Теорія Ймовір. та Матем. Статист.
Вип. 69, 2003

Theor. Probability and Math. Statist.
No. 69, 2004, Pages 129–140
S 0094-9000(05)00620-4
Article electronically published on February 9, 2005

APPLICATIONS OF ESTIMATES OF THE PROBABILITY THAT A RANDOM k-DIMENSIONAL SUBSPACE IS OF MINIMAL WEIGHT

UDC 519.21

V. V. MASOL

Abstract. We find nontrivial estimates of the probability that a random k-dimensional subspace of an n-dimensional vector space over a finite field $GF(q)$ is of minimal weight. The conditions are $nq^{k-n} \le 1$ in Theorem 1 and $k \ge n-k \ge 4$ in Theorem 2. Some applications of the estimates for finding the asymptotic behavior of the above probability are given.

1. Setting of the problem

Let $\eta_{k,n}$ be the weight of a subspace chosen at random and equiprobably from the family of all k-dimensional subspaces $V_{k,n}$ of an n-dimensional vector space V_n, $V_{k,n} \subseteq V_n$, over a finite field $GF(q)$ of q elements (q is a power of a prime number), $1 \le k \le n$. It is known (see, for example, [1, p. 215]) that the total number of elements in the above family is $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_q$ where

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^{n-i}-1}{q^{k-i}-1}, \qquad k = 1, 2, \dots, n. \tag{1}$$

Therefore

$$\mathsf{P}\{\eta_{k,n} = \omega\} = \begin{bmatrix} n \\ k \end{bmatrix}_{\omega} \left(\begin{bmatrix} n \\ k \end{bmatrix}_q \right)^{-1}, \qquad \omega = 1, 2, \dots, n, \tag{2}$$

where $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \middle| \, \omega \right]$ is the total number of all k-dimensional subspaces $V_{k,n}$ of weight ω, $1 \le k \le n$, $1 \le \omega \le n$. (Recall that the minimal weight of nonzero vectors $v \in V_{k,n}$ is called the weight of the subspace $V_{k,n}$; the number of nonzero components of a vector is called its weight.) We are interested in finding estimates for the probability $\mathsf{P}\{\eta_{k,n} = 1\}$ and to obtain some applications of these estimates.

2. Estimates of the probability $\mathsf{P}\{\eta_{k,n} = 1\}$

Let m denote the difference $m = n - k$ where the integers k and n are such that $1 \le k \le n$.

Theorem 1. *If*

$$nq^{-m} \le 1, \tag{3}$$

2000 *Mathematics Subject Classification.* Primary 60C05.

then

$$\mathsf{P}\{\eta_{k,n}=1\}=nq^{-m}\left(1-q^{-k}\right)\left(1-q^{-n}\right)^{-1}A(k,n) \tag{4}$$

where $\left(1-q^{-m}\right)^{k-1}\prod_{i=1}^{k-1}\left(1-q^{-i}\right)\left(1-q^{-n+i}\right)^{-1}\le A(k,n)\le 1$.

Here and in what follows $\prod_{i=1}^{0}\equiv 1$.

Corollary 1. *If* $k=1$, *then* $\mathsf{P}\{\eta_{k,n}=1\}=n(q-1)\left(q^n-1\right)^{-1}$.

Theorem 2. *The following estimates hold for the probability of the event* $\{\eta_{k,n}=1\}$*:*

(i) *if* $k\ge m\ge 4$, *then*

$$\mathsf{P}\{\eta_{k,n}=1\}\le 1-\left(1-q^{-m}\right)^{k-m}r(q,m) \tag{5}$$

where

$$r(q,m)=1-\frac{1}{q^m\left(q-q^{-m+1}-1\right)}-\frac{m}{(q^m-1)(q-1)}\left[2q-1+\frac{q}{m(q-1)}-\frac{2m(q-1)+1}{q^{m-1}m(q-1)}\right];$$

(ii) *if* $k\ge m\ge 3$, *then*

$$\mathsf{P}\{\eta_{k,n}=1\}\ge 1-\left(1-q^{-m}\right)^{k}l(q,m) \tag{6}$$

where $l(q,m)=1+q^{-m+2}\left(q-q^{-m+1}-1\right)^{-1}(q-1)^{-2}-mq^{-m}\prod_{s=2}^{m}(1-q^{-s})$.

