RANDOM CODES AND MATRICES

A DISSERTATION SUBMITTED TO
THE DEPARTMENT OF MATHEMATICS
AND THE INSTITUTE OF ENGINEERING AND SCIENCE
OF BILKENT UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

By
İbrahim Özen
May, 2009

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of doctor of philosophy.

Prof. Dr. Alexander A. Klyachko(Supervisor)

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of doctor of philosophy.

Prof. Dr. Sinan Sertöz

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of doctor of philosophy.

Prof. Dr. Erdal Arıkan

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of doctor of philosophy.

Prof. Dr. Ferruh Özbudak

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of doctor of philosophy.

Ass. Prof. Dr. Alex Degtyarev

Approved for the Institute of Engineering and Science:

Prof. Dr. Mehmet B. Baray
Director of the Institute

Merhaba, hoş geldin ey ruh-ı revanım merhaba

ABSTRACT

RANDOM CODES AND MATRICES

İbrahim Özen
Ph.D. in Mathematics
Supervisor: Prof. Dr. Alexander A. Klyachko
May, 2009

Results of our study are two fold. From the code theoretical point of view our study yields the expectations and the covariances of the coefficients of the weight enumerator of a random code. Particularly interesting is that, the coefficients of the weight enumerator of a code with random parity check matrix are uncorrelated. We give conjectures for the triple correlations of the coefficients of weight enumerator of random codes. From the random matrix theory point of view we obtain results in the rank distribution of column submatrices. We give the expectations and the covariances between the ranks ($q^{-\mathrm{rank}}$) of such submatrices over $\mathbb{F}_q$. We conjecture the counterparts of these results for arbitrary submatrices. The case of higher correlations gets drastically complicated even in the case of three submatrices. We give a formula for the correlation of ranks of three submatrices and a conjecture for its closed form.

Keywords: random codes, random matrices, rank, weight enumerator of a random code.

ÖZET

RASTSAL KODLAR VE MATRİSLER

İbrahim Özen
Matematik, Doktora
Tez Yöneticisi: Prof. Dr. Alexander A. Klyachko
Mayıs, 2009

Çalışmamızın sonuçları iki yönlüdür. Kodlama teorisi açısından, rastsal kodun ağırlık polinomunun katsayılarının matematiksel beklentileri ve kovaryansları elde edilmiştir. Elde edilen önemli bir sonuç, rastsal parite kontrol ile oluşturulan kod polinomunun katsayılarının korelasyonunun sıfır oluşudur. Rastsal kod polinomunun katsayıları arasında üçlü korelasyonlar için varsayım öne sürülmüştür. Rastsal matrisler açısından bakıldığında, rastsal matrisin altmatrislerinin rank beklentisi ve aralarındaki kovaryanslar elde edilmiştir. Bu sonuçların sütun matrislerine sınırlandırılmamış sonuçları için varsayım ileri sürülmüştür. Daha yüksek derecelere bakıldığında, korelasyonların üçüncü derecede çok daha karmaşıklaştığı gözlenmiştir. Üçüncü derece korelasyon için bir toplam formülü elde edilmiş, kapalı formu için sav ileri sürülmüştür.

Anahtar sözcükler: rastsal kodlar, rastsal matrisler, rank, rastsal kodun ağırlık dağılımı.

Acknowledgement

I would like to express my deepest gratitude to my supervisor Professor Alexander A. Klyachko. His guidance through the work, insightful suggestions and his patience mostly made this study come along.

The department of mathematics in Bilkent university enabled me to keep my chance in spite of many delays. I am grateful to Prof. Mefharet Kocatepe and Prof. Metin Gürses for the flexibility they showed. I am also obliged to thank to those in the Institute of Science and Engineering that have share in this.

I have received support and encouragement from many friends. I want to thank especially to Murat Altunbulak and Ersin Üreyen for their hospitality during my stays at Ankara. I am also grateful to Süleyman Tek and Hatice Şahinoğlu for sending me a text which was very critical at the moment.

Finally I thank to my family for their support and encouragement.

Contents

Chapter 1

Introduction

1.1 A Brief Overview of Random Matrices

Study of random matrices has been an efficient way of understanding the average behavior of both mathematical and physical objects.

1.1.1 Complex Random Matrices

Over zero characteristic, the theory of random matrices is mainly developed on eigenvalue statistics. Three basic random matrix ensembles are the Gaussian Orthogonal, Unitary and Symplectic ensembles.

They consist of the sets of $n \times n$

- real symmetric matrices invariant under transformations $H \to W_1^T H W_1$,
- Hermitian matrices invariant under transformations $H \to W_2^* H W_2$,
- self dual quaternion real matrices invariant under $H \to W_3^R H W_3$

respectively, where W_1 is an orthogonal, W_2 is a unitary and W_3 is a symplectic matrix. W^* (resp. W^R) is complex (resp. quaternion) conjugation followed by transposition. Recall that a real quaternion q is of the form $q = r_0 + r_1e_1 + r_2e_2 + r_3e_3$, with conjugate $\bar{q} = r_0 - r_1e_1 - r_2e_2 - r_3e_3$, where r_i's are real. They form an algebra over real numbers by the multiplication rules $e_1^2 = e_2^2 = e_3^2 = -1$, $e_1e_2 = e_3$, $e_2e_3 = e_1$, $e_3e_1 = e_2$. A matrix $Q = [q_{ij}]$ with real quaternion elements has the dual matrix $Q^R = [\bar{q}_{ji}]$ and Q is self dual when we have $Q = Q^R$. Symplectic group is the set of real quaternion matrices W such that $W^{-1} = W^R$.

In these ensembles, probabilities to have eigenvalues within unit intervals centered at $(\lambda_1, \lambda_2, \dots, \lambda_n)$ are known. Correlations of eigenvalues of such matrices are extensively studied ([20, 6]).

While the initial aim was to understand the energy levels of complex nuclear systems, later developments indicated that eigenvalues of random matrices have similar statistics as the nontrivial zeros of Riemann zeta function ([22, 25]). So, the study of correlations of characteristic polynomials became important to understand the value distribution of this function([15, 5]).

Assuming Riemann Hypothesis Montgomery showed that the two point correlation function of Riemann zeta function in the zero mean scaling is similar to two point correlation function for eigenvalues of Circular unitary ensemble in the limit of large matrix size.

Assuming Riemann hypothesis let $1/2+i\gamma_j$ be the nontrivial zeros in the upper half plane and write $\tilde{\gamma}_j = \gamma_j \log(\gamma_j/2\pi)$. Montgomery conjectured that distances $\tilde{\gamma}_j - \tilde{\gamma}_i$ have the same distribution as arguments of eigenvalues of a large unitary matrix. He proved a weak version of this in ([22]).

Katz and Sarnak ([14]) proved Montgomery's conjecture for L functions of algebraic curves over finite fields. The three classical ensembles above appear as the monodromy groups of families of algebraic curves.

Monodromy groups also control the number of rational points. Curves with many rational points are essential for constructing algebaraic geometric codes. It turns out that the families of curves with irreducible monodromy group have big number of rational points ([13]).

1.1.2 Random matrices over finite fields

Over positive characteristic, random matrix theory switches from the eigenvalue statistics to the conjugacy class properties of square matrices $\mathrm{Mat}(n, q)$ over $\mathbb{F}_q$, $\mathrm{GL}(n, q)$ and the classical groups $\mathrm{O}(n, q), \mathrm{U}(n, q)$ and $\mathrm{Sp}(2m, q)$. The problems studied include the proportion of matrices that have equal minimal and characteristic polynomials (*cyclic matrices*), that have characteristic polynomial free from multiple roots (*separable matrices*), the same property for minimal polynomial (*semisimple matrices*).(See ([7]) for example.)

Stong ([26]) showed that the expectation and the variance of the number of different irreducible factors in the characteristic polynomial of a random matrix in $\mathrm{GL}(n, q)$ are asymptotically

$$\log(n) + O(1).$$

Goh and Schmutz ([11]) proved that the distribution is asymptotically normal.

Borodin ([2]) studied the distribution of sizes $s_1 \geq s_2 \geq \ldots$ of the Jordan blocks of upper triangular matrices over $\mathbb{F}_q$. He showed that asymptotically as $n \to \infty$ any finite initial segment of the random vector $(s_1, s_2, \ldots)$ is normally distributed with mean $(p_1, p_2, \ldots)$ and covariance matrix with entries $c_{ij} = \delta_{ij} p_i - p_i p_j$ where $p_i = 1/q^{i-1} - 1/q^i$.

1.2 Random codes

Random codes are closely related with the random matrices over finite fields. Specifically, parameters of random codes depend on the distribution and the correlations between the ranks of submatrices.

A *linear code* C is a linear subspace of $\mathbb{F}_q^n$ where $\mathbb{F}_q$ is a finite field of q elements. The number n is called the *length* and the dimension k of C is called the *number* *of information symbols* of the code. The number of nonzero coordinates of a code vector e is said to be the *weight* $|e|$ of e. Minimum of the weights of nonzero code vectors in C is the *minimum distance* of the code and it is usually denoted by d. We call a code with parameters n, k, d over $\mathbb{F}_q$ an $[n, k, d]_q$ code.

If we consider $\mathbb{F}_q^n$ as a linear space with the standard scalar product $\langle u, v\rangle = \sum_i u_i v_i$, then the orthogonal complement $C^\perp$ of C is called the *dual code* to C.

Let C be an $[n, k]_q$ code and fix a basis $\{b_i\}$ of C. Let G be a $k \times n$ matrix whose rows consist of the basis vectors b_i of C. Then any element $e \in C$ is a linear combination of row-vectors of G. We call G a *generator matrix* of C. G is also an important matrix for the dual code $C^\perp$. Since any vector $e' \in C^\perp$ is orthogonal to the basis vectors of C, the product $G \times (e')^T$ is the zero vector and this is the criterion for lying in $C^\perp$. G is called a *parity check matrix* of the code $C^\perp$.

Let $C \subset \mathbb{F}_q^n$ be a code and let A_i be the number of code vectors with exactly i nonzero coordinates

$$A_i = |\{e \in C : |e| = i\}|.$$

Then we define the *weight enumerator* $W_C(t)$ of the code C as the polynomial

$$W_C(t) = \sum_i A_i t^{n-i}. \tag{1.1}$$

We find the following form of the weight enumerator vital for our purposes (see [27])

$$W_C(1+t) = \sum_{I \subset \{1,2,\dots,n\}} q^{k-r_I} t^{|I|}, \tag{1.2}$$

where r_I is rank of the column submatrix of G, spanned by the columns indexed by I.

All the parameters of codes can be extracted from the weight enumerator $W_C(t)$ which is given by the *rank function* q^{-r_I}, $I \subset \{1, 2, \dots, n\}$, of the generator matrix. A code can be considered as a configuration of points (columns of the generator matrix) in the projective space. Then existence of a code with given weights turns out to be equivalent to existence of a configuration with given rank function as we see in Equations (1.1) and (1.2). But this is a classical wild problem and it can be arbitrarily complicated ([21]). So we pass to the statistical approach rather than trying to determine the explicit structure.

Existence of a code with parameters n, k, d over $\mathbb{F}_q$ amounts to simultaneous vanishing of the coefficients

$$A_1 = A_2 = \ldots = A_{d-1} = 0.$$

This involves the joint distribution of the coefficients of the weight enumerator. Given the relation between the rank functions and the code weights, it is a natural course of action to study the statistics of the rank functions. The main results of this work are the explicit formulas for the expectation and the covariances between the rank functions of random matrices. They provide the answers to the counterpart problems for the code weights. In particular we find out that the coefficients of weight enumerator of a code constructed by random parity check matrix are uncorrelated.

For a matrix G, *we take randomness in the sense that the entries are independent and they are uniformly distributed along the field* $\mathbb{F}_q$. One can easily deduce from Equation (3.5) that probability of a square $n \times n$ matrix over $\mathbb{F}_q$ to be singular is positive even when $n \to \infty$, while for a $k \times n$ matrix with $R = k/n < 1$ the matrix is almost sure to have maximal rank k. Hence we will tacitly assume maximality of the rank when fixing a random $k \times n$ matrix with $k/n < 1$. One must keep in mind that there are two ways that a random matrix gives rise to a code. Once we are given a $k \times n$ matrix G there is the $[n, k]_q$ code which assumes G as its generator matrix; and the second, the code which assumes G as its parity check matrix. Both codes will be referred as *random code*. We denote the random code in the first sense by C and the code in the second sense by $C^{\perp}$. Their weight enumerators will be referred as $W_C(t) = \sum_i A_i t^{n-i}$ and $W_{C^{\perp}}(t) = \sum_i A_i^{\perp} t^{n-i}$ respectively.

Throughout the text G is a random $k \times n$ matrix over the finite field $\mathbb{F}_q$. We denote its rank, considered as a random quantity, by $r_{k\times n}$. When we deal with column sub-matrices we refer to the matrix as G_I and its rank by r_I, where $I \subset \{1, 2, , \ldots, n\}$ is the index set of columns in G_I.

1.3 Statement of Results

Results in this thesis have been published online with the DOI reference 10.1016/j.ffa.2009.03.002 ([18]).

Our main results are as follows. The sth moment of the rank function $q^{-r_{k\times n}}$ of a $k \times n$ random matrix is given by

$$\begin{aligned}
\mu_s(q^{-r_{k\times n}}) &= q^{-kn} \sum_{0\le r\le k} q^{r(n-s)} \begin{bmatrix} k \\ r \end{bmatrix} \prod_{0\le i<r} (1-q^{-n+i}), \\
\mu_s(q^{-r_{k\times n}}) &= \prod_{0\le i<k} (q^{-n}+q^{-s}-q^{-n-s+i}),
\end{aligned}$$

where the product in the second formula is noncommutative in $x = q^{-n}$ and $y = q^{-s}$ with the commutation rule $yx = qxy$. The moment $\mu_s(q^{-r_{k\times n}})$ is symmetric in n and k. Furthermore if s is a nonnegative integer then it is also symmetric in s. For example the expectation of $q^{-r_{k\times n}}$ is given by

$$\mathbb{E}(q^{-r_{k\times n}}) = q^{-n} + q^{-k} - q^{-n-k}.$$

The covariance between the rank functions q^{-r_I} and q^{-r_J} of two column submatrices is given by

$$\mathrm{cov}(q^{-r_I}, q^{-r_J}) = \frac{(q-1)(q^k-1)(q^{|I\cap J|}-1)}{q^{2k+|I|+|J|}}.$$

One may ask about the covariance between the rank functions $q^{-r_{KI}}$ where r_{KI} denotes rank of the submatrix spanned by the row set K and the column set I. We conjecture that

$$\mathrm{cov}(q^{-r_{LI}}, q^{-r_{MJ}}) = \frac{(q-1)(q^{|I\cap J|}-1)(q^{|L\cap M|}-1)}{q^{|I|+|J|+|L|+|M|}}. \tag{1.3}$$

Next we show that the covariances between the coefficients of weight enumerator of the random code $C^\perp$ are given by

$$\begin{aligned}
\mathrm{cov}(W_{C^\perp}(x), W_{C^\perp}(y)) &= \sum_{i,j} \mathrm{cov}(A_i^\perp, A_j^\perp) x^{n-i} y^{n-j} \\
&= \frac{(q-1)(q^{n-k}-1)}{q^{2(n-k)}}((xy+q-1)^n - (xy)^n).
\end{aligned}$$

An important corollary of this theorem is that the coefficients of weight enumerator of the code $C^{\perp}$ with random parity check matrix are uncorrelated. This result is not valid for the code C given by random generator matrix.

