BULL. AUSTRAL. MATH. SOC. 15A03, 12E99, 60C05
VOL. 45 (1992) [467–477]

THE EXPECTED DIMENSION OF A SUM OF VECTOR SUBSPACES

DAVID E. DOBBS AND MARK J. LANCASTER

Let W be an n-dimensional vector space over a field F. It is shown that the expected dimension of a vector subspace of W is $n/2$. If F is infinite, the expected dimension of a sum of a pair of subspaces of W is $(n+1)/2$ if $n > 1$; and $3/4$ if $n = 1$. If F is finite, with q elements, the expected dimension of a sum of subspaces of W depends on q and n. For fixed n, the limiting value of this expectation as $q \to \infty$ is n if n is even; and $n - 1/4$ if n is odd. Moreover, if F is finite and $n > 1$, the expected dimension of a sum of three (not necessarily distinct) subspaces of W has limit n as $q \to \infty$.

1. INTRODUCTION

The problems discussed in this article have the following geometric motivation. Consider the usual two- (respectively three-) dimensional space of geometric vectors in the Euclidean plane (respectively in Euclidean three-space). The "typical" vector subspace is a line (respectively line or plane) through the origin, and hence its "expected" dimension is 1 (respectively, as likely to be 1 as 2, say 3/2). To generalise such observations, one may ask for the expected dimension of a subspace of an n-dimensional vector space. As the above examples suggest, the answer is $n/2$. This is proved in Corollary 2.2(a) in case the underlying field of scalars is infinite, and in Theorem 3.4 in case the field is finite.

A related question asks for the "typical" dimension of a sum of two subspaces of an n-dimensional space. In case the underlying field of scalars is infinite, we show via cardinal arithmetic in Corollary 2.2(b) that if $n > 1$, then this expected dimension is $(n+1)/2$, or equivalently that the expected dimension of an intersection of subspaces is $(n-1)/2$. Contrary to what was announced in the preceding paragraph, the situation is different in case the underlying field is finite, say with q elements. As shown in Example 3.6, this expected value of the dimension of the sum depends on both q and n. The main result of this paper is the determination of the limiting tendency of this function of (fixed) n as $q \to \infty$. As one might expect, this limiting value is asymptotic to n, but, somewhat surprisingly, this value depends on the parity of n. If n is even, the limiting value is n (see Theorem 4.1); if n is odd, the limiting value is $n - 1/4$ (see

Received 29 May 1991

Theorem 5.1). It is noteworthy that the analysis for odd n in Section 5 depends on the result established in Section 4 for even n; both sections depend on the counting results regarding subspaces over finite fields in Section 3.

2. The infinite field case

We begin by establishing *running hypotheses and notation* for the rest of this paper. Let W be an n-dimensional vector space over a field F, where n is a positive integer. For each integer i, $0 \leqslant i \leqslant n$, let ν_i be the cardinality of the set B_i of i-dimensional subspaces of W.

We proceed to calculate the ν_i in case F is infinite. Our calculations assume the usual facts about arithmetic with infinite cardinal numbers (for instance, $\alpha + \alpha = \alpha$ for infinite α) that follow from Zorn's Lemma.

Proposition 2.1. *Assume that* $\operatorname{card}(F) = \alpha$ *is infinite. If* i *is an integer such that* $1 \leqslant i \leqslant n-1$, *then* $\nu_i = \alpha$.

Proof: Let A be the set of (ordered) i-tuples of linearly independent vectors in W, and let $B = B_i$ be the set of i-dimensional subspaces of W. The function $A \to B$, $(w_1, \ldots, w_i) \mapsto \operatorname{span}(\{w_1, \ldots, w_i\})$, is evidently surjective, and so $\nu_i = \operatorname{card}(B) \leqslant \operatorname{card}(A)$. Using an F-basis of W, we see that $\operatorname{card}(W) = \alpha^n = \alpha$. It follows that $\alpha \leqslant \operatorname{card}(A) \leqslant \alpha^i = \alpha$, and so $\nu_i \leqslant \alpha$. To complete the proof, it suffices to find an injection $F \to B$ (for then $\alpha \leqslant \nu_i$). To this end, choose an F-basis $\{v_1, \ldots, v_n\}$ of W and, for each scalar r, define $W_r = \operatorname{span}(\{v_1, \ldots, v_{i-1}, v_i + rv_{i+1}\})$. Then the desired injection is given by $r \mapsto W_r$. Indeed, it is straightforward to verify that each $W_r \in B$; and that $v_i + rv_{i+1} \in W_r \setminus W_s$ if r and s are distinct scalars. □

Using intuitive combinatorial probability, we next infer the desired expected values in case F is infinite.

Corollary 2.2. *Assume that* $\operatorname{card}(F) = \alpha$ *is infinite. Then:*

(a) *The expected dimension of a subspace of* W *is* $n/2$.