3. Proof of Theorem 1

It follows from (1) that

$$\begin{bmatrix} n\\ k\end{bmatrix}_q=q^{km}\left(\prod_{\nu=1}^{k}\left(1-q^{-\nu}\right)\right)^{-1}\prod_{i=0}^{k-1}\left(1-q^{-n+i}\right). \tag{7}$$

Relation (7) together with the inequality

$$\left[\begin{matrix} n\\ k\end{matrix}\,\middle|\, 1\right]\le nq^{(k-1)m}\prod_{j=1}^{k-1}\frac{1-q^{-n+j}}{1-q^{-j}} \tag{8}$$

obtained in [2] imply that

$$\mathsf{P}\{\eta_{k,n}=1\}\le nq^{-m}\left(1-q^{-k}\right)\left(1-q^{-n}\right)^{-1} \tag{9}$$

in view of equality (2) for $\omega=1$.

Using (3) we find that $nq^{-m}\left(1-q^{-k}\right)\left(1-q^{-n}\right)^{-1}<1$ for $n>1$. Thus (9) is a nontrivial estimate of the probability $\mathsf{P}\{\eta_{k,n}=1\}$.

Representation (7) and the inequality

$$\left[\begin{matrix} n\\ k\end{matrix}\,\middle|\, 1\right]\ge nq^{(k-1)m}\left(1-q^{-m}\right)^{k-1} \tag{10}$$

proved in [2] imply that

$$\mathsf{P}\{\eta_{k,n}=1\}\ge nq^{-m}\left(1-q^{-m}\right)^{k-1}\left(\prod_{i=0}^{k-1}\left(1-q^{-n+i}\right)\right)^{-1}\prod_{i=1}^{k}\left(1-q^{-i}\right) \tag{11}$$

by taking into account equality (2) for $\omega=1$. Combining (9) and (11) we obtain relation (4). Theorem 1 is proved. □

4. Auxiliary results for the proof of Theorem 2

Lemma 1. *Let*

$$\sigma_1 = \left(\begin{bmatrix} n \\ k \end{bmatrix}_q \right)^{-1} \sum_{\mu=1}^{k-m} \left[\begin{matrix} n-\mu \\ k-\mu+1 \end{matrix} \middle| \, 1 \right] (q^m - 1)^{\mu-1}. \tag{12}$$

If

$$2 \le m \le k, \tag{13}$$

then

$$\sigma_1 \le (1 - q^{-m})^{k-m} q^{-m} \left(q - q^{-m+1} - 1 \right)^{-1}. \tag{14}$$

(Here and in what follows $\sum_{\mu=1}^{0} \equiv 0$.)

Proof. It is known that

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = q^{km} \prod_{s=1}^{m} \left(q^s - q^{-k} \right) \left(q^s - 1 \right)^{-1} \tag{15}$$

(see, for example, [1, p. 46]). Let

$$\tilde{\sigma}_1 = \left(\begin{bmatrix} n \\ k \end{bmatrix}_q \right)^{-1} \sum_{\mu=1}^{k-m} \begin{bmatrix} n-\mu \\ k-\mu+1 \end{bmatrix}_q (q^m - 1)^{\mu-1}.$$

Then

$$\sigma_1 \le \tilde{\sigma}_1. \tag{16}$$

The sum $\tilde{\sigma}_1$ can be represented as follows:

$$\tilde{\sigma}_1 = q^{-k} \left(q^m - 1 \right) \left(q^m - q^{-k} \right)^{-1} \sum_{\mu=1}^{k-m} \left(q - q^{-m+1} \right)^{\mu-1} \prod_{s=1}^{m-1} \frac{q^s - q^{-k+\mu-1}}{q^s - q^{-k}},$$

whence

$$\tilde{\sigma}_1 \le q^{-k} \sum_{\mu=1}^{k-m} \left(q - q^{-m+1} \right)^{\mu-1}. \tag{17}$$

Evaluating the right-hand side of (17) as a sum of a geometric series and taking into account conditions (13), $q \ge 2$, and (16) we obtain (14). Lemma 1 is proved. □

Lemma 2. *Let*

$$\sigma_2 = \left(\begin{bmatrix} n \\ k \end{bmatrix}_q \right)^{-1} \sum_{\mu=1}^{k-m} \begin{bmatrix} n-\mu \\ k-\mu \end{bmatrix}_q (q^m - 1)^{\mu-1}. \tag{18}$$

If

$$1 \le m \le k, \tag{19}$$

then

$$\sigma_2 \le 1 - \left(1 - q^{-m} \right)^{k-m}. \tag{20}$$

Proof. It follows from (15) that

$$\sigma_2 = q^{-m} \sum_{\mu=1}^{k-m} \left(1 - q^{-m}\right)^{\mu-1} \prod_{s=1}^{m} \left(1 - \frac{q^{\mu}-1}{q^{s+k}-1}\right).$$