We also studied the triple correlations between the ranks of three submatrices. Using the classification of triplets of subspaces we managed to deduce an extremely complicated formula. To our surprise computer experiments show beyond reasonable doubt that the formula is equivalent to a simple closed one. It is even simpler when we switch from the correlations to the cumulants. We conjecture that the closed formula of the joint cumulant of ranks of three submatrices is given by

$$\sigma(q^{-r_I}, q^{-r_J}, q^{-r_K}) = \frac{(q-1)^2(q^k-1)}{q^{3k+I+J+K}}\big(q^{IJ+JK+KI-IJK} - (q^{IJ}+q^{JK}+q^{KI}) \\ + 2 + (q^k-q)(q^{IJK}-1)\big),$$

where on the right hand side of the equation the multiplicative notation for sets like IJ means the cardinality of their intersection $|I \cap J|$. We remind that the joint cumulant of a triplet of random variables is

$$\begin{aligned} \sigma(X,Y,Z) &= \mathbb{E}(XYZ) - \mathbb{E}(X)\mathrm{cov}(Y,Z) - \mathbb{E}(Y)\mathrm{cov}(Z,X) \\ &\quad -\mathbb{E}(Z)\mathrm{cov}(X,Y) - \mathbb{E}(X)\mathbb{E}(Y)\mathbb{E}(Z). \end{aligned}$$

This conjecture is equivalent to the following formula for joint cumulants of the coefficients of $W_{C^{\perp}}(t)$,

$$\begin{aligned} &\sigma(W_{C^\perp}(x), W_{C^\perp}(y), W_{C^\perp}(z)) = \sum_{i,j,l} \sigma(A_i^\perp, A_j^\perp, A_l^\perp) x^{n-i} y^{n-j} z^{n-l} \\ &= q^{-3(n-k)}(q-1)^2(q^{n-k}-1)\Big\{\big(xyz+(q-1)(x+y+z+q-2)\big)^n - (xyz)^n \\ &-((xy+q-1)^n-(xy)^n)z^n - ((yz+q-1)^n-(yz)^n)x^n \\ &-((zx+q-1)^n-(zx)^n)y^n + (q^{n-k}-q)\Big[(xyz+q-1)^n-(xyz)^n\Big]\Big\}. \end{aligned}$$

For the random code C the corresponding equation is

$$
\begin{aligned}
&\sigma(W_C(x), W_C(y), W_C(z)) = (q-1)^2(q^k-1)\Big\{q^{-n}(xyz+q-1)^n \\
- \quad & q^{-2n}\big((xy+q-1)^n(z+q-1)^n + (yz+q-1)^n(x+q-1)^n \\
+ \quad & (zx+q-1)^n(y+q-1)^n\big) + 2q^{-3n}(x+q-1)^n(y+q-1)^n(z+q-1)^n \\
+ \quad & (q^k-q)\big[q^{-2n}(xyz+(q-1)(x+y+z+q-2))^n \\
- \quad & q^{-3n}(x+q-1)^n(y+q-1)^n(z+q-1)^n\big]\Big\}.
\end{aligned}
$$

There exists a classification of quadruples of subspaces due to Gelfand and Ponomarev ([10]). For further study of this subject, one may wonder whether it may lead to a closed formula for the quadruple correlations.

The above results on correlations imply, for example, that the roots of weight enumerator $W_C(1+z)$ of a selfdual code $C = C^\perp$ are almost sure to be on the circle $z = |\sqrt{q}|$, provided $q > 9$. Here by almost sure we mean that the probability to have a root off the circle tends to 0 as $n \to \infty$. Similar but less sharp results hold for all $[n,k]_q$ codes where $q > q_0(R), R = k/n$ ([17]).

The thesis is organized as follows. Chapter 2 is a survey to summarize the well known results over finite fields. Results mentioned in this chapter are not used nor needed to proceed to the rest of the thesis.

In Chapter 3 we evaluate the moments and the covariances between the rank functions. Moments are given by Theorem (3.3). We derive the covariance between the ranks of two submatrices in Theorem (3.6). Using this, we show that the coefficients of the weight enumerator of the random code $C^\perp$ are uncorrelated by Theorem (3.10) and Corollary (3.11).

In Chapter 4 we study the triple correlations between the coefficients of the weight enumerators. To proceed in this direction we need the triple correlations between the ranks of three submatrices. A triplet of submatrices gives a triplet of subspaces. We review the classification of triplets of subspaces and obtain the number of triplets with given invariants. This enables us to obtain a formula for the triple correlations between the ranks of three submatrices which is given by Theorem (4.7). The main Conjecture (4.8) provides the closed form of the joint cumulant of three ranks. Equivalent to this conjecture we give Corollaries (4.10) and (4.11) on the joint cumulant of coefficients of $W_C(t)$ and $W_{C^\perp}(t)$ respectively.

Chapter 2

Known Results Over Finite Fields

Random matrix theory over finite fields focuses on conjugacy classes of random elements of the classical groups. Some of the properties that are invariant for the same class are separability, semisimplicity, being cyclic, number of Jordan blocks and so on. Similarity classes of matrices in $\mathrm{Mat}(n,q)$ and $\mathrm{GL}(n,q)$ are well known, conjugacy classes in $\mathrm{O}(n,q), \mathrm{U}(n,q)$ and $\mathrm{Sp}(2n,q)$ are studied by Wall ([30]).

We remind the reader that our purpose is to provide a survey. Results of this chapter won't be used in the rest of the thesis.

2.1 Results for $\mathrm{Mat}(n,q)$ and $\mathrm{GL}(n,q)$

2.1.1 Similarity Classes

Similarity classes of matrices in $\mathrm{Mat}(n,q)$ are given by the rational canonical form. For a monic polynomial $\phi(z) = z^m + a_{m-1}z^{m-1} + \ldots + a_1 z + a_0$ define the companion matrix $C(\phi)$ to be

$$C(\phi) = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \dots & 1 \\ -a_0 & -a_1 & -a_3 & \dots & -a_{m-1} \end{bmatrix}. \tag{2.1}$$

A matrix $A \in \mathrm{Mat}(n, q)$ is said to be in rational canonical form if it is the direct sum of companion matrices of nonscalar monic polynomials ϕ_i

$$A = \begin{bmatrix} C(\phi_1) & 0 & 0 & \dots & 0 \\ 0 & C(\phi_2) & 0 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \dots & C(\phi_t) \end{bmatrix} \tag{2.2}$$

such that $\phi_{i+1} \mid \phi_i$. *Any matrix is similar to a unique matrix in rational form.*

This form follows from the fact that the space on which A acts decomposes as direct sum of cyclic subspaces. So A is cyclic if and only if its rational form is companion matrix $C(\phi)$ of a polynomial ϕ.

One can parameterize a similarity class by a collection of monic irreducible polynomials $\{p_i\}$ with corresponding partitions of natural numbers $\lambda_i = \lambda_{i,1} \geq \lambda_{i,2} \geq \dots$ satisfying

$$\sum_i |\lambda_i| \deg(p_i) = n. \tag{2.3}$$

Rational form of such a class is given by the matrix

$$\begin{bmatrix} C(\prod_i p_i^{\lambda_{i,1}}) & 0 & 0 & \dots & 0 \\ 0 & C(\prod_i p_i^{\lambda_{i,2}}) & 0 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \dots & C(\prod_i p_i^{\lambda_{i,t}}) \end{bmatrix}. \tag{2.4}$$

Characteristic polynomial of any matrix in the class is given by $\prod_i p_i^{|\lambda_i|}$.

For the conjugacy classes of $\mathrm{GL}(n, q)$ the only restriction is that characteristic polynomial can not have z as a factor, so $|\lambda_z| = 0$.

Let $A \in \mathrm{Mat}(n,q)$ with characteristic polynomial $\phi(z)$. If ϕ completely factors in $\mathbb{F}_q$ then similarity the class of A is given by the Jordan form. To describe it define J_c to be the elementary Jordan matrix with characteristic value c

$$J_c = \begin{bmatrix} c & 0 & \dots & 0 & 0 \\ 1 & c & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & & c & 0 \\ 0 & 0 & \dots & 1 & c \end{bmatrix}. \tag{2.5}$$

Now let p be an irreducible polynomial over $\mathbb{F}_q$ with roots in the closure of the field $\beta, \beta^q, \beta^{q^2}, \dots, \beta^{\deg p - 1}$. For any natural number λ we define the companion matrix $J_{p,\lambda}$ as

$$J_{p,\lambda} = \begin{bmatrix} J_\beta & 0 & \dots & 0 & 0 \\ & J_{\beta^q} & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & J_{\beta^{\deg p-1}} \end{bmatrix}, \tag{2.6}$$

where each J is a $\lambda \times \lambda$ Jordan matrix with the corresponding characteristic value.

Suppose the similarity class of A has data p_i and λ_i. Then A is similar to a matrix

$$\mathcal{A} = \begin{bmatrix} J_{p_1,\lambda_{1,1}} & 0 & \dots & 0 & 0 \\ 0 & J_{p_1,\lambda_{1,2}} & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & & J_{p_i,\lambda_{i,1}} & \dots \\ & & & & \ddots \end{bmatrix}. \tag{2.7}$$

2.1.2 Cycle Indices

Cycle indices for $Mat(n,q)$ and $\mathrm{GL}(n,q)$ are first introduced by Kung and Stong. These are polynomials that the cycle structures are encoded in their coefficients. Let x_{p,λ_p} be variables corresponding to pairs of monic irreducible polynomials p

and corresponding partitions of natural numbers $|\lambda_p|$. Then one defines the cycle index generating function of $\mathrm{GL}(n,q)$ as the power series

$$1+\sum_n \frac{u^n}{|\mathrm{GL}(n,q)|}\sum_{\alpha\in\mathrm{GL}(n,q)}\prod_{p\neq z} x_{p,\lambda_p(\alpha)}$$

where the product is over all monic irreducible polynomials over $\mathbb{F}_q$. Cycle index for Mat differs only in including the polynomial z in the product.

Stong gives a factorization for the cycle index, using a quantity $c_{\mathrm{GL,p,q}}(\lambda)$. For a partition λ with m_i parts of size i, define

$$d_i = m_1 1 + m_2 2 + \ldots + m_{i-1}(i-1) + (m_i + m_{i+1} + \ldots)i.$$

For empty partition λ set $c_{\mathrm{GL,p,q}}(\lambda) = 0$, otherwise

$$c_{\mathrm{GL,p,q}}(\lambda) = \prod_i \prod_{l=1}^{m_i} (q^{\deg(p)d_i} - q^{\deg(p)(d_i-l)}). \tag{2.8}$$

Then the cycle index generating functions of $\mathrm{GL}(n,q)$ and $\mathrm{Mat}(n,q)$ have the following factorizations respectively

$$1+\sum_n \frac{u^n}{|\mathrm{GL}(n,q)|}\sum_{\alpha\in\mathrm{GL}(n,q)}\prod_{p\neq z} x_{p,\lambda_p(\alpha)} = \prod_{p\neq z}\sum_\lambda x_{p,\lambda}\frac{u^{|\lambda|\deg(p)}}{c_{\mathrm{GL,p,q}}(\lambda)}, \tag{2.9}$$

$$1+\sum_n \frac{u^n}{|\mathrm{GL}(n,q)|}\sum_{\alpha\in\mathrm{Mat}(n,q)}\prod_{p} x_{p,\lambda_p(\alpha)} = \prod_{p}\sum_\lambda x_{p,\lambda}\frac{u^{|\lambda|\deg(p)}}{c_{\mathrm{GL,p,q}}(\lambda)}. \tag{2.10}$$

We need a few lemmas that will be useful in deriving results from the cycle indices. In the following we use the notation $[u^n]f(u)$ to denote the coefficient of u^n in the Taylor expansion of $f(u)$ around 0.

Lemma 2.1 *If $f(1) < \infty$ and the Taylor series of f around 0 converges at $u = 1$, then*

$$\lim_{n\to\infty}[u^n]\frac{f(u)}{1-u} = f(1). \tag{2.11}$$

Proof. Let $f(u) = \sum_{n=0}^{\infty} a_n u^n$. Then

$$\frac{f(u)}{1-u} = \left(\sum_{i=0}^{\infty} u^i\right)\left(\sum_{n=0}^{\infty} a_n u^n\right) = \sum_{n=0}^{\infty}(\sum_{i=0}^{n} a_{n-i})u^n.$$

The lemma is clear from the last equality. □

Lemma 2.2

$$\prod_p \left(1 - \frac{u^{\deg(p)}}{q^{\deg(p)t}}\right) = 1 - \frac{u}{q^{t-1}}, \tag{2.12}$$

where the product is over all monic irreducible polynomials over $\mathbb{F}_q$.

Proof. Assume that $t = 1$ and let $v = \frac{u}{q}$. Then using

$$\frac{1}{1 - v^{\deg(p)}} = \sum_{i=0}^{\infty} (v^{\deg(p)})^i$$

we get

$$\prod_p \frac{1}{1 - v^{\deg(p)}} = \sum_{i_p} v^{\deg(\prod_p p^{i_p})}.$$

So coefficient of v^d is the number of monic polynomials of degree d, which is equal to q^d. Hence when we pass to u notation we get

$$\frac{1}{1 - \frac{u^{\deg(p)}}{q^{\deg(p)}}} = \sum_{d=0}^{\infty} u^d = \frac{1}{1-u}.$$

So for $t = 1$ we get the result and the general case follows by changing u to $\frac{u}{q^{t-1}}$. □

Lemma 2.3

$$\prod_{p \neq z} \prod_{r=1}^{\infty} \left(1 - \frac{u^{\deg(p)}}{q^{\deg(p)r}}\right) = 1 - u, \tag{2.13}$$

where p runs through monic irreducible polynomials not equal to z.

Proof. By the previous lemma we get

$$\prod_{p \neq z} \prod_{r=1}^{\infty} \left(1 - \frac{u^{\deg(p)}}{q^{\deg(p)r}}\right) = \prod_{r=1}^{\infty} \left(\frac{1 - \frac{u}{q^{r-1}}}{1 - \frac{u}{q^r}}\right)$$

and the cancelations bring the result. □

Gordon's generalization of Rogers-Ramanujan identities [cite] gives the following corollary that will be used later

$$\prod_{r=1}^{\infty} \left(1 - \frac{1}{q^{r\deg(p)}}\right) \sum_{\lambda:\lambda_1<k} \frac{1}{c_{\mathrm{GL},p,q}(\lambda)} = \prod_{\substack{r=1 \\ r=0,\pm k (mod 2k+1)}}^{\infty} \left(1 - \frac{1}{q^{r\deg(p)}}\right). \tag{2.14}$$

Now we are ready to show how the cycle index machinery is used. For large matrices probability of being semi-simple, cyclic and separable matrices will be obtained.

Theorem 2.4 *As* $n \to \infty$*, probability that a random element of* $\mathrm{Mat}(n,q)$ *is semi-simple tends to*

$$\prod_{\substack{r=1 \\ r=0,\pm 2(mod5)}}^{\infty} \left(1 - \frac{1}{q^{r-1}}\right). \tag{2.15}$$

Proof. Semi-simplicity of a matrix in $\mathrm{Mat}(n,q)$ is equivalent that Jordan form has no block of size greater than 1. So that partitions of the similarity class satisfy $\lambda_1 < 2$. Cycle index for Mat and its factorization is

$$1 + \sum_n \frac{u^n}{|\mathrm{GL}(n,q)|} \sum_{\alpha \in \mathrm{GL}(n,q)} \prod_p x_{p,\lambda_p(\alpha)} = \prod_p \sum_\lambda x_{p,\lambda} \frac{u^{|\lambda| \deg(p)}}{c_{\mathrm{GL,p,q}}(\lambda)},$$

where the products are over all monic irreducible polynomials over $\mathbb{F}_q$. If we set $x_{p,\lambda_p} = 1$ for those pairs with the partition satisfying $\lambda_1 < 2$ and $x_{p,\lambda_p} = 0$ otherwise, we get

$$\sum_n u^n \frac{|(\text{semisimple matrices in } \mathrm{Mat}(n,q))|}{|\mathrm{GL}(n,q)|} =$$

on the left hand side. Hence limiting probability becomes

$$\begin{aligned}
&\lim\nolimits_{n\to\infty} \quad \frac{|\mathrm{GL}(n,q)|}{q^{n^2}} [u^n] \prod_p \sum_{\lambda:\lambda_1<2} \frac{u^{|\lambda|\deg(p)}}{c_{\mathrm{GL},p,q}(\lambda)} \\
&\overset{=}{\scriptstyle Eq.}2.13 \quad \lim_{n\to\infty} \frac{|\mathrm{GL}(n,q)|}{q^{n^2}} [u^n] \frac{\prod_p \left(\prod_{r=1}^\infty \left(1 - \frac{u^{\deg(p)}}{q^{r\deg(p)}}\right) \sum_{\lambda:\lambda_1<2} \frac{u^{|\lambda|\deg(p)}}{c_{\mathrm{GL},p,q}(\lambda)}\right)}{(1-u)\prod_{r=1}^\infty \left(1 - \frac{u}{q^r}\right)} \\
&\overset{=}{\scriptstyle Eq.}2.11 \quad \prod_p \left(\prod_{r=1}^\infty \left(1 - \frac{1}{q^{r\deg(p)}}\right) \sum_{\lambda:\lambda_1<2} \frac{1}{c_{\mathrm{GL},p,q}(\lambda)}\right) \\
&\overset{=}{\scriptstyle Eq.}2.14 \quad \prod_{\substack{r=1 \\ r=0,\pm 2(mod5)}}^{\infty} \left(1 - \frac{1}{q^{r-1}}\right).
\end{aligned}$$

□

Probability to get semi-simple element in $\mathrm{GL}(n,q)$ is given by the next theorem.