(b) *The expected dimension of the sum of a pair of subspaces of* W *is* $(n+1)/2$ *if* $n > 1$; *and* $3/4$ *if* $n = 1$.

(c) *The expected dimension of the intersection of a pair of subspaces of* W *is* $(n-1)/2$ *if* $n > 1$; *and* $1/4$ *if* $n = 1$.

Proof: (a) Evidently, $\nu_0 = 1 = \nu_n$. Suppose that $n > 1$. In view of Proposition 2.1, the intuitive "frequency" approach leads to the probability function p given by $p(0) = 0 = p(n)$ and $p(i) = 1/(n-1)$ for $1 \leqslant i \leqslant n-1$. The expected dimension is therefore $\Sigma j p(j) = (1 + \ldots + n - 1)/(n-1) = [(n-1)n/2]/(n-1) = n/2$. In case $n = 1$, the function p satisfies $p(0) = 1/2 = p(1)$, and so the expected dimension is $(0+1)1/2 = 1/2 = n/2$.

https://doi.org/10.1017/S0004972700030367 Published online by Cambridge University Press

(b) For any subspaces U and V of W, $\dim(U+V) = \dim(U) + \dim(V) - \dim(U \cap V)$. Since "expected value" is a linear operator, the assertion will follow from (a) and (c); for instance, if $n > 1$, then $E(\dim(U+V)) = n/2 + n/2 - (n-1)/2 = (n+1)/2$.

(c) Suppose that $n > 1$. The number of subspaces of W is $1+\alpha+\ldots+\alpha+1 = \alpha$. Since each subspace V of W can trivially be expressed as $V \cap W$, it follows that if $0 \leqslant i \leqslant n-1$, there are (at least, hence exactly) α ways to express i-dimensional subspaces as intersections of an ordered pair of (possibly equal) subspaces of W. Of course, there is only one way to express W as such an intersection, namely as $W \cap W$. Hence, the appropriate probability function p satisfies $p(n) = 0$ and $p(i) = 1/n$ for $0 \leqslant i \leqslant n-1$. The expected value is therefore $\Sigma j p(j) = (0+\ldots+n-1)/n = [(n-1)n/2]/n = (n-1)/2$. Finally, if $n = 1$, one of the four ordered pairs of subspaces leads to the intersection being W; this leads to the function given by $p(0) = 3/4$, $p(1) = 1/4$ and the expected value $\Sigma j p(j) = 1/4$. □

REMARK 2.3. In the proof of Corollary 2.2(b), it was assumed that $E(\dim(U)) = E(\dim(V)) = n/2$. While this may be intuitively clear on the basis of Corollary 2.2(a), it will be helpful to sketch a rigorous proof.

As above, assume that F is an infinite field and W is an n-dimensional F-vector space, where n is a positive integer. Let $k \geqslant 2$ be a positive integer, and let $(U_1, \cdots, U_k)$ range over (ordered) k-tuples of subspaces of W. (In Corollary 2.2, $k = 2$, but the extra generality will be needed in Proposition 5.3.) Then $E(\dim(U_i)) = n/2$ for each i, $1 \leqslant i \leqslant k$.

For the proof, observe first that the case $n = 1$ is easy. Assume $n > 1$ and, for definiteness, take $i = 1$. Consider the random variables $X_j = \dim(U_j)$ for $1 \leqslant j \leqslant k$. Recall that W has α subspaces of dimension d for each $d = 1, \cdots, n-1$. Hence the probability function $p(x_1, \cdots, x_k)$ vanishes at the 2^k k-tuples whose components are either 0 or n; and p takes the value $1/[(n+1)^k - 2^k]$ at the other $(n+1)^k - 2^k$ k-tuples. The marginal probability function $p_1(j) = \Sigma p(j, x_2, \cdots, x_k)$ therefore satisfies $p_1(j) = (n+1)^{k-1}/[(n+1)^k - 2^k]$ for $j = 1, \cdots, n-1$ and $p_1(n) = [(n+1)^{k-1} - 2^{k-1}]/[(n+1)^k - 2^k]$. It follows that $E(\dim(U_1)) = [1 + \cdots + (n-1)](n+1)^{k-1}/[(n+1)^k - 2^k] + n[(n+1)^{k-1} - 2^{k-1}]/[(n+1)^k - 2^k]$. Since $1 + \cdots + (n-1) = (n-1)n/2$, this simplifies to $n/2$, as asserted.

In the proofs of Sections 4 and 5 (which pertain to finite F), it will also be necessary to observe rigorously that $E(\dim(U_i)) = n/2$, but that is a much simpler matter which can be left to the reader.