Using (19) we get

$$\sigma_2 \le q^{-m} \sum_{\mu=1}^{k-m} \left(1 - q^{-m}\right)^{\mu-1} = 1 - \left(1 - q^{-m}\right)^{k-m}.$$

Lemma 2 is proved. □

Lemma 3. *Let*

$$\sigma_3 = \left(\begin{bmatrix} n \\ k \end{bmatrix}_q\right)^{-1} \sum_{\nu=0}^{m-1} (q^m - 1)^{k-\nu-1} \left(\begin{bmatrix} m+\nu \\ \nu \end{bmatrix}_q + \left[\begin{array}{c|c} m+\nu & \\ \nu+1 & 1 \end{array}\right]\right). \tag{21}$$

If condition (19) *holds, then*

$$\begin{aligned} \sigma_3 \le{}& (1 - q^{-m})^{k-m} (q^m - 1)^{-1} \\ &\times \left[(q-1)^{-1} m \left(2q - 1 - 2q^{-m+1}\right) + (q-1)^{-2} \left(q - q^{-m+1}\right)\right]. \end{aligned} \tag{22}$$

Proof. Inequality (8) yields

$$\sigma_3 \le \tilde{\sigma}_3 \tag{23}$$

where

$$\tilde{\sigma}_3 = \left(\begin{bmatrix} n \\ k \end{bmatrix}_q\right)^{-1} \sum_{\nu=0}^{m-1} (q^m - 1)^{k-\nu-1} \left(\begin{bmatrix} m+\nu \\ \nu \end{bmatrix}_q + (m+\nu) q^{\nu(m-1)} \prod_{j=1}^{\nu} (1 - q^{-j})^{-1}\right).$$

Using equality (15) we reduce the sum $\tilde{\sigma}_3$ to the following form:

$$\begin{aligned} \tilde{\sigma}_3 = {}& (1 - q^{-m})^{k-1} q^{-m} \sum_{\nu=0}^{m-1} (1 - q^{-m})^{-\nu} \\ &\times \left[\prod_{s=1}^{m} \frac{q^s - q^{-\nu}}{q^s - q^{-k}} \right. \\ &\left. + (m+\nu) q^{-\nu} \left(\prod_{j=1}^{\nu} \left(1 - q^{-j}\right)\right)^{-1} \prod_{s=1}^{m} \left(q^s - 1\right) \left(q^s - q^{-k}\right)^{-1}\right]. \end{aligned} \tag{24}$$

Since $m \le k$, we have for $\nu \le m$ that

$$\prod_{s=1}^{m} \left(q^s - q^{-\nu}\right) \left(q^s - q^{-k}\right)^{-1} \le 1. \tag{25}$$

Further,

$$\begin{aligned} \left(\prod_{j=1}^{\nu} \left(1 - q^{-j}\right)\right)^{-1} \prod_{s=1}^{m} \left(q^s - 1\right) \left(q^s - q^{-k}\right)^{-1} &= \prod_{s=\nu+1}^{m} \left(1 - q^{-s}\right) \prod_{s=1}^{m} \left(1 - q^{-s-k}\right)^{-1} \\ \le \prod_{s=1}^{m} \left(1 - q^{-s-k}\right)^{-1} &= \prod_{i=0}^{m-1} \left(1 - q^{-n+i}\right)^{-1} \le \prod_{i=0}^{k-1} \left(1 - q^{-n+i}\right)^{-1} \end{aligned}$$

for $\nu \le m$ in view of condition (19). Combining (24) and (25) we obtain

$$\tilde{\sigma}_3 \le (1-q^{-m})^{k-1} q^{-m} \sum_{\nu=0}^{m-1} (1-q^{-m})^{-\nu} \left[1 + (m+\nu) q^{-\nu} \prod_{i=0}^{k-1} (1-q^{-n+i})^{-1} \right]. \tag{26}$$

Applying

$$\prod_{i=1}^{n} (1-x_i) \ge 1 - \sum_{i=1}^{n} x_i, \qquad 0 \le x_i \le 1,\ i = 1, 2, \ldots, n, \tag{27}$$

$$q^{-n} \sum_{i=0}^{k-1} q^i \le q^{-m},$$

and

$$(1-q^{-m})^{-\nu} \le (1-q^{-m})^{-m+1}, \qquad 0 \le \nu \le m-1,$$

to inequality (26), we get

$$\tilde{\sigma}_3 \le (1-q^{-m})^{k-m-1} q^{-m} \sum_{\nu=0}^{m-1} \left[1 + (m+\nu) q^{-\nu} \right]. \tag{28}$$

