Discrete Mathematics 66 (1987) 35–49
North-Holland

DETERMINANTS AND RANKS OF RANDOM MATRICES OVER $\mathbb{Z}_m$

Richard P. BRENT
Centre for Mathematical Analysis, Australian National University, Canberra, ACT 2601, Australia

Brendan D. McKAY
Computer Science Department, Australian National University, Canberra, ACT 2601, Australia

Received 24 September 1985
Revised 6 October 1986

Let $\mathbb{Z}_m$ be the ring of integers modulo m. The *m-rank* of an integer matrix is the largest order of a square submatrix whose determinant is not divisible by m. We determine the probability that a random rectangular matrix over $\mathbb{Z}_m$ has a specified m-rank and, if it is square, a specified determinant. These results were previously known only for prime m.

1. Introduction

Let m be an integer. The *m-rank* of an integer matrix A is the greatest integer k such that A has a $k \times k$ submatrix (not necessarily contiguous) whose determinant is nonzero $(\bmod m)$, or 0 if there is no such submatrix. If m is a prime, the m-rank is equivalent to the usual rank over the field GF(m). In this paper we investigate the m-rank when the entries are chosen at random, independently and uniformly, from $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$. Our results appear to be new except for the case when m is a prime. For corresponding results when A is constrained to be symmetric, see [3].

We begin with some notation. For integer $n \geq 0$ and indeterminate q, define $\Pi_n(q) = (1-q)(1-q^2)\cdots(1-q^n)$. In particular, $\Pi_0(q) = 1$. For integers $0 \leq k \leq n$, define

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{\Pi_n(q)}{\Pi_k(q)\Pi_{n-k}(q)}.$$

The polynomials $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]$ are called *Gaussian coefficients* or *q-binomial coefficients* and have many combinatorial interpretations. For example, $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]$ is the number of sub-spaces of dimension k in a vector space of dimension n over a field of q elements. Gaussian coefficients are also of interest as generalizations of ordinary binomial coefficients, since $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right] \to \binom{n}{k}$ as $q \to 1$. Expositions of the theory of Gaussian coefficients can be found in [1], [2] and [5].

For integers $n \geq 1$, $\Delta \geq 0$, $0 \leq \delta \leq n$ and $m \geq 1$, define $P_{\Delta,\delta}(n, m)$ to be the probability that a random $(n + \Delta) \times n$ matrix over $\mathbb{Z}_m$ has m-rank $n - \delta$. It will also be convenient to define $P_{\Delta,0}(0, m) = 1$.

The value of $P_{\Delta,\delta}(n, m)$ has previously been determined for prime m, as shown by the following theorem [4, 6].

Theorem 1.1. *Let $n \geq 0$, $\Delta \geq 0$, $0 \leq \delta \leq n$ and let p be a prime. Define $q = 1/p$. Then*

$$P_{\Delta,\delta}(n, p) = q^{\delta(\delta+\Delta)} \begin{bmatrix} n \\ \delta \end{bmatrix} \frac{\Pi_{n+\Delta}(q)}{\Pi_{\delta+\Delta}(q)}.$$

Theorem 1.1 is also true if, instead of $\mathbb{Z}_p$ with p prime, we use any field of p elements, whether or not p is prime. Note that Theorem 1.1 disproves the result claimed by [7].

When m is not a prime, the evaluation of $P_{\Delta,\delta}(n, m)$ becomes more involved because we are no longer working over a field. However, it is not difficult to show that we can restrict our attention to the case when m is a prime power. For $-1 \leq \delta \leq n$, define

$$Q_{\Delta,\delta}(n, m) = \sum_{j=\delta+1}^{n} P_{\Delta,j}(n, m).$$

Lemma 1.1. *Suppose $m = p_1^{\mu_1} p_2^{\mu_2} \cdots p_k^{\mu_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes. Then*

$$Q_{\Delta,\delta}(n, m) = \prod_{i=1}^{k} Q_{\Delta,\delta}(n, p_i^{\mu_i}).$$

Proof. The m-rank of a random matrix over $\mathbb{Z}_m$ is less than $n - \delta$ if and only if the $p_i^{\mu_i}$-rank is less than $n - \delta$ for $i = 1, 2, \ldots, k$. By the Chinese Remainder Theorem, the latter events are independent. □

2. The full rank case

In this section we consider the case $\delta = 0$, i.e., we consider the probability $P_{\Delta,0}(n, p^{\mu})$ that a random $(n + \Delta) \times n$ matrix over $\mathbb{Z}_{p^{\mu}}$ has full p^{μ}-rank, where p is a prime. Results for a general modulus $m = p_1^{\mu_1} \cdots p_k^{\mu_k}$ are easily deduced from the multiplicative property of Q stated in Lemma 1.1.

The principal tool for this section and the next will be Gaussian elimination. We begin with a simple lemma which has enough generality to cover both cases.

Lemma 2.1. *Let A be an $N \times n$ integer matrix with rows $R_1, R_2, \ldots, R_N$. For some integers i, j, α where $1 \leq i, j \leq N$ and $i \neq j$, form the $N \times n$ matrix A' from A by executing the row-operation $R_i := R_i - \alpha R_j$. Then, for any integers $m \geq 1$ and $t \geq 1$, A has a $t \times t$ submatrix with nonzero determinant mod m if and only if A' has such a submatrix.*

Proof. Suppose that $B = A[r_1, r_2, \ldots, r_t; c_1, c_2, \ldots, c_t]$ is such a submatrix of A, where the notation indicates that $B = (b_{uv})$, where $b_{uv} = a_{r_u c_v}$ for $1 \leq u, v \leq t$.

The determinant of $B' = A'[r_1, r_2, \ldots, r_t; c_1, c_2, \ldots, c_t]$ is the same as that of B if $i, j \in \{r_1, r_2, \ldots, r_t\}$ or $i \notin \{r_1, r_2, \ldots, r_t\}$. Suppose instead that $r_1 = i$ but $j \notin \{r_2, \ldots, r_t\}$. Define $B'' = A'[j, r_2, \ldots, r_t; c_1, c_2, \ldots, c_t]$. Then we have $\det B' = \det B - \alpha \det B''$. Since $\det B \not\equiv 0 \pmod m$, we must either have $\det B' \not\equiv 0 \pmod m$ or $\det B'' \not\equiv 0 \pmod m$. □

Lemma 2.1 can be used to derive a 3-term recurrence from which $P_{\Delta,0}(n, p^\mu)$ can be determined, using the boundary conditions $P_{\Delta,0}(0, p^\mu) = 1$ $(\mu \geq 1)$ and $P_{\Delta,0}(n, 1) = 0$. Here and below we write $q = 1/p$.

