Laws of matrices

Teo Banica

Department of Mathematics, University of Cergy-Pontoise, F-95000 Cergy-Pontoise, France. teo.banica@gmail.com

2010 *Mathematics Subject Classification.* 60C05

Key words and phrases. Infinite matrix, Random matrix

Abstract. This is an introduction to the laws of various types of matrices, and their computation, with all the needed preliminaries included. We first review the basics of probability theory, notably with the binomial and Poisson laws and their versions, and with a look into central limits too. Then we discuss the laws of the usual scalar matrices, which correspond to discrete probability theory, with theory and numerous examples. We then discuss the case of the random matrices, notably with the asymptotic results of Wigner and Marchenko-Pastur, and their versions. Finally, we have a look into operator algebras and free probability, and we discuss a number of more abstract matrices, having as entries random variables over various quantum spaces.

Preface

This is an introduction to the laws of various types of matrices, and their computation, with all needed preliminaries included. The book is organized in 4 parts, as follows:

I. We first review the basics of probability theory, notably with the binomial and Poisson laws and their versions, and with a look into central limits too.

II. Then we discuss the laws of the usual scalar matrices, which correspond to discrete probability theory, with theory and numerous examples.

III. We then discuss the case of the random matrices, notably with the asymptotic results of Wigner and Marchenko-Pastur, and their versions.

IV. Finally, we have a look into operator algebras and free probability, and we discuss matrices having as entries random variables over various quantum spaces.

Many thanks to my cats, for some help with navigating the quantum spaces.

Cergy, January 2026
Teo Banica

Contents

Part I

Discrete laws

CHAPTER 1

Binomial laws

1a. Coins and dice

You surely know a bit about random variables $f : X \to \mathbb{R}$, their means, also called expectations, $E(f) \in \mathbb{R}$, and about their variances $V(f) = E(f^2) - E(f)^2 \geq 0$ too. We will be talking about such things, and their generalizations, in this book.

Getting started now, there are many possible entry points to probability, with a quite standard one, focusing on the discrete case, which is the simplest, being as follows:

Definition 1.1. *A discrete probability space is a set X, usually finite or countable, whose elements $x \in X$ are called events, together with a function*

$$P : X \to [0, \infty)$$

called probability function, which is subject to the condition

$$\sum_{x \in X} P(x) = 1$$

telling us that the overall probability for something to happen is 1.

As a first comment, our condition $\sum_{x \in X} P(x) = 1$ perfectly makes sense, and this even if X is uncountable, because the sum of positive numbers is always defined, as a number in $[0, \infty]$, and this no matter how many positive numbers we have.

As a second comment, we have chosen in the above not to assume that X is finite or countable, and this for instance because we want to be able to regard any probability function on $\mathbb{N}$ as a probability function on $\mathbb{R}$, by setting $P(x) = 0$ for $x \notin \mathbb{N}$.

As a third comment, once we have a probability function $P : X \to [0, \infty)$ as above, with $P(x) \in [0, 1]$ telling us what the probability for an event $x \in X$ to happen is, we can compute what the probability for a set of events $Y \subset X$ to happen is, by setting:

$$P(Y) = \sum_{y \in Y} P(y)$$

But more on this, mathematical aspects of discrete probability theory, later, when further building on Definition 1.1. For the moment, what we have above will do.

With this discussed, let us explore now the basic examples, coming from the real life. And here, there are many things to be learned. As a first example, we have:

Example 1.2. *Flipping coins.*

Here things are simple and clear, because when you flip a coin the corresponding discrete probability space, together with its probability measure, is as follows:

$$X=\Big\{\text{heads, tails}\Big\}\quad,\quad P(\text{heads})=P(\text{tails})=\frac{1}{2}$$

In the case where the coin is biased, as to land on heads with probability $2/3$, and on tails with probability $1/3$, the corresponding probability space is as follows:

$$X=\Big\{\text{heads, tails}\Big\}\quad,\quad P(\text{heads})=\frac{2}{3}\quad,\quad P(\text{tails})=\frac{1}{3}$$

More generally, given any number $p\in[0,1]$, we have an abstract probability space as follows, where we have replaced heads and tails by win and lose:

$$X=\Big\{\text{win, lose}\Big\}\quad,\quad P(\text{win})=p\quad,\quad P(\text{lose})=1-p$$

Finally, things become more interesting when flipping a coin, biased or not, several times in a row. We will be back to this in a moment, with details.

