^{n-i} \) for \( i = 0,1, \ldots, n \). Then \( E(X) = \sum_{i=0}^{n} ip(i) = n/2 \).

The proofs of the preceding can be either found directly in or derived easily from [1, Corollaries 3.2 and 3.3, Theorem 3.4] and [4, equation (23)]. Then Theorem 2.2 follows easily from Parts (b) and (c) of Lemma 2.1.

**Theorem 2.2.** Fix \( n \geq 1 \). Let \( p = p_n \) be the probability function associated to the random variable \( X \), as defined in the statement of Lemma 2.1(d). (Recall that \( X = \text{dim}_F(U) \), where \( U \) varies uniformly over the vector subspaces of \( W \).) If \( i = 0,1, \ldots, n \), then

\[
\lim_{q \to \infty} p_q(i) = \left\{ \begin{array}{ll}
\delta_{i,n/2}, & \text{if } n \text{ is even,} \\
\frac{1}{2} (\delta_{i,(n-1)/2} + \delta_{i,(n+1)/2}), & \text{if } n \text{ is odd.}
\end{array} \right.
\]

**Corollary 2.3.** Fix \( n \geq 1 \). Then we have the following.

(a) If \( k > 0 \), then

\[
\lim_{q \to \infty} \mathbb{E}_q(X^k) = \left\{ \begin{array}{ll}
\frac{n^k}{2^k}, & \text{if } n \text{ is even,} \\
2^{k+1} ((n-1)^k + (n+1)^k), & \text{if } n \text{ is odd.}
\end{array} \right.
\]

(b) \[
\lim_{q \to \infty} \text{var}_q(X) = \left\{ \begin{array}{ll}
0, & \text{if } n \text{ is even,} \\
\frac{1}{4}, & \text{if } n \text{ is odd.}
\end{array} \right.
\]

It is customary for \( k \) to be a positive integer when speaking of “the \( k \)th moment” of a random variable. However, in pursuing moment-like calculations such as those in Corollary 2.3, we shall assume only that, as above, \( k \) is a positive real number.

We close Section 2 with a result that initiates our study of limiting statistics as \( n \to \infty \).

**Proposition 2.4.** Fix \( q \); that is, fix \( F \). Let \( k > 1 \). For each \( d \geq 1 \), let \( E_d(X^k) \) denote the expected value of \( X^k \) if \( \text{dim}_F(W) = d \). Then \( \lim_{n \to \infty} E_n(X^k) = \infty \).

**Proof.** Let \( M > 0 \). Put \( B := 2M + 1 \). It suffices to show that if \( n > B \), then \( E_n(X^k) > M \). Fix \( n > B \). We need only show that \( \sum_{i=0}^{n} i^k \nu_{i,n} > MN \).

Consider the function defined by \( f(x) = x^k + (n - x)^k \) for \( 0 \leq x \leq \lfloor n/2 \rfloor \). (As usual, \( \lfloor \ldots \rfloor \) denotes the floor, or greatest-integer, function.) Since \( f'(x) = k[x^{k-1} - (n - x)^{k-1}] < 0 \) for \( 0 < x < \lfloor n/2 \rfloor \), we see by the mean value theorem that \( f \) is minimized at \( x = n/2 \) (respectively, \( x = (n - 1)/2 \) if \( n \) is even (respectively, odd). It follows that \( i^k + (n - i)^k \geq 2M \) if \( 0 \leq i \leq \lfloor n/2 \rfloor \). Therefore, by the symmetry result in Lemma 2.1(a),

\[
\sum_{i=0}^{n} i^k \nu_{i,n} = \begin{cases} 
\sum_{i=0}^{(n-2)/2} (i^k + (n - i)^k) \nu_{i,n} + \binom{n}{2} \nu_{n/2,n}, & \text{if } n \text{ is even,} \\
\sum_{i=0}^{(n-1)/2} (i^k + (n - i)^k) \nu_{i,n}, & \text{if } n \text{ is odd,} \\
2M \sum_{i=0}^{(n-2)/2} \nu_{i,n} + M \nu_{n/2,n}, & \text{if } n \text{ is even,} \\
2M \sum_{i=0}^{(n-1)/2} \nu_{i,n}, & \text{if } n \text{ is odd,}
\end{cases} = MN.
\]
3. RATIOS AND MONOTONICITY

The first three results of this section establish “eventual” monotonicity for certain sequences as \( q \to \infty \) (with \( n \) fixed). We begin with a deeper analysis of the limit processes studied in Corollary 2.3.

