Two-stage allocations and the double Q-function

Sergey Agievich
National Research Center for Applied Problems of Mathematics and Informatics
Belarusian State University
Fr. Skorina av. 4, 220050 Minsk, Belarus
agievich@bsu.by

Submitted: Apr 2, 2002; Accepted: Jun 10, 2002; Published: May 12, 2003
MR Subject Classifications: 05A15, 05A16, 60C05

Abstract

Let $m+n$ particles be thrown randomly, independently of each other into N cells, using the following two-stage procedure.

1. The first m particles are allocated equiprobably, that is, the probability of a particle falling into any particular cell is $1/N$. Let the ith cell contain m_i particles on completion. Then associate with this cell the probability $a_i = m_i/m$ and withdraw the particles.
2. The other n particles are then allocated polynomially, that is, the probability of a particle falling into the ith cell is a_i.

Let $\nu = \nu(m, N)$ be the number of the first particle that falls into a non-empty cell during the second stage. We give exact and asymptotic expressions for the expectation $\mathbf{E}\,\nu$.

1 Introduction

Problems that deal with random allocations of particles into N cells (balls into urns, pellets into boxes) are classical in discrete probability theory and combinatorial analysis (see [3, 7] for details). The main results are concerned with determining the probability characteristics of (i) the number μ_r of cells that contain exactly r particles after allocation, (ii) the number $\nu_{r,s}$ of the first particle that falls so that some s cells contain at least r particles each, and other random variables.

Equiprobable allocations are the most simple and well studied. Consider, for example, an Internet voting on the theme: "Which of the N teams will win the world cup?". If voters don't know anything about the teams, then they make a choice (particle) for each team (cell) with equal probability $1/N$. The more common model is so-called polynomial allocations. In this case, the probabilities $a_1, \ldots, a_N$ to fall into each cell are given. For example, we can assume that common preferences exist and voters make a choice for the ith team with the probability a_i.

Pose the question: how are preferences formed in the absence of a priori information? In this paper we introduce two-stage allocations. At the first stage particles are allocated equiprobably. The number of particles that fell into a particular cell determines the probability to occupy this cell by particles at the second stage. In this model, preferences are formed after the public announcement of the preliminary voting results, i. e. the numbers $m_1, \ldots, m_N$ of votes for each team. We can suppose that after seeing these results, influenced voters will make a choice for the ith team with the probability $a_i = m_i/m$, where $m = m_1 + \ldots + m_N$.

In the next section, using the generating function for the numbers μ_r, we obtain an expectation of the random variable $\nu = \nu_{2,1}$ for allocations at the second stage. To illustrate our interest to the analysis of ν, take the example of cryptographic hash functions [8, chapter 9].

Let $\mathcal{A}$ and $\mathcal{B}$ be finite alphabets, $|\mathcal{B}| = N$, and let $\mathcal{A}^*$ be a set of all finite words over $\mathcal{A}$. The hash function $h\colon \mathcal{A}^* \to \mathcal{B}$ is applied in cryptography for data compression such that it is computationally infeasible to find a collision: two different words with the same hash value.

The model of random equiprobable allocations of particles (hash values of different input words) into N cells (elements of $\mathcal{B}$) is often used in the analysis of collision search algorithms. The collision waiting time ν is the number of the first particle that occupies non-empty cell. The difficulty of the collision search can be measured by the expectation $\mathbf{E}\,\nu$. From the asymptotic expansion for Ramanujan's Q-function [6, § 1.2.11.3] it follows that

$$\mathbf{E}\,\nu = \sqrt{\frac{\pi N}{2}} + \frac{2}{3} + o(1)$$

as $N \to \infty$.

Most cryptographic hash functions have iterative structure based on the compression function $\sigma\colon \mathcal{A} \times \mathcal{B} \to \mathcal{B}$. The input word $X = X_1 \ldots X_l$ is processed in the following way: Beginning with a fixed symbol $Y_0 \in \mathcal{B}$, successively compute $Y_k = \sigma(X_k, Y_{k-1})$, $k = 1, \ldots, l$, and set the hash value $h(X)$ to $\sigma(L, Y_l)$, where L is the representation of the length l by a symbol of $\mathcal{A}$.