Example 1.3. *Rolling dice.*

Again, things here are simple and clear, because when you throw a die the corresponding probability space, together with its probability measure, is as follows:

$$X=\Big\{1,\ldots,6\Big\}\quad,\quad P(i)=\frac{1}{6}\ ,\ \forall i$$

As before with coins, we can further complicate this by assuming that the die is biased, say landing on face i with probability $p_i\in[0,1]$. In this case the corresponding probability space, together with its probability measure, is as follows:

$$X=\Big\{1,\ldots,6\Big\}\quad,\quad P(i)=p_i\quad,\quad p_i\geq 0\ ,\ \sum_i p_i=1$$

Also as before with coins, things become more interesting when throwing a die several times in a row, or equivalently, when throwing several identical dice at the same time. In this latter case, with n identically biased dice, the probability space is as follows:

$$X=\Big\{1,\ldots,6\Big\}^n\quad,\quad P(i_1\ldots i_n)=p_{i_1}\ldots p_{i_n}\quad,\quad p_i\geq 0\ ,\ \sum_i p_i=1$$

Observe that the sum 1 condition in Definition 1.1 is indeed satisfied, and with this proving that our dice modeling is bug-free, due to the following computation:

$$\begin{aligned}\sum_{i\in X}P(i) &= \sum_{i_1,\ldots,i_n}P(i_1\ldots i_n)\\ &= \sum_{i_1,\ldots,i_n}p_{i_1}\ldots p_{i_n}\\ &= \sum_{i_1}p_{i_1}\ldots\sum_{i_n}p_{i_n}\\ &= 1\times\ldots\times 1\\ &= 1\end{aligned}$$

Getting back now to theory, in the general context of Definition 1.1, we can see that what we have there is very close to the biased die, from Example 1.3. Indeed, in the general context of Definition 1.1, we can say that what happens is that we have a die with $|X|$ faces, which is biased such that it lands on face i with probability $P(i)$.

Which is something quite interesting, allowing us to have some intuition on what is going on, in discrete probability. So, let us record this finding, as follows:

Conclusion 1.4. *Discrete probability can be understood as being about throwing a general die, having an arbitrary number of faces, and which is arbitrarily biased too.*

Finally, no discussion about games and probability would be complete without playing cards too. We have here the following result, of key importance in the real life:

Theorem 1.5. *The probabilities at poker are as follows:*

(1) *One pair:* 0.533.
(2) *Two pairs:* 0.120.
(3) *Three of a kind:* 0.053.
(4) *Full house:* 0.006.
(5) *Straight:* 0.005.
(6) *Four of a kind:* 0.001.
(7) *Flush:* 0.000.
(8) *Straight flush:* 0.000.

Proof. Let us consider indeed our deck of 32 cards:

$$\{7,8,9,10,J,Q,K,A\}\times\{\clubsuit,\diamondsuit,\heartsuit,\spadesuit\}$$

The total number of possibilities for a poker hand is:

$$\binom{32}{5}=\frac{32\cdot 31\cdot 30\cdot 29\cdot 28}{2\cdot 3\cdot 4\cdot 5}=32\cdot 31\cdot 29\cdot 7$$

(1) For having a pair, the number of possibilities is:

$$N = \binom{8}{1}\binom{4}{2} \times \binom{7}{3}\binom{4}{1}^3 = 8 \cdot 6 \cdot 35 \cdot 64$$

Thus, the probability of having a pair is:

$$P = \frac{8 \cdot 6 \cdot 35 \cdot 64}{32 \cdot 31 \cdot 29 \cdot 7} = \frac{6 \cdot 5 \cdot 16}{31 \cdot 29} = \frac{480}{899} = 0.533$$

(2) For having two pairs, the number of possibilities is:

$$N = \binom{8}{2}\binom{4}{2}^2 \times \binom{24}{1} = 28 \cdot 36 \cdot 24$$

Thus, the probability of having two pairs is:

$$P = \frac{28 \cdot 36 \cdot 24}{32 \cdot 31 \cdot 29 \cdot 7} = \frac{36 \cdot 3}{31 \cdot 29} = \frac{108}{899} = 0.120$$