**THEOREM 3.1.** Fix \( n > 1 \). Then there exists (a prime-power) \( q_0 > 0 \) such that for each \( k > 1 \), the sequence \( \{E_q(X^k) : \text{prime-power } q > q_0 \} \) is monotonically decreasing, and for each \( 0 < k < 1 \), the sequence \( \{E_q(X^k) : \text{prime-power } q > q_0 \} \) is monotonically increasing.

**PROOF.** We give the proof for \( k > 1 \), as the proof carries over in case \( 0 < k < 1 \), mutatis mutandis. As \( E_q(X^k) = \sum_{i=0}^{n} i^k v_i N/N \) where \( N = \sum_{i=0}^{n} v_{i,n} \), it follows from Lemma 2.1(b) that for each \( k \), we may view \( E_q(X^k) \) as a positive rational function of the positive real variable \( q \). Accordingly, it suffices to find \( q_0 > 0 \) such that \( q_0 \) is independent of \( k > 1 \) and \( \frac{d}{dq}(E_q(X^k)) < 0 \) for all \( q > q_0 \). Now,

\[
\frac{d}{dq}(E_q(X^k)) = \frac{1}{N^2} \left[ \left( \sum_{i=0}^{n} \nu_i \right) \left( \sum_{i=0}^{n} i^k \nu_i' \right) - \left( \sum_{i=0}^{n} i^k \nu_i \right) \left( \sum_{i=0}^{n} \nu_i' \right) \right] = \frac{1}{N^2} \sum_{i=0}^{n} \sum_{j=0}^{n} i^k (\nu_i' \nu_j - \nu_i \nu_j').
\]

Thus, in view of the symmetry result in Lemma 2.1(a), we have that

\[
\frac{d}{dq}(E_q(X^k)) = \begin{cases} \frac{2}{N^2} \sum_{i=0}^{(n-1)/2} \sum_{j=0}^{(n-1)/2} (i^k + (n-i)^k) (\nu_i' \nu_j - \nu_i \nu_j'), & \text{if } n \text{ is odd,} \\ \frac{1}{N^2} \sum_{i=0}^{n/2-1} \sum_{j=0}^{n/2-1} (i^k + (n-i)^k) (\nu_i' \nu_j - \nu_i \nu_j') + \sum_{i=0}^{n/2-1} (i^k + (n-i)^k - 2 \left( \frac{n}{2} \right)^k) (\nu_i' \nu_{n/2} - \nu_i \nu'_{n/2}), & \text{if } n \text{ is even.} \end{cases}
\]

We shall find \( q_0 > 0 \) such that each of the just-displayed sums is negative for all \( q > q_0 \).