To define σ, we must choose N values $\sigma(L, Y)$, where Y runs over $\mathcal{B}$. Suppose that a value B was chosen N_B times. Now, if for a random input word of length l an intermediate hash value Y_l has uniform distribution on $\mathcal{B}$, then a final hash value B will appear with probability N_B/N, that is in general not equal to $1/N$. It is clear that collision waiting time for this case is not greater on average than for the case of equiprobable allocations. Indeed, we will show that

$$\mathbf{E}\,\nu = \frac{\sqrt{\pi N}}{2} + \frac{5}{6} + o(1)$$

for the two-stage procedure "the random choice of σ — the hashing of words with the same length". This expression follows from the asymptotic expansion for the double Q-function introduced in Section 3.

2 Two-stage allocations

Let $m+n$ particles be thrown randomly, independently of each other into N cells, using the following two-stage procedure.

1. The first m particles are allocated equiprobably, that is, the probability of a particle falling into any particular cell is $1/N$. Let the ith cell contain m_i particles on completion. Then associate with this cell the probability $a_i = m_i/m$ ($a_i = 0$ if $m = 0$) and withdraw the particles.

2. The next n particles are allocated polynomially, that is, the probability of a particle falling into the ith cell is a_i.

Let $\mu_r(N,m,n)$ be the number of cells that contain exactly r particles, $\mathbf{r} = (r_1,\dots,r_s)$ be the vector of different non-negative integers, and $\mathbf{x} = (x_1,\dots,x_s)$. Consider the generating function

$$\Phi_{N,\mathbf{r}}(\mathbf{x},y,z) = \sum_{\substack{\mathbf{k}\geq\mathbf{0}\\ m,n\geq 0}} \frac{N^m m^n}{m!n!}\mathbf{x}^{\mathbf{k}} y^m z^n \mathsf{P}\left\{\mu_{\mathbf{r}}(N,m,n) = \mathbf{k}\right\}, \tag{1}$$

where $0^0 = 1$, $\mathbf{k} = (k_1,\dots,k_s)$, $\mathbf{x}^{\mathbf{k}} = x_1^{k_1}\dots x_s^{k_s}$ and

$$\mathsf{P}\left\{\mu_{\mathbf{r}}(N,m,n) = \mathbf{k}\right\} = \mathsf{P}\left\{\mu_{r_i}(N,m,n) = k_i,\ i = 1,\dots,s\right\}.$$

Theorem 1. *The generating function* (1) *has the form:*

$$\Phi_{N,\mathbf{r}}(\mathbf{x},y,z) = \left(\exp(ye^z) + \sum_{i=1}^{s}(x_i - 1)\psi_{r_i}(y)\frac{z^{r_i}}{r_i!}\right)^N, \tag{2}$$

where $\psi_r(y) = \sum_{m\geq 0}\frac{m^r}{m!}y^m$ *and moreover* $\psi_0(y) = e^y$, $\psi_{r+1}(y) = y\psi_r'(y)$, $r = 0,1,\dots$.

Proof. Divide N cells into two groups of sizes N_1 and $N_2 = N - N_1$. By the total probability theorem,

$$\begin{aligned}\mathsf{P}\left\{\mu_{\mathbf{r}}(N,m,n) = \mathbf{k}\right\} = &\sum_{\substack{\mathbf{k}_1+\mathbf{k}_2=\mathbf{k},\ \mathbf{k}_i\geq\mathbf{0}\\ m_1+m_2=m,\ m_i\geq 0\\ n_1+n_2=n,\ n_i\geq 0}} \binom{m}{m_1}\left(\frac{N_1}{N}\right)^{m_1}\left(\frac{N_2}{N}\right)^{m_2}\binom{n}{n_1}\left(\frac{m_1}{m}\right)^{n_1}\left(\frac{m_2}{m}\right)^{n_2}\\ &\times \mathsf{P}\left\{\mu_{\mathbf{r}}(N_1,m_1,n_1) = \mathbf{k}_1\right\}\mathsf{P}\left\{\mu_{\mathbf{r}}(N_2,m_2,n_2) = \mathbf{k}_2\right\},\end{aligned}$$

where $m_i/m = 0$ if $m = 0$. Multiplying both sides by $\frac{N^m m^n}{m!n!}\mathbf{x}^{\mathbf{k}}y^m z^n$ and then summing over all $\mathbf{k}\geq\mathbf{0}$, $m,n\geq 0$, we obtain

$$\Phi_{N,\mathbf{r}}(\mathbf{x},y,z) = \Phi_{N_1,\mathbf{r}}(\mathbf{x},y,z)\Phi_{N_2,\mathbf{r}}(\mathbf{x},y,z).$$