(3) For having three of a kind, the number of possibilities is:

$$N = \binom{8}{1}\binom{4}{3} \times \binom{7}{2}\binom{4}{1}^2 = 8 \cdot 4 \cdot 21 \cdot 16$$

Thus, the probability of having three of a kind is:

$$P = \frac{8 \cdot 4 \cdot 21 \cdot 16}{32 \cdot 31 \cdot 29 \cdot 7} = \frac{3 \cdot 16}{31 \cdot 29} = \frac{48}{899} = 0.053$$

(4) For having full house, the number of possibilities is:

$$N = \binom{8}{1}\binom{4}{3} \times \binom{7}{1}\binom{4}{2} = 8 \cdot 4 \cdot 7 \cdot 6$$

Thus, the probability of having full house is:

$$P = \frac{8 \cdot 4 \cdot 7 \cdot 6}{32 \cdot 31 \cdot 29 \cdot 7} = \frac{6}{31 \cdot 29} = \frac{6}{899} = 0.006$$

(5) For having a straight, the number of possibilities is:

$$N = 4\left[\binom{4}{1}^4 - 4\right] = 16 \cdot 63$$

Thus, the probability of having a straight is:

$$P = \frac{16 \cdot 63}{32 \cdot 31 \cdot 29 \cdot 7} = \frac{9}{2 \cdot 31 \cdot 29} = \frac{9}{1798} = 0.005$$

(6) For having four of a kind, the number of possibilities is:

$$N = \binom{8}{1}\binom{4}{4} \times \binom{7}{1}\binom{4}{1} = 8 \cdot 7 \cdot 4$$

Thus, the probability of having four of a kind is:

$$P = \frac{8 \cdot 7 \cdot 4}{32 \cdot 31 \cdot 29 \cdot 7} = \frac{1}{31 \cdot 29} = \frac{1}{899} = 0.001$$

(7) For having a flush, the number of possibilities is:

$$N = 4\left[\binom{8}{4} - 4\right] = 4 \cdot 66$$

Thus, the probability of having a flush is:

$$P = \frac{4 \cdot 66}{32 \cdot 31 \cdot 29 \cdot 7} = \frac{33}{4 \cdot 31 \cdot 29 \cdot 7} = \frac{9}{25172} = 0.000$$

(8) For having a straight flush, the number of possibilities is:

$$N = 4 \cdot 4$$

Thus, the probability of having a straight flush is:

$$P = \frac{4 \cdot 4}{32 \cdot 31 \cdot 29 \cdot 7} = \frac{1}{2 \cdot 31 \cdot 29 \cdot 7} = \frac{1}{12586} = 0.000$$

Thus, we have obtained the numbers in the statement. □

So far, so good, but you might argue, what if we model our problem as for our poker hand to be ordered, do we still get the same answer? In answer, sure yes, but let us check this. The probability for having four of a kind, computed in this way, is then:

$$P(\text{four of a kind}) = \frac{8 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 28}{32 \cdot 31 \cdot 30 \cdot 29 \cdot 28} = \frac{1}{31 \cdot 29} = \frac{1}{899}$$

To be more precise, here on the bottom $32 \cdot 31 \cdot 30 \cdot 29 \cdot 28$ stands for the total number of possibilities for an ordered poker hand, 5 out of 32, and on top, exercise for you to figure out what the above numbers 8, 5, then $4 \cdot 3 \cdot 2$, and 28, stand for.

1b. Variables, laws

Moving ahead now, let us go back to the context of Definition 1.1, which is the most convenient one, technically speaking. As usual in probability, we are mainly interested in winning. But, winning what? In case we are dealing with a usual die, what we win is what the die says, and on average, what we win is the following quantity:

$$E = \frac{1 + 2 + 3 + 4 + 5 + 6}{6} = 3.5$$

In case we are dealing with the biased die in Example 1.3, again what we win is what the die says, and on average, what we win is the following quantity:

$$E = \sum_i i \times p_i$$

With this understood, what about coins? Here, before doing any computation, we have to assign some numbers to our events, and a standard choice here is as follows:

$$f:\Big\{\text{heads, tails}\Big\}\to\mathbb{R}\quad,\quad f(\text{heads})=1\quad,\quad f(\text{tails})=0$$

With this choice made, what we can expect to win is the following quantity:

$$\begin{aligned}E(f) &= f(\text{heads})\times P(\text{heads})+f(\text{tails})\times P(\text{tails})\\ &= 1\times\frac{1}{2}+0\times\frac{1}{2}\\ &= \frac{1}{2}\end{aligned}$$

Of course, in the case where the coin is biased, this computation will lead to a different outcome. And also, with a different convention for f, we will get a different outcome too. Moreover, we can combine if we want these two degrees of flexibility.