3. THE FINITE FIELD CASE

An additional *running hypothesis* for the rest of this paper is that the field F

is finite, say with q elements. In this section, Theorem 3.4 presents the analogue of Corollary 2.2(a) by finding the expected dimension of a subspace of W (in case F is finite). In Sections 4 and 5, analogues of Corollary 2.2(b), (c) are developed. If $1 \leqslant d \leqslant n$, it will be convenient to let u_d denote the number of invertible $d \times d$ matrices with entries in F. We begin with a useful result that gives formulas for u_d and ν_i.

PROPOSITION 3.1. *(a) If $1 \leqslant d \leqslant n$, then*

$$u_d = (q^d - 1)(q^d - q)(q^d - q^2) \cdots (q^d - q^{d-1}).$$

(b) If $1 \leqslant i \leqslant n$, then $\nu_i = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{i-1})/u_i$.

PROOF: (a) This assertion is well known and is included here for reference purposes.

(b) We adapt the proof of Proposition 2.1. Let A be the set of (ordered) i-tuples of linearly independent vectors in W, and let B be the set of i-dimensional subspaces of W. The function $g: A \to B$, $(w_1, \ldots, w_i) \mapsto \operatorname{span}(\{w_1, \ldots, w_i\})$, is evidently surjective. Now, $\operatorname{card}(B) = \nu_i$ and it is easy to see (as in the standard proof of (a)) that $\operatorname{card}(A) = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{i-1})$. Therefore, to complete the proof, it suffices to show that the g-preimage of each element of B has cardinality u_i. In other words, we must show that if $(w_1, \ldots, w_i) \in A$, then there are exactly u_i elements $(v_1, \ldots, v_i) \in A$ such that $\operatorname{span}(\{v_1, \ldots, v_i\}) = \operatorname{span}(\{w_1, \ldots, w_i\})$. This, in turn, follows because such $(v_1, \ldots, v_i)$ are in one-to-one correspondence with the invertible F-linear endomorphisms of $\operatorname{span}(\{w_1, \ldots, w_i\})$, that is, with the invertible $i \times i$ matrices with entries in F. □

The proof of Theorem 3.4 will be facilitated with the aid of the following symmetry result.

COROLLARY 3.2. *If $0 \leqslant i \leqslant n$, then $\nu_i = \nu_{n-i}$.*

PROOF: A computational proof of this assertion is available via Proposition 3.1(b); we leave the detailed verification to the reader. There is a more conceptual proof, which has the additional benefit of not depending on the riding hypothesis that F is finite. We give this proof next, using dual spaces and their properties.

If $0 \leqslant j \leqslant n$, we again let B_j denote the set of j-dimensional subspaces of W. If $V \in B_i$, then $\operatorname{Ann}(V) = \{f \in W^* : f(v) = 0 \text{ for each } v \in V\}$ is in B_{n-i}. Indeed, $\operatorname{Ann}(V)$ is the kernel of the restriction epimorphism from W^* to V^*, so that $W^*/\operatorname{Ann}(V) \cong V^*$; then equating dimensions leads to $\dim(W) - \dim(\operatorname{Ann}(V)) = \dim(V)$, whence $\operatorname{Ann}(V) \in B_{n-i}$. Now, fix any F-vector-space isomorphism $g: W^* \to W$. It follows that the assignment $V \mapsto g(\operatorname{Ann}(V))$ gives a function from B_i to B_{n-i}. It suffices to show that this function is injective; for then $\nu_i \leqslant \nu_{n-i}$ and, by the same

argument with i replaced by $n-i$, we would obtain the reverse inequality. Hence, it suffices to show that if V_1 and V_2 in B_i satisfy $\mathrm{Ann}(V_1) = \mathrm{Ann}(V_2)$, then $V_1 = V_2$. Consider the natural isomorphism $\gamma: W \to W^{**}$. For each subspace V of W, it is easy to verify that $\gamma(V) \subset \mathrm{Ann}(\mathrm{Ann}(V))$ is an inclusion of two spaces having the same dimension, so that $\gamma(V) = \mathrm{Ann}(\mathrm{Ann}(V))$. In particular, $\gamma(V_1) = \gamma(V_2)$, whence $V_1 = V_2$. □

Next, we record another upshot of Proposition 3.1. Its statement will be useful in asymptotic arguments in Sections 4 and 5. It asserts that ν_i is an $(ni - i^2)$-degree polynomial in q with integer coefficients. It is important to note that these coefficients do not depend on q.