This yields

$$\Phi_{N,\mathbf{r}}(\mathbf{x},y,z) = (\Phi_{1,\mathbf{r}}(\mathbf{x},y,z))^N$$

and it is enough to note that

$$\begin{aligned}\Phi_{1,\mathbf{r}}(\mathbf{x},y,z) &= \sum_{m,n\geq 0} \frac{m^n y^m z^n}{m!n!} + \sum_{i=1}^{s} (x_i - 1)\frac{z^{r_i}}{r_i!} \sum_{m\geq 0} \frac{m^{r_i} y^m}{m!} \\ &= \exp(ye^z) + \sum_{i=1}^{s} (x_i - 1)\psi_{r_i}(y)\frac{z^{r_i}}{r_i!}.\end{aligned}$$

□

For comparison, if n particles are equiprobably allocated into N cells, then [7]:

$$\Phi_{N,\mathbf{r}}(\mathbf{x},z) = \sum_{\substack{\mathbf{k}\geq\mathbf{0}\\ n\geq 0}} \frac{N^n}{n!} \mathbf{x}^{\mathbf{k}} z^n \mathsf{P}\left\{\mu_{\mathbf{r}}(N,n) = \mathbf{k}\right\} = \left(e^z + \sum_{i=1}^{s}(x_i - 1)\frac{z^{r_i}}{r_i!}\right)^N.$$

Let $\nu = \nu(m,N)$ be the number of the first particle that falls into a non-empty cell at the second stage.

Theorem 2. *If $m \geq 1$, then the expectation*

$$\mathsf{E}\,\nu(m,N) = \sum_{n=0}^{\min(m,N)} \frac{m^{[n]} N^{[n]}}{m^n N^n}, \tag{3}$$

where $u^{[k]} = u(u-1)\dots(u-k+1)$ is the kth factorial power of u, $u^{[0]} = 1$.

Proof. Obviously, $\mathsf{P}\{\nu = n\} = 0$ if $n > m$ or $n > N$. Therefore,

$$\mathsf{E}\,\nu = \sum_{n=1}^{\min(m,N)} n\mathsf{P}\{\nu = n\} = \sum_{n=0}^{\min(m,N)} \mathsf{P}\{\nu > n\}$$

and it is enough to show that

$$\mathsf{P}\{\nu > n\} = \frac{m^{[n]} N^{[n]}}{m^n N^n}$$

for $n \leq \min(m,N)$. We have

$$\mathsf{P}\{\nu > n\} = \mathsf{P}\{\mu_0(N,m,n) = N - n\} = \frac{m!n!}{N^m m^n}\left[x^{N-n} y^m z^n\right]\Phi_{N,0}(x,y,z).$$

By Theorem 1, $\Phi_{N,0}(x,y,z) = (\exp(ye^z) + (x-1)e^y)^N$ and

$$\begin{aligned}
[x^{N-n}y^m z^n]\Phi_{N,0}(x,y,z) =& [y^m z^n]\binom{N}{n}\left(\exp(ye^z) - e^y\right)^n e^{(N-n)y} \\
=& [y^m z^n]\binom{N}{n}\left(\sum_{i\ge 0,\, j\ge 1}\frac{y^i i^j z^j}{i!j!}\right)^n e^{(N-n)y} \\
=& [y^m]\binom{N}{n}\left(\sum_{i\ge 0}\frac{iy^i}{i!}\right)^n e^{(N-n)y} = [y^m]\binom{N}{n}\left(ye^y\right)^n e^{(N-n)y} \\
=& [y^{m-n}]\binom{N}{n}e^{Ny} = \binom{N}{n}\frac{N^{m-n}}{(m-n)!}.
\end{aligned}$$

This implies the required result. $\square$

For comparison, if particles are equiprobably allocated into N cells and $\nu(N)$ is the number of the first particle that falls into a non-empty cell, then

$$\mathbf{E}\,\nu(N) = \sum_{n=0}^{N}\frac{N^{[n]}}{N^n}.$$

In the next section we will give an asymptotic analysis of the sum in the right-hand side of (3).