In short, you get the point. In order to do some math, in the context of Definition 1.1, we need a random variable $f:X\to\mathbb{R}$, and the math will consist in computing the expectation of this variable, $E(f)\in\mathbb{R}$. Alternatively, in order to do some business in the context of Definition 1.1, we need some form of "money", and our random variable $f:X\to\mathbb{R}$ will stand for that money, and then $E(f)\in\mathbb{R}$, for the average gain.

Let us axiomatize this situation as follows:

Definition 1.6. *A random variable on a probability space X is a function*

$$f:X\to\mathbb{R}$$

and the expectation of such a random variable is the quantity

$$E(f)=\sum_{x\in X}f(x)P(x)$$

which is best thought as being the average gain, when the game is played.

Here the word "game" refers to the probability space interpretation from Conclusion 1.4. Indeed, in that context, with our discrete set of events X being thought of as corresponding to a generalized die, and by thinking of f as representing some sort of money, the above quantity $E(f)$ is what we win, on average, when playing the game.

We have already seen some good illustrations for Definition 1.6, so time now to get into more delicate aspects. Imagine that you want to set up some sort of business, with your variable $f:X\to\mathbb{R}$. You are of course mostly interested in the expectation $E(f)\in\mathbb{R}$, but passed that, the way this expectation comes in matters too. For instance:

(1) When your variable is constant, $f=c$, you certainly have $E(f)=c$, and your business will run smoothly, with not so many surprises on the way.

(2) On the opposite, for a complicated variable satisfying $E(f) = c$, your business will be more bumpy, with wins or loses on the way, depending on your skills.

In short, and extrapolating now from business to mathematics, physics, chemistry and everything else, we must complement Definition 1.6 with something finer, regarding the "quality" of the expectation $E(f) \in \mathbb{R}$ appearing there. And the first thought here, which is the correct one, goes to the following number, called variance of our variable:

$$\begin{aligned} V(f) &= E\left((f - E(f))^2\right) \\ &= E(f^2) - E(f)^2 \end{aligned}$$

However, let us not stop here. For a total control of your business, be that of financial, mathematical, physical or chemical type, you will certainly want to know more about your variable $f : X \to \mathbb{R}$. Which leads us into general moments, constructed as follows:

Definition 1.7. *The moments of a variable $f : X \to \mathbb{R}$ are the numbers*

$$M_k = E(f^k)$$

which satisfy $M_0 = 1$, then $M_1 = E(f)$, and then $V(f) = M_2 - M_1^2$.

And, good news, with this we have all the needed tools in our bag for doing some good business. To put things in a very compacted way, M_0 is about foundations, M_1 is about running some business, M_2 is about running that business well, and M_3 and higher are advanced level, about ruining all the competing businesses.

As a further piece of basic probability, coming this time as a theorem, we have:

Theorem 1.8. *Given a random variable $f : X \to \mathbb{R}$, if we define its law as being*

$$\mu = \sum_{x \in X} P(x) \delta_{f(x)}$$

regarded as probability measure on $\mathbb{R}$, then the moments are given by the formula

$$E(f^k) = \int_{\mathbb{R}} y^k d\mu(y)$$

with the usual convention that each Dirac mass integrates up to 1.

Proof. There are several things going on here, the idea being as follows:

(1) To start with, given a random variable $f : X \to \mathbb{R}$, we can certainly talk about its law μ, as being the formal linear combination of Dirac masses in the statement. Our claim is that this is a probability measure on $\mathbb{R}$, in the sense of Definition 1.1. Indeed, the weight of each point $y \in \mathbb{R}$ is the following quantity, which is positive, as it should:

$$d\mu(y) = \sum_{f(x) = y} P(x)$$

Moreover, the total mass of this measure is 1, as it should, due to:

$$\begin{aligned}\sum_{y\in\mathbb{R}} d\mu(y) &= \sum_{y\in\mathbb{R}}\sum_{f(x)=y} P(x)\\ &= \sum_{x\in X} P(x)\\ &= 1\end{aligned}$$

Thus, we have indeed a probability measure on $\mathbb{R}$, in the sense of Definition 1.1.