Theorem 2.5 *As $n \to \infty$, probability that a random element of $\mathrm{GL}(n,q)$ is semi-simple tends to*

$$\prod_{\substack{r=1 \\ r=0,\pm 2 (mod 5)}}^{\infty} \frac{\left(1-\frac{1}{q^{r-1}}\right)}{\left(1-\frac{1}{q^r}\right)}. \tag{2.16}$$

Proof. In the cycle index of $\mathrm{GL}(n,q)$ we set $x_{p,\lambda_p} = 1$ if λ satisfies $\lambda_1 < 2$ and $x_{p,\lambda_p} = 0$ otherwise. This gives the desired probability on the right hand side and it is equal to

$$\begin{aligned}
& \lim_{n\to\infty} [u^n] \prod_{p\neq z} \sum_{\lambda:\lambda_1<2} \frac{u^{|\lambda|\deg(p)}}{c_{\mathrm{GL},p,q}(\lambda)} \\
\overset{=}{_{Eq.}2.13} \quad & \lim_{n\to\infty} [u^n] \frac{1}{1-u} \prod_{p\neq z} \left(\prod_{r=1}^{\infty} \left(1 - \frac{u^{\deg(p)}}{q^{r\deg(p)}}\right) \sum_{\lambda:\lambda_1<2} \frac{u^{|\lambda|\deg(p)}}{c_{\mathrm{GL},p,q}(\lambda)} \right) \\
\overset{=}{_{Eq.}2.11} \quad & \prod_{p\neq z} \left(\prod_{r=1}^{\infty} \left(1 - \frac{1}{q^{r\deg(p)}}\right) \sum_{\lambda:\lambda_1<2} \frac{1}{c_{\mathrm{GL},p,q}(\lambda)} \right) \\
\overset{=}{_{Eq.}2.14} \quad & \prod_{p\neq z} \prod_{\substack{r=1 \\ r=0,\pm 2\ (mod 5)}}^{\infty} \left(1-\frac{1}{q^r}\right) \\
= \quad & \prod_{\substack{r=1 \\ r=0,\pm 2\ (mod 5)}}^{\infty} \frac{1}{\left(1-\frac{1}{q^r}\right)} \prod_{p} \prod_{\substack{r=1 \\ r=0,\pm 2\ (mod 5)}}^{\infty} \left(1-\frac{1}{q^r}\right) \\
= \quad & \prod_{\substack{r=1 \\ r=0,\pm 2\ (mod 5)}}^{\infty} \frac{\left(1-\frac{1}{q^{r-1}}\right)}{\left(1-\frac{1}{q^r}\right)}.
\end{aligned}$$

$\square$

Next, we give probabilities that the random element is cyclic.

Theorem 2.6 *As $n \to \infty$, probability that a random element in $\mathrm{Mat}(n,q)$ is cyclic tends to*

$$\left(1-\frac{1}{q^5}\right)\prod_{r=3}^{\infty}\left(1-\frac{1}{q^r}\right).$$

Proof. A matrix is cyclic if and only if all the partitions in its rational canonical form have at most one part. Once again manipulating cycle index accordingly, we obtain the probability as

$$
\begin{aligned}
&\lim_{n\to\infty} \frac{|\mathrm{GL}(n,q)|}{q^{n^2}}[u^n]\prod_p \left(1+\sum_{j=1}^{\infty}\frac{u^{j\deg(p)}}{q^{j\deg(p)-\deg(p)}(q^{\deg(p)}-1)}\right) \\
\overset{=}{_{Eq.}2.12}\ & \prod_{r=1}^{\infty}\left(1-\frac{1}{q^r}\right)\lim_{n\to\infty}[u^n]\frac{\prod_p\left(1-\frac{u^{\deg(p)}}{q^{\deg(p)}}\right)\left(1+\sum_{j=1}^{\infty}\frac{u^{j\deg(p)}}{q^{j\deg(p)-\deg(p)}(q^{\deg(p)}-1)}\right)}{1-u} \\
\overset{=}{_{Eq.}2.11}\ & \prod_{r=1}^{\infty}\left(1-\frac{1}{q^r}\right)\prod_p\left(1+\frac{1}{q^{\deg(p)}(q^{\deg(p)}-1)}\right) \\
\overset{=}{_{Eq.}2.12}\ & \prod_{r=3}^{\infty}\left(1-\frac{1}{q^r}\right)\prod_p\left(1-\frac{1}{q^{6\deg(p)}}\right) \\
=\ & \left(1-\frac{1}{q^5}\right)\prod_{r=3}^{\infty}\left(1-\frac{1}{q^r}\right).
\end{aligned}
$$

□

Theorem 2.7 *As $n\to\infty$, probability that a random element of* $\mathrm{GL}(n,q)$ *is cyclic tends to*

$$\frac{1-\frac{1}{q^5}}{1+\frac{1}{q^3}}.$$

Proof. Proof is similar to the previous case. □

Now we give the probabilities that a random element is separable.

Theorem 2.8 *As $n\to\infty$, probability that a random element of* $\mathrm{Mat}(n,q)$ *is separable tends to*

$$\prod_{r=1}^{\infty}\left(1-\frac{1}{q^r}\right)$$

Proof. A matrix is separable if and only if the partitions in its Jordan form have size 1. So we get the probability from the cycle index as

$$
\begin{aligned}
&\lim_{n\to\infty} \frac{|\mathrm{GL}(n,q)|}{q^{n^2}}[u^n]\prod_p \left(1+\frac{u^{\deg(p)}}{q^{\deg(p)}-1}\right)\\
\underset{Eq.2.12}{=}\; &\lim_{n\to\infty} \frac{|\mathrm{GL}(n,q)|}{q^{n^2}}[u^n]\frac{\prod_p \left(1+\frac{u^{\deg(p)}}{q^{\deg(p)}-1}\right)\left(1-\frac{u^{\deg(p)}}{q^{\deg(p)}}\right)}{1-u}\\
\underset{Eq.2.11}{=}\; &\prod_{r=1}^{\infty}\left(1-\frac{1}{q^r}\right).
\end{aligned}
$$

□

Theorem 2.9 *As $n \to \infty$, probability that a random element of* $\mathrm{GL}(n,q)$ *is separable tends to*

$$1-\frac{1}{q}$$

Proof. Cycle index of $\mathrm{GL}(n,q)$ and the condition on the partitions give the probability

$$
\begin{aligned}
&\lim_{n\to\infty}[u^n]\prod_{p\neq z}\left(1+\frac{u^{\deg(p)}}{q^{\deg(p)}-1}\right)\\
\underset{Eq.2.12}{=}\; &\lim_{n\to\infty}[u^n]\frac{\left(1-\frac{u}{q}\right)\prod_{p\neq z}\left(1+\frac{u^{\deg(p)}}{q^{\deg(p)}-1}\right)}{1-u}\\
\underset{Eq.2.11}{=}\; &1-\frac{1}{q}.
\end{aligned}
$$

□

2.2 Results for Other Classical Groups

Unitary Groups: Unitary group $\mathrm{U}(n,q)$ is defined as the subgroup of $\mathrm{GL}(n,q^2)$ that preserves a nondegenerate skew linear form. A skew linear form on an n dimensional vector space V over $\mathbb{F}_{q^2}$ is a bilinear map $\langle,\rangle : V\times V \to \mathbb{F}_{q^2}$ satisfying $\langle x,y\rangle = \langle y,x\rangle^q$. One such form is given by $\langle x,y\rangle = \sum_i x_i y_i^q$. Any two nondegenerate skew linear forms are equivalent ([4, page 7]), so $\mathrm{U}(n,q)$ is unique up to isomorphism. Cardinality of the unitary group is given by $|\mathrm{U}(n,q)| = q^{\binom{n}{2}}\prod_{i=1}^n(q^i-(-1)^i)$.

Description of conjugacy classes in the classical groups requires combinatorial properties of polynomials. For a polynomial $\phi(z) \in \mathbb{F}_{q^2}[z]$ with nonzero constant term, define

$$\tilde{\phi}(z) = \frac{z^{\deg(\phi)}\phi^q(\frac{1}{z})}{(\phi(0))^q},$$

where ϕ^q raises each coefficient of ϕ to the qth power. A conjugacy class in $\mathrm{U}(n,q)$ is given by a collection of monic irreducible polynomials p and corresponding partitions λ_p of nonnegative integers. This collection gives a conjugacy class if and only if

1. $|\lambda_z| = 0$,
2. $\lambda_p = \lambda_{\tilde{p}}$,
3. $\sum_p |\lambda_p| \deg(p) = n$.

Let $\tilde{N}(q,d)$ be the number of monic, irreducible polynomials $p(z) \in \mathbb{F}_{q^2}(z)$ of degree d such that $p = \tilde{p}$. The number $\tilde{N}(q,d)$ is given by

$$\tilde{N}(q,d) = \begin{cases} 0 & \text{if } d \text{ is even,} \\ \frac{1}{d}\sum_{r|d}\mu(r)(q^{\frac{d}{r}}+1) & \text{if } d \text{ is odd.} \end{cases} \tag{2.17}$$

Furthermore, let $\tilde{M}(q,d)$ be the number of unordered pairs of monic, irreducible, degree d polynomials over $\mathbb{F}_{q^2}$, where $p \neq \tilde{p}$. This number is given by

$$\tilde{M}(q,d) = \begin{cases} \frac{1}{2}(q^2-q-2) & \text{if } d = 1, \\ \frac{1}{2d}\sum_{r|d}\mu(r)(q^{\frac{2d}{r}} - q^{\frac{d}{r}}) & \text{if } d > 1 \text{ and } d \text{ is odd,} \\ \frac{1}{2d}\sum_{r|d}\mu(r)q^{\frac{2d}{r}} & \text{if } d \text{ is even.} \end{cases} \tag{2.18}$$

Symplectic Groups: Symplectic group is defined as as the subgroup of GL that preserves a non-degenerate alternating form. An alternating form on a vector space V over $\mathbb{F}_q$ is a bilinear map $\langle , \rangle : V \times V \to \mathbb{F}_q$ such that $\langle x, y\rangle = -\langle y, x\rangle$. Alternating forms exist only on vector spaces of even dimension and they are all equivalent, so the Symplectic group $\mathrm{Sp}(2n,q)$ is unique up to isomorphism. An example to such forms is $\langle x, y\rangle = \sum_i (x_{2i-1}y_{2i} - x_{2i}y_{2i-1})$. Order of the group $\mathrm{Sp}(2n,q)$ is given by $q^{n^2}\prod_i^n (q^{2i}-1)$.

Given a polynomial $\phi(z) \in \mathbb{F}_q[z]$ with non-vanishing constant term, define the polynomial

$$(\phi)^*(z) = \frac{z^{\deg(\phi)}\phi^q(\frac{1}{z})}{\phi(0)}.$$

Conjugacy classes in the Symplectic group $\mathrm{Sp}(2n, q)$ are defined by the following data on the monic,non-constant irreducible polynomials $p \in \mathbb{F}_q[z]$ and corresponding partitions λ_p of non-negative integers. For $p(z) = z \pm 1$, the corresponding partition $\lambda_p^{\pm}$ must have an even number of odd parts; and to each non-zero even part a sign is associated. This data gives a conjugacy class if and only if

1. $|\lambda_z| = 0$,
2. $\lambda_p = \lambda_{(p)^*}$,
3. $\sum_{p=z\pm1} |\lambda_p^{\pm}| + \sum_{p\neq z\pm1} |\lambda_p| \deg(p) = 2n$.

Combinatorial properties of polynomials for $\mathrm{Sp}(2n, q)$ depends on the parity of characteristic. So define

$$e(q) = \begin{cases} 2 & \text{if } q \text{ is odd,} \\ 1 & \text{if } q \text{ is even.} \end{cases}$$

We also need the number $N(q, d)$ of monic, irreducible polynomials of degree d over $\mathbb{F}_q$. This number is given by

$$N(q, d) = \begin{cases} q - 1 & \text{if } d = 1 \\ \frac{1}{d}\sum_{r|d} \mu(r) q^{\frac{d}{r}} & \text{if } d > 1. \end{cases} \tag{2.19}$$

Now let $N^*(q, d)$ be the number of monic, irreducible, degree d polynomials p over $\mathbb{F}_q$ such that $p = \bar{p}$; and let $M^*(q, d)$ be the number of un-ordered pairs $\{p, \bar{p}\}$ of monic, irreducible, degree d polynomials over $\mathbb{F}_q$ where $p \neq \bar{p}$. These numbers are given by

$$N^*(q,d) = \begin{cases} e(q) & \text{if } d=1, \\ 0 & \text{if } d \text{ is odd and } d>1, \\ d^{-1}\sum_{r|d,\ r\ odd}\mu(r)(q^{\frac{d}{2r}}+1-e(q)) & \text{if } d \text{ is even,} \end{cases} \tag{2.20}$$

$$M^*(q,d) = \begin{cases} \frac{1}{2}(q-e(q)-1) & \text{if } d=1, \\ \frac{1}{2}N(q,d) & \text{if } d \text{ is odd and } d>1, \\ \frac{1}{2}\big(N(q,d)-N^*(q,d)\big) & \text{if } d \text{ is even.} \end{cases} \tag{2.21}$$

Orthogonal Groups: Orthogonal groups can be defined as subgroups of $\mathrm{GL}(n,q)$ that preserves a non-degenerate symmetric bilinear form. We assume that the characteristic is not equal to 2. For $n = 2l+1$ odd, there are two such forms up to isomorphism. Their corresponding groups $\mathrm{O}^+(2l+1,q)$ and $\mathrm{O}^-(2l+1,q)$ are isomorphic, with inner product matrices A and δA, where δ is a non-square in $\mathbb{F}_q$ and A is given by

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0_l & I_l \\ 0 & I_l & 0_l \end{pmatrix}.$$

Order of these groups is given by $2q^{l^2}\prod_{i=1}^{l}(q^{2i}-1)$.

For $n = 2l$ even, there are again two forms up to isomorphism with inner product matrices

$$\begin{pmatrix} 0_l & I_l \\ I_l & 0_l \end{pmatrix},$$

$$\begin{pmatrix} 0_{l-1} & I_{l-1} & 0 & 0 \\ I_{l-1} & 0_{l-1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -\delta \end{pmatrix},$$

where δ is a non-square in $\mathbb{F}_q$. If we denote the two orthogonal groups by $\mathrm{O}^+(2l,q)$ and $\mathrm{O}^+(2l,q)$, their cardinalities are given by $2q^{l^2-l}(q^l \mp 1)\prod_{i=1}^{l}(q^{2i}-1)$.

2.2.1 Separable Matrices

Let $s_{\mathrm{G}}(\infty, q)$ denote limiting probability that a random element in G is separable as $n \to \infty$ where G is one of the classical groups. Fulman et. al. give the following table of these probabilities ([7]).