3 The double Q-function

For positive integers m and n define the *double Q-function*

$$Q(m,n) = \sum_{k=0}^{\min(m,n)}\frac{m^{[k]}n^{[k]}}{m^k n^k}.$$

The ordinary Q-function

$$Q(n) = \sum_{k=1}^{n}\frac{n^{[k]}}{n^k}$$

was studied by Ramanujan [1], Watson [10], Knuth [6]. Using the integral representation

$$Q(n) + 1 = \int_0^\infty e^{-z}\left(1 + \frac{z}{n}\right)^n dz,$$

they derived the asymptotic expansion

$$Q(n) \sim \sqrt{\frac{\pi n}{2}} - \frac{1}{3} + \frac{1}{12}\sqrt{\frac{\pi}{2n}} - \frac{4}{135n} + \dots .$$

In [4] Ramanujan's conjecture on the remainder term of this expansion was proven using another representation:

$$Q(n) = \frac{n!}{n^{n-1}}\,[z^n]\log\frac{1}{1-t(z)}, \quad t(z) = \sum_{n\ge 1}\frac{n^{n-1}}{n!}z^n = ze^{t(z)}$$

($t(z)$ is the exponential generating function of rooted labeled trees).

There exists the third representation

$$Q(n) + 1 = \frac{n!}{n^n}\,[z^n]\,\frac{e^{nz}}{1-z}$$

that provides the next "double" analog

$$Q(m,n) = \frac{m!n!}{m^m n^n}\,[x^m y^n]\,\frac{e^{mx+ny}}{1-xy}. \tag{4}$$

Use (4) to prove the following theorem.

Theorem 3. *Let $m, n \to \infty$ so that $0 < c_1 \le n/m \le c_2 < \infty$. Then*

$$Q(m,n) = \sqrt{\frac{\pi mn}{2(m+n)}} + \frac{2}{3}\left(1 + \frac{mn}{(m+n)^2}\right) + o(1). \tag{5}$$

Proof. Without loss of generality, assume that $n \le m$. Consider the generating function

$$f(x,y) = \frac{e^{-m(1-x)-n(1-y)}}{1-xy} = \sum_{k,l\ge 0} q_{kl}x^k y^l.$$

By (4),

$$Q(m,n) = m!n!\left(\frac{e}{m}\right)^m\left(\frac{e}{n}\right)^n q_{mn}. \tag{6}$$

To obtain numbers q_{mn}, $n > 1$, we use the Cauchy formula

$$q_{mn} = \frac{1}{(2\pi i)^2}\oint_{|x|=1}\oint_{\Gamma_1\cup\Gamma_2}\frac{f(x,y)}{x^{m+1}y^{n+1}}dydx.$$

Here for fixed $x = e^{i\theta}$, $-\pi \le \theta \le \pi$, the positively oriented contour $\Gamma_1 \cup \Gamma_2$ in the complex plane y is given by (see Fig. 1):

$$\Gamma_1 = \Gamma_1(\theta) = \left\{y = e^{-i\theta}(1 - re^{i\varphi}) \mid -\pi/2 + \delta \le \varphi \le \pi/2 - \delta\right\},$$
$$\Gamma_2 = \Gamma_2(\theta) = \left\{y = e^{i\varphi} \mid -\pi \le \varphi \le \pi, |\theta + \varphi| \ge 2\delta\right\},$$

where $r = n^{-2+6\varepsilon}$, $0 < \varepsilon < \frac{1}{12}$, $\delta = \arcsin\frac{r}{2}$, and the result of the summation $\theta + \varphi$ is reduced to the interval $[-\pi, \pi]$ by adding $\pm 2\pi$ as needed. Note that $\delta < r$ because