(2) Still talking basics, let us record as well the following alternative formula for the law, which is clear from definitions, and that we will often use, in what follows:

$$\mu = \sum_{y\in\mathbb{R}} P(f=y)\delta_y$$

(3) Now let us compute the moments of f. With the usual convention that each Dirac mass integrates up to 1, as mentioned in the statement, we have:

$$\begin{aligned}E(f^k) &= \sum_{x\in X} P(x)f(x)^k\\ &= \sum_{y\in\mathbb{R}} y^k \sum_{f(x)=y} P(x)\\ &= \int_{\mathbb{R}} y^k d\mu(y)\end{aligned}$$

Thus, we are led to the conclusions in the statement. □

The above theorem is quite interesting, because we can see here a relation with integration, as we know it from calculus. In view of this, it is tempting to further go this way, by formulating the following definition, which is something purely mathematical:

Definition 1.9. *Given a set X, which can be finite, countable, or even uncountable, a discrete probability measure on it is a linear combination as follows,*

$$\mu = \sum_{x\in X} \lambda_x \delta_x$$

with the coefficients $\lambda_i \in \mathbb{R}$ satisfying $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$. For $f : X \to \mathbb{R}$ we set

$$\int_X f(x)d\mu(x) = \sum_{x\in X} \lambda_x f(x)$$

with the convention that each Dirac mass integrates up to 1.

Observe that, with this, we are now into pure mathematics. However, and we insist on this, it is basic probability, as developed before, which is behind all this. Now by staying abstract for a bit more, with Definition 1.9 in hand, we can recover our previous basic probability notions, from Definition 1.1 and from Theorem 1.8, as follows:

THEOREM 1.10. *With the above notion of discrete probability measure in hand:*

(1) *A discrete probability space is simply a space X, with a discrete probability measure on it ν. In this picture, the probability function is $P(x) = d\nu(x)$.*
(2) *Each random variable $f : X \to \mathbb{R}$ has a law, which is a discrete probability measure on $\mathbb{R}$. This law is given by $\mu = f_*\nu$, push-forward of ν by f.*

PROOF. This might look a bit scary, but is in fact a collection of trivialities, coming straight from definitions, the details being as follows:

(1) Nothing much to say here, with our assertion being plainly clear, just by comparing Definition 1.1 and Definition 1.9. As a interesting comment, however, in the general context of Definition 1.9, a probability measure $\mu = \sum_{x \in X} \lambda_x \delta_x$ as there depends only on the following function, called density of our probability measure:

$$\varphi : X \to \mathbb{R} \quad , \quad \varphi(x) = \lambda_x$$

And, with this notion in hand, our equation $P(x) = d\nu(x)$ simply says that the probability function P is the density of ν. Which is something which is good to know.

(2) Pretty much the same story here, with our first assertion being clear, just by comparing Theorem 1.8 and Definition 1.9. As for the second assertion, consider more generally a probability space (X, ν), and a function $f : X \to Y$. We can then construct a probability measure $\mu = f_*\nu$ on Y, called push-forward of ν by f, as follows:

$$\nu = \sum_{x \in X} \lambda_x \delta_x \implies \mu = \sum_{y \in Y} \left(\sum_{f(x) = y} \lambda_x \right) \delta_y$$

Alternatively, at the level of the corresponding measures of the parts $Z \subset Y$, we have the following abstract formula, which looks more conceptual:

$$\mu(Z) = \nu(f^{-1}(Z))$$

In any case, one way or another we can talk about push-forward measures $\mu = f_*\nu$, and in the case of a random variable $f : X \to \mathbb{R}$, we obtain in this way the law of f. □

Very nice all this, and needless to say, welcome to measure theory. In what follows we will rather go back to probability theory developed in the old way, as in the beginning of the present chapter, and keep developing that material, because we still have many interesting things to be learned. But, let us keep Definition 1.9 and Theorem 1.10, which are quite interesting, somewhere in our head. We will be back to these later.