Inequalities (23) and (28) together with

$$\sum_{\nu=0}^{m-1} \left[1 + (m+\nu) q^{-\nu} \right] = m \left(2q - 1 - 2q^{-m+1} \right) (q-1)^{-1} + \left(q - q^{-m+1} \right) (q-1)^{-2}$$

imply (22). Lemma 3 is proved. □

Lemma 4. *If $k \ge m \ge 2$, then*

$$(1-q^{-m})^{k-m} r(q,m) < 1; \tag{29}$$

while if $m \ge 4$, then

$$r(q,m) > 0. \tag{30}$$

Proof. It is clear that inequality (29) follows from the estimates

$$(1-q^{-m})^{k-m} \le 1$$

for $k \ge m \ge 1$, and

$$(q - q^{-m+1} - 1)^{-1} > 0, \qquad \lambda(q,m) > 0,$$

for $m \ge 2$ where

$$\lambda(q,m) = 2q - 1 + \frac{q}{m(q-1)} - \frac{2m(q-1)+1}{q^{m-1} m(q-1)}.$$

Let $q \ge 3$ and $m \ge 3$. Then $q^{-m}(q - q^{-m+1} - 1)^{-1} \le 1/51$ and

$$m\lambda(q,m)(q^m-1)^{-1}(q-1)^{-1} \le m(3^m-1)^{-1}(5 + 3/2m)\, 2^{-1} < 1/3.$$

This implies that $r(q,m) > 11/17$. Thus relation (30) holds for $q \ge 3$ and $m \ge 3$. If $q = 2$ and $m \ge 5$, then $q^{-m}\left(q - q^{-m+1} - 1\right)^{-1} \le 1/30$ and

$$m(q^m-1)^{-1}(q-1)^{-1}\lambda(q,m) \le m(2^m-1)^{-1}(3 + 2/m) \le 17/31.$$

Therefore inequality (30) holds for $q = 2$ and $m \ge 5$. Finally, inequality (30) is easy to check for $q = 2$ and $m = 4$. Lemma 4 is proved. □

Lemma 5. *Let*

$$S_1 = \left(\begin{bmatrix} n \\ k \end{bmatrix}_q\right)^{-1} \sum_{\mu=1}^{k} (q^m-1)^{\mu-1} \begin{bmatrix} n-\mu \\ k-\mu \end{bmatrix}_q. \tag{31}$$

Then

$$S_1 \geq 1 - \left(1-q^{-m}\right)^k \left[1 + q^{-m+2}(q-1)^{-2}\left(q-q^{-m+1}-1\right)^{-1}\right] \tag{32}$$

for $m \geq 2$.

Proof. Using representation (15) we rewrite the sum S_1 in the following form:

$$S_1 = q^{-m} \sum_{\mu=1}^{k} \left(1-q^{-m}\right)^{\mu-1} \prod_{s=1}^{m} \left(1 - \frac{q^\mu - 1}{q^{k+s}-1}\right).$$

Applying (27) again we get

$$S_1 \geq 1 - \left(1-q^{-m}\right)^k - q^{-m+1} \sum_{\mu=1}^{k} \left(q-q^{-m+1}\right)^{\mu-1} \left(1-q^{-\mu}\right) \sum_{s=1}^{m} \left(q^{k+s}-1\right)^{-1}. \tag{33}$$

It is clear that

$$\sum_{s=1}^{m} \left(q^{k+s}-1\right)^{-1} \leq q^{-k} \sum_{s=1}^{m} \left(q^s-1\right)^{-1} \leq q^{-k}(q-1)^{-1} \sum_{s=1}^{m} q^{-s+1} \leq q^{-k+1}(q-1)^{-2}$$

and for $m \geq 2$

$$\sum_{\mu=1}^{k} \left(q-q^{-m+1}\right)^{\mu-1} \left(1-q^{-\mu}\right) \leq \left(q-q^{-m+1}\right)^k \left(q-q^{-m+1}-1\right)^{-1}.$$

Substituting these two estimates into (33) we obtain (32). Lemma 5 is proved. □

Lemma 6. *Let*

$$S_2 = \left(\begin{bmatrix} n \\ k \end{bmatrix}_q\right)^{-1} \sum_{\mu=1}^{k} (q^m-1)^{\mu-1} \left[\begin{array}{c|c} n-\mu & \\ k-\mu+1 & 1 \end{array}\right]. \tag{34}$$