Lemma 2.2. *If $n > 0$, $\Delta \geq 0$ and $\mu \geq 0$, then*

$$P_{\Delta,0}(n, p^{\mu+1}) = (1 - q^{n+\Delta})P_{\Delta,0}(n-1, p^{\mu+1}) + q^{n+\Delta}P_{\Delta,0}(n, p^\mu). \tag{2.1}$$

Proof. Let A be a random $(n + \Delta) \times n$ matrix over $\mathbb{Z}_{p^{\mu+1}}$. There are two cases. With probability $q^{n+\Delta}$, the first column of A is divisible by p. In this case, we may obtain a random matrix A' by dividing the first column of A by p and adding random multiples of p^μ to that column. Clearly A has full $p^{\mu+1}$-rank if and only if A' has full p^μ-rank. The (conditional) probability of this is $P_{\Delta,0}(n, p^\mu)$.

The remaining case, which occurs with probability $1 - q^{n+\Delta}$, is that the first column of A is not divisible by p. Since p is prime, we can apply a row interchange (if necessary) and a sequence of row operations of the form considered by Lemma 2.1, until A is reduced to the form

$$\begin{bmatrix} b_1 & b_2 \cdots b_n \\ 0 & A'' \end{bmatrix},$$

where $b_1 \not\equiv 0 \pmod p$. By Lemma 2.1, A has full $p^{\mu+1}$-rank if and only if A'' has full $p^{\mu+1}$-rank. Since A'' is clearly a random $(n + \Delta - 1) \times (n-1)$ matrix over $\mathbb{Z}_{p^{\mu+1}}$, this happens with probability $P_{\Delta,0}(n-1, p^{\mu+1})$. The result follows. □

From Lemma 2.2 we can obtain several explicit expressions for $P_{\Delta,0}$ as sums of polynomials in q.

Theorem 2.1. *If $n \geq 1$, $\Delta \geq 0$ and $\mu \geq 0$, then*

$$P_{\Delta,0}(n, p^{\mu+1}) = \frac{\Pi_{\Delta+n}(q)}{\Pi_\Delta(q)} \sum_{k=0}^{\mu} q^{k(\Delta+1)} \begin{bmatrix} n+k-1 \\ k \end{bmatrix} \tag{2.2}$$

$$= \frac{\Pi_{\mu+n}(q)}{\Pi_\mu(q)} \sum_{k=0}^{\Delta} q^{k(\mu+1)} \begin{bmatrix} n+k-1 \\ k \end{bmatrix} \tag{2.3}$$

$$= 1 - \frac{q^{(\Delta+1)(\mu+1)}}{\Pi_\Delta(q)\Pi_\mu(q)} \sum_{k=0}^{n-1} \frac{q^k \Pi_{\Delta+k}(q)\Pi_{\mu+k}(q)}{\Pi_k(q)}. \tag{2.4}$$

Proof. Expression (2.2) gives the correct values for $\mu=0$ or $n=1$. Furthermore, for $\mu \geq 1$,

$$\begin{aligned}
&\frac{\Pi_{\Delta+n}(q)}{\Pi_\Delta(q)} \sum_{k=0}^{\mu} q^{k(\Delta+1)} \begin{bmatrix} n+k-1 \\ k \end{bmatrix} - (1-q^{n+\Delta}) \frac{\Pi_{\Delta+n-1}(q)}{\Pi_\Delta(q)} \sum_{k=0}^{\mu} q^{k(\Delta+1)} \begin{bmatrix} n+k-2 \\ k \end{bmatrix} \\
&\qquad - q^{n+\Delta} \frac{\Pi_{\Delta+n}(q)}{\Pi_\Delta(q)} \sum_{k=0}^{\mu-1} q^{k(\Delta+1)} \begin{bmatrix} n+k-1 \\ k \end{bmatrix} \\
&= \frac{\Pi_{\Delta+n}(q)}{\Pi_\Delta(q)\Pi_{n-1}(q)} \left(\sum_{k=0}^{\mu} q^{k(\Delta+1)} \frac{\Pi_{n+k-1}(q)}{\Pi_k(q)} - \sum_{k=0}^{\mu} (1-q^{n-1}) q^{k(\Delta+1)} \frac{\Pi_{n+k-2}(q)}{\Pi_k(q)} \right. \\
&\qquad \left. - q^{n-1} \sum_{k=0}^{\mu-1} q^{(k+1)(\Delta+1)} \frac{\Pi_{n+k-1}(q)}{\Pi_k(q)} \right) \\
&= \frac{\Pi_{\Delta+n}(q)}{\Pi_\Delta(q)\Pi_{n-1}(q)} \left(\sum_{k=0}^{\mu} q^{k(\Delta+1)} ((1-q^{n+k-1}) - (1-q^{n-1})) \frac{\Pi_{n+k-2}(q)}{\Pi_k(q)} \right. \\
&\qquad \left. - q^{n-1} \sum_{k=1}^{\mu} q^{k(\Delta+1)} \frac{\Pi_{n+k-2}(q)}{\Pi_{k-1}(q)} \right) \\
&= \frac{\Pi_{\Delta+n}(q) q^{n-1}}{\Pi_\Delta(q)\Pi_{n-1}(q)} \left(\sum_{k=0}^{\mu} (1-q^k) q^{k(\Delta+1)} \frac{\Pi_{n+k-2}(q)}{\Pi_k(q)} - \sum_{k=1}^{\mu} q^{k(\Delta+1)} \frac{\Pi_{n+k-2}(q)}{\Pi_{k-1}(q)} \right) \\
&= 0,
\end{aligned}$$

so (2.1) is satisfied as well. Equation (2.2) follows by induction.

To establish (2.4), note from (2.2) and (2.1) that

$$P_{\Delta,0}(n, p^{\mu+1}) - P_{\Delta,0}(n, p^{\mu}) = q^{\mu(\Delta+1)} \frac{\Pi_{\Delta+n}(q)\Pi_{n+\mu-1}(q)}{\Pi_\Delta(q)\Pi_\mu(q)\Pi_{n-1}(q)},$$

and

$$P_{\Delta,0}(n, p^{\mu+1}) - q^{n+\Delta} P_{\Delta,0}(n, p^{\mu}) = (1-q^{n+\Delta}) P_{\Delta,0}(n-1, p^{\mu+1}).$$

Eliminating $P_{\Delta,0}(n, p^{\mu})$ yields

$$P_{\Delta,0}(n, p^{\mu+1}) = P_{\Delta,0}(n-1, p^{\mu+1}) - q^{n+\Delta+\mu+\Delta\mu} \frac{\Pi_{n+\Delta-1}(q)\Pi_{n+\mu-1}(q)}{\Pi_\Delta(q)\Pi_\mu(q)\Pi_{n-1}(q)},$$

from which (2.4) follows by induction.

Noting that (2.4) is symmetric in Δ and μ, (2.3) follows immediately from (2.2). □

Note that the identity (2.2) = (2.4) is also true if Δ is not an integer, provided that we interpret $\Pi_{x+t}(q)/\Pi_x(q) = (1-q^{x+1})(1-q^{x+2}) \cdots (1-q^{x+t})$ for integer $t \geq 0$. The proof is the same. One of the referees has noticed that the identities (2.2) = (2.3) = (2.4) can also be derived from Heine's Transformation (see [8, eq. 4.7] and [1, p. 19]).