Group G	q	Limiting separability probability $s_{\mathrm{G}}(\infty, q)$
$\mathrm{GL}(n, q)$	any	$1 - \frac{1}{q}$
$\mathrm{U}(n, q)$	any	$\left(1 + \frac{1}{q}\right) \prod_{d \ odd} \left(1 - \frac{2}{q^d(q^d+1)}\right)^{\tilde{N}(q,d)}$
	any	$\frac{q^2-1}{q^2+1} \prod_{d \ odd} \left(1 - \frac{1}{(q^d+1)^2}\right)^{\tilde{N}(q,d)} \prod_{d\geq 1} \left(1 + \frac{1}{q^{4d}-1}\right)^{\tilde{M}(q,d)}$
$\mathrm{SP}(2m, q)$	odd	$\left(1 - \frac{1}{q}\right)^2 \prod_{d\geq 1} \left(1 - \frac{2}{q^d(q^d+1)}\right)^{N^*(q,2d)}$
	even	$\left(1 - \frac{1}{q}\right) \prod_{d\geq 1} \left(1 - \frac{2}{q^d(q^d+1)}\right)^{N^*(q,2d)}$
	odd	$\frac{q(q-1)^3}{(q^2-1)^2} \prod_{d\geq 1} \left(1 - \frac{1}{(q^d+1)^2}\right)^{N^*(q,2d)} \prod_{d\geq 1} \left(1 + \frac{1}{(q^{2d}-1)}\right)^{M^*(q,d)}$
	even	$\frac{(q-1)^2}{(q^2-1)} \prod_{d\geq 1} \left(1 - \frac{1}{(q^d+1)^2}\right)^{N^*(q,2d)} \prod_{d\geq 1} \left(1 + \frac{1}{(q^{2d}-1)}\right)^{M^*(q,d)}$
$\mathrm{O}(2m+1, q)$	any	$s_{\mathrm{Sp}}(\infty, q)$
$\mathrm{O}^{\pm}(2m, q)$	odd	$s_{\mathrm{Sp}}(\infty, q)$
$\mathrm{O}^{\pm}(2m, q)$	even	$\frac{1}{2} s_{\mathrm{Sp}}(\infty, q)$

Table 2.1: Separable matrix limiting probabilities.

They also give the following Table (2.2) of lower and upper bounds for the complicated limiting probabilities $s_{\mathrm{G}}(\infty, q)$.

Group G	q	$s_{\mathrm{Sp}}(\infty, q)$ lower bound	$s_{\mathrm{Sp}}(\infty, q)$ upper bound
$\mathrm{GL}(n, q)$	any	$1 - q^{-1}$	$1 - q^{-1}$
$\mathrm{U}(n, q)$	any	$1 - q^{-1} - 2q^{-3} + 2q^{-4}$	$1 - q^{-1} - 2q^{-3} + 6q^{-4}$
	2	0.4147	0.4157
	3	0.6283	0.6286
$\mathrm{Sp}(2m, q)$	odd	$1 - 2q^{-1} + 2q^{-2} - 4q^{-3} + 4q^{-4}$	$1 - 2q^{-1} + 2q^{-2} - 4q^{-3} + 9q^{-4}$
	even	$1 - 3q^{-1} + 5q^{-2} - 10q^{-3} + 12q^{-4}$	$1 - 3q^{-1} + 5q^{-2} - 10q^{-3} + 23q^{-4}$
	2	0.2833	0.2881
	3	0.3487	0.3493
$\mathrm{O}(2m+1, q)$	any	same as for $s_{\mathrm{Sp}}(\infty, q)$	same as for $s_{\mathrm{Sp}}(\infty, q)$
$\mathrm{O}^{\pm}(2m, q)$	odd	same as for $s_{\mathrm{Sp}}(\infty, q)$	same as for $s_{\mathrm{Sp}}(\infty, q)$
	even	$\frac{1}{2}$ bound for $s_{\mathrm{Sp}}(\infty, q)$	$\frac{1}{2}$ bound for $s_{\mathrm{Sp}}(\infty, q)$

Table 2.2: Explicit bounds for separable matrix limiting probabilities.

One can find table of convergence rates for the separability limiting probabilities in ([7]).

2.2.2 Cyclic and Regular Matrices

Let $c_{\mathrm{G}}(\infty, q)$ denote the limiting probability of cyclicness in G as $n \to \infty$. For the classical groups, the probabilities are given in ([7]) and we take the Table (2.3) of results from there.

Group G	q	Limiting probability $c_{\mathrm{G}}(\infty, q)$
$\mathrm{GL}(n,q)$	any	$(1-q^{-5})/(1+q^{-3})$
$\mathrm{U}(n,q)$	any	$\left(1+\frac{1}{q}\right)\prod_{d\ odd}\left(1-\frac{1}{q^d(q^d+1)}\right)^{\tilde{N}(q,d)}\prod_{d\geq 1}\left(1+\frac{1}{q^{2d}(q^{2d}-1)}\right)^{\tilde{M}(q,d)}$
	any	$\left(1-\frac{1}{q^2}\right)\prod_{d\ odd}\left(1+\frac{q^d-1}{q^{3d}(q^d+1)}\right)^{\tilde{N}(q,d)}\prod_{d\geq 1}\left(1+\frac{1}{q^{6d}}\right)^{\tilde{M}(q,d)}$
	any	$\frac{(q^2-1)(q^3-1)}{q(q^4+1)}\prod_{d\ odd}\left(1+\frac{1}{(q^d+1)(q^{2d}-1)}\right)^{\tilde{N}(q,d)}\prod_{d\geq 1}\left(1+\frac{1}{(q^{2d}-1)(q^{4d}+1)}\right)^{\tilde{M}(q,d)}$
$\mathrm{Sp}(2m,q)$	any	$\prod_{d\geq 1}\left(1-\frac{1}{q^d(q^d+1)}\right)^{N^*(q,2d)}\prod_{d\geq 1}\left(1+\frac{1}{q^d(q^d-1)}\right)^{M^*(q,d)}$
	odd	$\frac{q^3(q^3-1)}{(q^2+1)(q^4-1)}\prod_{d\geq 1}\left(1+\frac{1}{(q^d+1)(q^{2d}-1)}\right)^{N^*(q,2d)}\prod_{d\geq 1}\left(1+\frac{1}{(q^d-1)(q^{2d}+1)}\right)^{M^*(q,d)}$
	even	$\frac{q^3-1}{q(q^2+1)}\prod_{d\geq 1}\left(1+\frac{1}{(q^d+1)(q^{2d}-1)}\right)^{N^*(q,2d)}\prod_{d\geq 1}\left(1+\frac{1}{(q^d-1)(q^{2d}+1)}\right)^{M^*(q,d)}$
$\mathrm{O}(2m+1,q)$	any	$\left(1-\frac{1}{q}\right)c_{\mathrm{Sp}}(\infty,q)$
$\mathrm{O}^{\pm}(2m,q)$	odd	$\left(1-\frac{1}{q}+\frac{1}{2q^2}\right)c_{\mathrm{Sp}}(\infty,q)$
	even	$\left(1-\frac{1}{2q}\right)c_{\mathrm{Sp}}(\infty,q)$

Table 2.3: Cyclic matrix limiting probabilities.

Upper and lower bounds for the limiting probabilities are given in Table (2.4). In that table, the constants k_1, k_2, k_3 are given by

$$k_1 = 1 - q^{-1}, \quad k_2 = 1 - q^{-1} + \frac{1}{2}q^{-2}, \quad k_3 = 1 - \frac{1}{2}q^{-1}.$$

One can find tables of convergence rates and limiting probabilities expanded in $q^{-1}\ mod O(q^{-10})$ in ([7]).

An element of a finite classical group G of characteristic p is called regular if its centralizer in the corresponding group over $\overline{\mathbb{F}_q}$ has minimal possible dimension,

Group G	q	$c_{\mathrm{G}}(\infty, q)$ lower bound	$c_{\mathrm{G}}(\infty, q)$ upper bound
$\mathrm{GL}(n, q)$	any	$(1-q^{-5})/(1+q^{-3})$	$(1-q^{-5})/(1+q^{-3})$
$\mathrm{U}(n, q)$	any	$(1-q^{-3})/(1+q^{-4})$	$1-q^{-3}$
$\mathrm{Sp}(2m, q)$	odd	$1-3q^{-3}+q^{-4}-q^{-5}$	$1-3q^{-3}+2q^{-4}+q^{-5}$
	even	$1-2q^{-3}-q^{-5}$	$1-2q^{-3}+q^{-4}+q^{-5}$
$\mathrm{O}(2m+1, q)$	any	k_1 bound for $c_{\mathrm{Sp}}(\infty, q)$	k_1 bound for $c_{\mathrm{Sp}}(\infty, q)$
$\mathrm{O}^{\pm}(2m, q)$	odd	k_2 bound for $c_{\mathrm{Sp}}(\infty, q)$	k_2 bound for $c_{\mathrm{Sp}}(\infty, q)$
	even	k_3 bound for $c_{\mathrm{Sp}}(\infty, q)$	k_3 bound for $c_{\mathrm{Sp}}(\infty, q)$

Table 2.4: Explicit bounds for cyclic matrix limiting probabilities.

which is equal to rank of G. For the general linear, unitary and symplectic groups, notions of cyclic and regular elements coincide. For the orthogonal groups, the two concepts are different. Table (2.5) from ([7]) shows the limiting probabilities $r_{\mathrm{G}}(\infty, q)$ of regular elements in the corresponding orthogonal groups.

Group G	q	Limiting probability $r_{\mathrm{G}}(\infty, q)$
$\mathrm{O}(2m+1, q)$	odd	$\left(1+\frac{1}{q^2(q+1)}\right) c_{\mathrm{Sp}}(\infty, q)$
	even	$c_{\mathrm{Sp}}(\infty, q)$
$\mathrm{O}^{\pm}(2m, q)$	odd	$\left(1+\frac{1}{q^2(q+1)}+\frac{1}{2q^4(q+1)^2}\right) c_{\mathrm{Sp}}(\infty, q)$
	even	$\left(1+\frac{1}{2q^2(q+1)}\right) c_{\mathrm{Sp}}(\infty, q)$

Table 2.5: Regular orthogonal matrix limiting probabilities.

Cyclic matrices in a more general range of groups are investigated for design and analysis of algorithms for efficient computation in matrix groups ([23, 24]). Authors give estimations for the probabilities of random element to be non-cyclic in the groups

$$\begin{aligned} \mathrm{SL}(n, q) \leq G \leq \mathrm{GL}(n, q), \\ \mathrm{SU}(n, q) \leq G \leq \mathrm{GU}(n, q), \\ \mathrm{Sp}(2m, q) \leq G \leq \mathrm{GSp}(2m, q), \\ \Omega^{\varepsilon}(n, q) \leq G \leq \mathrm{GO}^{\varepsilon}(n, q). \end{aligned}$$

Here general unitary group $\mathrm{GU}(n, q)$ and general symplectic group $\mathrm{GSp}(2m, q)$ consist of matrices in $\mathrm{GL}(n, q^2)$ and $\mathrm{GL}(2m, q)$ that preserve the corresponding form up to a scalar multiplication. The group $\Omega(n, q)$ is defined as the commutator subgroup of the orthogonal group $\mathrm{O}(n, q)$. The authors denote the probability for the random element in G to be non-cyclic by ν_{G}. Their results are summarized in Table (2.6).

Group G	n, m	q	Upper bound for ν_{G}
$\mathrm{SL}(n,q) \leq \mathrm{G} \leq \mathrm{GL}(n,q)$	$n \geq 3$	any	$\frac{1}{q(q^2-1)}$
$\mathrm{SU}(n,q) \leq \mathrm{G} \leq \mathrm{GU}(n,q)$	$n = 3$	any	$\frac{q+3}{q^2(q^2-1)}$
	$n \geq 4$	any	$\frac{q^2+2}{q^2(q-1)(q^2+1)}$
$\mathrm{Sp}(2m,q) \leq \mathrm{G} \leq \mathrm{GSp}(2m,q)$	$m \geq 2$	any	$\frac{1+t(\mathrm{G})}{q(q^2-1)} + \frac{1}{2q^2(q^2-1)} + \frac{t(\mathrm{G})}{q^2(q-1)(q^2-1)}$
$\Omega^{\varepsilon}(2m,q) \leq \mathrm{G} \leq \mathrm{GO}^{\varepsilon}(2m,q)$	$m \geq 3$	odd	$\frac{s(\mathrm{G})}{2q} + \frac{q+4}{2q(q^2-1)}$
		even	$\frac{s(\mathrm{G})}{2q} + \frac{2}{q(q^2-1)}$
$\Omega(2m+1,q) \leq \mathrm{G} \leq \mathrm{O}(2m+1,q)$	$m \geq 2$	odd	$\frac{1}{q-1} + \frac{3}{(q-1)(q^2+1)}$

Table 2.6: Bounds for probability of non-cyclicity.

In this table, the quantity $t(\mathrm{G})$ is 1 or 2 depending on the group. Similarly, $s(\mathrm{G})$ takes values $1, 2, 4$ when q is odd and 1 or 2 when q is even.

2.2.3 Semisimple Matrices

In this subsection let $ss_{\mathrm{G}}(\infty, q)$ denote the limiting probability of semisimple matrices as $n \to \infty$. We give the Table (2.7) of probabilities from ([7]). In this table results are expressed in terms of the following quantities

$$
\begin{aligned}
A_{q,d}(1) &= \left(1 - \frac{1}{q^d}\right)\left(1 + \sum_{m\geq 1} \frac{1}{|\mathrm{U}(m,q^d)|}\right), \\
B_{q,d}(1) &= \left(1 - \frac{1}{q^d}\right)\left(1 + \sum_{m\geq 1} \frac{1}{|\mathrm{GL}(m,q^d)|}\right), \\
F_{+}(1) &= 1 + \sum_{m\geq 1}\left(\frac{1}{|\mathrm{O}^{-}(m,q)|} + \frac{1}{|\mathrm{O}^{+}(m,q)|}\right), \\
F(1) &= 1 + \sum_{m\geq 1} \frac{1}{|\mathrm{Sp}(m,q)|}
\end{aligned}
$$

In Table (2.8) we quote the lower and upper bounds for the limiting probability $ss_{\mathrm{G}}(\infty, q)$ from ([7]). The reader can also find convergence rates for the limiting probabilities and power series expansions in $q^{-1}\ modO(q^{-10})$ there.

Group G	q	Limiting probability $ss_{\mathrm{G}}(\infty, q)$
$\mathrm{GL}(n,q)$	any	$\prod_{r=0,\pm 2 (mod\ 5)} \frac{\left(1-\frac{1}{q^{r-1}}\right)}{\left(1-\frac{1}{q^r}\right)}$
$\mathrm{U}(n,q)$	any	$\left(1+\frac{1}{q}\right)\prod_{d\ odd} A_{q,d}(1)^{\tilde{N}(q,d)}\prod_{d\geq 1} B_{q^2,d}(1)^{\tilde{M}(q,d)}$
$\mathrm{Sp}(2m,q)$	odd	$\left(1-\frac{1}{q}\right)^2 F(1)^2\prod_{d\geq 1} A_{q,d}(1)^{N^*(q,2d)}\prod_{d\geq 1} B_{q,d}(1)^{M^*(q,d)}$
	even	$\left(1-\frac{1}{q}\right) F(1)\prod_{d\geq 1} A_{q,d}(1)^{N^*(q,2d)}\prod_{d\geq 1} B_{q,d}(1)^{M^*(q,d)}$
$\mathrm{O}(2m+1,q)$	odd	$\left(1-\frac{1}{q}\right)^2 F_+(1)F(1)\prod_{d\geq 1} A_{q,d}(1)^{N^*(q,2d)}\prod_{d\geq 1} B_{q,d}(1)^{M^*(q,d)}$
	even	$s_{\mathrm{Sp}(\infty,q)}$
$\mathrm{O}^{\pm}(2m,q)$	odd	$\frac{1}{2}\left(F_+(1)^2+F(1)^2\right)\left(1-\frac{1}{q}\right)^2\prod_{d\geq 1} A_{q,d}(1)^{N^*(q,2d)}\prod_{d\geq 1} B_{q,d}(1)^{M^*(q,d)}$
	even	$\frac{1}{2}F_+(1)\left(1-\frac{1}{q}\right)\prod_{d\geq 1} A_{q,d}(1)^{N^*(q,2d)}\prod_{d\geq 1} B_{q,d}(1)^{M^*(q,d)}$

Table 2.7: Semisimple matrix limiting probabilities.