We suppose that \( n \) is odd (leaving the case of even \( n \) for the reader). Consider the \((i,j)\)-term, namely, \((i^k + (n-i)^k)(\nu_i' \nu_j - \nu_i \nu_j')\). If this term is nonnegative, then \( \nu_i' \nu_j \geq \nu_i \nu_j' \). The only concern arises if this inequality persists as \( q \to \infty \). However, if \( i \neq j \), Lemma 2.1(b) ensures that \( \nu_i' \nu_j - \nu_i \nu_j' \) is an integral polynomial in \( q \) with leading term \( ((n-i)i-(n-j)j)q^{(n-i)i+(n-j)j-1} \). As \((n-x)x\) is strictly increasing for \( 0 \leq x \leq (n-1)/2 \), \( \nu_i' \nu_j - \nu_i \nu_j' \) is of what may be termed “maximal q-degree”, namely \((n-i)i+(n-j)j-1\), as long as \( i \neq j \). In the case \( i = j \), \( \nu_i' \nu_j - \nu_j' \nu_i \) vanishes and so may be ignored. Also note that if \( 0 \leq i, j \leq (n-1)/2 \), and \((n-i)i-(n-j)j > 0 \), then \( i > j \). Thus, if the \((i,j)\)-term occasions concern, then \( i > j \). Moreover, in that case, we claim that the \((j,i)\)-term is not only negative, but it is also greater in absolute value than the \((i,j)\)-term. To prove the claim, it suffices to show that if \( 0 \leq j < i \leq (n-1)/2 \), then \( i^k + (n-i)^k < j^k + (n-j)^k \), as \( \nu_i' \nu_j - \nu_i \nu_j' \) and \( \nu_j' \nu_i - \nu_j \nu_i' \) each have the same “maximal q-degree” with opposite leading coefficients. In fact, \( f(x) := x^k + (n-x)^k \) defines a strictly decreasing function for \( 0 \leq x \leq (n-1)/2 \), since \( f'(x) = k[x^{k-1} - (n-x)^{k-1}] < 0 \). Therefore, the claim has been proved. As \( n \geq 3 \), there exists \((i,j)\) so that \( 0 \leq j < i \leq (n-1)/2 \), and so the argument shows that the sum describing \( \frac{d}{dq}(E_q(X^k)) \) is “eventually” negative, that is, negative for all \( q \) exceeding some \( q_0 \). Notice that the positive factors \( i^k + (n-i)^k \) played no role after we arrived at the inequality \( \nu_i' \nu_j \geq \nu_i \nu_j' \), and so \( q_0 \) may be chosen independently of \( k \). \]

We pause to explain why Theorem 3.1 did not treat the cases \( n = 1 \) and \( k = 1 \). If \( n = 1 \) and \( k > 0 \), then \( E_q(X^k) = v_1/v_0 + v_1 = 1/2 \); and if \( k = 1 \) and \( n \geq 1 \), then \( E_q(X^k) = n/2 \) by Lemma 2.1(d). Thus, if \( n = 1 \) or \( k = 1 \), then \( \{E_q(X^k) : \text{prime-power } q \} \) is a constant sequence, and so does not satisfy the “strictly” monotonic conclusion in Theorem 3.1.

**COROLLARY 3.2.** Fix \( n \geq 1 \). If \( q_0 \) is as in the statement of Theorem 3.1, then the sequence \( \{\text{var}_q(X) : \text{prime-power } q > q_0 \} \) is monotonically decreasing.

We next determine the limit of one of the ratios mentioned in the title of this section, and we identify its underlying monotonicity. Part (a) follows from Lemma 2.1(d) and Corollary 2.3(a),
while Part (b) follows since the proof of Theorem 3.1 ensures that $\frac{d}{dq}(E_q(X^k)) < 0$ for all $q >$ some $q_0$.

**PROPOSITION 3.3.** Fix $n \geq 1$. Then we have the following.

(a) If $k > 0$, then

$$\lim_{q \to \infty} \frac{E_q(X^k)}{E_q(X)} = \begin{cases} \left(\frac{n}{2}\right)^{k-1}, & \text{if } n \text{ is even,} \\ \frac{1}{2^k} \left[\frac{(n-1)^k + (n+1)^k}{n}\right], & \text{if } n \text{ is odd.} \end{cases}$$

(b) Let $q_0$ be as in the statement of Theorem 3.1. If $k > 1$ (respectively, $0 < k < 1$), then the sequence \{E_q(X^k)/E_q(X) : prime-power $q > q_0$\} is monotonically decreasing (respectively, monotonically increasing).

We devote the rest of this section to studying limits as $n \to \infty$ (for fixed $q$). In (3.4)–(3.6), we often write $E_d$ instead of $E_{q,d}$ for the sake of brevity; this notation should not be confused with the above $E_q$ notation, for it was $n$ (rather than $q$) that was fixed in discussing $E_q$ in the earlier results. Although computer-generated data suggest monotonicity conclusions in Theorem 3.4 and Proposition 3.5, we have only been able to establish what might be termed “pseudo-monotonicity”.

**THEOREM 3.4.** Let $k > 1$. Then for each positive integer $n$, there exists a prime-power $q_0 > 0$ such that $E_{q,n}(X^k) < E_{q,n+1}(X^k)$ for all $q > q_0$.