Comparison of (2.2) and (2.3), or examination of (2.4), reveals the following interesting symmetry, for which we do not have a direct combinatorial explanation.

Corollary 2.1. *For $n \geq 0$, $\Delta \geq 0$ and $\mu \geq 0$, we have*

$$P_{\Delta,0}(n, p^{\mu+1}) = P_{\mu,0}(n, p^{\Delta+1}).$$

Corollary 2.2. *Let A be a random $n \times n$ matrix over $\mathbb{Z}_{p^\mu}$. Then, for $0 \leq i \leq p^\mu - 1$,*

$$\operatorname{Prob}(\det A \equiv i \pmod{p^\mu}) = \begin{cases} q^\mu \dfrac{1-q^n}{1-q} \dfrac{\Pi_{n+k-1}(q)}{\Pi_k(q)}, & \text{for } i \neq 0,\ \gcd(i, p^\mu) = p^k, \\ 1 - \dfrac{\Pi_{n+\mu-1}(q)}{\Pi_{\mu-1}(q)}, & \text{for } i = 0. \end{cases}$$

Proof. By multiplying the first row of A by numbers prime to p^μ, it is easy to show that two determinant values $(\operatorname{mod} p^\mu)$ are equally likely if they are divisible by the same powers of p. The corollary now follows from (2.3). □

The Chinese Remainder Theorem can be used to extend Corollary 2.2 to arbitrary moduli.

3. The general case

In this section we determine $P_{\Delta,\delta}(n, p^\mu)$ where p is prime. As in Section 2, the result for general modulus follows from Lemma 1.1.

In order to derive a recurrence for $Q_{\Delta,\delta}(n, p^\mu)$, we need to generalize it. For $0 \leq d \leq n$, define $Q^{(d)}_{\Delta,\delta}(n, p^\mu)$ to be the probability that an $(n + \Delta) \times n$ random matrix A over $\mathbb{Z}_{p^\mu}$ has p^μ-rank less than $n - \delta$, subject to the event that the first $n - d$ columns of A are divisible by p. In particular, $Q^{(n)}_{\Delta,\delta}(n, p^\mu) = Q_{\Delta,\delta}(n, p^\mu)$. Let $q = 1/p$ as before.

Lemma 3.1. *Suppose that $\Delta \geq 0$, $\mu \geq 0$, $0 \leq \delta \leq n$ and $0 \leq d \leq n$. Then*

$$Q^{(d)}_{\Delta,\delta}(n, p^\mu) = \begin{cases} 0, & \text{if } \delta = n, \quad (3.1) \\ 1, & \text{if } \delta < n,\ \mu + \delta - n + d \leq 0, \quad (3.2) \\ Q^{(n)}_{\Delta,\delta}(n, p^{\mu+\delta-n}), & \text{if } d = 0,\ \delta < n,\ \mu + \delta - n > 0, \quad (3.3) \\ q^{n+\Delta} Q^{(d-1)}_{\Delta,\delta}(n, p^\mu) + (1 - q^{n+\Delta}) Q^{(d-1)}_{\Delta,\delta}(n-1, p^\mu), & \text{otherwise.} \quad (3.4) \end{cases}$$

Proof. (3.1) follows from the definition of Q. To obtain (3.2), note that, since at least $n - d$ columns of A are divisible by p, any $(n - \delta) \times (n - \delta)$ submatrix of A has at least $n - \delta - d$ columns divisible by p. To obtain (3.3), divide every matrix entry by p.

Under the stated conditions for (3.4), there are two possibilities. With probability $q^{n+\Delta}$, the $(n - d + 1)$th column is divisible by p. If not, we can choose an element which is not divisible by p in the $(n - d + 1)$th column and perform one phase of Gaussian elimination, just as in Lemma 2.2. □

Our next task is the elimination of the variable d. For notational convenience, define $Q_{\Delta,\delta}(n, p^{\mu}) = 1$ for $\mu \leqslant 0$. The following theorem generalises Theorem 1.1.

Theorem 3.1. *For $\Delta \geqslant 0$, $\mu \geqslant 1$, $n \geqslant 1$, and $-1 \leqslant \delta \leqslant n$,*

$$Q_{\Delta,\delta}(n, p^{\mu}) = \sum_{t=\delta+1}^{n} q^{t(t+\Delta)} \frac{\Pi_{n+\Delta}(q)}{\Pi_{t+\Delta}(q)} \begin{bmatrix} n \\ t \end{bmatrix} Q_{\Delta,\delta}(t, p^{\mu+\delta-t}).$$

Proof. Define

$$R^{(d)}(n, p^{\mu}) = \frac{\Pi_{\delta+\Delta}(q)}{\Pi_{n+\Delta}(q)} (1 - Q_{\Delta,\delta}^{(d)}(n, p^{\mu})).$$

Equations (3.1)–(3.4) can now be written thus:

$$R^{(d)}(n, p^{\mu}) = \begin{cases} 1, & \text{if } \delta = n, & (3.5) \\ 0, & \text{if } \delta < n,\ \mu + \delta - n + d \leqslant 0, & (3.6) \\ R^{(n)}(n, p^{\mu+\delta-n}), & \text{if } d = 0,\ \delta < n,\ \mu + \delta - n > 0, & (3.7) \\ q^{n+\Delta} R^{(d-1)}(n, p^{\mu}) + R^{(d-1)}(n-1, p^{\mu}), & \text{otherwise.} & (3.8) \end{cases}$$

In Fig. 1, A is the line segment from $(\delta, 0)$ to (δ, δ), B is the semi-infinite ray $n = \mu + \delta + d$ $(d \geqslant 0)$, and C is the line segment from $(\delta + 1, 0)$ to $(\delta + \mu - 1, 0)$. A, B and C are places on the (n, d) plane where (3.5), (3.6) and (3.7) are applicable.