If

$$k \geq m \geq 3, \tag{35}$$

then

$$S_2 \geq \left(1-q^{-m}\right)^k m q^{-m} \prod_{s=2}^{m} \left(1-q^{-s}\right). \tag{36}$$

Proof. It follows from (10) that

$$S_2 \geq \tilde{S}_2 \tag{37}$$

where

$$\tilde{S}_2 = \left(\begin{bmatrix} n \\ k \end{bmatrix}_q\right)^{-1} \sum_{\mu=1}^{k} (q^m-1)^{\mu-1} (n-\mu) q^{(k-\mu)(m-1)} \left(1-q^{-m+1}\right)^{k-\mu}.$$

Using (15) we get

$$\tilde{S}_2 = q^{-n} \left(1-q^{-m+1}\right)^k \left(1-q^{-m}\right)^{-1} \varphi(n) \prod_{s=1}^{m} \left(q^s-1\right) \left(q^s-q^{-k}\right)^{-1} \tag{38}$$

where

$$\varphi(n) = \sum_{\mu=1}^{k} (n-\mu) \left(\frac{q - q^{-m+1}}{1 - q^{-m+1}} \right)^{\mu}.$$

It is clear that

$$\varphi(n) = v \left[n \sum_{\mu=1}^{k} v^{\mu-1} - \left(\sum_{\mu=0}^{k} v^{\mu} \right)' \right]$$

where $'$ denotes the derivative with respect to v, $v = \left(q - q^{-m+1}\right)\left(1 - q^{-m+1}\right)^{-1}$. After an easy calculation we get

$$\varphi(n) = mq^{k+1}(q-1)^{-1}\left(1-q^{-m}\right)^{k+1}\left(1-q^{-m+1}\right)^{-k}\left(1 + m^{-1}(q-1)^{-1} f(n)\right) \tag{39}$$

where

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

If (35) holds, then

$$f(n) \geq 0. \tag{40}$$

Indeed,

$$\left(\frac{1 - q^{-m+1}}{1 - q^{-m}} \right)^{k} \leq 1, \qquad q \geq 2,$$

and (35) implies that

$$f(n) \geq 3/4 - q^{-k}\left(1 + 2k(q-1)\right). \tag{41}$$

The maximum of $q^{-k}\left(1 + 2k(q-1)\right)$ for $k \geq 4$ is attained at $k = 4$. This means that (40) holds for $k \geq 4$ and $q \geq 2$.

Let $k = 3$. Then (41) implies (40) if $q \geq 3$. Finally, $f(n) = f(6)$ by condition (35) if $k = 3$ and $q = 2$. Since $f(6) > 0$, relation (40) is proved.

It follows from (38)–(40) that

$$\tilde{S}_2 \geq mq^{-m}\left(1 - q^{-m}\right)^{k} \prod_{s=2}^{m} \left(q^s - 1\right)\left(q^s - q^{-k}\right)^{-1}.$$

The latter inequality implies (36) in view of (37). Lemma 6 is proved. □

Lemma 7. *If* (35) *holds, then*

$$0 < \left(1 - q^{-m}\right)^{k} l(q,m) < 1. \tag{42}$$

Proof. Since $\left(1 - q^{-m}\right)^{k} > 0$ for $m > 0$ and $q > 1$ and $l(q,m) > 1 - 2q^{-2}\left(1 - q^{-2}\right) > 0$ for $m \geq 2$ and $q \geq 2$, we have

$$\left(1 - q^{-m}\right)^{k} l(q,m) > 0. \tag{43}$$

Now we show that

$$\left(1 - q^{-m}\right)^{k} l(q,m) < 1. \tag{44}$$

Indeed,

$$d_1(q,m) - d_2(q,m) < -1 \tag{45}$$

for $m \geq 3$ and $q \geq 3$ where $d_1(q,m) = q^2(q-1)^{-2}\left(q - q^{-m+1} - 1\right)^{-1}$ and

$$d_2(q,m) = m \prod_{s=2}^{m} \left(1 - q^{-s}\right),$$

since $d_1(q,m) \le 81/68$ and $d_2(q,m) \ge 3\prod_{s=2}^{\infty}(1-q^{-s})$. Thus

$$\prod_{s=2}^{\infty}\left(1-3^{-s}\right) \ge 5/6$$

by inequality (27).

It follows from (45) that

$$\left(1-q^{-m}\right)^k l(q,m) = \left(1-q^{-m}\right)^k \left\{1+q^{-m}\left[d_1(q,m)-d_2(q,m)\right]\right\} < 1,$$

that is, (44) holds for $k \ge m \ge 3$ and $q \ge 3$.