$$\sin r \ge r - \frac{r^3}{6} > r - \frac{r}{6} > \frac{r}{2} = \sin\delta.$$

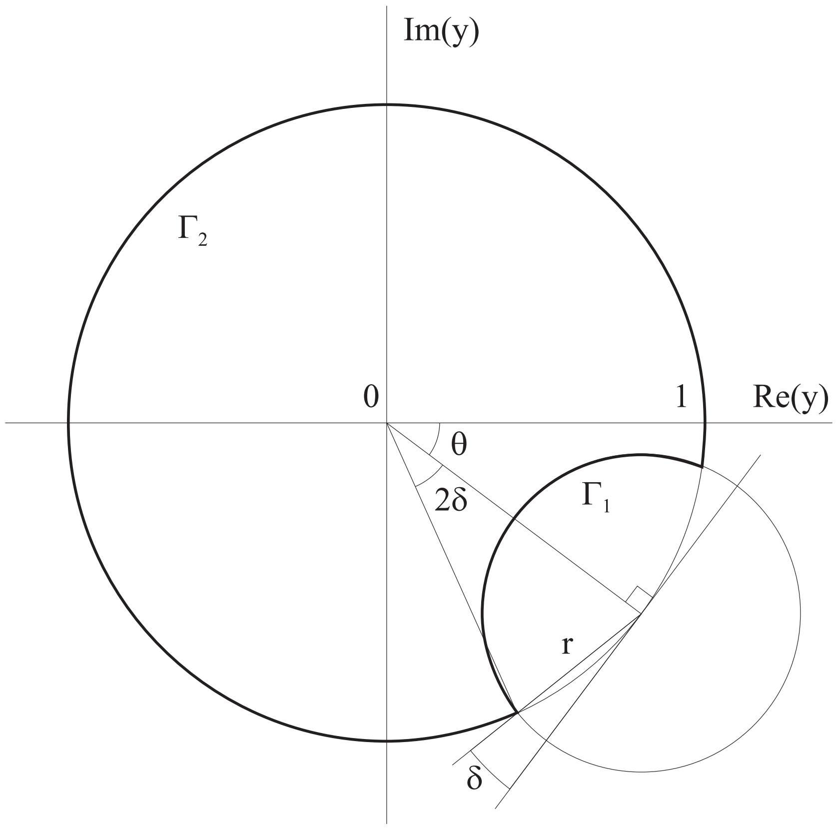

Figure 1: The contour $\Gamma_1 \cup \Gamma_2$

The chosen integration surface in two-dimensional complex space (x, y) encircles the origin and does not intersect with the surface $xy = 1$ of poles of $f(x, y)$.

Denote

$$I_k = \frac{1}{(2\pi i)^2} \oint_{|x|=1} \oint_{\Gamma_k} \frac{f(x,y)}{x^{m+1} y^{n+1}} dy dx.$$

After some calculations,

$$I_1 = \frac{1}{4\pi^2} \int_{-\pi}^{\pi} \exp(g_1(\theta)) \int_{-\pi/2+\delta}^{\pi/2-\delta} \frac{\exp(-nre^{i(\varphi-\theta)})}{(1-re^{i\varphi})^{n+1}} d\varphi d\theta,$$

$$I_2 = \frac{1}{4\pi^2} \iint_{\substack{-\pi \le \theta, \varphi \le \pi \\ |\theta+\varphi| \ge 2\delta}} \frac{\exp(g_2(\theta,\varphi))}{1-e^{i(\theta+\varphi)}} d\varphi d\theta,$$

where

$$g_1(\theta) = -m(1-e^{i\theta}) - mi\theta - n(1-e^{-i\theta}) + ni\theta,$$
$$g_2(\theta,\varphi) = -m(1-e^{i\theta}) - mi\theta - n(1-e^{i\varphi}) - ni\varphi.$$

Further we prove that the integral I_1 gives the main contribution to $Q(m, n)$ (the first term in the right-hand side of (5)). To estimate I_1, we use the technique related to Laplace's method (see [9] for references). Firstly, we approximate the integrand near $\theta = 0$ by a simpler function and evaluate the contribution of the approximation. Then we show that remaining regions of integration contribute a negligible amount.

We apply a similar technique to the integral I_2. The main difficulty is to estimate the contribution of a punctured neighborhood of the singularity $\varphi = -\theta$. The integration regions near this singularity contribute large in magnitude, but these contributions mostly cancel each other. The chosen integration path $\Gamma_2(\theta)$ allows us to control this cancellation with desired accuracy.