**PROOF.** $E_{n}(X^k) < E_{n+1}(X^k)$ if and only if

$$\frac{E_{n+1}(X^k)}{E_{n}(X^k)} = \left(\sum_{i=0}^{n+1} \left(\sum_{i=0}^{n+1} \frac{n_i \nu_{i,n+1}}{\nu_{i,n+1}}\right)\right) \left(\sum_{i=0}^{n} \nu_{i,n}\right) = \frac{\sum_{i=0}^{n+1} \sum_{j=0}^{n} i^k \nu_{i,n+1} \nu_{j,n}}{\sum_{i=0}^{n+1} \sum_{j=0}^{n} j^k \nu_{i,n+1} \nu_{j,n}} > 1;$$

that is, if and only if $\sum_{i=0}^{n} \sum_{j=0}^{n} (i^k - j^k) \nu_{i,n+1} \nu_{j,n} > 0$. Now, by Lemma 2.1(a),

$$\sum_{i=0}^{n} \sum_{j=0}^{n} (i^k - j^k) \nu_{i,n+1} \nu_{j,n} = \begin{cases} 2 \sum_{i=0}^{n} \left(\sum_{j=0}^{n} \left(\frac{n+1-i}{2}\right)^k - \frac{n-i}{2} \nu_{(n+1)/2,n+1} \nu_{n,i}\right), & \text{if } n \text{ is odd,} \\ 2 \sum_{i=0}^{n/2} \sum_{j=0}^{n/2-1} \frac{n}{2} \nu_{i,n+1} \nu_{j,n} = \frac{n}{2} \nu_{i,n+1} \nu_{j,n} + 2 \sum_{i=0}^{n} \left(\frac{n+1-i}{2}\right)^k - \frac{n-i}{2} \nu_{(n+1)/2,n+1} \nu_{n,i}, & \text{if } n \text{ is even.} \end{cases}$$

For fixed $n \geq 1$, we shall find $q_0 > 0$ such that each of the just-displayed sums is positive for all $q > q_0$.

Suppose first that $n$ is even. (The case of odd $n$ is handled similarly.) By calculus, $i^k + (n+1-i)^k - 2(n/2)^k > 0$ if $0 \leq i \leq n/2$. (Observe that the function defined by $x^k + (n+1-x)^k$ has negative derivative for $0 \leq x \leq n/2$.) Hence, each term of the singly-indexed sum is positive. We turn to the doubly-indexed sum. If the term indexed by $(n/2, j)$ is negative for arbitrary large $q$, we claim that its absolute value is exceeded, for all sufficiently large $q$, by the (positive) $(j+1)$-term of the singly-indexed sum. Indeed, it suffices to compare the degrees (in $q$) of these terms,
as the \((j + 1)\)-term has a nonvanishing leading coefficient, and hence, is of "maximal q-degree": note, using Lemma 2.1(c), that
\[
\deg(\nu_{n/2,n+1}) + \deg(\nu_{j,n}) < \deg(\nu_{j+1,n+1}) + \deg(\nu_{n/2,n}).
\]

Also, by the above upshot of calculus, if \(0 \leq i \leq j + 1 \leq n/2\), then the \((i,j)\)-term of the doubly-indexed sum is positive. Therefore, if the \((i,j)\)-term is nonpositive and \(i \neq n/2\), then \(i > j + 1\) and we need only show that its absolute value is exceeded, for all sufficiently large \(q\), by the term indexed by \((j + 1, i)\). Similarly to the proof of Theorem 3.1, each coefficient of the \((j + 1, i)\)‐term is strictly positive. Hence, the term is of "maximal q-degree" and once again, the verification can be done by comparing degrees. With the help of Lemma 2.1(b),(c)
\[
\deg(z_{i,n+1}) + \deg(\nu_{j,n}) = (n+1-i)i+(n-j)j < (n-j)(j+1)+(n-i)i = \deg(\nu_{j+1,n+1}) + \deg(\nu_{i,n}),
\]
the inequality holding since \(i + j < n\). As in the proof of Theorem 3.1, a suitable \(q_0\) can now be found independently of \(k\).