COROLLARY 3.3. *If $0 \leqslant i \leqslant n$, then the formula in Proposition 3.1(b) gives a polynomial $f \in \mathbb{Z}[X]$ of degree $(n-i)i$ such that $\nu_i = f(q)$.*

PROOF: The assertion is clear if i is 0 or n (for ν_i is then the constant 1). Also, $\nu_{n-1} = \nu_1 = (q^n - 1)/(q-1) = q^{n-1} + q^{n-2} + \cdots + q + 1$ and so we may assume that $2 \leqslant i \leqslant n-2$. Consider $g, h \in \mathbb{Z}[X]$ given by

$$g = (X^n - 1)(X^{n-1} - 1)(X^{n-2} - 1) \cdots (X^{n-i+1} - 1)$$

and

$$h = (X^i - 1)(X^{i-1} - 1)(X^{i-2} - 1) \cdots (X - 1).$$

After some cancellation, we see via Proposition 3.1(b) that $\nu_i = f(q)$, where f is the complex rational function given by $f = g/h$. It suffices to show that $f \in \mathbb{Z}[X]$ (for the assertion about degree would then be clear).

Evidently, none of the displayed factors of g or h has repeated roots. Moreover, if $r \in \mathbb{C}$ is a root of h of multiplicity k, then r is a root of g of multiplicity at least k. (This is clear if $r = 1$, in which case $k = i$. Assume that $r \neq 1$, with order m $(\geqslant 2)$ in the group $\mathbb{C} \setminus \{0\}$. Then $1 \leqslant k = [i/m] \leqslant i$. If λ is the minimal integer such that $n - i + 1 \leqslant \lambda m$, it follows that $(\lambda - 1)m \leqslant n - i$, and so $(\lambda + k - 1)m \leqslant n - i + km \leqslant n$. Hence, r is a root of g of multiplicity at least k.) Thus, $f \in \mathbb{C}[X]$. As g and h have integral coefficients, it now follows from uniqueness of the remainder in the division algorithm that $f \in \mathbb{Z}[X]$. □

We next present the main result of this section.

THEOREM 3.4. *If F is finite, then the expected dimension of a subspace of W is $n/2$.*

PROOF: Dimension of a subspace of W is a discrete random variable X taking on the values $0, 1, \cdots, n$. Let p denote the associated probability function. It will be convenient to let Σ_j denote a sum of terms as x ranges from 0 to j. In case n is odd,

https://doi.org/10.1017/S0004972700030367 Published online by Cambridge University Press

say $n = 2e + 1$, we have the expected value

$$E(X) = \Sigma x p(x) = \Sigma_e x p(x) + [(e+1)p(e+1) + \cdots + np(n)]$$
$$= \Sigma_e x p(x) + \Sigma_e (n-x)p(n-x).$$

Since $p(n-x) = p(x)$ according to the symmetry result, Corollary 3.2, $E(X) = \Sigma_e[x + (n-x)]p(x) = n\Sigma_e p(x)$. However, $\Sigma_e p(x) = 1/2$ by symmetry, and so $E(X) = n/2$ if n is odd.

Assume now that n is even, say $n = 2e$. In this case, we may argue as above, via symmetry, that $\Sigma_{e-1} x p(x) + [(e+1)p(e+1) + \cdots + np(n)] = n\Sigma_{e-1} p(x)$. Therefore, adding $ep(e)$ to this sum, we have $E(X) = n[\Sigma_{e-1} p(x) + p(e)/2] = (n/2)S$, where $S = 2\Sigma_{e-1} p(x) + p(e)$. By symmetry, $S = \Sigma_n p(x) = 1$, and so $E(X) = n/2$ in this case as well. □

The next counting result will be of use in Sections 4 and 5, as well as in Example 3.6, which serves as motivation for those sections.

PROPOSITION 3.5. *Let V be a d-dimensional subspace of W, where $0 \leqslant d \leqslant n-1$. Then the number of $(d+1)$-dimensional subspaces of W which contain V is $(q^n - q^d)/(q^d(q-1))$.*

PROOF: Let $A = W \setminus V$ and let B be the set of $(d+1)$-dimensional subspaces of W which contain V. The function $g: A \to B$, given by $w \mapsto \text{span}(V \cup \{w\})$, is evidently surjective. As in the proof of Proposition 3.1, $\text{card}(A) = q^n - q^d$, and so it suffices to show that the g-preimage of each element of B has cardinality $q^d(q-1)$. In other words, we must show that if $w_1 \in A$, then there are exactly $q^d(q-1)$ elements $w_2 \in A$ such that $\text{span}(V \cup \{w_1\}) = \text{span}(V \cup \{w_2\})$. This, in turn, follows because if $(v_1, \cdots, v_d)$ is an F-basis of V, then such w_2 are the linear combinations $\Sigma r_j v_j + r w_1$, with scalars r_j, $r \in F$ such that $r \neq 0$; of course, the number of such $(r_1, \cdots, r_d, r)$ is $q^d(q-1)$. □

It remains to develop the analogues of Proposition 2.2(b), (c) for finite F. This is done in Sections 4 and 5. Data motivating that work are given next in this section's final result.