Group G	q	$ss_{\mathrm{G}}(\infty,q)$ lower bound	$ss_{\mathrm{G}}(\infty,q)$ upper bound
$\mathrm{GL}(n,q)$	any	$1-q^{-1}+q^{-3}-2q^{-4}$	$1-q^{-1}+q^{-3}$
$\mathrm{U}(n,q)$	any	$1-q^{-1}-q^{-3}-2q^{-4}$	$1-q^{-1}-q^{-3}+3q^{-4}$
	2	0.4698	0.4724
	3	0.6498	0.6501
$\mathrm{Sp}(2m,q)$	odd	$1-3q^{-1}+5q^{-2}-7q^{-3}+6q^{-4}$	$1-3q^{-1}+5q^{-2}-7q^{-3}+13q^{-4}$
	even	$1-2q^{-1}+2q^{-2}-2q^{-3}+q^{-4}$	$1-2q^{-1}+2q^{-2}-2q^{-3}+5q^{-4}$
	2	0.3476	0.3481
	3	0.3819	0.3821
$\mathrm{O}(2m+1,q)$	odd	$1-2q^{-1}+2q^{-2}-2q^{-3}-2q^{-4}$	$1-2q^{-1}+2q^{-2}-2q^{-3}+7q^{-4}$
	3	0.5046	0.5053
$\mathrm{O}^{\pm}(2m,q)$	odd	$1-2q^{-1}+\frac{5}{2}q^{-2}-\frac{7}{2}q^{-3}$	$1-2q^{-1}+\frac{5}{2}q^{-2}-\frac{7}{2}q^{-3}+\frac{21}{2}q^{-4}$
	3	0.5244	0.5252
	even	$\frac{1}{2}(1-q^{-1}-3q^{-4})$	$\frac{1}{2}(1-q^{-1}+5q^{-4})$
	2	0.2513	0.2515

Table 2.8: Explicit bounds for semisimple matrix limiting probabilities.

Chapter 3

Random Codes

This section is devoted to calculation of expectations and covariances between the coefficients of weight enumerator of random codes.

3.1 Expectations of Coefficients of Weight Enumerator

We will start with the moments of the random variable $q^{-r_{k\times n}}$ where $r_{k\times n}$ is the rank of a $k\times n$ matrix. The basic tool for evaluation of moments is the probability $P(n,k,r)$ of the random $k\times n$ matrix to have rank r.

We need q-analogues $[n]_q$ of positive integers n and the q-factorials to express this probability. Instead of the usual definition $[n]_q = (q^n-1)/(q-1)$ we use the following form

$$[n]_q := q^n - 1.$$

These functions extend the Binomial coefficients as follows

$$\begin{aligned}
[0]_q! &= 1, \\
[n]_q! &= [n]_q[n-1]_q \dots [1]_q, \\
\begin{bmatrix} n \\ r \end{bmatrix}_q &= \frac{[n]_q!}{[r]_q![n-r]_q!}. \qquad (3.1)
\end{aligned}$$

The quantum Binomial coefficient in Eq. (3.1) gives the number of r dimensional subspaces of an n dimensional linear space over $\mathbb{F}_q$. Cardinality of the group $\mathrm{GL}(k,q)$ is given by the factorial

$$|\mathrm{GL}(k,q)| = q^{\frac{k(k-1)}{2}}[k]_q! \qquad (3.2)$$

In the following part, we drop the subscript q in the notation. We will need two classical formulas in the sequel

q-Binomial Theorem (Commutative)

$$\prod_{0\le j<d}(1-q^j t) = \sum_{0\le i\le d}(-1)^i q^{\frac{i(i-1)}{2}} \begin{bmatrix} d \\ i \end{bmatrix} t^i, \qquad (3.3)$$

q-Binomial Theorem (Noncommutative)

$$(x+y)^d = \sum_{0\le i\le d} \begin{bmatrix} d \\ i \end{bmatrix} x^i y^{d-i}, \qquad (3.4)$$

where the power on the left hand side is noncommutative in x and y. The power is to be expanded so that every monomial is in the form $x^i y^j$ by the relation yx=qxy.

Note that the q-Binomial identities are expressed in q-Binomial coefficients and our convention on $[n]_q$ doesn't change them. See ([12]) for the theory of the subject and proofs of the items above.

Proposition 3.1 *The probability $P(n,k,r)$ of a $k \times n$ matrix to have rank r is given by*

$$P(n,k,r) = q^{-kn+\frac{r(r-1)}{2}} \frac{[n]!}{[n-r]!} \frac{[k]!}{[k-r]!} \frac{1}{[r]!}. \qquad (3.5)$$

Proof. This is a standard formula, see for example ([28]). □

In the next theorem we will use the following simple lemma.

Lemma 3.2
$$\frac{[k]!}{[k-d]!} = q^{-\frac{d(d-1)}{2}} \sum_{0 \le i \le d} (-1)^i q^{\frac{i(i-1)}{2}} \begin{bmatrix} d \\ i \end{bmatrix} q^{k(d-i)} \tag{3.6}$$

Proof.
$$\frac{[k]!}{[k-d]!} = \prod_{0 \le i < d} (q^{k-i} - 1) = q^{kd - \frac{d(d-1)}{2}} \prod_{0 \le i < d} (1 - q^{i-k})$$
When we replace the last product with the corresponding sum by Eq. (3.3) we get the result. □

The following theorem gives the moments of the rank function of a random matrix.

Theorem 3.3 *The* s^{th} *moment* $\mu_s(q^{-r_{k\times n}})$ *of the rank function* $q^{-r_{k\times n}}$ *is given by*

$$\mu_s(q^{-r_{k\times n}}) = q^{-kn} \sum_{0 \le r \le k} q^{r(n-s)} \begin{bmatrix} k \\ r \end{bmatrix} \prod_{0 \le i < r} (1 - q^{-n+i}), \tag{3.7}$$

$$\mu_s(q^{-r_{k\times n}}) = \prod_{0 \le i < k} (x + y - q^{-n-s+i}) \Bigg|_{x=q^{-n}, y=q^{-s}}, \tag{3.8}$$

where the product in the second formula is noncommutative in x *and* y*. Every term should be put in the form* $x^i y^j$ *before substituting* q^{-n} *and* q^{-s} *using the commutation rule* $yx = qxy$*. Moment* $\mu_s(q^{-r_{k\times n}})$ *is symmetric in* n *and* k*. Furthermore if* s *is a nonnegative integer then the formula is also symmetric in* s*.*

Proof. We use the formula in Equation (3.5) for probability.

$$\begin{aligned}
\mu_s(q^{-r_{k\times n}}) &= \sum_r q^{-rs} P(n,k,r) \\
&= \sum_r q^{-kn+\frac{r(r-1)}{2}-rs} \frac{[k]!}{[k-r]![r]!} \frac{[n]!}{[n-r]!} \qquad (3.9) \\
&\underset{\text{Eq.}(3.6)}{=} q^{-kn} \sum_{r,i} q^{-rs} \begin{bmatrix} k \\ r \end{bmatrix} (-1)^i q^{\frac{i(i-1)}{2}} \begin{bmatrix} r \\ i \end{bmatrix} q^{n(r-i)} \qquad (3.10) \\
&= q^{-kn} \sum_r q^{r(n-s)} \begin{bmatrix} k \\ r \end{bmatrix} \prod_{0\le i<r} (1-q^{-n+i}) \qquad (3.11)
\end{aligned}$$

To get the second formula of moments we proceed from Equation (3.10) as follows

$$\begin{aligned}
\mu_s(q^{-r_{k\times n}}) &= q^{-kn} \sum_r q^{-rs} \begin{bmatrix} k \\ r \end{bmatrix} \sum_i (-1)^i q^{\frac{i(i-1)}{2}} \begin{bmatrix} r \\ i \end{bmatrix} (q^n)^{r-i} \\
&\underset{r\to k-r}{=} q^{-kn} \sum_{r,i} q^{-s(k-r)} \begin{bmatrix} k \\ r \end{bmatrix} (-1)^i q^{\frac{i(i-1)}{2}} \begin{bmatrix} k-r \\ i \end{bmatrix} q^{n(k-r-i)} \\
&= \sum_{r,i} (-1)^i q^{\frac{i(i-1)}{2}} \begin{bmatrix} k \\ i \end{bmatrix} q^{i(-n-s)} \begin{bmatrix} k-i \\ r \end{bmatrix} (q^{-n})^r (q^{-s})^{k-i-r} \\
&= \sum_i (-1)^i q^{\frac{(i)(i-1)}{2}} \begin{bmatrix} k \\ i \end{bmatrix} (q^{-n-s})^i (q^{-n}+q^{-s})^{k-i} \qquad (3.12)
\end{aligned}$$

The last equation follows from the noncommutative q-Binomial formula (Eq. (3.4)). Finally by the commutative q-Binomial formula given in Eq. (3.3) we get

$$\mu_s(q^{-r_{k\times n}}) = \prod_{0\le i<k} (q^{-n}+q^{-s}-q^{-n-s+i})$$

where we remind that the product is noncommutative. It should be expanded in $x = q^{-n}$, $y = q^{-s}$ so that every monomial is put in the form $x^i y^j$ by the commutation relation $yx = qxy$ and then substitute for x and y.

The probability formula $P(n,k,r)$ is symmetric in n and k hence the same holds for the moment formulas. This can be proven by expanding $[k]!/[k-r]!$ instead of $[n]!/[n-r]!$ in Eq. (3.9). If s is nonnegative integer the formula is completely symmetric in n, k and s. This follows from the symmetry of the noncommutative q-Binomial formula (3.4). $\square$

Example 3.1 *An easy calculation gives the expectation* $\mathbb{E}$ *and the second moment* μ_2 *of* $q^{-r_{k\times n}}$ *as follows*

$$\begin{aligned}\mathbb{E}(q^{-r_{k\times n}}) &= q^{-n}+q^{-k}-q^{-n-k}, &(3.13)\\ \mu_2(q^{-r_{k\times n}}) &= q^{-2n}+q^{-2k}+q^{-2n-2k+1}+q^{-n-k}(q+1)(1-q^{-n}-q^{-k}). &(3.14)\end{aligned}$$

The following examples give the expectations of coefficients of weight enumerators of the random codes C and $C^{\perp}$. In the following example and henceforth C is an $[n,k]$ code given by a $k\times n$ random generator matrix.

Example 3.2 *Expectation of weight enumerator of the random code* C *is given by*

$$\mathbb{E}(W_C(t)) = \sum_i \mathbb{E}(A_i)t^{n-i} = t^n + \frac{(q^k-1)}{q^n}(t+q-1)^n. \tag{3.15}$$

Let G be a random $k\times n$ matrix and let C be the code with generator matrix G. Weight enumerator $W_C(t)$ is expressed via rank function by

$$W_C(t) = \sum_{I\subset\{1,2,\ldots n\}} q^{k-r_I}(t-1)^{|I|},$$

where r_I is rank of the column submatrix spanned by the column set I. Expectation of the weight enumerator is given by

$$\mathbb{E}(W_C(t)) = \sum_{I\subset\{1,2,\ldots n\}} q^k\mathbb{E}(q^{-r_I})(t-1)^{|I|}.$$

The result follows when we substitute $\mathbb{E}(q^{-r_I}) = \mathbb{E}(q^{-r_{k\times|I|}})$ given by Equation (3.13).

We will obtain an analogous result for the random code $C^{\perp}$ by Mac-Williams duality ([19])

$$W_{C^{\perp}}(1+t) = q^{-k}t^nW_C\left(1+\frac{q}{t}\right). \tag{3.16}$$

Recall that $C^{\perp}$ is considered to be an $[n,n-k]$ code given by a random $k\times n$ parity check matrix.

Example 3.3 *Expectation of weight enumerator of the random code* $C^{\perp}$ *is given by*

$$\mathbb{E}\,W_{C^{\perp}}(t) = \sum_i \mathbb{E}(A_i^{\perp})t^{n-i} = q^{-k}((t+q-1)^n+(q^k-1)t^n). \tag{3.17}$$

Let G be the random $k \times n$ parity check matrix of $C^{\perp}$. We know expectation of weight enumerator of the code C which assumes G as its generator matrix (Example 3.2). Taking expectations of both sides of Eq. (3.16) and using Eq. (3.15) we obtain the assertion.

Expectations and the second moments of the code weights are not new results. One can find them in ([9, page 10]) and ([1, page 44]) for example.

3.2 Covariances Between the Coefficients of Weight Enumerators

We will obtain the covariances between the coefficients of weight enumerators from the covariance of rank functions. The covariance between two rank functions is given by

$$\mathrm{cov}(q^{-r_I}, q^{-r_J}) = \mathbb{E}(q^{-r_I - r_J}) - \mathbb{E}(q^{-r_I})\mathbb{E}(q^{-r_J}). \tag{3.18}$$

The new ingredient $\mathbb{E}(q^{-r_I - r_J})$ requires the joint probability $P(r_I, r_J)$ of ranks of sub-matrices G_I and G_J spanned by the column sets I and J respectively. In order to express $P(r_I, r_J)$ we need an auxiliary function. Let G be a $k \times n$ matrix and let M fixed columns of G span a matrix of rank m. Denote by $P(n, k, M, m, r)$ the probability that G has rank r.

Lemma 3.4

$$P(n, k, M, m, r) = P(n - M, k - m, r - m). \tag{3.19}$$

Proof. Let V_0 be the column space of given M vectors. We have to find $n - M$ column vectors of rank $r - m$ in the space $\mathbb{F}_q^k / V_0$ and then lift them up to $\mathbb{F}_q^k$. So the number $N(n, k, M, m, r)$ of complementary matrices is given by

$$N(n, k, M, m, r) = q^{(n-M)(k-m)} P(n - M, k - m, r - m) q^{(n-M)m}.$$

To find the probability we multiply by $q^{-(n-M)k}$ and the exponents cancel. $\square$

The following proposition gives the moments of this partial probability function.

Proposition 3.5 *Moments of the partial rank function is given by*

$$\begin{aligned}\sum_r q^{-rs} P(n,k,r-m) &= q^{-sm}\mu_s(q^{-r_{k\times n}}) && (3.20)\\ &= q^{-sm-kn}\sum_{0\le r\le k} q^{r(n-s)}\begin{bmatrix}k\\ r\end{bmatrix}\prod_{0\le i<r}(1-q^{-n+i}) && (3.21)\\ &= q^{-sm}\prod_{0\le i<k}(q^{-n}+q^{-s}-q^{-n-s+i}) && (3.22)\end{aligned}$$

where in the last formula the product is noncommutative in the variables $x = q^{-n}$ and $y = q^{-s}$. Moment formula is symmetric in n and k. Moreover when $m = 0$ and s is a nonnegative integer the formula is completely symmetric in n, k and s.

