

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 $nq^{k-n} \leq 1$ in Theorem 1 and $k \geq n-k \geq 4$ 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), $1 \leq k \leq n$. It is known (see, for example, [1, p. 215]) that the total number of elements in the above family is $\begin{bmatrix} n \\ k \end{bmatrix}_q$ where

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

Therefore

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

where $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is the total number of all k -dimensional subspaces $V_{k,n}$ of weight ω , $1 \leq k \leq n$, $1 \leq \omega \leq n$. (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 $\mathbb{P}\{\eta_{k,n} = 1\}$ and to obtain some applications of these estimates.

2. ESTIMATES OF THE PROBABILITY $\mathbb{P}\{\eta_{k,n} = 1\}$

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

Theorem 1. *If*

$$(3) \quad nq^{-m} \leq 1,$$

2000 *Mathematics Subject Classification.* Primary 60C05.

then

$$(4) \quad \mathbb{P}\{\eta_{k,n} = 1\} = nq^{-m} (1 - q^{-k}) (1 - q^{-n})^{-1} A(k, n)$$

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

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

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

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

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

$$(5) \quad \mathbb{P}\{\eta_{k,n} = 1\} \leq 1 - (1 - q^{-m})^{k-m} r(q, m)$$

where

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

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

$$(6) \quad \mathbb{P}\{\eta_{k,n} = 1\} \geq 1 - (1 - q^{-m})^k l(q, m)$$

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

3. PROOF OF THEOREM 1

It follows from (1) that

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

Relation (7) together with the inequality

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

obtained in [2] imply that

$$(9) \quad \mathbb{P}\{\eta_{k,n} = 1\} \leq nq^{-m} (1 - q^{-k}) (1 - q^{-n})^{-1}$$

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

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

Representation (7) and the inequality

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

proved in [2] imply that

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

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

4. AUXILIARY RESULTS FOR THE PROOF OF THEOREM 2

Lemma 1. *Let*

$$(12) \quad \sigma_1 = \left(\begin{bmatrix} n \\ k \end{bmatrix}_q \right)^{-1} \sum_{\mu=1}^{k-m} \begin{bmatrix} n-\mu \\ k-\mu+1 \end{bmatrix}_q (q^m - 1)^{\mu-1}.$$

If

$$(13) \quad 2 \leq m \leq k,$$

then

$$(14) \quad \sigma_1 \leq (1 - q^{-m})^{k-m} q^{-m} (q - q^{-m+1} - 1)^{-1}.$$

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

Proof. It is known that

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

(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

$$(16) \quad \sigma_1 \leq \tilde{\sigma}_1.$$

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

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

whence

$$(17) \quad \tilde{\sigma}_1 \leq q^{-k} \sum_{\mu=1}^{k-m} (q - q^{-m+1})^{\mu-1}.$$

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

Lemma 2. *Let*

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

If

$$(19) \quad 1 \leq m \leq k,$$

then

$$(20) \quad \sigma_2 \leq 1 - (1 - q^{-m})^{k-m}.$$

Proof. It follows from (15) that

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

Using (19) we get

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

Lemma 2 is proved. □

Lemma 3. *Let*

$$(21) \quad \sigma_3 = \left(\left[\begin{matrix} n \\ k \end{matrix} \right]_q \right)^{-1} \sum_{\nu=0}^{m-1} (q^m - 1)^{k-\nu-1} \left(\left[\begin{matrix} m + \nu \\ \nu \end{matrix} \right]_q + \left[\begin{matrix} m + \nu \\ \nu + 1 \end{matrix} \right]_q \right).$$

If condition (19) holds, then

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

Proof. Inequality (8) yields

$$(23) \quad \sigma_3 \leq \tilde{\sigma}_3$$

where

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

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

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

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

$$(25) \quad \prod_{s=1}^m (q^s - q^{-\nu}) (q^s - q^{-k})^{-1} \leq 1.$$

Further,

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

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

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

Applying

$$(27) \quad \prod_{i=1}^n (1 - x_i) \geq 1 - \sum_{i=1}^n x_i, \quad 0 \leq x_i \leq 1, \quad i = 1, 2, \dots, n,$$

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

and

$$(1 - q^{-m})^{-\nu} \leq (1 - q^{-m})^{-m+1}, \quad 0 \leq \nu \leq m - 1,$$

to inequality (26), we get

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

Inequalities (23) and (28) together with

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

imply (22). Lemma 3 is proved. □

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

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

while if $m \geq 4$, then

$$(30) \quad r(q, m) > 0.$$

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

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

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

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

for $m \geq 2$ where

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

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

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

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

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

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

Lemma 5. *Let*

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

Then

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

for $m \geq 2$.

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

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

Applying (27) again we get

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

It is clear that

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

and for $m \geq 2$

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

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

Lemma 6. *Let*

$$(34) \quad S_2 = \left(\left[\begin{matrix} n \\ k \end{matrix} \right]_q \right)^{-1} \sum_{\mu=1}^k (q^m - 1)^{\mu-1} \left[\begin{matrix} n - \mu \\ k - \mu + 1 \end{matrix} \middle| 1 \right].$$

If

$$(35) \quad k \geq m \geq 3,$$

then

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

Proof. It follows from (10) that

$$(37) \quad S_2 \geq \tilde{S}_2$$

where

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

Using (15) we get

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

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 , $v = (q - q^{-m+1}) (1 - q^{-m+1})^{-1}$. After an easy calculation we get

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

where

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

If (35) holds, then

$$(40) \quad f(n) \geq 0.$$

Indeed,

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

and (35) implies that

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

The maximum of $q^{-k} (1 + 2k(q-1))$ 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

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

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

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

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

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

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

Now we show that

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

Indeed,

$$(45) \quad d_1(q, m) - d_2(q, m) < -1$$

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

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

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

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

by inequality (27).