The integral I_1. Since

$$\int_{-\pi/2+\delta}^{\pi/2-\delta} \frac{\exp(-nre^{i(\varphi-\theta)})}{(1-re^{i\varphi})^{n+1}} d\varphi = \int_{-\pi/2+\delta}^{\pi/2-\delta} (1+O(nr))d\varphi = (\pi - 2\delta)(1+O(nr)),$$

we get

$$I_1 = \frac{1}{4\pi} \int_{-\pi}^{\pi} \exp(g_1(\theta))(1+O(n^{-1+6\varepsilon}))d\theta.$$

Denote $\theta_0 = m^{-1/2+\varepsilon}$ and split the integral into two parts: $|\theta| \le \theta_0$ and $\theta_0 \le |\theta| \le \pi$. We have

$$g_1(\theta) = -(m+n)\theta^2/2 - i(m-n)\theta^3/6 + O(m\theta_0^4)$$

in the first part and

$$|\exp(g_1(\theta))| = \exp(-(m+n)(1-\cos\theta)) < \exp(-m(1-\cos\theta_0)) = O(\exp(-m\theta_0^2/3))$$

in the second one. So, accurate to an exponentially small term,

$$\begin{aligned}
I_1 &= \frac{1}{4\pi} \int_{-\theta_0}^{\theta_0} \exp(-(m+n)\theta^2/2 - i(m-n)\theta^3/6)(1+O(n^{-1+6\varepsilon}))d\theta \\
&= \frac{1}{4\pi} \int_{0}^{\theta_0} \exp(-(m+n)\theta^2/2) \left(e^{-i(m-n)\theta^3/6} + e^{i(m-n)\theta^3/6}\right)(1+O(n^{-1+6\varepsilon}))d\theta \\
&= \frac{1}{4\pi} \int_{0}^{\theta_0} \exp(-(m+n)\theta^2/2)(2+O((m-n)^2\theta^6))(1+O(n^{-1+6\varepsilon}))d\theta \\
&= \frac{1}{2\pi} \int_{0}^{\theta_0} \exp(-(m+n)\theta^2/2)(1+O(n^{-1+6\varepsilon}))d\theta.
\end{aligned}$$

Integrating from 0 to ∞, we get

$$I_1 = \frac{1}{2\pi}\sqrt{\frac{\pi}{2(m+n)}}(1+O(n^{-1+6\varepsilon})). \tag{7}$$

The integral I_2. If $\theta_0 \le |\theta| \le \pi$, then

$$\left|\frac{\exp(g_2(\theta,\varphi))}{1-e^{i(\theta+\varphi)}}\right| \le r^{-1}|\exp(g_2(\theta,\varphi))| = r^{-1}O(\exp(-m\theta_0^2/3)) = O(\exp(-m\theta_0^2/4)).$$

Similarly, if $\varphi_0 = n^{-1/2+2\varepsilon}$ and $\varphi_0 \le |\varphi| \le \pi$, then the integrand has the order $O(\exp(-n\varphi_0^2/4))$. For m and n sufficiently large we have $\varphi_0 \ge \theta_0 + 2\delta$ and accurate to an exponentially small term

$$I_2 = \frac{1}{4\pi^2} \iint_{S_0 \cup S_1} \frac{\exp(g_2(\theta,\varphi))}{1 - e^{i(\theta+\varphi)}} d\varphi d\theta,$$

where

$$S_k = \{(\theta,\varphi) \mid 0 \le (-1)^k\theta \le \theta_0,\ \varphi \in [-\varphi_0, -\theta - 2\delta] \cup [-\theta + 2\delta, \varphi_0]\}.$$

Expanding

$$g_2(\theta,\varphi) = -m\theta^2/2 - im\theta^3/6 - n\varphi^2/2 - in\varphi^3/6 + O(m\theta_0^4 + n\varphi_0^4)$$

and changing in S_1 directions of integration, we obtain

$$I_2 = \frac{1}{4\pi^2} \iint_{S_0} \exp(-m\theta^2/2 - n\varphi^2/2) J(\alpha,\beta)(1 + O(n^{-1+8\varepsilon})) d\varphi d\theta,$$

where $\alpha = m\theta^3/6 + n\varphi^3/6$, $\beta = \theta + \varphi$,

$$\begin{aligned} J(\alpha,\beta) &= \frac{e^{-i\alpha}}{1 - e^{i\beta}} + \frac{e^{i\alpha}}{1 - e^{-i\beta}} = \frac{\cos\alpha - \cos(\alpha+\beta)}{1 - \cos\beta} = \cos\alpha + \frac{\sin\alpha}{\sin\beta}(1 + \cos\beta) \\ &= 1 + O(\alpha^2) + \frac{2\alpha}{\beta}(1 + O(\alpha^2) + O(\beta^2)) \\ &= \left(1 + \frac{n}{3}(\theta^2 - \theta\varphi + \varphi^2) + \frac{(m-n)\theta^3}{3(\theta+\varphi)}\right)(1 + O(n^{-1/2+6\varepsilon})). \end{aligned}$$