EXAMPLE 3.6: (a) Assume that $n = 1$. Just as in the proof of Corollary 2.2(c), we see that if (U, V) ranges over ordered pairs of subspaces of W, then $E(\dim(U \cap V)) = 1/4$ and $E(\dim(U + V)) = 3/4$.

(b) Assume that $n = 2$. Using Proposition 3.1, we see that the number of subspaces of W is $N = \nu_0 + \nu_1 + \nu_2 = 1 + (q^2 - 1)/(q-1) + 1 = q + 3$; so the number of ordered pairs (U, V) of subspaces of W is $N^2 = q^2 + 6q + 9$. Only one of these, namely (W, W), leads to the intersection W. Moreover, the number of pairs that lead to a one-dimensional intersection is $\nu_1 + 2\nu_1 = 3q + 3$. (The first summand counts

self-intersections of one-dimensional subspaces; the second, inclusions/containments of one-dimensional subspaces in W.) Thus, the number of ordered pairs that lead to the intersection 0 is $N^2 - 1 - (3q+3) = q^2 + 3q + 5$. If the discrete random variable $\dim(U \cap V)$ is denoted by X, then the associated probability function p is given by $p(0) = (q^2 + 3q + 5)/N^2$, $p(1) = (3q+3)/N^2$ and $p(2) = 1/N^2$. It follows that $E(\dim(U \cap V)) = \Sigma j p(j) = (3q+5)/(q^2 + 6q + 9)$. Notice that this expression depends on q. Moreover, as $q \to \infty$, this expression has limit 0. (Indeed, it is easy to check via calculus that the convergence to 0 is monotonic.) As in the proof of Corollary 2.2(b), it now follows from Theorem 3.4 and linearity of the operator E that $E(\dim(U+V)) = 2/2 + 2/2 - E(\dim(U \cap V)) = (2q^2 + 9q + 13)/(q^2 + 6q + 9)$; notice that, as $q \to \infty$, this expression increases monotonically to 2.

(c) Assume that $n = 3$. Using Proposition 3.1, we see that the number of subspaces of W is $N = \nu_0 + \nu_1 + \nu_2 + \nu_3 = 1 + (q^2 + q + 1) + (q^2 + q + 1) + 1 = 2q^2 + 2q + 4$; so the number of ordered pairs (U, V) of subspaces of W is $N^2 = 4q^4 + 8q^3 + 20q^2 + 16q + 16$. The nature of the various intersections $U \cap V$ can be determined by reasoning as above and using the following observations. If $U \in B_1$ and $V \in B_2$ (or the other way around), apply Proposition 3.5; if U, V are distinct elements of B_2, observe that their sum is W (for reasons of dimension), and so their intersection has dimension 1. If the discrete random variable $\dim(U \cap V)$ is denoted by X, then the associated probability function p is given by $p(0) = (3q^4 + 4q^3 + 8q^2 + 5q + 7)/N^2$, $p(1) = (q^4 + 4q^3 + 9q^2 + 8q + 5)/N^2$, $p(2) = (3q^2 + 3q + 3)/N^2$ and $p(3) = 1/N^2$. It follows that $E(\dim(U \cap V)) = \Sigma j p(j) = (q^4 + 4q^3 + 15q^2 + 14q + 14)/N^2$. Notice that this expression depends on q. Moreover, as $q \to \infty$, this expression has limit 1/4. (Indeed, it is easy to check via calculus that this convergence to 1/4 is monotonic decreasing. In order to motivate Theorem 5.1, this fact should be compared with the result in (a).) As in (b), it now follows that $E(\dim(U+V)) = 3/2 + 3/2 - E(\dim(U \cap V))$; you may verify readily that, as $q \to \infty$, this expression increases monotonically to $3 - 1/4$: for motivational purposes, this should be compared with the corresponding result in (a).

(d) Assume that $n = 4$. If one tries to analyse the expected dimension of $U \cap V$, complications enter that were not present in (a)–(c). The interested reader may verify that the expected values are easier to find in this case if one focuses first on sums rather than on intersections. We leave the details to such readers but, for the purpose of motivating Theorem 4.1, we note the following upshots (which should be compared with the results in (b)). As $q \to \infty$, $E(\dim(U \cap V))$ has limiting value 0 and $E(\dim(U+V))$ has limiting value 4.

4. The case of finite F and even n

Suppose that n is even, say $n = 2e$. According to Proposition 3.3, if $0 \leqslant i \leqslant n$,

then ν_i can be expressed as a (monic) polynomial in q of degree $(2e-i)i$. It is easy to see that this degree is maximised only once, namely at $i=e$. (The point is that if $0 \leqslant i < j \leqslant e$, then $(2e-i)i < (2e-j)j$.) It follows that N, the number of subspaces of W, is a monic polynomial in q of degree $(2e-e)e = e^2$. Accordingly, if we are interested only in the limit of either $E(\dim(U+V))$ or $E(\dim(U \cap V))$ as $q \to \infty$, it suffices to count the dimensions of sums (or intersections) arising from $U, V \in B_e$. This is done in the next result, which is motivated by Example 3.6(b), (d). Its proof is a generalisation of the analysis suggested in Example 3.6(d).