The next result follows easily from Lemma 2.1(d),(a); in the proof of Part (b), one also needs to argue as in the first step of the proof of Theorem 3.4.

**Proposition 3.5.** Let \(k > 1\). Then we have the following.

(a) \(\lim_{n \to \infty}(E_{q,n}(X^k)/E_{q,n}(X)) = \infty\), the convergence being uniform in \(q\).

(b) For each positive integer \(n\), there exists (a prime-power) \(q_0 > 0\) such that
\[
\frac{E_{q,n}(X^k)}{E_{q,n}(X)} < \frac{E_{q,n+1}(X^k)}{E_{q,n+1}(X)},
\]
for all \(q > q_0\).

It is interesting to note that the conclusion of Proposition 3.5(b) may be rephrased as follows: \(E_{q,n+1}(X^k)/E_{q,n}(X^k) > 1 + 1/n\) for all \(q > q_0\).

While Theorem 3.1 and Proposition 3.3(b) showed that the size of \(k\) can affect the increasing/decreasing nature of certain monotonic limits processes of statistics as \(q \to \infty\), Theorem 3.6 shows that the size of \(k\) can affect whether other limit processes of statistics are (pseudo-) monotonic as \(n \to \infty\).

**Theorem 3.6.** If \(n \geq 1\), \(k > 0\), and \(q \geq 2\) is a prime-power, let
\[
a_n := a_{q,n,k} := \frac{E_{q,n}(X^k)}{E_{q,n+1}(X^k)},
\]
then we have the following.

(a) If \(n\) is a positive even integer, then there exists (a prime-power) \(q_0 > 0\) such that for all \(k > 0\), \(a_n < a_{n+1}\) for all (prime-powers) \(q > q_0\).

(b) Let \(k > 0\). Then there exists \(M > 0\) such that if \(n\) is an odd integer and \(n > M\), then there exists (a prime-power) \(q_0 > 0\) such that if \(k \geq 2\) (respectively, \(0 < k < 2\)), then \(a_n > a_{n+1}\) (respectively, \(a_n < a_{n+1}\)) for all (prime-powers) \(q > q_0\).

**Proof.** For the moment, consider any positive integer \(n\), any real number \(k > 0\), and any prime-power \(q\). Observe that \(a_n < a_{n+1}\) if and only if \((E_{n+1}(X^k))^2 > E_{n+2}(X^k)E_n(X^k)\); that is, if and only if
\[
\sum_{w=0}^{n/2} \sum_{i=0}^{n+1} \sum_{j=0}^{n+1} \sum_{z=0}^{n} ((ij)^k - (wz)^k) \nu_{w,n+2+i,n+1+1} \nu_{j,n+1+1} \nu_{z,n} > 0.
\]
Similarly, \(a_n > a_{n+1}\) if and only if the above quadruply-indexed sum is negative. We determine next when \(\Delta := \deg(\nu_{w,n+2+i,n+1+1} \nu_{j,n+1+1} \nu_{z,n})\) is maximized.
Suppose first that \( n \) is even. Then Lemma 2.1(c) shows that \( \Delta \) is maximized precisely when \( w = (n + 2)/2, \ i \in \{n/2, (n + 2)/2\}, \ j \in \{n/2, (n + 2)/2\}, \) and \( z = n/2. \) Thus, when the above quadruply-indexed sum is expressed as an integral polynomial in \( q, \) a straightforward calculation reveals that its leading coefficient is

\[
\sum_{i=n/2}^{(n+2)/2} \sum_{j=n/2}^{(n+2)/2} (ij)^k - \left( \frac{n+2}{2} \right)^k \left( \frac{n}{2} \right)^k - \frac{1}{2^{2k}} [(n+2)^k - n^k]^2 > 0.
\]

Accordingly, for all sufficiently large \( q \) (the lower bound \( q_0 \) being independent of \( k \)), the quadruply-indexed sum is indeed positive. Hence, (a) follows.