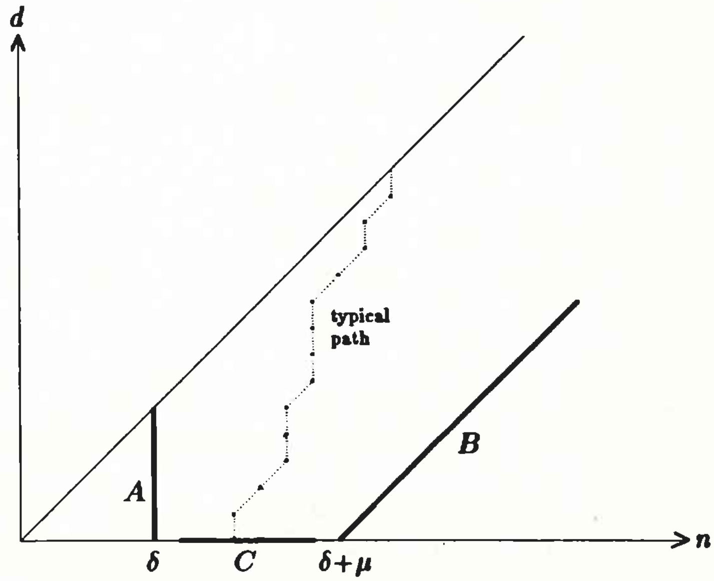

Fig. 1

Application of (3.8) to the evaluation of $R^{(n)}(n, p^{\mu})$ corresponds to enumerating a family of paths $L = (n_0, d_0), (n_1, d_1), \ldots, (n_k, d_k)$, where $(n_0, d_0) = (n, n)$ and, for $1 \leqslant i \leqslant k$, either $(n_i, d_i) = (n_{i-1}, d_{i-1} - 1)$ or $(n_i, d_i) = (n_{i-1} - 1, d_{i-1} - 1)$. It is required that (n_k, d_k) is the first point on L which belongs to $A \cup B \cup C$. The *weight* of L is defined to be $q^{\sum_{i \in I(L)}(n_i + \Delta)}$, where $I(L) = \{i \mid 0 \leqslant i < k, n_i = n_{i+1}\}$.

Let W_A be the total weight of all the paths whose last point belongs to A. For $\delta + 1 \leqslant t \leqslant \delta + \mu - 1$, let W_t be the total weight of all paths whose last point is $(t, 0)$. Then, by (3.5)–(3.8),

$$R^{(n)}(n, p^{\mu}) = W_A + \sum_{t=\delta+1}^{\delta+\mu-1} W_t R^{(t)}(t, p^{\mu+\delta-t}). \tag{3.9}$$

To determine W_A, notice from the diagram that it is independent of μ. Thus, by (3.9), $W_A = R^{(n)}(n, p)$.

Next consider W_t. If $t > \min(\delta + \mu - 1, n)$ then clearly $W_t = 0$, so suppose that $t \leqslant \min(\delta + \mu - 1, n)$. Let $L = (n_0, d_0), \ldots, (n_n, d_n)$ be a path with $(n_n, d_n) = (t, 0)$, and let $i_1 < i_2 < \cdots < i_{n-t}$ be the values of d_j for $j \in \{0, 1, \ldots, n-1\} - I(L)$. In other words, $i_1, i_2, \ldots, i_{n-t}$ are (in reverse order) the values of d at the points from which L moves down diagonally. The weight of L is

$$q^{(n-i_{n-t})(n+\Delta)+(i_{n-t}-i_{n-t-1}-1)(n+\Delta-1)+\cdots+(i_1-1)(t+\Delta)} = q^{(n+\Delta)t+(n-t)(n-t+1)/2-(i_1+i_2+\cdots+i_{n-t})}.$$

Therefore, the total weight of all such paths is

$$W_t = q^{(n+\Delta)t+(n-t)(n-t+1)/2}\alpha_{n,t}(q),$$

where

$$\begin{aligned}\alpha_{n,t}(q) &= \begin{cases} 1, & \text{if } t = 0, \\ \displaystyle\sum_{1 \leqslant i_1 < \cdots < i_{n-t} \leqslant n} q^{-(i_1+i_2+\cdots+i_{n-t})}, & \text{if } 1 \leqslant t \leqslant n, \end{cases} \\ &= \text{the coefficient of } x^{n-t} \text{ in } \prod_{i=1}^{n} (1 + q^{-i}x) \\ &= q^{-(n-t)(n-t+1)/2-(n-t)t}\begin{bmatrix} n \\ t \end{bmatrix},\end{aligned}$$

by [5, Exercise 2.6.10(b)]. Therefore, $W_t = q^{t(t+\Delta)}\left[\begin{smallmatrix} n \\ t \end{smallmatrix}\right]$, and so

$$R^{(n)}(n, p^{\mu}) = R^{(n)}(n, p) + \sum_{t=\delta+1}^{\min(\delta+\mu-1,n)} q^{t(t+\Delta)}\begin{bmatrix} n \\ t \end{bmatrix} R^{(t)}(t, p^{\mu+\delta-t}). \tag{3.10}$$

The theorem follows on applying the definition of R and Theorem 1.1. □

If care is taken to avoid unneccessary repetition of computation, either Lemma 3.1 or Theorem 3.1 can be used to compute $P_{\Delta,\delta}(n, p^{\mu})$ using a number of arithmetic operations bounded by a polynomial in $n + \Delta$ and μ.

We are now equipped to develop expressions for $Q_{\Delta,\delta}(n, p^{\mu})$ and $P_{\Delta,\delta}(n, p^{\mu})$.

Theorem 3.2. *Let $\Delta \geqslant 0$, $\mu \geqslant 1$, $n \geqslant 1$ and $0 \leqslant \delta \leqslant n$. Then*

$$P_{\Delta,\delta}(n, p^\mu) = \Pi_n(q)\Pi_{n+\Delta}(q) \times \left(\sum_{A_{n-\delta}(\mu)} f(\alpha_1, \ldots, \alpha_r) - \sum_{B_{n-\delta}(\mu)} f(\alpha_1, \ldots, \alpha_r) \right) \quad (3.11)$$

and

$$Q_{\Delta,\delta}(n, p^\mu) = \Pi_n(q)\Pi_{n+\Delta}(q) \sum_{C_{n-\delta}(\mu)} f(\alpha_1, \ldots, \alpha_r), \quad (3.12)$$

where

$$f(\alpha_1, \ldots, \alpha_r) = \frac{q^{\sum_{i=1}^r (\alpha_i+\delta)(\alpha_i+\delta+\Delta)}}{\Pi_{\alpha_1+\delta}(q)\Pi_{\alpha_1+\delta+\Delta}(q)\Pi_{\alpha_2-\alpha_1}(q) \cdots \Pi_{\alpha_r-\alpha_{r-1}}(q)\Pi_{n-\delta-\alpha_r}(q)},$$

$$A_{n-\delta}(\mu) = \{(\alpha_1, \ldots, \alpha_r) \mid 0 \leqslant \alpha_1 \leqslant \cdots \leqslant \alpha_r \leqslant n-\delta, \quad r \geqslant 1, \\ \alpha_2 + \cdots + \alpha_r \leqslant \mu - r \leqslant \alpha_1 + \cdots + \alpha_r \leqslant \mu - 1\},$$

$$B_{n-\delta}(\mu) = \{(\alpha_1, \ldots, \alpha_r) \mid 0 \leqslant \alpha_1 \leqslant \cdots \leqslant \alpha_r \leqslant n-\delta, \quad r \geqslant 2, \\ \mu - r + 1 \leqslant \alpha_2 + \cdots + \alpha_r \leqslant \mu - 1 < \alpha_1 + \cdots + \alpha_r\},$$

and

$$C_{n-\delta}(\mu) = \{(\alpha_1, \ldots, \alpha_r) \mid 1 \leqslant \alpha_1 \leqslant \cdots \leqslant \alpha_r \leqslant n-\delta, \\ \alpha_2 + \cdots + \alpha_r \leqslant \mu - 1 < \alpha_1 + \cdots + \alpha_r\}.$$