1c. Independence

Let us talk now about the key notion in probability, which is independence. This appears for instance when flipping a coin k times in a row, and we first have here:

Proposition 1.11. *When flipping a coin k times, the following happen,*

1. *The probability of you winning $\$k$ is $1/2^k$.*
2. *The probability of you winning $\$k-1$ is 0.*
3. *The probability of you winning $\$k-2$ is $k/2^k$.*
4. *The probability of you winning $\$k-3$ is again 0.*
5. *The probability of you winning $\$k-4$ is $k(k-1)/2^{k+1}$.*

and so on, with the probability increasing, up to the tie situation, and then decreasing.

Proof. This follows indeed from some simple mathematics, as follows:

(1) You winning $\$k$ means you winning every time, over k attempts, so your probability here is $P=(1/2)\times\ldots\times(1/2)$, with k terms in the product, which reads $P=1/2^k$.

(2) The point here is that you cannot win $\$k-1$, exactly. Indeed, you must lose at least once, and so you profit will be $\leq(k-1)-1=k-2$.

(3) Here we have a similar computation as in (1). For winning $\$k-2$ you need to lose exactly once, and since there are k possibilities of losing exactly once, $P=k/2^k$.

(4) Here the situation is similar to that in (2). Indeed, for winning exactly $\$k-3$ you would certainly need to lose twice, so you profit will be $\leq(k-2)-2=k-4$.

(5) With the same reasoning as in (3), here you need to lose exactly twice, and since there are $k(k-1)/2$ possibilities of losing exactly twice, $P=k(k-1)/2^{k+1}$.

(6) Finally, regarding the last assertion, which is a bit informal, we will leave the clarification here, both statement and proof, to you, as an instructive exercise. □

Obviously, some interesting mathematics is going on here, that needs to be better understood. We have the following result, generalizing Proposition 1.11:

Theorem 1.12. *When flipping a coin k times what you can win are quantities of type $\$k-2s$, with $s=0,1,\ldots,k$, with the probability for this to happen being:*

$$P(k-2s)=\frac{1}{2^k}\binom{k}{s}$$

Geometrically, your winning curve starts with probability $1/2^k$ of winning $-\$k$, then increases up to the tie situation, and then decreases, up to probability $1/2^k$ of winning $\$k$.

PROOF. All this is quite clear, by fine-tuning our various observations from Proposition 1.11 and its proof, the point here being that, in order for you to win $k-s$ times and lose s times, over your k attempts, the number of possibilities is:

$$\binom{k}{s}=\frac{k!}{s!(k-s)!}$$

Thus, by dividing now by 2^k, which is the total number of possibilities, for the whole game, we are led to the probability in the statement, namely:

$$P(k-2s)=\frac{1}{2^k}\binom{k}{s}$$

Shall we doublecheck this? Sure yes, doublecheking is the first thing to be done, when you come across a theorem, in your mathematics. As a first check, the sum of probabilities that we found should be 1, which is intuitive, right, and 1 that is, as shown by:

$$\begin{aligned}\sum_{s=0}^k P(k-2s) &= \frac{1}{2^k}\sum_{s=0}^k\binom{k}{s}\\ &= \frac{1}{2^k}\sum_{s=0}^k\binom{k}{s}1^s1^{k-s}\\ &= \frac{1}{2^k}(1+1)^k\\ &= \frac{1}{2^k}\times 2^k\\ &= 1\end{aligned}$$

But shall we really trust this. Imagine for instance that you play your game for \$1000 instead of \$1 as basic gain, your life is obviously at stake, so all this is worth a second doublecheck, before being used in practice. So, as second doublecheck, let us verify that, on average, what you win is exactly \$0, which is something very intuitive, the game itself obviously not favoring you, nor your partner. But this can be checked as follows:

$$\begin{aligned}\sum_{s=0}^k P(k-2s)\times(k-2s) &= \frac{1}{2^k}\sum_{s=0}^k\binom{k}{s}(k-2s)\\ &= \frac{1}{2^k}\sum_{s=0}^k\binom{k}{s}(k-s)-\frac{1}{2^k}\sum_{s=0}^k\binom{k}{s}s\\ &= \frac{1}{2^k}\sum_{s=0}^k\binom{k}{s}(k-s)-\frac{1}{2^k}\sum_{t=0}^k\binom{k}{k-t}(k-t)\\ &= \frac{1}{2^k}\sum_{s=0}^k\binom{k}{s}(k-s)-\frac{1}{2^k}\sum_{t=0}^k\binom{k}{t}(k-t)\\ &= 0\end{aligned}$$