Let $q = 2$. Then

$$d_1(q,m) \le 32/7, \quad \text{and} \quad d_2(q,m) \ge 4\prod_{s=2}^{\infty}\left(1-2^{-s}\right) \ge 2$$

for $m \ge 4$, whence

$$l(q,m) \le 1 + 2^{-m}\cdot 18/7. \tag{46}$$

Estimate (46) together with the equality

$$\ln(1+x) = \sum_{n=1}^{\infty}(-1)^{n-1}\frac{x^n}{n}, \qquad |x| < 1,$$

implies (44) for $k \ge m \ge 4$ and $q = 2$.

Finally, let $q = 2$, $m = 3$, and $k \ge m$. Then

$$d_1(q,m) = 16/3, \qquad d_2(q,m) = 3\prod_{s=2}^{3}\left(1-2^{-s}\right), \qquad \left(1-q^{-m}\right)^k l(q,m) \le 0.96.$$

Thus estimate (44) is proved. Relation (42) follows from (43) and (44). Lemma 7 is proved. □

5. Proof of Theorem 2

Applying (2) for $\omega = 1$ together with the equality

$$\begin{bmatrix} n \\ k \end{bmatrix}_1 = \sum_{\mu=1}^{k}(q^m-1)^{\mu-1}\left(\begin{bmatrix} n-\mu \\ k-\mu \end{bmatrix}_q + \begin{bmatrix} n-\mu \\ k-\mu+1 \end{bmatrix}_1\right) \tag{47}$$

proved in [3] we obtain

$$\mathsf{P}\{\eta_{k,n}=1\} = \sigma_1+\sigma_2+\sigma_3 \tag{48}$$

where σ_1, σ_2, and σ_3 are defined in (12), (18), and (22), respectively. With the help of equality (48) and Lemmas 1, 2, and 3 we get estimate (5), which is nontrivial in view of Lemma 4. Further, equality (48) can be rewritten as follows:

$$\mathsf{P}\{\eta_{k,n}=1\} = S_1+S_2 \tag{49}$$

according to (47) where S_1 and S_2 are defined in (31) and (34), respectively. Equality (49) together with Lemmas 5, 6, and 7 imply the nontrivial estimate (6). Theorem 2 is proved.

6. Applications of Theorem 1

Theorem 3. *(i) If*

$$kq^{-m} \to x \tag{50}$$

as $n \to \infty$ *where* $0 \le x \le 1$ *and* $m \ge 1$, *then*

$$\mathsf{P}\{\eta_{k,n} = 1\} \le x, \qquad n \to \infty; \tag{51}$$

(ii) if

$$kq^{-m} \to x \tag{52}$$

as $n \to \infty$ *for some* $0 \le x < \infty$, *and*

$$q \to \infty, \qquad n \to \infty, \tag{53}$$

then

$$\mathsf{P}\{\eta_{k,n} = 1\} \ge xe^{-x}, \qquad n \to \infty; \tag{54}$$

(iii) if (52) *holds and* $q = \text{const}$, *then*

$$\mathsf{P}\{\eta_{k,n} = 1\} \ge xe^{-x} \prod_{i=1}^{\infty} \left(1 - q^{-i}\right), \qquad n \to \infty. \tag{55}$$

Proof. Condition (50) implies that

$$q^m \to \infty, \qquad n \to \infty. \tag{56}$$

Since $n = k + m$, we have

$$nq^{-m} \to x, \qquad n \to \infty. \tag{57}$$

Using (57) and (9) we prove (51), since $\left(1 - q^{-k}\right)\left(1 - q^{-n}\right)^{-1} \to 1$ as $n \to \infty$. The latter relation follows from $q^{-n} \to 0$ as $n \to \infty$ and $q^{-k} \to 0$ as $n \to \infty$, since $k \ge m$ by (56). Condition (50) implies that $kq^{-m} \to 0$ as $n \to \infty$ if $k < m$. Thus $nq^{-m} \to 0$ as $n \to \infty$, whence (51) follows according to (4) (the values of $\underline{\lim}_{n\to\infty} q^{-k}$ and $\overline{\lim}_{n\to\infty} q^{-k}$ do not matter in this case).