Proof. Consider the computation of $Q_{\Delta,\delta}(n, p^\mu)$ by repeated application of Theorem 3.1, with the boundary conditions $Q_{\Delta,\delta}(n, p^\mu) = 1$ if $\mu \leqslant 0$. We see that $Q_{\Delta,\delta}(n, p^\mu)$ thus has the form

$$\sum_{(t_1,\ldots,t_r)\in T(n,\delta,\mu)} \frac{\Pi_{n+\Delta}(q)}{\Pi_{t_r+\Delta}(q)} \begin{bmatrix} n \\ t_1 \end{bmatrix} \begin{bmatrix} t_1 \\ t_2 \end{bmatrix} \cdots \begin{bmatrix} t_{r-1} \\ t_r \end{bmatrix} q^{\sum_{i=1}^r t_i(t_i+\Delta)}, \quad (3.13)$$

where $T(n, \delta, \mu)$ is the set of all possible sequences of values of the summation index t (in Theorem 3.1). A particular vector $(t_1, \ldots, t_r)$ occurs if $n \geqslant t_1 \geqslant \cdots \geqslant t_r \geqslant \delta + 1$, $t_1 + \cdots + t_{r-1} \leqslant \mu + (r-1)\delta - 1$ (if $r \geqslant 2$) and $t_1 + \cdots + t_r \geqslant \mu + r\delta$. Equation (3.12) now follows on substituting $\alpha_i = t_{r-i+1} - \delta$ for $1 \leqslant i \leqslant r$.

To prove (3.11) note that, for $0 \leqslant \delta \leqslant n$,

$$T(n, \delta-1, \mu)\backslash T(n, \delta, \mu) = \{(t_1, \ldots, t_r) \mid n \geqslant t_1 \geqslant \cdots \geqslant t_r \geqslant \delta, \\ t_1 + \cdots + t_{r-1} \leqslant \mu + r\delta - \delta - r \quad (r \geqslant 2), \\ \mu + r\delta - r \leqslant t_1 + \cdots + t_r \leqslant \mu + r\delta - 1\},$$

and

$$T(n, \delta, \mu)\backslash T(n, \delta-1, \mu) \\ = \{(t_1, \ldots, t_r) \mid n \geqslant t_1 \geqslant \cdots \geqslant t_r \geqslant \delta, r \geqslant 2, t_1 + \cdots + t_r \geqslant \mu + r\delta \\ \mu + r\delta - \delta - r + 1 \leqslant t_1 + \cdots + t_{r-1} \leqslant \mu + r\delta - \delta - 1\}.$$

Since the summand in (3.13) is independent of δ, we can find $P_{\Delta,\delta}(n, p^\mu) = Q_{\Delta,\delta-1}(n, p^\mu) - Q_{\Delta,\delta}(n, p^\mu)$ by subtracting the sum over $T(n, \delta, \mu)\setminus T(n, \delta-1, \mu)$ from the sum over $T(n, \delta-1, \mu)\setminus T(n, \delta, \mu)$. Equation (3.11) now follows on substituting $\alpha_i = t_{r-i+1} - \delta$ for $1 \leqslant i \leqslant r$. □

A similar evaluation of $R^{(n)}(n, p^\mu)$ for $\delta = 0$ by applying (3.10) yields the following identity when compared to (2.2). It may also be proved by induction on μ from the q-Vandermonde identity ([5, Exercise 2.6.3(c)]).

Corollary 3.1. *If $n \geqslant 1$ and $\mu \geqslant 1$, then*

$$\sum_{(\alpha_1,\ldots,\alpha_r)\in\mathcal{P}_n(\mu)} q^{\alpha_1^2+\cdots+\alpha_r^2}\begin{bmatrix} n \\ \alpha_r \end{bmatrix}\begin{bmatrix} \alpha_r \\ \alpha_{r-1} \end{bmatrix}\cdots\begin{bmatrix} \alpha_2 \\ \alpha_1 \end{bmatrix} = q^\mu \begin{bmatrix} n+\mu-1 \\ \mu \end{bmatrix},$$

where

$$\mathcal{P}_n(\mu) = \{(\alpha_1, \alpha_2, \ldots, \alpha_r) \mid 1 \leqslant \alpha_1 \leqslant \cdots \leqslant \alpha_r \leqslant n,\ \alpha_1 + \alpha_2 + \cdots + \alpha_r = \mu\}.$$

4. Asymptotics and bounds

Lemma 1.1 and Theorem 3.1 enable us to obtain various bounds on $Q_{\Delta,\delta}(n, m)$ and, using Corollaries 4.3 and 4.4 below, it is easy to deduce corresponding bounds on $P_{\Delta,\delta}(n, m)$ and $\bar{\delta}(\Delta, n, m) = \sum_{\delta=0}^{n} \delta P_{\Delta,\delta}(n, m)$. The last quantity is n minus the average m-rank of random $(n+\Delta) \times n$ matrices over $\mathbb{Z}_m$.

Throughout this section we assume that $m = p_1^{\mu_1} p_2^{\mu_2} \cdots p_k^{\mu_k}$ where $p_1 < p_2 < \cdots < p_k$ are distinct primes, $\mu_j \geqslant 1$ and $k \geqslant 1$. We define $q_j = 1/p_j$ for $j = 1, \ldots, k$ and $q_0 = \prod_{j=1}^{k} q_j$. If $k = 1$ we may write $m = p^\mu$, $q = 1/p$ for simplicity.

We also define $h = \prod_{j=1}^{k} (p_j/(p_j - 1))$. Although h is unbounded, it increases very slowly. In fact, it may be shown that $h \leqslant e^\gamma \ln(4.44 \ln m)$, where $\gamma = 0.5772\ldots$ is Euler's constant.

Define

$$f(\Delta, q, n, t) = \frac{\Pi_{n+\Delta}(q)}{\Pi_{t+\Delta}(q)}\begin{bmatrix} n \\ t \end{bmatrix} \quad \text{and} \quad \Pi_\infty(q) = \prod_{j=1}^{\infty} (1 - q^j).$$

The proof of the following lemma is straightforward and will be omitted.

Lemma 4.1. *If $\Delta \geqslant 0$, $1 \leqslant t \leqslant n$ and $0 < q \leqslant \frac{1}{2}$, then*

$$1 \leqslant f(\Delta, q, n, t) \leqslant 1/\Pi_\infty(q),$$
$$0 \leqslant f(\Delta, q, n+1, t) - f(\Delta, q, n, t) \leqslant q^{n+1-t}/\Pi_\infty(q),$$

and $q^{t(t+\Delta)} f(\Delta, q, n, t)$ is a monotonic increasing function of q.