Proof. Proof of this proposition repeats the same steps as Theorem (3.3) so we skip the proof. □

Theorem 3.6 *Let G be a random $k \times n$ matrix, $I, J \subset \{1, 2, \dots, n\}$ be two sets of columns. Then covariance between the rank functions q^{-r_I} and q^{-r_J} is given by*

$$\operatorname{cov}(q^{-r_I}, q^{-r_J}) = \frac{(q-1)(q^k-1)(q^{|I\cap J|}-1)}{q^{2k+|I|+|J|}}. \tag{3.23}$$

Proof. Covariance is given by

$$\operatorname{cov}(q^{-r_I}, q^{-r_J}) = \mathbb{E}(q^{-r_I-r_J}) - \mathbb{E}(q^{-r_I})\mathbb{E}(q^{-r_J}). \tag{3.24}$$

So we need the expectation of $q^{-r_I-r_J}$, hence the joint probability $P(r_I, r_J)$ of ranks r_I and r_J. This probability is given by the following sum

$$P(r_I, r_J) = \sum_r P(IJ, k, r)P(I, k, IJ, r, r_I)P(J, k, IJ, r, r_J),$$

where IJ is the shortcut notation for $|I \cap J|$. The sum runs over the rank of the intersection. We extend the intersection to the sets I and J with ranks r_I and r_J. Substituting for the auxiliary probabilities by Equation (3.19) we get

$$\mathbb{E}(q^{-r_I-r_J}) = \sum_{r,r_I,r_J} q^{-r_I-r_J} P(IJ, k, r)P(\bar{\bar{I}}, k-r, r_I-r)P(\bar{\bar{J}}, k-r, r_J-r)$$

where $\bar{\bar{I}} = |I \setminus J|$ and $\bar{\bar{J}} = |J \setminus I|$. We can sum up over r_I and r_J by Equations (3.13) and (3.20)

$$\mathbb{E}(q^{-r_I-r_J}) = \sum_r P(IJ,k,r)\big(q^{-k}(1-q^{-\bar{\bar{I}}}) + q^{-r-\bar{\bar{I}}}\big)\big(q^{-k}(1-q^{-\bar{\bar{J}}}) + q^{-r-\bar{\bar{J}}}\big).$$

Finally summation over r gives

$$\begin{aligned}\mathbb{E}(q^{-r_I-r_J}) &= q^{-2k}(1-q^{-\bar{\bar{I}}})(1-q^{-\bar{\bar{J}}}) + q^{-\bar{\bar{I}}-\bar{\bar{J}}}\mu_2(q^{-r_{k\times IJ}}) + \Big(q^{-\bar{\bar{I}}-k}(1-q^{-\bar{\bar{J}}}) \\ &\quad + q^{-\bar{\bar{J}}-k}(1-q^{-\bar{\bar{I}}})\Big)\mathbb{E}(q^{-r_{k\times IJ}}).\end{aligned}$$

We have expressed $\mathbb{E}(q^{-r_I-r_J})$ in terms of the first and the second moments of the rank function and they are given by Equations (3.13) and (3.14). If we substitute this with the product $\mathbb{E}(q^{-r_I})\mathbb{E}(q^{-r_J})$ in Equation (3.24) we get the assertion. $\square$

While the covariances between the rank functions of column submatrices are enough for code theoretical purposes the same question about arbitrary submatrices is still an interesting problem. Let G be a random $k \times n$ matrix. Let $I \subset \{1, 2, \ldots, n\}$ be a column set and $L \subset \{1, 2, \ldots, k\}$ be a row set. We denote by r_{LI} rank of the submatrix spanned by the rows in L and the columns in I.

Conjecture 3.7 *Covariance between the rank functions $q^{-r_{LI}}, q^{-r_{MJ}}$ of two submatrices is given by*

$$\operatorname{cov}(q^{-r_{LI}}, q^{-r_{MJ}}) = \frac{(q-1)(q^{|I\cap J|}-1)(q^{|L\cap M|}-1)}{q^{|I|+|J|+|L|+|M|}}.$$

Before we proceed with the covariance of code weights, we need the following lemma.

Lemma 3.8 *Let*

$$S_{ij} = \sum_{\substack{I,J\subset\{1,2,\ldots n\}\\ |I|=i,|J|=j}} q^{|I\cap J|}. \tag{3.25}$$

We have the following generating function for S_{ij}

$$\sum_{i,j} S_{ij}x^i y^j = (1+x+y+qxy)^n. \tag{3.26}$$

Proof. If we fix the cardinality $|I \cap J|$ by m, we can choose the elements in the symmetric difference and then split this set to I and J. This gives

$$S_{ij} = \sum_m \binom{n}{m,\ j-m,\ i-m,\ n+m-i-j} q^m.$$

The sum above shows that S_{ij} is the coefficient of $x^i y^j$ in $(1+x+y+qxy)^n$. $\square$

We have developed the necessary tools for the covariance between the code weights. The following theorem gives the covariance of coefficients of a code with random generator matrix.

Theorem 3.9 *Covariances between the coefficients of the weight enumerator of a random code C are given by*

$$\operatorname{cov}(W_C(x), W_C(y)) = \frac{(q-1)(q^k-1)}{q^n}\left((xy+q-1)^n - \frac{(x+q-1)^n(y+q-1)^n}{q^n}\right). \tag{3.27}$$

Proof. Let S_i be the coefficient of z^i in $W_C(1+z)$ given by Equation (1.2)

$$S_i = \sum_{|I|=i} q^{k-r_I}.$$

The covariance of the coefficients S_i and S_j is obtained by Equation (3.23)

$$\begin{aligned}
\operatorname{cov}(S_i, S_j) &= \frac{(q-1)(q^k-1)}{q^{i+j}} \sum_{|I|=i,|J|=j} (q^{|I\cap J|}-1) \\
&= \frac{(q-1)(q^k-1)}{q^{i+j}} \left(S_{ij} - \binom{n}{i}\binom{n}{j}\right),
\end{aligned}$$

where S_{ij} was defined by Equation (3.25). For the covariance of weight enumerators we substitute this

$$\begin{aligned}
&\operatorname{cov}(W_C(1+x), W_C(1+y)) = \sum_{i,j} \operatorname{cov}(S_i, S_j) x^i y^j \\
&= (q-1)(q^k-1)\left(\left(\sum_{i,j} S_{ij}\left(\frac{x}{q}\right)^i \left(\frac{y}{q}\right)^j\right) - \left(1+\frac{x}{q}\right)^n \left(1+\frac{y}{q}\right)^n\right) \\
&= \frac{(q-1)(q^k-1)}{q^n}\left((xy+x+y+q)^n - \frac{(x+q)^n(y+q)^n}{q^n}\right).
\end{aligned}$$

When we substitute $x-1$ for x and $y-1$ for y we get the assertion. $\square$

When we transform this theorem to the case of random code $C^\perp$ the result is more interesting. We see in the covariance formula (3.27) that the coefficients A_i and A_j are correlated as the coefficients of $x^i y^j$ for $i \neq j$ can be nonzero. However this is not the case for $C^\perp$.

Theorem 3.10 *Covariances of coefficients of weight enumerator of the random code $C^\perp$ are given by*

$$\operatorname{cov}(W_{C^\perp}(x), W_{C^\perp}(y)) = \frac{(q-1)(q^k-1)}{q^{2k}}((xy+q-1)^n - (xy)^n). \tag{3.28}$$

Proof. By Mac-Williams duality we have

$$\operatorname{cov}(W_{C^\perp}(1+x), W_{C^\perp}(1+y)) = \operatorname{cov}\left(q^{-k}x^n W_C\left(1+\frac{q}{x}\right), q^{-k}y^n W_C\left(1+\frac{q}{y}\right)\right).$$

When we substitute the covariance of weight enumerators from Equation (3.27) the assertion follows from a simple calculation. □

Note that there are only diagonal terms in the covariance of weight enumerator of a random code in this sense. The following corollary is for emphasizing the fact that the coefficients are uncorrelated.

Corollary 3.11 *Coefficients of weight enumerator of the random code $C^\perp$ are uncorrelated*

$$\operatorname{cov}(A_i^\perp, A_j^\perp) = 0. \tag{3.29}$$

Proof. We see in Equation (3.28) that there is no $x^i y^j$ for $i \neq j$. Hence the coefficients are uncorrelated. □

Wadayama obtains the same result independently in his preprint ([29]).

Chapter 4

Triple Correlations

In this chapter we will study triple correlations between the coefficients of weight enumerators. The key ingredient is the triple correlations between the rank functions of column submatrices.

A triplet of submatrices gives a triplet of subspaces. So we will start with the classification of the triplets of subspaces. The classification enables us to evaluate the triple correlations of the rank functions. The formula for the rank correlations turns out to be highly complicated. We made numerous evaluations with computer and we observed that the formula simplifies to a closed form. We give the closed form of this formula as a conjecture. We will give triple correlation formulas for the coefficients of weight enumerators as equivalent forms of this conjecture.

4.1 Classification of Triplets of Subspaces

We will obtain the classification of triplets from the quiver representations. After reviewing the basic definitions and the finiteness theorem of the representations of quivers we will get the classification.

4.1.1 Quiver Representations

A quiver Q is a set of vertices some of which are connected by arrows. Set of vertices of Q is denoted by Q_v and set of arrows by Q_a. The maps $t, h : Q_a \to Q_v$ map an arrow to its tail and to its head respectively.

Definition 4.1. Let Q be a finite quiver and k be an algebraically closed field. A representation of Q is a collection of linear spaces $V(x)$ for each vertex x and linear maps $V(\alpha) : V(t(\alpha)) \to V(h(\alpha))$ for each arrow α in Q. Alternatively, a representation of Q is a left module over k category of paths kQ.

A morphism $f : V_1 \to V_2$ between two representations V_1 and V_2 of a quiver Q is a collection of linear maps $f(x) : V_1(x) \to V_2(x)$ such that $V_2(\alpha)f(x) = f(y)V_1(\alpha)$ for each arrow $x \xrightarrow{\alpha} y$ in Q.

The classification of indecomposable representations of a quiver Q is connected with the positive roots of the following quadratic form

$$r_Q(d) = \sum_{a \in Q_v} d(a)^2 - \sum_{\alpha \in Q_a} d(t\alpha)d(h\alpha)$$

where $d(x)$ is the value of the dimension function $\underline{\dim} V : x \mapsto \dim V(x)$ at vertex x. A *root* of the form r is an integral vector $x \in \mathbb{Z}^|Q_v|$ such that $r(x) = 1$. Note that the canonical basis elements of $\mathbb{Z}^n$ are roots of the form, they are called the *simple roots.* When x is a root and $x_i \geq 0$ for every position i then we call x a *positive root.*

The following theorem gives the finiteness condition and classification of indecomposable representations of a quiver. (See [8][Theorems (6.2) and (7.1)] for proof.)

Theorem 4.2 *The number of isomorphism classes of indecomposable representations of a quiver Q is finite if and only if Q is disjoint union of the simply-laced Dynkin diagrams A_n, D_n, E_6, E_7 and E_8 with arbitrary orientation. If this is the case, the map $V \mapsto \underline{\dim} V$ provides a bijection between the set of isomorphism classes of indecomposable representations and the set of positive roots of r_Q.*

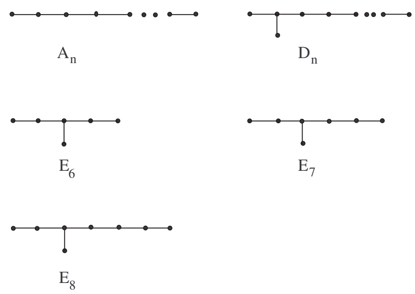

Figure 4.1: Simply Laced Dynkin Graphs

Example 4.1 Consider the Dynkin diagram E_6 with the following orientation

$$\begin{array}{ccccccccc} x_1 & \rightarrow & x_3 & \rightarrow & x_4 & \leftarrow & x_5 & \leftarrow & x_6 \\ & & & & \uparrow & & & & \\ & & & & x_2 & & & & \end{array}$$

Let us call the simple roots e_i. Let $a = (a_1, a_2, a_3, a_4, a_5, a_6) = \sum_i a_i e_i$ be a positive root. We will denote the *dimension vector* of the corresponding indecomposable by

$$\begin{array}{ccccccccc} a_1 & \rightarrow & a_3 & \rightarrow & a_4 & \leftarrow & a_5 & \leftarrow & a_6 \\ & & & & \uparrow & & & & \\ & & & & a_2 & & & & \end{array} \quad . \tag{4.1}$$

4.1.2 Triplets of Subspaces

A triplet $U, V, W \subset E$ is a representation of the Dynkin diagram D_4 with the following orientation

$$\begin{array}{ccccc} & & V & & \\ & & \downarrow & & \\ U & \rightarrow & E & \leftarrow & W \end{array}$$

where each arrow is an inclusion. By Theorem (4.2) indecomposable representations of D_4 are those configurations with the dimension vector coming from the positive roots of the form r_{D_4}. We take the positive roots of the form from ([3]).

Proposition 4.3 *Dimension vectors of the indecomposables of the Dynkin diagram D_4 are given below.*

$$\begin{array}{ccccc} & & 1 & & \\ & & \downarrow & & \\ 1 & \rightarrow & 1 & \leftarrow & 1\end{array}, \qquad \begin{array}{ccccc} & & 0 & & \\ & & \downarrow & & \\ 0 & \rightarrow & 1 & \leftarrow & 0\end{array} \tag{4.2}$$

$$\begin{array}{ccccc} & & 0 & & \\ & & \downarrow & & \\ 1 & \rightarrow & 0 & \leftarrow & 0\end{array}, \qquad \begin{array}{ccccc} & & 1 & & \\ & & \downarrow & & \\ 0 & \rightarrow & 0 & \leftarrow & 0\end{array}, \qquad \begin{array}{ccccc} & & 0 & & \\ & & \downarrow & & \\ 0 & \rightarrow & 0 & \leftarrow & 1\end{array} \tag{4.3}$$

$$\begin{array}{ccccc} & & 1 & & \\ & & \downarrow & & \\ 1 & \rightarrow & 1 & \leftarrow & 0\end{array}, \qquad \begin{array}{ccccc} & & 1 & & \\ & & \downarrow & & \\ 0 & \rightarrow & 1 & \leftarrow & 1\end{array}, \qquad \begin{array}{ccccc} & & 0 & & \\ & & \downarrow & & \\ 1 & \rightarrow & 1 & \leftarrow & 1\end{array} \tag{4.4}$$

$$\begin{array}{ccccc} & & 1 & & \\ & & \downarrow & & \\ 0 & \rightarrow & 1 & \leftarrow & 0\end{array}, \qquad \begin{array}{ccccc} & & 0 & & \\ & & \downarrow & & \\ 1 & \rightarrow & 1 & \leftarrow & 0\end{array}, \qquad \begin{array}{ccccc} & & 0 & & \\ & & \downarrow & & \\ 0 & \rightarrow & 1 & \leftarrow & 1\end{array} \tag{4.5}$$

$$\begin{array}{ccccc} & & 1 & & \\ & & \downarrow & & \\ 1 & \rightarrow & 2 & \leftarrow & 1\end{array} \tag{4.6}$$

Since we are interested in the triplets of subspaces we don't take the roots in Equation (4.3) into account. The 1 dimensional subspace can not be embedded into 0 subspace without kernel so they don't correspond to a triplet of subspaces.

We denote a 1 dimensional indecomposable with dimension vector

$$\begin{array}{ccc} & j & \\ i & 1 & k \end{array}$$

by $[ijk]$ and the number of them by m_{ijk}. Also we fix our notation for the two dimensional indecomposable as $[111]_2$ and for its multiplicity as h. So the triplet $U, V, W \subset E$ has the following decomposition

$$\begin{aligned}(E; U, V, W) \quad = \quad & m_{111}[111] + m_{000}[000] + m_{110}[110] + m_{011}[011] + m_{101}[101] \\ & + m_{100}[100] + m_{010}[010] + m_{001}[001] + h[111]_2. \end{aligned} \tag{4.7}$$

Multiplicities $m_{111}, m_{000}, m_{110}, m_{011}, m_{101}, m_{100}, m_{010}, m_{001}, h$ of the indecomposables are called the natural invariants of the triplet and they have the following interpretations

$$m_{110} = \dim\tfrac{U\cap V}{U\cap V\cap W} \qquad m_{011} = \dim\tfrac{V\cap W}{U\cap V\cap W} \qquad m_{101} = \dim\tfrac{W\cap U}{U\cap V\cap W}$$

$$m_{100} = \dim\tfrac{U}{U\cap(V+W)} \qquad m_{010} = \dim\tfrac{V}{V\cap(W+U)} \qquad m_{001} = \dim\tfrac{W}{W\cap(U+V)}$$

$$m_{111} = \dim(U\cap V\cap W) \qquad m_{000} = \operatorname{codim}(U+V+W)$$

and

$$\begin{aligned} h &= \dim\frac{U\cap(V+W)}{(U\cap V)+(W\cap U)} = \dim\frac{V\cap(W+U)}{(V\cap W)+(U\cap V)} \\ &= \dim\frac{W\cap(U+V)}{(W\cap U)+(V\cap W)} = \frac{1}{2}\dim\frac{(U+V)\cap(V+W)\cap(W+U)}{(U\cap V)+(V\cap W)+(W\cap U)}. \end{aligned} \tag{4.8}$$

4.2 Number of Triplets with Given Invariants

For the triple correlation problem we need the number of triplets of subspaces with given invariants. Since GL acts transitively on the triplets with fixed invariants, the number of triplets is the index of the automorphism group. Thus as the first attempt we calculate the order of the automorphism group of a triplet. Following that we can obtain the number of triplets.