Now, suppose that \( n \geq 5 \) is odd. By Lemma 2.1(c), \( \Delta \) is maximized precisely when \( w \in \{(n + 1)/2, (n + 3)/2\}, \ i = j = (n + 1)/2, \) and \( z \in \{(n - 1)/2, (n + 1)/2\}. \) Thus, when the above quadruply-indexed sum is expressed as an integral polynomial in \( q, \) a calculation shows that its leading coefficient is

\[
\sum_{w=(n+1)/2}^{(n+3)/2} \sum_{z=(n-1)/2}^{(n+1)/2} \left( \left( \frac{n+1}{2} \right)^{2k} - (wz)^k \right) = \frac{1}{2^{2k}} \left[ 3(n+1)^{2k} - (n+3)^k(n+1)^k - (n+3)^k(n-1)^k - (n+1)^k(n-1)^k \right].
\]

To prove (b), it suffices to show that

\[
c := 3(n+1)^{2k} - (n+3)^k(n+1)^k - (n+3)^k(n-1)^k - (n+1)^k(n-1)^k
\]

is negative (respectively, positive) for all sufficiently large \( n \) if \( k \geq 2 \) (respectively, \( 0 < k < 2 \)).

Notice that \( c \) has the same algebraic sign as

\[
d := cn^{-2k} = 3(1+\frac{1}{n})^{2k} - \left( 1+\frac{3}{n} \right)^k \left( 1+\frac{1}{n} \right)^k - \left( 1+\frac{3}{n} \right)^k \left( 1-\frac{1}{n} \right)^k - \left( 1+\frac{1}{n} \right)^k \left( 1-\frac{1}{n} \right)^k.
\]

To study \( d, \) consider the function \( f \) defined by

\[
f(x) := 3(1+x)^{2k} - (1+3x)^k(1+x)^k - (1+3x)^k(1-x)^k - (1+x)^k(1-x)^k.
\]

By Newton’s binomial theorem, for \( |x| < 1/3, \) the factors \((1+x)^{2k}, \ (1+3x)^k, \) and \((1\pm x)^k\) are each given by absolutely convergent power series; hence, by Mertens’ theorem, \( f(x) \) can be simplified by Cauchy multiplication if \( |x| < 1/3. \) Straightforward calculation reveals that in the resulting Maclaurin series for the analytic function \( f, \) both the constant coefficient and the coefficient of \( x \) are zero. Moreover, the coefficient of \( x^2 \) is seen to be \(-4k^2 + 8k = 4k(2 - k)\). Thus,

\[
f(x) = 4k(2 - k)x^2 + x^3g(x)
\]

for some analytic function \( g, \) if \( |x| < 1/3. \) As analytic functions are continuous, \( \lim_{x \to 0^+} (f(x)/x^2) = 4k(2 - k). \) So, if \( k > 2 \) (respectively, \( 0 < k < 2 \)), there exists \( \delta > 0 \) such that if \( 0 < x < \delta, \) then \( f(x) \) is negative (respectively, positive). Thus, if \( n > 1/\delta \), we see that \( d = f(1/n) \) is negative (respectively, positive), and so (b) has been established for all \( k \neq 2. \) Finally, if \( k = 2, \) the defining expression for \( f \) simplifies with the aid of the (algebraic) binomial theorem, yielding \( f(x) = -16x^4, \) whence \( d = f(1/n) = -16n^{-4} < 0 \) (and \( c = -16 < 0 \)), to complete the proof.  

**Remark 3.7.** Although Theorem 3.6(b) resolves the situation for all sufficiently large odd \( n, \) its methodology can be used, in principle, to study any particular “small” odd \( n. \)
4. MULTIPLE SUBSPACES

For \( m \geq 2 \), this brief, elementary section states some results on the statistics \( X_{m,1} \) and \( X_{m,2} \) over finite fields that are analogous to the studies in Section 2. In the spirit of Section 2 and the earlier literature, we emphasize limiting values for \( q \to \infty \). Material concerning relevant probability functions and expected value formulas useful in proving the following results can be derived easily from [1, Theorems 4.1 and 5.1 and Corollary 5.2]. We begin with the analogue of Corollary 2.3 for \( m \geq 2 \).