Let conditions (52) and (53) hold. Then relation (57) holds and moreover

$$\prod_{i=0}^{k-1} \left(1 - q^{-n+i}\right)^{-1} \ge 1, \qquad n \to \infty, \tag{58}$$

since $\prod_{i=0}^{k-1} \left(1 - q^{-n+i}\right)^{-1} \ge \exp\{-kq^{-n}\}$ and

$$\prod_{i=1}^{k} \left(1 - q^{-i}\right) \to 1, \qquad n \to \infty. \tag{59}$$

The latter relation follows from the inequality

$$\prod_{i=1}^{k} \left(1 - q^{-i}\right) \ge 1 - \frac{1}{q} \sum_{i=0}^{k-1} q^{-i},$$

which, in turn, is a consequence of (27). Now we apply (11), (57)–(59), and

$$\left(1 - q^{-m}\right)^{k-1} \to e^{-x}, \qquad n \to \infty,$$

and obtain estimate (54).

Now let (52) hold and $q = \text{const}$. Then (57), (58), and

$$\prod_{i=1}^{k} \left(1 - q^{-i}\right) \ge \prod_{i=1}^{\infty} \left(1 - q^{-i}\right)$$

hold. This easily implies bound (55) in view of (11). Theorem 3 is proved. □

Corollary 2. *If* $kq^{-m} \to 0$ *as* $n \to \infty$, *then*

$$\mathsf{P}\{\eta_{k,n} = 1\} \to 0, \qquad n \to \infty. \tag{60}$$

Moreover, in this case relation (4) *provides upper and lower estimates for the rate of convergence in* (60).

7. Applications of Theorem 2

Put $\delta(m,x) = \mathsf{P}\{\eta_{n-m,n} = 1\} - 1 + e^{-x}$ for $m \geq 0$ and $x \in [0,\infty)$.

Theorem 4. *If*

$$kq^{-m} \to x, \qquad n \to \infty, \tag{61}$$

for some $0 < x < \infty$ *and* $m \geq 1$, *then*

$$\delta(m,x) \to 0, \qquad n \to \infty, \tag{62}$$

and moreover

$$\delta(m,x) \leq e^{-x} - \left(1 - q^{-m}\right)^{k-m} r(q,m) \tag{63}$$

for $m \geq 4$;

$$e^{-x} - \left(1 - q^{-m}\right)^{k} l(q,m) \leq \delta(m,x) \tag{64}$$

for $m \geq 3$; *and*

$$\delta(m,x) \leq e^{-x} - \left(1 - q^{-3}\right)^{n-3} r(q) \tag{65}$$

for $m = 3$, *where the functions* $r(q,m)$ *and* $l(q,m)$ *are defined in* (5) *and* (6), *respectively, and*

$$r(q) = 1 - \frac{1-q^{-3}}{1-q^{-n}} \left[\left(q - q^{-2} - 1\right)^{-1} - q^{-1}\left(1 - q^{-2}\right)^2 \left(1 + q^{-1}\right)\right].$$

Proof. Relation (62) is proved in [4] for $m = 1$ and $m = 2$. Let $m = 3$. The parameter q increases as $n \to \infty$ if condition (61) holds, and thus

$$l(q,3) \to 1, \qquad n \to \infty, \tag{66}$$

$$r(q) \to 1, \qquad n \to \infty. \tag{67}$$

Note that estimate (65) is obtained in [4], while inequality (64) is proved in Theorem 2. Thus (64)–(67) complete the proof of Theorem 4 for $m = 3$.

Now let $m \geq 4$. Then condition (61) implies that $q^m \to \infty$ as $n \to \infty$, whence $r(q,m) \to 1$ and $l(q,m) \to 1$ as $n \to \infty$. Since $0 < x < \infty$, we have $k \geq m$ as $n \to \infty$, and it follows from Theorem 2 that relations (63) and (64) hold for $m \geq 4$. Estimates (63) and (64) and the limits of the functions $r(q,m)$ and $l(q,m)$ as $n \to \infty$ lead to (62) for $m \geq 4$. Theorem 4 is proved. □

Theorem 5. *If conditions* (61) *and* (53) *hold, then* (62)–(65) *hold and moreover*

$$\mathsf{P}\{\eta_{n-m,n} = 2\} \to e^{-x}, \qquad n \to \infty. \tag{68}$$

Proof. The equality

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \left[\begin{array}{c|c} n & 1 \\ k & \end{array}\right] + \left[\begin{array}{c|c} n & 2 \\ k & \end{array}\right] \tag{69}$$

holds if and only if

$$\frac{1-q^{-m}}{q-1} < \frac{n}{q^m} \tag{70}$$

(see [3]). Using conditions (61) and (53) we derive estimate (70) as $n \to \infty$ and therefore

$$\mathsf{P}\{\eta_{n-m,n} = 1\} + \mathsf{P}\{\eta_{n-m,n} = 2\} = 1, \qquad n \to \infty, \tag{71}$$

by (69) and (2). Now Theorem 5 follows from Theorem 4 and equality (71). □

Theorem 6. *If*

$$kq^{-m} \to x, \qquad n \to \infty, \tag{72}$$

for some $(q-1)^{-1} < x < \infty$ *where* q *is a fixed number, then estimates* (63) *and* (64) *are satisfied and relations* (62) *and* (68) *hold as* $n \to \infty$.