Theorem 4.1. *$Q_{\Delta,\delta}(n, m)$ is a monotonic increasing function of $n \geqslant 1$, and a monotonic decreasing function of $\Delta \geqslant 0$, $\delta \geqslant 0$, $\mu_j \geqslant 1$ and prime p_j ($j = 1, \ldots, k$).*

Proof. By Theorem 3.1 and Lemma 4.1,

$$\begin{aligned} Q_{\Delta,\delta}(n+1, p^\mu) &\geq \sum_{t=\delta+1}^{n} q^{t(t+\Delta)} f(\Delta, q, n+1, t) Q_{\Delta,\delta}(t, p^{\mu+\delta-t}) \\ &\geq \sum_{t=\delta+1}^{n} q^{t(t+\Delta)} f(\Delta, q, n, t) Q_{\Delta,\delta}(t, p^{\mu+\delta-t}) \\ &= Q_{\Delta,\delta}(n, p^\mu), \end{aligned}$$

so monotonicity in n follows from Lemma 1.1. Monotonicity in Δ is obvious as adding a row to a matrix cannot decrease its m-rank. Monotonicity in δ is also obvious, as $Q_{\Delta,\delta}(n, m) - Q_{\Delta,\delta+1}(n, m) = P_{\Delta,\delta+1}(n, m) \geq 0$. Monotonicity of $Q_{\Delta,\delta}(n, p^\mu)$ in μ follows by induction on μ from Theorem 3.1, and monotonicity in $p = 1/q$ follows from Theorem 3.1 and the last part of Lemma 4.1. □

Corollary 4.1. *$Q_{\Delta,\delta}(\infty, m) = \lim_{n\to\infty} Q_{\Delta,\delta}(n, m)$ exists.*

The following theorem sharpens the monotonicity results of Theorem 4.1.

Theorem 4.2. *If $\Delta \geq 0, \delta \geq 0$ and $n \geq 1$, then*

$$Q_{\Delta,\delta+1}(n, m) \leq \zeta(\delta+2) q_0^{\delta+\Delta+2} Q_{\Delta+1,\delta}(n-1, m), \tag{4.1}$$

$$Q_{\Delta+1,\delta}(n, m) \leq \zeta(\delta+\Delta+2) q_0^{\delta+1} Q_{\Delta,\delta}(n, m), \tag{4.2}$$

and

$$Q_{\Delta,\delta}(n+1, p^\mu) - Q_{\Delta,\delta}(n, p^\mu) \leq 2.20 q^{n+1+(\delta+1)(\delta+\Delta)}/(1-q), \tag{4.3}$$

where $\zeta(x)$ is the Riemann zeta function.

Proof. To prove (4.1) it is sufficient to prove by induction on μ that

$$Q_{\Delta,\delta+1}(n, p^\mu) \leq \left(\frac{q^{\delta+\Delta+2}}{1-q^{\delta+2}}\right) Q_{\Delta+1,\delta}(n-1, p^\mu). \tag{4.4}$$

Using the inequality $\left[{n \atop t+1}\right] \leq \left[{n-1 \atop t}\right]/(1-q^{t+1})$ and Theorem 3.1, the induction hypothesis gives

$$\begin{aligned} Q_{\Delta,\delta+1}(n, p^\mu) &= \sum_{t=\delta+1}^{n-1} q^{(t+1)(t+\Delta+1)} \frac{\Pi_{n+\Delta}(q)}{\Pi_{t+\Delta+1}(q)} \begin{bmatrix} n \\ t+1 \end{bmatrix} Q_{\Delta,\delta+1}(t+1, p^{\mu+\delta-t}) \\ &\leq \left(\frac{q^{\delta+\Delta+2}}{1-q^{\delta+2}}\right) \sum_{t=\delta+1}^{n-1} q^{t(t+\Delta+1)} \frac{\Pi_{n+\Delta}(q)}{\Pi_{t+\Delta+1}(q)} \begin{bmatrix} n-1 \\ t \end{bmatrix} Q_{\Delta+1,\delta}(t, p^{\mu+\delta-t}), \end{aligned}$$

so (4.4) follows.

To prove (4.2) it is sufficient to prove by induction on $\mu \geq 1$ that

$$Q_{\Delta+1,\delta}(n, p^\mu) \leq \left(\frac{q^{\delta+1}}{1-q^{\delta+\Delta+2}}\right) Q_{\Delta,\delta}(n, p^\mu). \tag{4.5}$$

The proof of (4.5) is similar to that of (4.4), using Theorem 3.1 and the inequality

$$\frac{\Pi_{n+\Delta+1}(q)}{\Pi_{t+\Delta+1}(q)} \leqslant \frac{\Pi_{n+\Delta}(q)}{\Pi_{t+\Delta}(q)(1-q^{t+\Delta+1})}.$$

To prove (4.3), we have from Theorem 3.1 and Lemma 4.1 that

$$\begin{aligned} Q_{\Delta,\delta}(n+1, p^{\mu}) - Q_{\Delta,\delta}(n, p^{\mu}) &\leqslant \sum_{t=\delta+1}^{\infty} q^{t(t+\Delta)+n+1-t}/\Pi_{\infty}(q) \\ &\leqslant q^{n+1+(\delta+1)(\delta+\Delta)} \sum_{j=1}^{\infty} q^{j(j-1)}/\Pi_{\infty}(q) \\ &\leqslant 2.20 q^{n+1+(\delta+1)(\delta+\Delta)}/(1-q), \end{aligned}$$

where the constant 2.20 arises in the worst case $q = \frac{1}{2}$. □

Corollary 4.2.

$$Q_{\Delta,\delta+1}(n, m) \leqslant \frac{\pi^4}{36} q_0^{2\delta+\Delta+3} Q_{\Delta,\delta}(n, m). \tag{4.6}$$

Proof. This is immediate from (4.1), (4.2), the monotonicity of $Q_{\Delta,\delta}(n, m)$ in n, and the fact that $\zeta(\delta+\Delta+2) \leqslant \zeta(\delta+2) \leqslant \zeta(2) = \frac{1}{6}\pi^2$. □

Corollary 4.3. *If $\delta \geqslant 1$ then*

$$\left(1 - \frac{\pi^4}{36} q_0^{2\delta+\Delta+1}\right) Q_{\Delta,\delta-1}(n, m) \leqslant P_{\Delta,\delta}(n, m) \leqslant Q_{\Delta,\delta-1}(n, m).$$

Proof. This is immediate from Corollary 4.2 with δ replaced by $\delta - 1$. □

Corollary 4.4. *$\bar{\delta}(\Delta, n, m)$ is a monotonic increasing function of $n \geqslant 1$, and a monotonic decreasing function of $\Delta \geqslant 0$, $\mu_j \geqslant 1$ and prime p_j ($j = 1, \ldots, k$). Also,*

$$Q_{\Delta,0}(n, m) \leqslant \bar{\delta}(\Delta, n, m) \leqslant Q_{\Delta,0}(n, m) \Big/ \left(1 - \frac{\pi^4}{36} q_0^{\Delta+3}\right).$$

Proof. This is immediate from Theorem 4.1 and Corollary 4.2, as

$$\bar{\delta}(\Delta, n, m) = \sum_{\delta=0}^{n} Q_{\Delta,\delta}(n, m). \quad \square$$

We now give some upper and lower bounds on $Q_{\Delta,\delta}(n, m)$. Corresponding bounds on $P_{\Delta,\delta}(n, m)$ and $\bar{\delta}(\Delta, n, m)$ may easily be deduced from Corollaries 4.3 and 4.4.