**Proposition 4.1.** Fix \( n \geq 1 \) and \( k > 0 \). Then we have the following.

(a) \[
\lim_{q \to \infty} E(X_{2,1}^k) = \begin{cases} 
n^k, & \text{if } n \text{ is even}, \\
\frac{(n-1)^k + 3n^k}{4}, & \text{if } n \text{ is odd}.
\end{cases}
\]

(b) \[
\lim_{q \to \infty} E(X_{2,2}^k) = \begin{cases} 
0, & \text{if } n \text{ is even}, \\
\frac{1}{4}, & \text{if } n \text{ is odd}.
\end{cases}
\]

(c) \[
\lim_{q \to \infty} \text{var}(X_{2,1}) = \lim_{q \to \infty} \text{var}(X_{2,2}) = \begin{cases} 
0, & \text{if } n \text{ is even}, \\
\frac{3}{16}, & \text{if } n \text{ is odd}.
\end{cases}
\]

**Proposition 4.2.** Fix \( m \geq 3 \) and \( k > 0 \). Then we have the following.

(a) If \( n = 1 \), then \( E(X_{m,1}^k) = (2m - 1)/2m \) for all \( q \).

(b) If \( n > 1 \), then \( \lim_{q \to \infty} E(X_{m,1}^k) = n^k \).

(c) If \( n = 1 \), then \( E(X_{m,2}^k) = 1/2m \) for all \( q \).

(d) If \( n > 1 \), then \( \lim_{q \to \infty} E(X_{m,2}^k) = 0 \).

(e) If \( n = 1 \), then \( \text{var}(X_{m,1}) = \text{var}(X_{m,2}) = (1/2m)(1 - 1/2m) \) for all \( q \).

(f) If \( n > 1 \), then \( \lim_{q \to \infty} \text{var}(X_{m,1}) = \lim_{q \to \infty} \text{var}(X_{m,2}) = 0 \).

5. THE CASE OF AN INFINITE BASE FIELD

In this section, our *riding hypothesis* is that \( F \) is an infinite field, and we consider analogues of some of the above work that was done over finite fields. Analogues of Propositions 4.1 and 4.2 for infinite base fields are easily derived by combining [1, Corollary 2.2 and Proposition 5.3] with the definition of expected value and the formula for variance. The probability function associated to the random variable \( X \) is needed to prove the following results and can be found in [1, Corollary 2.2(a)].

The following result documents how differently the probability distribution for \( X \) behaves from that of any random variable \( Y \) enjoying a normal (or Gaussian) distribution with mean \( \mu \) and standard deviation \( \sigma \). Theorem 5.1(a) might lead one to expect that \( X \) is more widely "scattered" than \( Y \), but Theorem 5.1(b),(c) indicate quite the opposite. The proof of Theorem 5.1 is omitted for reasons of space and can be obtained by contacting the authors directly.

**Theorem 5.1.** Assume that the field \( F \) is infinite. Let \( \mu \) and \( \sigma \) denote the mean and standard deviation, respectively, of \( X \). (In fact, \( \mu = n/2 \) by [1, Corollary 2.2(a)]; and \( \sigma = \sqrt{(n(n-2))/12} \) (respectively, \( 1/4 \)) if \( n \geq 2 \) (respectively, if \( n = 1 \)). Then we have the following.

(a) \( \lim_{n \to \infty} P(|X - \mu| < \sigma) = 1/(\sqrt{3}) \approx 0.577. \)

(b) If \( n \neq 2 \), then \( P(|X - \mu| < 2\sigma) = 1 \). If \( n = 2 \), then \( P(|X - \mu| \leq 2\sigma) = 1 \).

(c) \( \inf\{k > 0 : \lim_{n \to \infty} P(|X - \mu| < k\sigma) = 1\} = \sqrt{3} \approx 1.732. \)

The deepest results in this paper are, arguably, Theorems 3.4, 3.6, and 5.1. We close by stating an analogue of Theorems 3.4 and 3.6 for infinite base fields.
PROPOSITION 5.2. Assume that $F$ is an infinite field. If $k > 0$, then

$$\lim_{n \to \infty} \frac{E_n(X^k)}{E_{n+1}(X^k)} = 1.$$ 

REFERENCES