Proof. It is easy to check that $m \to \infty$ and $k \geq m$ as $n \to \infty$ under the assumptions of Theorem 6. Thus Theorem 2 implies estimates (63) and (64). If (72) holds, then so does (61). As proved in Theorem 2, this implies (62). Relation (72) implies that (70) holds as $n \to \infty$. Thus relation (71) follows. Taking (71) and (62) into account we get (68). Theorem 6 is proved. □

Put $\delta(m) = \mathsf{P}\{\eta_{n-m,n} = 1\} - 1$, $m \geq 0$.

Theorem 7. *If*

$$kq^{-m} \to \infty, \qquad n \to \infty, \tag{73}$$

for $m \geq 0$, *then*

$$\delta(m) \to 0, \qquad n \to \infty. \tag{74}$$

Moreover

$$\delta(m) \leq -\left(1 - q^{-m}\right)^{k-m} r(q,m) \tag{75}$$

for $m \geq 4$;

$$-\left(1 - q^{-m}\right)^{k} l(q,m) \leq \delta(m) \tag{76}$$

for $m \geq 3$; *and*

$$\delta(m) \leq -\left(1 - q^{-3}\right)^{n-3} r(q) \tag{77}$$

for $m = 3$ *where the functions* $r(q,m)$, $l(q,m)$, *and* $r(q)$ *are defined in Theorem* 4.

Proof. The following equalities are proved in [4]:

$$\begin{aligned}
\mathsf{P}\{\eta_{n,n} = 1\} &= 1, \\
\mathsf{P}\{\eta_{n-1,n} = 1\} &= 1 - (q-1)^n \left(q^n - 1\right)^{-1}, \\
\mathsf{P}\{\eta_{n-2,n} = 1\} &= 1 - \left(1 - q^{-2}\right)^n \\
&\quad - \left(1 + q^{-1}\right)(q-1)^n \left(q^{n-1} - 1\right)^{-1} \left(q^n - 1\right)^{-1} \\
&\quad \times \left[\left(q^{-1} - 1 + q^{-n}\right)\left(1 + q^{-1}\right)^{n-1} - 1\right].
\end{aligned}$$

These three equalities prove (74) for $m \in \{0,1,2\}$ if condition (73) is satisfied.

Estimates (75) and (76) are obtained in Theorem 2, while estimate (77) is proved in [4].

Since the functions $l(q,m)$, $m \geq 3$, are bounded by a constant independent of the parameter n, we apply (76) and find under condition (73) that

$$\delta(m) \geq 0, \qquad n \to \infty,$$

for $m \geq 3$. The latter inequality and the estimate $\delta(m) \leq 0$ for $m \geq 0$ complete the proof of Theorem 7. □

Bibliography

1. G. Andrews, *The Theory of Partitions*, Addison-Wesley, New York, 1976. MR0557013 (58:27738)
2. V. V. Masol, *The limit behavior of the distribution of certain characteristics of random spaces over a finite field*, Teor. Imovir. ta Matem. Statist. **67** (2002), 97–103; English transl. in Theory Probab. Math. Statist. **67** (2003), 107–114. MR1956623 (2003k:60022)
3. V. I. Masol, *Asymptotics of the number of certain k-dimensional subspaces over a finite field*, Mat. Zametki **59** (1996), no. 5, 729–736; English. transl. in Math. Notes **59** (1996), no. 5–6, 525–530. MR1445454 (98c:15005)
4. V. V. Masol, *Some applications of the explicit formula for the probability that a random k-dimensional subspace is of minimal weight*, Visnyk Kyiv University, Ser. Mathematics, Mechanics **10** (2003), 113–117. (Ukrainian)

Department of Probability Theory and Mathematical Statistics, Faculty for Mechanics and Mathematics, National Taras Shevchenko University, Academician Glushkov Avenue 6, Kyiv 03127, Ukraine

E-mail address: vicamasol@pochtamt.ru

Received 14/MAR/2003

Translated by OLEG KLESOV