Summarizing, we have a good theorem here, proved, doublechecked and triplechecked, as per the highest scientific standards, ready to be used in practice. □

Motivated by the above, let us formulate now the following definition:

Definition 1.13. *Given $p\in[0,1]$, the Bernoulli law of parameter p is given by:*

$$P(\text{win})=p\quad,\quad P(\text{lose})=1-p$$

More generally, the k-th binomial law of parameter p, with $k\in\mathbb N$, is given by

$$P(s)=p^s(1-p)^{k-s}\binom{k}{s}$$

with the Bernoulli law appearing at $k=1$, with $s=1,0$ here standing for win and lose.

Let us try now to understand the relation between the Bernoulli and binomial laws. Indeed, we know that the Bernoulli laws produce the binomial laws, simply by iterating the game, from 1 throw to $k\in\mathbb N$ throws. Obviously, what matters in all this is the "independence" of our coin throws, so let us record this finding, as follows:

Theorem 1.14. *The following happen, in the context of the biased coin game:*

1. *The Bernoulli laws μ_{ber} produce the binomial laws μ_{bin}, by iterating the game $k\in\mathbb N$ times, via the independence of the throws.*
2. *We have in fact $\mu_{bin}=\mu_{ber}^{*k}$, with $*$ being the convolution operation for real probability measures, given by $\delta_x*\delta_y=\delta_{x+y}$, and linearity.*

Proof. Obviously, this is something a bit informal, but let us prove this as stated, and we will come back later to it, with precise definitions, general theorems and everything. In what regards the first assertion, nothing to be said there, this is what life teaches us. As for the second assertion, the formula $\mu_{bin}=\mu_{ber}^{*k}$ there certainly looks like mathematics, so job for us to figure out what this exactly means. And, this can be done as follows:

(1) The first idea is to encapsulate the data from Definition 1.13 into the probability measures associated to the Bernoulli and binomial laws. For the Bernoulli law, the corresponding measure is as follows, with the δ symbols standing for Dirac masses:

$$\mu_{ber}=(1-p)\delta_0+p\delta_1$$

As for the binomial law, here the measure is as follows, constructed in a similar way, you get the point I hope, again with the δ symbols standing for Dirac masses:

$$\mu_{bin}=\sum_{s=0}^k p^s(1-p)^{k-s}\binom{k}{s}\delta_s$$

(2) Getting now to independence, the point is that, as we will soon discover abstractly, the mathematics there is that of the following formula, with $*$ standing for the convolution operation for the real measures, which is given by $\delta_x*\delta_y=\delta_{x+y}$ and linearity:

$$\mu_{bin}=\underbrace{\mu_{ber}*\ldots*\mu_{ber}}_{k\ terms}$$

(3) To be more precise, this latter formula does hold indeed, as a straightforward application of the binomial formula, the formal proof being as follows:

$$\begin{aligned}
\mu_{ber}^{*k}
&= \big((1-p)\delta_0+p\delta_1\big)^{*k}\\
&= \sum_{s=0}^k p^s(1-p)^{k-s}\binom{k}{s}\delta_0^{*(k-s)}*\delta_1^{*s}\\
&= \sum_{s=0}^k p^s(1-p)^{k-s}\binom{k}{s}\delta_s\\
&= \mu_{bin}
\end{aligned}$$

(4) Summarizing, save for some uncertainties regarding what independence exactly means, mathematically speaking, and more on this in a moment, theorem proved. □

Getting to formal mathematical work now, let us start with the following straightforward definition, inspired by what happens for coins, dice and cards:

DEFINITION 1.15. *We say that two variables $f,g:X\to\mathbb R$ are independent when*

$$P(f=x,g=y)=P(f=x)P(g=y)$$

happens, for any $x,y\in\mathbb R$.