THEOREM 4.1. *Assume that F is finite and n is even. Then $\lim_{q\to\infty} E(\dim(U+V)) = n$ and $\lim_{q\to\infty} E(\dim(U\cap V)) = 0$.*

PROOF: By Theorem 3.4, $E(\dim(U\cap V)) = n/2 + n/2 - E(\dim(U+V))$, and so it suffices to prove the first assertion. To this end, we claim that if $U \in B_e$, then the number of $V \in B_e$ such that $U+V=W$ is the e^2-power of q.

Given the claim, it follows that the probability function p associated with $\dim(U+V)$ assigns to n some integral rational function in q whose numerator and denominator are each monic of degree $2e^2$. (This is clear for the denominator N^2. As for the numerator, one need simply apply the claim, in conjunction with the case $i=e$ of Corollary 3.3. We shall see that the coefficients of this rational function do not depend on q.) Therefore, if $j \neq n$, then p assigns to j an integral rational function in q whose numerator has degree less than $2e^2$ (and whose denominator is N^2). It follows that in applying $\lim_{q\to\infty}$ to $E(\dim(U+V)) = \Sigma j p(j)$, the first n terms each have limit 0 and the last term has limit n; that is, $\lim_{q\to\infty} E(\dim(U+V)) = n$, as desired.

It remains only to prove the above claim. Let $B = \{V \in B_e : U+V=W\}$ and let A be the set of (ordered) e-tuples of vectors forming bases of elements in B. The function $G\colon A \to B$, $(v_1, \ldots, v_e) \mapsto \operatorname{span}(\{v_1, \ldots, v_e\})$, is evidently surjective. Now, since $\operatorname{card}(U) = q^e$, we see (as in the standard proof of Proposition 3.1(a)) that $\operatorname{card}(A) = (q^n - q^e)(q^n - q^{e+1})(q^n - q^{e+2}) \cdots (q^n - q^{n-1})$. Moreover, the G-preimage of each element of B has cardinality u_e. Indeed, if $(v_1, \ldots, v_e) \in A$, then there are exactly u_e elements $(w_1, \ldots, w_e) \in A$ such that $\operatorname{span}(\{v_1, \ldots, v_e\}) = \operatorname{span}(\{w_1, \ldots, w_e\})$ because such $(w_1, \ldots, w_e)$ are in one-to-one correspondence with the invertible F-linear endomorphisms of $\operatorname{span}(\{v_1, \ldots, v_e\})$. Therefore

$$\operatorname{card}(B) = (q^n - q^e)(q^n - q^{e+1})(q^n - q^{e+2}) \cdots (q^n - q^{n-1})/u_e.$$

It remains to show that the above expression for $\operatorname{card}(B)$ reduces to just the e^2-power of q. To see this, express u_e via Proposition 3.1(a) and, using $n=2e$, perform algebraic cancellations. □

5. The case of finite F and odd n

In this section, it will be convenient to *refine notation* by letting $\nu_{i,d}$ denote the number of i-dimensional subspaces of a given d-dimensional F-vector space; ν_i will continue to mean $\nu_{i,n}$.

Suppose that n is odd, say $n = 2e+1$. According to Proposition 3.3, if $0 \leqslant i \leqslant n$, then ν_i can be expressed as a (monic) polynomial in q of degree $(2e+1-i)i$. This degree is maximised only twice, namely at $i = e$ and at $i = e+1$; the maximum value is $e^2 + e$. It follows that N, the number of subspaces of W, is an integral polynomial in q whose term of highest degree is $2q^{e(e+1)}$. Hence, N^2 is an integral polynomial in q with leading term $4q^{2e(e+1)}$. Accordingly, if we are interested only in the limit of either $E(\dim(U+V))$ or $E(\dim(U \cap V))$ as $q \to \infty$, it suffices to count the dimensions of sums (or intersections) arising from at least $4q^{2e(e+1)}$ pairs (U, V) of subspaces of W. By the above comments, we may restrict attention to $U, V \in B_e \cup B_{e+1}$. This is done in the next result, which is motivated by Example 3.6(a), (c). Its proof depends on both Section 3 and Section 4.

Theorem 5.1. *Assume that F is finite and n is odd. Then* $\lim_{q\to\infty} E(\dim(U+V)) = n - 1/4$ *and* $\lim_{q\to\infty} E(\dim(U \cap V)) = 1/4$.

Proof: As in the proof of Theorem 4.1, we see via Theorem 3.4 and linearity of the operator E that it suffices to prove the first assertion.