Theorem 4.3. *If $\Delta \geqslant 0$, $\delta \geqslant 0$, $n \geqslant 1$ and $\tau = \sqrt{\delta(\delta+\Delta)}$, then*

$$Q_{\Delta,0}(n, m) \leqslant 2.30h/m^{\Delta+1}, \tag{4.7}$$

$$Q_{\Delta,\delta}(n, m) \leqslant 12.09hq_0^{\delta(\delta+\Delta+2)}/m^{\Delta+1}, \tag{4.8}$$

and

$$Q_{\Delta,\delta}(n, m) \leqslant h^{7.66}/m^{2\delta+\Delta+2\tau}. \tag{4.9}$$

Also, if $n \geqslant \delta + 1$, then

$$Q_{\Delta,\delta}(n, m) \geqslant 1/m^{(\delta+1)(\delta+\Delta+1)}. \tag{4.10}$$

Proof. The lower bound (4.10) is trivial, as

$$Q_{\Delta,\delta}(n, m) \geqslant Q_{\Delta,\delta}(\delta+1, m) = 1/m^{(\delta+1)(\delta+\Delta+1)}.$$

To prove (4.7), observe that from Theorem 2.1,

$$\begin{aligned} Q_{\Delta,0}(n, p^\mu) &= 1 - P_{\Delta,0}(n, p^\mu) \\ &\leqslant q^{\mu(\Delta+1)} \sum_{j=0}^{n-1} q^j/\Pi_j(q) \\ &= q^{\mu(\Delta+1)}/\Pi_{n-1}(q) \leqslant q^{\mu(\Delta+1)}/\Pi_\infty(q). \end{aligned}$$

Thus, from Lemma 1.1,

$$Q_{\Delta,0}(n, m) \leqslant c_0 h/m^{\Delta+1}, \tag{4.11}$$

where

$$c_0 = \prod_{j=1}^{k} \prod_{t=2}^{\infty} (1-q_j^t)^{-1} \leqslant \prod_{t=2}^{\infty} \prod_{\text{prime } p} (1-p^{-t})^{-1} = \prod_{t=2}^{\infty} \zeta(t) = c,$$

say, and computation shows that $c < 2.30$.

To prove (4.8), observe that for $\delta \geqslant 1$

$$Q_{\Delta,\delta}(n, m) \leqslant \zeta(\delta+1)\zeta(\delta+\Delta+1)q_0^{2\delta+\Delta+1}Q_{\Delta,\delta-1}(n, m),$$

from (4.1) and (4.2). Thus, by induction on δ we have

$$Q_{\Delta,\delta}(n, m) \leqslant \left(\prod_{j=1}^{\delta} \zeta(j+1)(\zeta(j+\Delta+1)\right)q_0^{\delta(\delta+\Delta+2)}Q_{\Delta,0}(n, m).$$

Thus, from (4.11),

$$Q_{\Delta,\delta}(n, m) \leqslant c^3hq_0^{\delta(\delta+\Delta+2)}/m^{\Delta+1},$$

where $c^3 < 12.09$.

To prove (4.9) it is sufficient to show that

$$Q_{\Delta,\delta}(n, p^\mu) \leqslant q^{(2\delta+\Delta+2\tau)\mu}/(1-q)^\alpha, \tag{4.12}$$

where $\alpha \leqslant 7.66$. Define

$$K(n, \mu) = \begin{cases} 1, & \text{if } \mu \leqslant 0, \\ \sum_{j=1}^{n} q^{(j-\tau)^2} K(j, \mu - j)/\Pi_{n-j}(q), & \text{if } \mu > 0. \end{cases}$$

Then, by induction on μ, we have from Theorem 3.1 that

$$Q_{\Delta,\delta}(n + \delta, p^{\mu}) \leqslant q^{(2\delta+\Delta+2\tau)\mu} K(n, \mu),$$

so it is sufficient to show that $K(n, \mu) \leqslant 1/(1-q)^{\alpha}$. We shall only sketch the proof here.

Let σ be an integer such that $-0.5 \leqslant \varepsilon = \tau - \sigma \leqslant 0.7$ and $\beta_1 = \theta q^{(1+\varepsilon)^2} < 1$, where $\theta = \sum_{j=0}^{\infty} q^{j(j+2+2\varepsilon)}/\Pi_j(q)$. By induction on μ we find that $n \leqslant \sigma - 1$ implies that $K(n, \mu) \leqslant (\theta q^{(1+\varepsilon)^2})^{\lceil \mu/n \rceil}$. Thus, by induction on μ, we have $K(\sigma, \mu) \leqslant f_0$, where

$$f_0 = \begin{cases} 1 + s/(1 - \beta_1), & \text{if } \varepsilon = 0, \\ \max_{j \geqslant 0} m_j, & \text{if } \varepsilon \neq 0, \end{cases}$$

where $m_0 = 1$, $m_{j+1} = \beta_0 m_j + \beta_1^j s$, $\beta_0 = q^{\varepsilon^2}$ and $s = \sum_{j=1}^{\infty} q^{(j+\varepsilon)^2}/\Pi_j(q)$. Now, for all integers $j > 0$, we have $K(\sigma + j, \mu) \leqslant f_i$, where

$$f_j = \max\left(1, \frac{\sum_{i=0}^{j-1} q^{(i-\varepsilon)^2} f_i/\Pi_{j-i}(q) + \sum_{i=1}^{\infty} q^{(i+\varepsilon)^2}/\Pi_{j+i}(q)}{1 - q^{(j-\varepsilon)^2}}\right)$$

and $f_\infty = \lim_{j\to\infty} f_j$ satisfies

$$f_\infty \leqslant \max\left(1, \frac{\sum_{i=0}^{j-1} q^{(i-\varepsilon)^2} f_i + \sum_{i=1}^{\infty} q^{(i+\varepsilon)^2}}{\Pi_\infty(q) - \sum_{i=j}^{\infty} q^{(i-\varepsilon)^2}}\right),$$

for all $j \geqslant 3$.