It follows from (45) that

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

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

Let $q = 2$. Then

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

for $m \geq 4$, whence

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

Estimate (46) together with the equality

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

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

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

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

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

5. PROOF OF THEOREM 2

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

$$(47) \quad \left[\begin{matrix} n \\ k \end{matrix} \middle| 1 \right] = \sum_{\mu=1}^k (q^m - 1)^{\mu-1} \left(\left[\begin{matrix} n - \mu \\ k - \mu \end{matrix} \right]_q + \left[\begin{matrix} n - \mu \\ k - \mu + 1 \end{matrix} \right]_q \middle| 1 \right)$$

proved in [3] we obtain

$$(48) \quad \mathbf{P}\{\eta_{k,n} = 1\} = \sigma_1 + \sigma_2 + \sigma_3$$

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:

$$(49) \quad \mathbf{P}\{\eta_{k,n} = 1\} = S_1 + S_2$$

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

$$(50) \quad kq^{-m} \rightarrow x$$

as $n \rightarrow \infty$ where $0 \leq x \leq 1$ and $m \geq 1$, then

$$(51) \quad \mathbb{P}\{\eta_{k,n} = 1\} \leq x, \quad n \rightarrow \infty;$$

(ii) if

$$(52) \quad kq^{-m} \rightarrow x$$

as $n \rightarrow \infty$ for some $0 \leq x < \infty$, and

$$(53) \quad q \rightarrow \infty, \quad n \rightarrow \infty,$$

then

$$(54) \quad \mathbb{P}\{\eta_{k,n} = 1\} \geq xe^{-x}, \quad n \rightarrow \infty;$$

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

$$(55) \quad \mathbb{P}\{\eta_{k,n} = 1\} \geq xe^{-x} \prod_{i=1}^{\infty} (1 - q^{-i}), \quad n \rightarrow \infty.$$

Proof. Condition (50) implies that

$$(56) \quad q^m \rightarrow \infty, \quad n \rightarrow \infty.$$

Since $n = k + m$, we have

$$(57) \quad nq^{-m} \rightarrow x, \quad n \rightarrow \infty.$$

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

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

$$(58) \quad \prod_{i=0}^{k-1} (1 - q^{-n+i})^{-1} \geq 1, \quad n \rightarrow \infty,$$

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

$$(59) \quad \prod_{i=1}^k (1 - q^{-i}) \rightarrow 1, \quad n \rightarrow \infty.$$

The latter relation follows from the inequality

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

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

$$(1 - q^{-m})^{k-1} \rightarrow e^{-x}, \quad n \rightarrow \infty,$$

and obtain estimate (54).

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

$$\prod_{i=1}^k (1 - q^{-i}) \geq \prod_{i=1}^{\infty} (1 - q^{-i})$$

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

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

$$(60) \quad \mathbb{P}\{\eta_{k,n} = 1\} \rightarrow 0, \quad n \rightarrow \infty.$$

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

7. APPLICATIONS OF THEOREM 2

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

Theorem 4. *If*

$$(61) \quad kq^{-m} \rightarrow x, \quad n \rightarrow \infty,$$

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

$$(62) \quad \delta(m, x) \rightarrow 0, \quad n \rightarrow \infty,$$

and moreover

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

for $m \geq 4$;

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

for $m \geq 3$; and

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

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

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

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

$$(66) \quad l(q, 3) \rightarrow 1, \quad n \rightarrow \infty,$$

$$(67) \quad r(q) \rightarrow 1, \quad n \rightarrow \infty.$$

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 $q^m \rightarrow \infty$ as $n \rightarrow \infty$, whence $r(q, m) \rightarrow 1$ and $l(q, m) \rightarrow 1$ as $n \rightarrow \infty$. Since $0 < x < \infty$, we have $k \geq m$ as $n \rightarrow \infty$, 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 $n \rightarrow \infty$ lead to (62) for $m \geq 4$. Theorem 4 is proved. \square

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

$$(68) \quad \mathbb{P}\{\eta_{n-m,n} = 2\} \rightarrow e^{-x}, \quad n \rightarrow \infty.$$

Proof. The equality

$$(69) \quad \begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ k \\ 1 \end{bmatrix} + \begin{bmatrix} n \\ k \\ 2 \end{bmatrix}$$

holds if and only if

$$(70) \quad \frac{1 - q^{-m}}{q - 1} < \frac{n}{q^m}$$

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

$$(71) \quad \mathbb{P}\{\eta_{n-m,n} = 1\} + \mathbb{P}\{\eta_{n-m,n} = 2\} = 1, \quad n \rightarrow \infty,$$

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

Theorem 6. *If*

$$(72) \quad kq^{-m} \rightarrow x, \quad n \rightarrow \infty,$$

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 $n \rightarrow \infty$.

Proof. It is easy to check that $m \rightarrow \infty$ and $k \geq m$ as $n \rightarrow \infty$ 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 $n \rightarrow \infty$. Thus relation (71) follows. Taking (71) and (62) into account we get (68). Theorem 6 is proved. \square

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

Theorem 7. *If*

$$(73) \quad kq^{-m} \rightarrow \infty, \quad n \rightarrow \infty,$$

for $m \geq 0$, then

$$(74) \quad \delta(m) \rightarrow 0, \quad n \rightarrow \infty.$$

Moreover

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

for $m \geq 4$;

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

for $m \geq 3$; and

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

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]:

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

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

$$\delta(m) \geq 0, \quad n \rightarrow \infty,$$

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

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