First, consider $U \in B_e$. We claim that the number of $V \in B_{e+1}$ such that $U + V = W$ is (at least) given by a monic integral polynomial in q of degree $e(e+1)$. By reasoning as in the proof of Theorem 4.1, we see that this number is given by

$$(q^n - q^e)(q^n - q^{e+1})(q^n - q^{e+2}) \cdots (q^n - q^{n-1})/u_{e+1}.$$

Using Proposition 3.1(a), we simplify the displayed quantity to $q^{e(e+1)}$, thus proving the claim. Now, allowing (U, V) to vary over $B_e \times B_{e+1}$, we find $q^{e(e+1)}\nu_e$ pairs (U, V) such that $\dim(U+V) = n$. Using Corollary 3.3, we see that the number of such pairs is a monic integral polynomial in q of degree $2e(e+1)$. Consequently, the number of pairs $(U, V) \in (B_e \times B_{e+1} \cup B_{e+1} \times B_e)$ such that $U + V = W$ is (at least) $2q^{2e(e+1)} + \cdots$, where $\cdots$ denotes terms of lower degree in q.

Next, consider (U, V) ranging over $B_e \times B_e$. Fix a $2e$-dimensional subspace Y of W. By the proof of Theorem 4.1, the number of (U, V) such $U + V = Y$ is a monic integral polynomial in q of degree $2e^2$. Now, the number of such Y is $\nu_{2e} = \nu_{n-2e} = \nu_1$, which, by Corollary 3.3, is a $2e$-degree monic integral polynomial in q. Hence, the number of (U, V) in $B_e \times B_e$ such that $\dim(U+V) = 2e$ is a monic integral polynomial in q of degree $2e^2 + 2e = 2e(e+1)$.

Next, we claim that the number of pairs $(U, V) \in B_{e+1} \times B_{e+1}$ such that $U + V = W$ is asymptotic to (at least) $q^{2e(e+1)} + \cdots$. Given this claim (and the above remarks),

https://doi.org/10.1017/S0004972700030367 Published online by Cambridge University Press

it follows that the probability function p associated with $\dim(U+V)$ assigns to n a function having limit 0 as $q \to \infty$ plus some integral rational function in q of the form $\left(3q^{2e(e+1)} + \cdots\right)/N^2$; and to $2e = n-1$, p assigns a function having limit 0 as $q \to \infty$ plus an integral rational function in q of the form $\left(q^{2e(e+1)} + \cdots\right)/N^2$. Recalling that $N^2 = 4q^{2e(e+1)} + \cdots$, we see that the limit of the expected dimension of the sum of a pair of subspaces of W is $(n-1)1/4 + n(3/4) = n - 1/4$, as asserted.

It remains only to prove the above claim that there are, asymptotically, at least $q^{2e(e+1)} + \cdots$ elements $(U, V) \in B_{e+1} \times B_{e+1}$ such that $U + V = W$. Fix $U \in B_{e+1}$. As in the second paragraph of this proof, one may show that there are $q^{e(e+1)}$ elements $Y \in B_e$ such that $U + Y = W$. According to Proposition 3.5, each such Y is contained in $(q^n - q^e)/(q^e(q-1)) = q^e + q^{e-1} + \cdots + 1$ elements $V \in B_{e+1}$. In this way, the fixed U leads nominally to $q^{e(e+1)}\left(q^e + q^{e-1} + \cdots + 1\right)$ elements $V \in B_{e+1}$ such that $U + V = W$. However, different Y may lead to the same V, and so there has been an overcount. A given V arises at most $\nu_{e,e+1} = \nu_{1,e+1} = q^e + \cdots$ times from different Y. Therefore, the desired number of ordered pairs is at least

$$\nu_{e+1}\left(q^{e(e+1)}\left(q^e + q^{e-1} + \cdots + 1\right)\right)/(q^e + \cdots).$$

Since $\nu_{e+1} = q^{e(e+1)} + \cdots$, the displayed product is asymptotic to $q^{e(e+1)+e(e+1)+e-e} = q^{2e(e+1)}$. □

We can now say what happens to the limit of expected dimension when more than two subspaces of W are summed or intersected.

COROLLARY 5.2. *Assume that F is a finite field (with q elements) and W is an n-dimensional F-vector space, where n is a positive integer. Let $k \geqslant 3$ be a positive integer, and let $(U_1, \cdots, U_k)$ range over (ordered) k-tuples of subspaces of W. Then:*

(a) *If $n = 1$, then $\lim_{q\to\infty} E(\dim(U_1 + \cdots + U_k)) = 1 - 1/2^k$ and $\lim_{q\to\infty} E(\dim(U_1 \cap \cdots \cap U_k)) = 1/2^k$.*

(b) *If $n \geqslant 2$, then $\lim_{q\to\infty} E(\dim(U_1 + \cdots + U_k)) = n$ and $\lim_{q\to\infty} E(\dim(U_1 \cap \cdots \cap U_k)) = 0$.*

PROOF: (a) If $n = 1$, it suffices to observe that $\Sigma U_i = W$ and $\cap U_i = 0$ for all but one of the 2^k k-tuples $(U_1, \cdots, U_k)$.