4.2.1 Automorphism Group of a Triplet

A morphism M between the triplets $(E; U, V, W)$ and $(E'; U', V', W')$ is a linear map $M : E \to E'$ such that $M(U) \subset U'$,$M(V) \subset V'$ and $M(W) \subset W'$.

The triplet $U, V, W \subset E$ has a direct sum decomposition given in Equation (4.7). This decomposition gives

$$\operatorname{End}(E) = \sum \operatorname{Hom}(T_i, T_j)$$

where T_i, T_j runs through the indecomposables. Automorphisms of the triplet are the invertible elements of the endomorphisms. It turns out that the matrices

$M = \{M[i,j] = \mathrm{Hom}(T_j, T_i)\}$ of the endomorphisms are block triangular for a particular ordering of the isotypical components in the decomposition. So after finding the form of the endomorphisms it is easy to find the order of the stabilizer group and hence the number of triplets.

It is easy to see that the dimensions of spaces of morphisms $\mathrm{Hom}(T_i, T_j)$ between the indecomposables of $U, V, W \subset E$ are as given in the following table. The $[ij]$ entry of the table is dimension of $\mathrm{Hom}(T_j, T_i)$.

	[111]	[110]	[101]	[011]	$[111]_2$	[010]	[100]	[001]	[000]
[111]	1	1	1	1	2	1	1	1	1
[110]	0	1	0	0	1	1	1	0	1
[101]	0	0	1	0	1	0	1	1	1
[011]	0	0	0	1	1	1	0	1	1
$[111]_2$	0	0	0	0	1	1	1	1	2
[010]	0	0	0	0	0	1	0	0	1
[100]	0	0	0	0	0	0	1	0	1
[001]	0	0	0	0	0	0	0	1	1
[000]	0	0	0	0	0	0	0	0	1

(4.9)

Proposition 4.4 *Let U, V, W be a triplet in a k dimensional space E, with given invariants $m_{111}, m_{110}, m_{011}, m_{101}, h, m_{100}, m_{010}, m_{001}, m_{000}$. Then the order of automorphism group $\mathcal{A}$ of the triplet is given by*

$$|\mathcal{A}| = q^{EA}[m_{111}]![m_{110}]![m_{011}]![m_{101}]![h]![m_{100}]![m_{010}]![m_{001}]![m_{000}]! \tag{4.10}$$

where

$$\begin{aligned} EA &= \binom{k-h}{2} + h(m_{111} + m_{000}) - m_{110}m_{011} - m_{011}m_{101} - m_{101}m_{110} \\ &\quad - m_{110}m_{001} - m_{011}m_{100} - m_{101}m_{010} - m_{100}m_{010} - m_{010}m_{001} \\ &\quad - m_{001}m_{100}. \end{aligned} \tag{4.11}$$

Proof. Endomorphisms of the triplet splits into direct sum

$$\mathrm{End}(U, V, W \subset E) = \sum \mathrm{Hom}(m_i T_i, m_j T_j)$$

where T_i's are the indecomposables and m_i's are the number of T_i's in the decomposition. The nonzero entries in the Table (4.9) form a triangular matrix. This shows that nonsingularity is obtained if we choose the diagonal entries $\mathrm{Hom}(m_iT_i, m_iT_i)$ in $\mathrm{GL}(m_i)$. The other summands are completely free. Hence we have

$$\begin{aligned}|\mathcal{A}| &= q^{FS}|\mathrm{GL}(m_{111})||\mathrm{GL}(m_{110})||\mathrm{GL}(m_{011})||\mathrm{GL}(m_{101})||\mathrm{GL}(h)||\mathrm{GL}(m_{100})| \\ &\quad |\mathrm{GL}(m_{010})||\mathrm{GL}(m_{001})||\mathrm{GL}(m_{000})|\end{aligned}$$

where FS is the number of free summands and it is given by

$$\begin{aligned}FS &= (m_{111}+h+m_{000})(m_{110}+m_{011}+m_{101}+m_{100}+m_{010}+m_{001}) \\ &\quad +m_{110}(m_{100}+m_{010})+m_{011}(m_{010}+m_{001})+m_{101}(m_{001}+m_{100}) \\ &\quad +m_{111}m_{000}+2h(m_{111}+m_{000})\end{aligned}$$

Substituting cardinalities of GLs and collecting the exponents we obtain the result. □

4.2.2 The Number of Triplets

In this part we will obtain the number of triplets with given dimensions and dimensions of intersections. We denote dimension of a space U by u and dimension of intersections by the product notation, *e.g.* $\dim(U \cap V) = uv$. Correspondences between the natural invariants and the dimensions are as follows

$$m_{110} = uv - uvw, \qquad m_{100} = u - uv - wu + uvw - h, \tag{4.12}$$

$$m_{011} = vw - uvw, \qquad m_{010} = v - vw - uv + uvw - h, \tag{4.13}$$

$$m_{101} = wu - uvw, \qquad m_{001} = w - wu - vw + uvw - h, \tag{4.14}$$

$$m_{111} = uvw, \qquad m_{000} = k - d, \tag{4.15}$$

$$d = \dim(U+V+W) = u+v+w-uv-vw-wu+uvw-h. \tag{4.16}$$

Proposition 4.5 *The number $N_{U,V,W}$ of triplets U, V, W in a k dimensional space with given dimensions u, v, w, uv, vw, wu, uvw and h is given by*

$$N_{U,V,W} = q^{EXP}\frac{[k]!}{\mathcal{D}(U,V,W)} \tag{4.17}$$

where

$$\begin{aligned}
\mathcal{D}(U,V,W) &= [uvw]![uv-uvw]![vw-uvw]![wu-uvw]![h]![k-d]! \\
& \quad [u-uv-wu+uvw-h]![v-vw-uv+uvw-h]! \\
& \quad [w-wu-vw+uvw-h]!, \\
d &= u+v+w-uv-vw-wu+uvw-h, \\
EXP &= (uv+vw+wu)\big(uv+vw+wu-(u+v+w)+2h-3uvw\big) \\
& \quad +u\times v+v\times w+w\times u+(uvw-h)(u+v+w+3uvw) \\
& \quad +\frac{h(3h-1)}{2}.
\end{aligned}$$

Proof. The group GL(k) has transitive action on triplets, hence the number of triplets $N_{U,V,W}$ is the index of the automorphism group. We know the order of the automorphism group by Equation (4.10). An easy calculation gives the number of triplets with given natural invariants

$$N_{U,V,W} = q^{EC}\frac{[k]!}{[m_{111}]![m_{110}]![m_{011}]![m_{101}]![h]![m_{100}]![m_{010}]![m_{001}]![m_{000}]!} \qquad (4.18)$$

where

$$\begin{aligned}
EC &= kh+m_{110}m_{011}+m_{011}m_{101}+m_{101}m_{110}+m_{110}m_{001}+m_{011}m_{100} \\
& \quad +m_{101}m_{010}+m_{100}m_{010}+m_{010}m_{001}+m_{001}m_{100}-\frac{h(h+1)}{2} \\
& \quad -h(m_{111}+m_{000}). \qquad (4.19)
\end{aligned}$$

When we substitute dimensions and dimensions of intersections of the spaces by Equations (4.12) through (4.16) into the previous formula we get the number of triplets in desired form. □

4.3 Triple Correlation Between Ranks

Joint cumulants are generalizations of the covariance to the case of more than two variables. Let $\xi = (\xi_1, \xi_2, \dots, \xi_n)$ be a random vector. The joint cumulant of the random variables ξ_i is given by

$$\sigma(\xi) = \frac{\partial^n}{\partial\lambda_1\partial\lambda_2\ldots\partial\lambda_n}\log(\mathbb{E}(\exp(\lambda_1\xi_1+\lambda_2\xi_2+\ldots+\lambda_n\xi_n)))|_{\lambda=0}. \tag{4.20}$$

Correlations are expressed via joint cumulants in a simple way

$$\mathbb{E}(\xi_1\xi_2\ldots\xi_n) = \sum_I\prod_i\sigma(\xi_{I_i}), \tag{4.21}$$

where the summation is over all the disjoint partitions I of $\{1,2,\ldots,n\}$ into nonempty subsets I_i.

Example 4.2 *First three joint cumulants are given as follows*

$$\begin{aligned}
\sigma(X) &= \mathbb{E}(X),\\
\sigma(X,Y) &= \mathrm{cov}(X,Y),\\
\sigma(X,Y,Z) &= \mathbb{E}(XYZ)-\mathrm{cov}(X,Y)\mathbb{E}(Z)-\mathrm{cov}(Y,Z)\mathbb{E}(X)-\mathrm{cov}(Z,X)\mathbb{E}(Y)\\
&\quad -\mathbb{E}(X)\mathbb{E}(Y)\mathbb{E}(Z).
\end{aligned}$$

In this section we give the formula of the cumulant $\sigma(q^{-r_I},q^{-r_J},q^{-r_K})$ of the random variables $q^{-r_I},q^{-r_J},q^{-r_K}$. We remind that

$$\begin{aligned}
\sigma(q^{-r_I,-r_J,-r_K}) &= \mathbb{E}(q^{-r_I-r_J-r_K})-\mathbb{E}(q^{-r_I})\mathrm{cov}(q^{-r_J-r_K})-\mathbb{E}(q^{-r_J})\mathrm{cov}(q^{-r_K-r_I})\\
&\quad -\mathbb{E}(q^{-r_K})\mathrm{cov}(q^{-r_I-r_J})-\mathbb{E}(q^{-r_I})\mathbb{E}(q^{-r_J})\mathbb{E}(q^{-r_K}).
\end{aligned} \tag{4.22}$$

Through the calculations we use the following abbreviations for column sets and their cardinalities

$$IJ = I\cap J, \qquad \overline{IJ} = (I\cap J)\setminus K, \qquad \overline{I} = I\setminus(J\cup K), \tag{4.23}$$

$$JK = J\cap K, \qquad \overline{JK} = (J\cap K)\setminus I, \qquad \overline{J} = J\setminus(K\cup I), \tag{4.24}$$

$$KI = K\cap I, \qquad \overline{KI} = (K\cap I)\setminus J, \qquad \overline{K} = K\setminus(I\cup J), \tag{4.25}$$

$$IJK = I\cap J\cap K.$$

The column submatrix spanned for example by $I\cap J = IJ$ will be denoted by G_{IJ}.

Recall that we made use of the joint probability distribution of ranks of submatrices for the covariance between rank functions. For the triple correlations we need the joint probability distribution of ranks of three submatrices. Analogous to the previous case we will introduce an auxiliary probability which gives the joint distribution after summation over its parameters.

Let us consider a $k\times n$ matrix G, let $I, J, K \subset \{1, 2, \ldots, n\}$ be column sets such that the column sub-matrices G_I, G_J, G_K span the matrix, *i.e.* $|I \cup J \cup K| = n$. Let $U, V, W \subset \mathbb{F}_q^k$ be the column spaces of the sub-matrices G_{IJ}, G_{JK} and G_{KI}. Let r_I, r_J, r_K, r_{IJK} be the ranks of the column sub-matrices G_I, G_J, G_K and G_{IJK} respectively. To keep the notation short we will refer to invariants of the triplet as U, V, W as well. Let $P(r_I, r_J, r_K, U, V, W, r_{IJK})$ be the probability that G has the described properties.

Proposition 4.6 *The probability $P(r_I, r_J, r_K, U, V, W, r_{IJK})$ is given by*

$$P(r_I, r_J, r_K, U, V, W, r_{IJK}) = q^{-kn+EP} N_{U,V,W}\mathcal{P} \tag{4.26}$$

where $N_{U,V,W}$ is given in Equation (4.17), EP and $\mathcal{P}$ are defined as follows

$$\begin{aligned} EP &= IJKuvw + \overline{IJ}u + \overline{JK}v + \overline{KI}w + k(\overline{I} + \overline{J} + \overline{K}), && (4.27)\\ \mathcal{P} &= P(IJK, uvw, r_{IJK})P(\overline{IJ}, u - r_{IJK}, u - r_{IJK})P(\overline{JK}, v - r_{IJK}, v - r_{IJK}) \\ &\quad P(\overline{KI}, w - r_{IJK}, w - r_{IJK})P(\overline{I}, k - w - u + wu, r_I - w - u + wu) \\ &\quad P(\overline{J}, k - u - v + uv, r_J - u - v + uv) \\ &\quad P(\overline{K}, k - v - w + vw, r_K - v - w + vw). && (4.28) \end{aligned}$$

Proof. We will find the the number $N(r_I, r_J, r_K, U, V, W, r_{IJK})$ of matrices with given properties so that we will have

$$P(r_I, r_J, r_K, U, V, W, r_{IJK}) = q^{-kn} N(r_I, r_J, r_K, U, V, W, r_{IJK}). \tag{4.29}$$

The triplet of subspaces that G_{IJ}, G_{JK}, G_{KI} form can be fixed among $N_{U,V,W}$ triplets.

Columns in IJK must be chosen from uvw dimensional space with rank r_{IJK}. The number of column submatrices G_{IJK} is given by the factor
$q^{IJKuvw}P(IJK, uvw, r_{IJK})$.

We will extend this construction to the column sets IJ, JK and KI. Columns in IJ must be chosen in U and they must extend the IJK vectors to the matrix of rank u. Number of such vector sets is equal to $q^{\overline{IJ}u}P(\overline{IJ}, u - r_{IJK}, u - r_{IJK})$ in notation of (3.19). Extending the column set IJK to JK and KI brings $q^{\overline{JK}v}P(\overline{JK}, v - r_{IJK}, v - r_{IJK})$ and $q^{\overline{KI}w}P(\overline{KI}, w - r_{IJK}, w - r_{IJK})$ respectively.

Finally we will extend the construction to the column sets I, J and K. For the set I, we have the given $IJ \cup KI$ columns with rank $\dim(W + U) = w + u - wu$. Generators this time will be chosen in $\mathbb{F}_q^k$, they will extend the column set $IJ \cup KI$ to I to have rank r_I. So, the number of choices for the column set $\overline{I}$ is $q^{k\overline{I}}P(\overline{I}, k - (w + u - wu), r_I - (w + u - wu))$. Similarly the number of column sets for $\overline{J}$ and $\overline{K}$ are $q^{k\overline{J}}P(\overline{J}, k - (u + v - uv), r_J - (u + v - uv))$ and $q^{k\overline{K}}P(\overline{K}, k - (v + w - vw), r_K - (v + w - vw))$ respectively. Bringing these factors we get

$$N(r_I, r_J, r_K, U, V, W, r_{IJK}) = q^{EP} N_{U,V,W} \mathcal{P}$$

where $\mathcal{P}$ is product of all the probabilities mentioned and EP comes from the exponents appearing before them. The probability follows from Eq. (4.29). □

We will obtain the correlation between the ranks of a triplet of submatrices by the auxiliary probability.

Theorem 4.7 *Let G be a random $k \times n$ matrix. Let $I, J, K \subset \{1, 2, \ldots, n\}$ be three column subsets with $|I \cup J \cup K| = n$. The triple correlation $\mathbb{E}(q^{-r_I - r_J - r_K})$ between the ranks is given by*

$$\mathbb{E}(q^{-r_I - r_J - r_K}) = \sum q^{-kn + EP - r_I - r_J - r_K} N_{U,V,W} \mathcal{P} \tag{4.30}$$

where EP and $\mathcal{P}$ are given in Equations (4.27) and (4.28) respectively. The sum runs over r_I, r_J, r_K, all the invariants $u, v, w, uv, vw, wu, uvw, h$ of triplets with r_{IJK} that are subject to the constraints (4.33) trough (4.45) .