So,

$$I_2 = \left(\frac{1}{4\pi^2} I_{21} + \frac{m-n}{12\pi^2} I_{22}\right)(1 + O(n^{-1/2+6\varepsilon})),$$

where

$$\begin{aligned} I_{21} &= \iint_{S_0} \exp(-m\theta^2/2 - n\varphi^2/2)\left(1 + \frac{n}{3}(\theta^2 - \theta\varphi + \varphi^2)\right) d\varphi d\theta, \\ I_{22} &= \iint_{S_0} \exp(-m\theta^2/2 - n\varphi^2/2) \frac{\theta^3}{\theta+\varphi} d\varphi d\theta. \end{aligned}$$

Since

$$\left|1 + \frac{n}{3}(\theta^2 - \theta\varphi + \varphi^2)\right| = O(n\theta_0^2)$$

for $0 \le \theta \le \theta_0$ and $\varphi \in [-\theta - 2\delta, -\theta + 2\delta]$, we obtain

$$\begin{aligned} I_{21} &= \int_0^{\theta_0} \int_{-\varphi_0}^{\varphi_0} \exp(-m\theta^2/2 - n\varphi^2/2)\left(1 + \frac{n}{3}(\theta^2 - \theta\varphi + \varphi^2)\right) d\varphi d\theta + 4\delta\theta_0 O(n\theta_0^2) \\ &= \int_0^{\infty} \int_{-\infty}^{\infty} \exp(-m\theta^2/2 - n\varphi^2/2)\left(1 + \frac{n}{3}(\theta^2 + \varphi^2)\right) d\varphi d\theta + O(n^{-5/2+9\varepsilon}) \\ &= \frac{\pi}{\sqrt{mn}}\left(1 + \frac{1}{3} + \frac{n}{3m}\right) + O(n^{-5/2+9\varepsilon}). \end{aligned}$$

Further,

$$I_{22} = \int_0^{\theta_0} \left[\int_{-\varphi_0+\theta}^{-2\delta} + \int_{2\delta}^{\varphi_0+\theta} \right] \exp(-m\theta^2/2 - n(\varphi-\theta)^2/2) \frac{\theta^3}{\varphi} d\varphi d\theta$$

$$= \int_0^{\theta_0} \int_{2\delta}^{\varphi_0} \exp(-(m+n)\theta^2/2 - n\varphi^2/2) \frac{\theta^3(e^{n\theta\varphi} - e^{-n\theta\varphi})}{\varphi} d\varphi d\theta +$$

$$+ \int_0^{\theta_0} \left[-\int_{-\varphi_0}^{-\varphi_0+\theta} + \int_{\varphi_0}^{\varphi_0+\theta} \right] \exp(-m\theta^2/2 - n(\varphi-\theta)^2/2) \frac{\theta^3}{\varphi} d\varphi d\theta.$$

The last term is exponentially small and

$$\left| \frac{\theta^3(e^{n\theta\varphi} - e^{-n\theta\varphi})}{\varphi} \right| = O(n\theta_0^4)$$

for $0 \le \theta \le \theta_0$ and $\varphi \in [0, 2\delta]$. Therefore,

$$I_{22} = \int_0^{\theta_0} \int_0^{\varphi_0} \exp(-(m+n)\theta^2/2 - n\varphi^2/2) \frac{\theta^3(e^{n\theta\varphi} - e^{-n\theta\varphi})}{\varphi} d\varphi d\theta + 2\delta\theta_0 O(n\theta_0^4)$$

$$= \int_0^{\infty} \int_0^{\infty} \exp(-(m+n)\theta^2/2 - n\varphi^2/2) \frac{\theta^3(e^{n\theta\varphi} - e^{-n\theta\varphi})}{\varphi} d\varphi d\theta + O(n^{-7/2+11\varepsilon}).$$