(b) By Theorem 4.1, we may assume that n is odd, say $n = 2e+1$, with $e \geqslant 1$. Without loss of generality, $k = 3$. By the proof of Theorem 5.1, $\dim(U_1 + U_2) = n$ for "essentially" three-fourths of the triples (U_1, U_2, U_3). ("Essentially", in this context, will mean that the quantity in question has limit 3/4 as $q \to \infty$.) Also by the proof of Theorem 5.1, $\dim(U_1 + U_2) = n - 1$ for the remaining "essentially" one-fourth of the triples.

Suppose that a triple satisfies $\dim(U_1 + U_2) = n - 1$. Then the probability that $U_3 \subset U_1 + U_2$ is

$$p = (\nu_{0,n-1} + \nu_{1,n-1} + \cdots + \nu_{n-1,n-1})/(\nu_{0,n} + \nu_{1,n} + \cdots + \nu_{n,n}).$$

By the earlier arguments in Sections 4 and 5, p is asymptotic to $(q^e)^e/2q^{e(e+1)}$, which tends to 0 as $q \to \infty$. Therefore, the probability that (the given) U_1, U_2 and U_3 sum to W (that is, sum to an n-dimensional space) approaches 1 as $q \to \infty$.

It follows that $\lim_{q\to\infty} E(\dim(U_1 + U_2 + U_3)) = (3/4)n + (1/4)n = n$.

As for intersections, we see from the proof of Theorem 5.1 that "essentially" three-fourths of the triples satisfy $U_1 \cap U_2 = 0$ and "essentially" the remaining fourth satisfy $\dim(U_1 \cap U_2) = 1$ (or, equivalently, $\dim(U_1 + U_2) = n - 1$).

Suppose that a triple satisfies $\dim(U_1 \cap U_2) = 1$. Then the probability that $U_1 \cap U_2 \subset U_3$ is $p = \nu_{1,j}/\nu_{1,n}$ where $j = \dim(U_3)$. If $j \neq n$, it follows from Corollary 3.3 that $p < 1/q$. The probability that $j = n$ is $1/\Sigma\nu_i$, which approaches 0 as $q \to \infty$. Therefore, the probability that a given triple satisfies $U_1 \cap U_2 \cap U_3 = 0$ approaches 1 as $q \to \infty$.

It follows that $\lim_{q\to\infty} E(\dim(U_1 \cap U_2 \cap U_3)) = (3/4)0 + (1/4)0 = 0$. □

In contrast to the above result over finite fields, it is interesting to note that over infinite fields, the expected dimension of sums or intersections of subspaces of W does not change when the number of subspaces being summed or intersected increases beyond 2. Indeed, we have the following result. Its proof, which is similar to that of Corollary 2.2, is left to the reader.

PROPOSITION 5.3. *Assume that F is an infinite field and W is an n-dimensional F-vector space, where n is a positive integer. Let $k \geqslant 2$ be a positive integer, and let $(U_1, \cdots, U_k)$ range over (ordered) k-tuples of subspaces of W. Then:*

(a) *If $n = 1$, then $E(\dim(U_1 + \cdots + U_k)) = 1 - 1/2^k$ and $E(\dim(U_1 \cap \cdots \cap U_k)) = 1/2^k$.*

(b) *If $n \geqslant 2$, then $E(\dim(U_1 + \cdots + U_k)) = (n+1)/2$ and $E(\dim(U_1 \cap \cdots \cap U_k)) = (n-1)/2$.*

REMARK 5.4. In closing, we indicate a direction for further work. It may be of interest to develop formulas for $E(\dim(U_1 + \cdots + U_k))$ and $E(\dim(U_1 \cap \cdots \cap U_k))$ for all q and n. In this regard, we record here what was referred to in Example 3.6(a); namely, for $n = 4$, $E(\dim(U \cap V)) = \big(3q^7 + 9q^6 + 23q^5 + 40q^4 + 57q^3 + 57q^2 + 37q + 30\big)/\big(q^8 + 6q^7 + 17q^6 + 30q^5 + 44q^4 + 54q^3 + 49q^2 + 30q + 25\big)$.

Department of Mathematics
University of Tennessee
Knoxville, Tennessee 37996-1300
United States of America

Department of Mathematics
Hendrix College
Conway, Arkansas 72032
United States of America

https://doi.org/10.1017/S0004972700030367 Published online by Cambridge University Press