Proof. The triple correlation is given by

$$\mathbb{E}(q^{-r_I - r_J - r_K}) = \sum_{r_I, r_J, r_K} q^{-r_I - r_J - r_K} P(r_I, r_J, r_K),$$

where $P(r_I, r_J, r_K)$ is the joint probability of the ranks r_I, r_J and r_K. We get this probability by summing up over the rest of the parameters from $P(r_I, r_J, r_K, U, V, W, r_{IJK})$ given in Eq. (4.26). So the correlation becomes

$$\mathbb{E}(q^{-r_I-r_J-r_K}) = \sum_{r_I,r_J,r_K} q^{-r_I-r_J-r_K} \sum P(r_I, r_J, r_K, U, V, W, r_{IJK}) \tag{4.31}$$

with the inner sum running over parameters $r_{IJK}, h, uvw, uv, vw, wu, u, v, w$. When we substitute $P(r_I, r_J, r_K, U, V, W, r_{IJK})$ given in (4.26) we obtain

$$\mathbb{E}(q^{-r_I-r_J-r_K}) = \sum q^{-kn+EP-r_I-r_J-r_K} N_{U,V,W}\mathcal{P}, \tag{4.32}$$

where $N_{U,V,W}$, EP and $\mathcal{P}$ are given in Equations (4.17), (4.27) and (4.28) respectively.

The constraints for the parameters are natural bounds so that no negative q-factorial appears in the formula

$$0 \leq \quad r_{IJK} \quad \leq \min(IJK, uvw), \tag{4.33}$$

$$0 \leq \quad uvw \quad \leq \min(uv, vw, wu), \tag{4.34}$$

$$\max(u+v-r_J, 0) \leq \quad uv \quad \leq \min(u, v), \tag{4.35}$$

$$\max(v+w-r_K, 0) \leq \quad vw \quad \leq \min(v, w), \tag{4.36}$$

$$\max(w+u-r_I, 0) \leq \quad wu \quad \leq \min(w, u), \tag{4.37}$$

$$0 \leq \quad u \quad \leq \min(r_I, r_J, IJ, k), \tag{4.38}$$

$$0 \leq \quad v \quad \leq \min(r_J, r_K, JK, k), \tag{4.39}$$

$$0 \leq \quad w \quad \leq \min(r_K, r_I, KI, k), \tag{4.40}$$

$$0 \leq \quad r_I \quad \leq \min(I, k), \tag{4.41}$$

$$0 \leq \quad r_J \quad \leq \min(J, k), \tag{4.42}$$

$$0 \leq \quad r_K \quad \leq \min(K, k), \tag{4.43}$$

and finally for h we have

$$h \leq \min(u - uv - wu + uvw, v - vw - uv + uvw, w - wu - vw + uvw), \tag{4.44}$$

$$h \geq \max(u + v + w - uv - vw - wu + uvw - k, 0). \tag{4.45}$$

□

4.4 Main Conjecture

Although the triple correlation formula (4.30) is extremely complicated modern computers with algebra packages can easily handle it. We provide a Maple procedure for evaluation at the web address ([16]). Numerous computer experiments suggest that there exists a closed formula for the triple correlations. The formula becomes simpler for the cumulant (4.22). We give the formula for the cumulant suggested by experiments as a conjecture. Triple correlations can be obtained using the conjecture below and Eq. (4.22). The formula extends the previous results. When we set for example $K = \emptyset$ in the triple correlation formula, we get the pair correlations.

Conjecture 4.8 *Let G be a $k \times n$ matrix and let $I, J, K \subset \{1, 2, \ldots n\}$ be three column sets. Then the cumulant $\sigma(q^{-r_I}, q^{-r_J}, q^{-r_K})$ is given by*

$$\sigma(q^{-r_I}, q^{-r_J}, q^{-r_K}) = \frac{(q-1)^2(q^k-1)}{q^{3k+I+J+K}}\big(q^{IJ+JK+KI-IJK} - (q^{IJ} + q^{JK} + q^{KI}) + 2 + (q^k - q)(q^{IJK} - 1)\big)$$

We give an other conjecture for the joint cumulant of rank functions of three arbitrary sub-matrices. We remind the reader that when L is a row set and I is a column set r_{LI} denotes rank of the matrix spanned by the row set L and the column set I.

Conjecture 4.9 *Let G be a random $k \times n$ matrix, let $I, J, K \subset \{1, 2, \ldots, n\}$ be column sets and $L, M, N \subset \{1, 2, \ldots, k\}$ be row sets. Then the joint cumulant of the rank functions $q^{-r_{LI}}, q^{-r_{MJ}}$ and $q^{-r_{NK}}$ is*

$$\sigma(q^{-r_{LI}}, q^{-r_{MJ}}, q^{-r_{NK}}) = \frac{(q^2-1)}{q^{|I|+|J|+|K|+|L|+|M|+|N|}}\big((q^{IJK}-1)(q^{LM+MN+NL-LMN}-1) + (q^{LMN}-1)(q^{IJ+JK+KI-IJK}-1) - (q^{IJ}-1)(q^{LM}-1) - (q^{JK}-1)(q^{MN}-1) - (q^{KI}-1)(q^{NL}-1) - (q+1)(q^{IJK}-1)(q^{LMN}-1)\big).$$

Using similar arguments as in proof of Theorem (3.9) one gets the corresponding conjectures for the coefficients of weight enumerators. Let G be a random

$k \times n$ matrix and C be the code assuming G as a generator matrix. Let

$$S_i = \sum_{|I|=i} q^{k-r_I},$$

so that

$$W_C(1+x) = \sum_i S_i x^i$$

and

$$\sigma(W_C(1+x), W_C(1+y), W_C(1+z)) = \sum_{i,j,l} \sigma(S_i, S_j, S_l) x^i y^j z^l. \tag{4.46}$$

For $\sigma(S_i, S_j, S_l)$ we will calculate generating functions. For this we will put the third correlation function in the following form

$$\begin{aligned}\sigma(q^{-r_I}, q^{-r_J}, q^{-r_K}) = \frac{(q-1)^2(q^k-1)}{q^{3k}} \big(& q^{-(I\cup J\cup K)} - (q^{-(I\cup J)-K} + q^{-(J\cup K)-I} \\ &+ q^{-(K\cup I)-J}) + 2q^{-I-J-K} + (q^k - q)(q^{-I-J-J+IJK} - q^{-I-J-K})\big).\end{aligned}$$

This gives the correlation for the coefficients S_i's as follows

$$\begin{aligned}\sigma(S_i, S_j, S_l) \;=\; (q-1)^2(q^k-1) \sum_{|I|=i,|J|=j,|K|=l} \big(& q^{-(I\cup J\cup K)} - q^{-(I\cup J)-K} - q^{-(J\cup K)-I} \\ &- q^{-(K\cup I)-J} + 2q^{-I-J-K} + (q^k - q)(q^{-I-J-J+IJK} - q^{-I-J-K})\big).\end{aligned} \tag{4.47}$$

Let us introduce more notations now and let $[x^i y^j z^l]M(x,y,z)$ be the coefficient of $x^i y^j z^l$ in the polynomial $M(x,y,z)$. It is easy to check that

$$\begin{aligned}
\sum q^{-(I\cup J\cup K)} &= [x^i y^j z^l]((x+1)(y+1)(z+1) + q - 1)^n q^{-n}, \\
\sum q^{-(I\cup J)-K} &= [x^i y^j z^l]((x+1)(y+1) + q - 1)^n (z+q)^n q^{-2n}, \\
\sum q^{-(J\cup K)-I} &= [x^i y^j z^l]((y+1)(z+1) + q - 1)^n (x+q)^n q^{-2n}, \\
\sum q^{-(K\cup I)-J} &= [x^i y^j z^l]((z+1)(x+1) + q - 1)^n (y+q)^n q^{-2n}, \\
\sum q^{-I-J-K} &= [x^i y^j z^l](x+q)^n (y+q)^n (z+q)^n q^{-3n}, \\
\sum q^{-I-J-K+IJK} &= [x^i y^j z^l]((x+1)(y+1)(z+1) \\
&\qquad + (q-1)(x+y+z+q+1))^n q^{-2n},
\end{aligned}$$

where all the summations are over $I, J, K \subset \{1, 2, \dots n\}$ with $|I| = i, |J| = j$ and $|K| = l$. This set of sums once put in Eq.(4.47) gives the triple correlation $\sigma(S_i, S_j, S_l)$. Then summation over i, j, l gives the joint cumulant of coefficients of weight enumerator given in Eq.(4.46). When we substitute $x - 1$ for x, $y - 1$ for y and $z - 1$ for z we get the joint cumulant of triplet of the coefficients A_is

$$\sigma(W_C(x), W_C(y), W_C(z)) = \sum_{i,j,l} \sigma(A_i, A_j, A_l) x^{n-i} y^{n-j} z^{n-l}.$$

We give the joint cumulants of triplets of coefficients of weight enumerator as corollary to Conjecture (4.8).

Corollary 4.10 *Triple correlations between the coefficients of $W_C(t)$ are given by*

$$\begin{aligned} & \sigma(W_C(x), W_C(y), W_C(z)) = (q-1)^2(q^k-1)\Big\{q^{-n}(xyz+q-1)^n \\ - \ & q^{-2n}\big((xy+q-1)^n(z+q-1)^n + (yz+q-1)^n(x+q-1)^n \\ + \ & (zx+q-1)^n(y+q-1)^n\big) + 2q^{-3n}(x+q-1)^n(y+q-1)^n(z+q-1)^n \\ + \ & (q^k-q)\big[q^{-2n}(xyz+(q-1)(x+y+z+q-2))^n \\ - \ & q^{-3n}(x+q-1)^n(y+q-1)^n(z+q-1)^n\big]\Big\}. \end{aligned}$$

Given G we can consider the code $C^\perp$ which assumes G as parity check matrix with the weight enumerator $W_{C^\perp}(t) = \sum_i A_i^\perp t^{n-i}$. Once again Mac-Williams Duality transforms the previous coorollary to this case.

Corollary 4.11 *Triple correlations between the coefficients of $W_{C^\perp}(t)$ are given by*

$$\begin{aligned} & \sigma(W_{C^\perp}(x), W_{C^\perp}(y), W_{C^\perp}(z)) = \sum_{i,j,l} \sigma(A_i^\perp, A_j^\perp, A_l^\perp) x^{n-i} y^{n-j} z^{n-l} \\ & = q^{-3k}(q-1)^2(q^k-1)\Bigg\{\big(xyz+(q-1)(x+y+z+q-2)\big)^n - (xyz)^n \\ & -((xy+q-1)^n - (xy)^n)z^n - ((yz+q-1)^n - (yz)^n)x^n \\ & -((zx+q-1)^n - (zx)^n)y^n + (q^k-q)\Big[(xyz+q-1)^n - (xyz)^n\Big]\Bigg\}. \end{aligned}$$

Bibliography

[1] V. Blinovsky, *Asymptotic combinatorial coding theory*, Kluwer Academic Publishers, Boston, MA, 1997.

[2] A. M. Borodin, *The law of large numbers and the central limit theorem for the jordan normal form of large triangular matrices over a finite field*, J. Math. Sci. **96** (1999), no. 5, 3455–3471.

[3] N. Bourbaki, *Lie groups and lie algebras chapters 4-6*, Elements of mathematics, Springer, Berlin, 2002.

[4] R. Carter, *Simple groups of lie type*, John Wiley and Sons, 1972.

[5] J. B. Conrey, D. W. Farmer, and J. P. Keating, *Integral moments of l-functions*, Proc. London Math. Soc. (3) **91** (2005), no. 1, 33–104.

[6] F. J. Dyson, *Statistical theory of the energy levels of complex systems. i-ii-iii.*, J. Mathematical Phys. **3** (1962), no. 3, 140,157,166.

[7] J. Fulman, P. M. Neumann, and C. E. Praeger, *A generating function approach to the enumeration of matrices in classical groups over finite fields*, Mem. Amer. Math. Soc. **176** (2005), no. 830, vi+90pp.

[8] P. Gabriel and A. V. Roiter, *Representations of finite dimensional algebras.*, second edition ed., Springer, Berlin, 1997.

[9] R. G. Gallager, *Low density parity-check codes*, M.I.T. Press, Cambridge, Massachusetts, 1963.

[10] I. M. Gelfand and V. A. Ponomarev, *Problems of linear algebra and classification of quadruples of subspaces in a finite-dimensional vector space*, Hilbert space operators and operator algebras (Proc. Internat. Conf., Tihany, 1970) **176** (1972), no. 830, 163–237.

[11] W. M. Y. Goh and E. A. Schmutz, *A central limit theorem on* $\mathrm{GL}_n(f_q)$, Random Structures Algorithms **2** (1991), no. 1, 47–53.

[12] V. Kac and P. Cheung, *Quantum calculus*, Universitext, Springer, Berlin, 2001.

[13] N. M. Katz, *Frobenius-schur indicator and the ubiquity of brock-granville quadratic excess. dedicated to professor chao ko on the occasion of his 90th birthday.*, Finite Fields Appl. **7** (2001), no. 1, 45–69.

[14] N. M. Katz and P. Sarnak, *Random matrices, frobenius eigenvalues, and monodromy.*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999.

[15] J. P. Keating and N. C. Snaith, *Random matrix theory and* $\zeta(1/2+it)$*.*, Comm. Math. Phys. **214** (2000), no. 1, 57–89.

[16] A. A. Klyachko, *Maple procedure for joint cumulant of ranks of triplet of column submatrices*, http://www.fen.bilkent.edu.tr/∼iozen.

[17] ______, *Meeting notes.*

[18] A. A. Klyachko and İ. Özen, *Correlations between the ranks of submatrices and weights of random codes.*, Finite Fields and Their Applications **DOI: 10.1016/j.ffa.2009.03.002**.

[19] F. J. MacWilliams, *A theorem on the distribution of weights of a systematic code*, Bell System Tech. J. **42** (1963), no. 1, 79–94.

[20] M. L. Mehta, *Random matrices*, 2nd ed. ed., Academic Press, Inc., Boston, MA, 1991.

[21] N. E. Mnëv, *The universality theorems on the classification problem of configuration varieties and convex polytopes varieties. topology and geometry—rohlin seminar, 527–543*, Lecture Notes in Math, 1346, Springer,, Berlin, 1988.

[22] H. L. Montgomery, *The pair correlation of the zeta function*, Proc. Sympos. Pure Math. **24** (1973), 181–193.

[23] P. M. Neumann and C. E. Praeger, *Cyclic matrices over finite fields*, J. London Math. Soc. **52** (1995), no. 2, 263–284.

[24] ______, *Cyclic matrices in classical groups over finite fields.*, J. Algebra **234** (2000), no. 2, 367–418.

[25] Z. Rudnick and P. Sarnak, *Zeros of principal l-functions and random matrix theory. a celebration of john f. nash.*, Duke Math. J. **81** (1996), no. 2, 269–322.

[26] R. Stong, *Some asymptotic results on finite vector spaces*, Adv. in Appl. Math. **9** (1988), no. 2, 167–199.

[27] M. A. Tsfasman and S. G. Vladuţ, *Algebraic geometric codes*, Kluwer Academic Publishers, Dordrecht, 1991.

[28] J. H. van Lint and R. M. Wilson, *A course in combinatorics.*, second edition ed., Cambridge University Press, Cambridge, 2001.

[29] T. Wadayama, *Asymptotic concentration behaviors of linear combinations of weight distributions on random linear code ensemble*, arXiv:0803.1025 (2008).

[30] G. E. Wall, *On the conjugacy classes in the unitary, symplectic and orthogonal groups*, J. Austral. Math. Soc. **3** (1963), 1–63.