Write the integrand as the series

$$2 \sum_{k \ge 0} \exp(-(m+n)\theta^2/2 - n\varphi^2/2) \frac{n^{2k+1}\theta^{2k+4}\varphi^{2k}}{(2k+1)!}$$

and interchange the summation and integrations (it is easy to justify). We get

$$I_{22} = \frac{\pi\sqrt{n}}{(m+n)^{5/2}} \left(3 + \sum_{k \ge 1} \left(\frac{n}{m+n} \right)^k (2k+3) \prod_{l=1}^{k} \left(1 - \frac{1}{2l} \right) \right) + O(n^{-7/2+11\varepsilon}).$$

Additionally,

$$3 + \sum_{k \ge 1} u^k (2k+3) \prod_{l=1}^{k} \left(1 - \frac{1}{2l} \right) = 3(1-u)^{-1/2} + u(1-u)^{-3/2}$$

for a real u, $|u| < 1$. Thus

$$I_{22} = \frac{\pi\sqrt{n}}{(m+n)^2\sqrt{m}} \left(3 + \frac{n}{m} \right) + O(n^{-7/2+11\varepsilon})$$

and, therefore,

$$I_2 = \frac{1}{2\pi\sqrt{mn}} \left(\frac{2}{3} + \frac{n}{6m} + \frac{n(m-n)}{(m+n)^2} \left(\frac{1}{2} + \frac{n}{6m} \right) \right) (1 + O(n^{-1/2+6\varepsilon})). \tag{8}$$

Applying the Stirling formula to (6), we have

$$Q(m,n) = 2\pi\sqrt{mn}(I_1 + I_2)(1 + O(n^{-1})).$$

Using here estimates (7) and (8), we obtain the result stated. □

The proof above can be easily adapted to the one-dimensional case. In this case, we obtain the first two terms of the asymptotic expansion for $Q(n)$ by estimating the integral

$$\oint_{\Gamma_1 \cup \Gamma_2} \frac{e^{-n(1-y)}}{(1-y)y^{n+1}} dy, \quad \Gamma_k = \Gamma_k(0).$$

Note that the chosen contour $\Gamma_1 \cup \Gamma_2$ differs from ones used in the saddle point method [2, 9] or in the singularity analysis [5], the most useful tools for obtaining asymptotic expansions for the coefficients of generating functions. The saddle point technique cannot be applied to our generating function $e^{-n(1-y)}(1-y)^{-1}$ due to a small singularity at $y = 1$ that yields a slow decay of the corresponding integrand near its saddle point. The singularity analysis works with generating functions of the form $L((1-y)^{-1})(1-y)^{-1}$, where $L(u)$ must be a special "slowly varying at infinity" function, but this does not hold in our case.

Acknowledgment

The author would like to thank the anonymous referees for pointing out the "voting" interpretation of two-stage allocations.

References

[1] B. C. Berndt, *Ramanujan's notebooks*, Part II, Springer-Verlag, Berlin, 1989.

[2] N. G. de Bruijn, *Asymptotic methods in analysis*, North-Holland, Amsterdam, 1958.

[3] W. Feller, *An introduction to probability theory and its applications*, Volume I, 3rd edition, John Wiley & Sons, Inc., New York, 1968.

[4] P. Flajolet, P. Grabner, P. Kirschenhofer, and H. Prodinger, On Ramanujan's Q-function, *J. Computational and Applied Mathematics* **58**(1995) 103-116.

[5] P. Flajolet, A. Odlyzko, Singularity analysis of generating functions. *SIAM Journal on Discrete Math.* **3**(1990) 216-240.

[6] D. E. Knuth, *The art of computer programming*, Vol. 1: Fundamental algorithms, Addison-Wesley, Reading, Massachusetts, 1973.

[7] V. F. Kolchin, B. Sevast'yanov, and V. Chistyakov, *Random allocations*, Wiley, New York, 1978.

[8] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of applied cryptology*, CRC Press, New York, 1997.

[9] A. Odlyzko. Asymptotic enumeration methods. In R. L. Graham, M. Grötschel, and L. Lovász (eds.), *Handbook of Combinatorics, Vol. II*, Elsevier, Amsterdam (1995) 1063-1229.

[10] G. H. Watson, Theorems stated by Ramanujan (V): Approximations connected with e^x, *Proc. London Math. Soc.* **29**(1929) 293-308.