Since $K(n, \mu)$ is a monotonic increasing function of n, we have the uniform bound $K(n, \mu) \leqslant f_\infty$. Moreover, using the result that $q^{\varepsilon^2} + q^{(1-\varepsilon)^2} \leqslant 1 + 27q/16$, it is easy to see that $f_0, f_1, \ldots, f_\infty$ are uniformly $1 + O(q)$, so $K(n, \mu) \leqslant 1/(1-q)^{\alpha}$ for some constant α. To show that we can take $\alpha \leqslant 7.66$, choose σ such that $-\frac{1}{2} < \varepsilon = \tau - \sigma \leqslant \frac{1}{2}$ for $p \geqslant 3$, and $\varepsilon_0 < \varepsilon = \tau - \sigma \leqslant 1 + \varepsilon_0$ for $p = 2$, where $\varepsilon_0 = -0.3006\ldots$ is defined by $\sum_{j=1}^{\infty} 2^{-(j+\varepsilon_0)^2}/\Pi_{j-1}(\frac{1}{2}) = 1$. This concludes our sketch of the proof of (4.12). □

We can now show that the convergence of $Q_{\Delta,\delta}(n, m)$ to $Q_{\Delta,\delta}(\infty, m)$ as $n \to \infty$ is rapid.

Corollary 4.5. *If* $\Delta \geqslant 0$, $\delta \geqslant 0$ *and* $n \geqslant 1$ *then*

$$Q_{\Delta,\delta}(n+1, m) - Q_{\Delta,\delta}(n, m) \leqslant 26.6hkq_1^{n-\delta} q_0^{(\delta+1)(\delta+\Delta+1)}.$$

Proof. Suppose $n \geqslant \delta$, for otherwise the result is trivial. From Theorem 4.1 we have

$$Q_{\Delta,\delta}(n+1, m) - Q_{\Delta,\delta}(n, m) \leqslant \sum_{j=1}^{k} (Q_{\Delta,\delta}(n+1, p_j^{\mu_j}) - Q_{\Delta,\delta}(n, p_j^{\mu_j}))Q_{\Delta,\delta}(n+1, m/p_j^{\mu_j})$$

so the result follows from (4.3) and (4.8). □

From Theorem 1.1 and Corollary 4.3, the lower bound (4.10) is almost attained if m is a large prime. On the other hand, if τ is a positive integer which divides μ, $n \geqslant \delta + \tau$, and $m = p^\mu$ for prime p, then $Q_{\Delta,\delta}(n, m) \geqslant 1/m^{2\delta+\Delta+2\tau}$. Thus, although the bounds (4.9) and (4.10) differ widely, the exponents of m are the best possible. However, the exponent 7.66 of h in (4.9) is not the best possible. From numerical evidence we conjecture that $\limsup_{\mu\to\infty} Q_{\Delta,\delta}(\infty, p^\mu)p^{(2\delta+\Delta+2\tau)\mu}$ is maximal when $\Delta = 0$ and $\delta = 2$ (if $p \leqslant 3$) or $\delta = 1$ (if $p \geqslant 5$). This leads to the following conjecture, in which the constant $\pi^4/36$ is best possible (since $\limsup_{\mu\to\infty} Q_{0,1}(n, p^\mu)p^{4\mu} = [\frac{n+1}{2}]^2$).

Conjecture 4.1.

$$Q_{\Delta,\delta}(n, m) \leqslant \frac{\pi^4}{36} h \max(h, 8.81)/m^{2\delta+\Delta+2\tau}$$
$$\leqslant \left(\frac{\pi^2 e^\gamma}{6} \ln(16 \ln m)\right)^2 / m^{2\delta+\Delta+2\tau}.$$

Table 1

	$P_{0,\delta}(\infty, m)$						
m	$\delta = 0$	$\delta = 1$	$\delta = 2$	$\delta = 3$	$\delta = 4$	$\delta = 5$	$\bar{\delta}(0, \infty, m)$
2	0.288 788 10	0.577 576 19	0.128 350 26	0.005 238 79	0.000 046 57	(−8)9.691	0.850 179 83
3	0.560 126 08	0.420 094 56	0.019 691 93	0.000 087 39	(−8)4.096	(−12)2.10	0.459 740 76
4	0.577 576 19	0.409 116 47	0.013 250 45	0.000 056 80	(−8)9.762	(−11)4.88	0.435 788 15
5	0.760 332 80	0.237 604 00	0.002 062 53	(−7)6.707	(−12)8.61	(−18)4.41	0.241 731 08
6	0.687 156 43	0.310 200 34	0.002 642 77	(−7)4.621	(−12)1.91	(−19)2.03	0.315 487 26
7	0.836 795 41	0.162 710 22	0.000 494 35	(−8)2.959	(−14)3.60	(−22)8.91	0.163 699 00
8	0.770 101 59	0.228 838 78	0.001 059 35	(−7)2.775	(−11)5.16	(−15)6.06	0.230 958 32
9	0.840 189 12	0.159 480 34	0.000 330 50	(−8)4.540	(−12)2.10	(−17)1.19	0.160 141 47
10	0.829 545 83	0.170 178 45	0.000 275 71	(−9)3.545	(−16)4.02	(−25)4.28	0.170 729 89
11	0.900 832 71	0.099 091 60	0.000 075 69	(−10)4.71	(−17)2.42	(−26)1.02	0.099 242 99
12	0.814 186 78	0.185 550 01	0.000 263 21	(−9)4.974	(−15)4.00	(−22)1.02	0.186 076 43
13	0.917 162 47	0.082 799 39	0.000 038 14	(−10)1.03	(−18)1.64	(−28)1.55	0.082 875 67
14	0.883 926 95	0.116 006 98	0.000 066 07	(−10)1.56	(−18)1.68	(−29)8.64	0.116 139 12
15	0.894 576 65	0.105 382 54	0.000 040 81	(−11)5.86	(−19)3.53	(−30)9.26	0.105 464 16
16	0.880 116 10	0.119 805 52	0.000 078 38	(−9)1.530	(−14)1.08	(−19)1.87	0.119 962 29

In Table 1 we give some values of $P_{0,\delta}(\infty, m)$ and $\bar{\delta}(0, \infty, m)$. The notation "(−9)1.23" means $1.23 \cdot 10^{-9}$.

References

[1] G.E. Andrews, The Theory of Partitions (Addison–Wesley, Reading, 1976).
[2] G.E. Andrews, Applications of basic hypergeometric functions, SIAM Rev. 16(4) (1974) 441–484.
[3] R.P. Brent and B.D. McKay, Determinants (mod m) of random symmetric integer matrices, to appear.
[4] J. Goldman and G.-C. Rota, On the foundations of combinatorial theory IV: Finite vector spaces and Eulerian generating functions, Stud. Appl. Math. 49(3) (1970) 239–258.
[5] I.P. Goulden and D.M. Jackson, Combinatorial Enumeration, (Wiley, New York, 1983).
[6] G. Landsberg, Über eine Anzahlbestimmung und eine damit zusammenhängende Reihe, J. Reine und Angewandte Math. 111 (1893) 87–88.
[7] A. Mukhopadhyay, On the probability that the determinant of an $n \times n$ matrix over a finite field vanishes, Discrete Math. 51 (1984) 311–315.
[8] D.B. Sears, On the transformation theory of basic hypergeometric functions, Proc. London Math. Soc. (Second Ser.) 53 (1951) 158–180.