As already mentioned, this is something very intuitive, inspired by what happens for coins, dice and cards. As a first result now regarding independence, we have:

Theorem 1.16. *Assuming that $f,g:X\to\mathbb R$ are independent, we have:*

$$E(fg)=E(f)E(g)$$

More generally, we have the following formula, for the mixed moments,

$$E(f^kg^l)=E(f^k)E(g^l)$$

and the converse holds, in the sense that this formula implies the independence of f,g.

Proof. We have indeed the following computation, using the independence of f,g:

$$\begin{aligned}
E(f^kg^l)&=\sum_{xy}x^ky^lP(f=x,g=y)\\
&=\sum_{xy}x^ky^lP(f=x)P(g=y)\\
&=\sum_x x^kP(f=x)\sum_y y^lP(g=y)\\
&=E(f^k)E(g^l)
\end{aligned}$$

As for the last assertion, this is clear too, because having the above computation work, for any $k,l\in\mathbb N$, amounts in saying that the independence formula for f,g holds. □

Regarding now the convolution operation, motivated by what we found before, in Theorem 1.14, let us start with the following abstract definition:

Definition 1.17. *Given a space X with a sum operation $+$, we can define the convolution of any two discrete probability measures on it,*

$$\mu=\sum_i a_i\delta_{x_i}\quad,\quad\nu=\sum_j b_j\delta_{y_j}$$

as being the discrete probability measure given by the following formula:

$$\mu*\nu=\sum_{ij}a_ib_j\delta_{x_i+y_j}$$

That is, the convolution operation $*$ is defined by $\delta_x*\delta_y=\delta_{x+y}$, and linearity.

As a first observation, our operation is well-defined, with $\mu*\nu$ being indeed a discrete probability measure, because the weights are positive, $a_ib_j\geq0$, and their sum is:

$$\sum_{ij}a_ib_j=\sum_i a_i\sum_j b_j=1\times1=1$$

Also, the above definition agrees with what we did before with coins, and Bernoulli and binomial laws. We have in fact the following general result:

THEOREM 1.18. *Assuming that $f,g:X\to\mathbb R$ are independent, we have*

$$\mu_{f+g}=\mu_f*\mu_g$$

where $*$ is the convolution of real probability measures.

PROOF. We have indeed the following straightforward verification, based on the independence formula from Definition 1.15, and on Definition 1.17:

$$\begin{aligned}\mu_{f+g}&=\sum_{x\in\mathbb R}P(f+g=x)\delta_x\\&=\sum_{y,z\in\mathbb R}P(f=y,g=z)\delta_{y+z}\\&=\sum_{y,z\in\mathbb R}P(f=y)P(g=z)\delta_y*\delta_z\\&=\left(\sum_{y\in\mathbb R}P(f=y)\delta_y\right)*\left(\sum_{z\in\mathbb R}P(g=z)\delta_z\right)\\&=\mu_f*\mu_g\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Before going further, let us attempt as well to find a proof of Theorem 1.18, based on the moment characterization of independence, from Theorem 1.16. For this purpose, we will need the following standard fact, which is of certain theoretical interest:

THEOREM 1.19. *The sequence of moments*

$$M_k=\int_{\mathbb R}x^kd\mu(x)$$

uniquely determines the law.

PROOF. Indeed, assume that the law of our variable is as follows:

$$\mu=\sum_i\lambda_i\delta_{x_i}$$

The sequence of moments is then given by the following formula:

$$M_k=\sum_i\lambda_ix_i^k$$

But it is then standard calculus to recover the numbers $\lambda_i,x_i\in\mathbb R$, and so the measure μ, out of the sequence of numbers M_k. Indeed, assuming that the numbers x_i are $0<x_1<\ldots<x_n$ for simplifying, in the $k\to\infty$ limit we have the following formula:

$$M_k\sim\lambda_nx_n^k$$

Thus, we got the parameters $\lambda_n, x_n \in \mathbb{R}$ of our measure μ, and then by substracting them and doing an obvious recurrence, we get the other parameters $\lambda_i, x_i \in \mathbb{R}$ as well. We will leave the details here as an instructive exercise, and come back to this problem later in this book, with more advanced and clever methods for dealing with it. □

Getting back now to our philosophical question above, namely recovering Theorem 1.18 via moment technology, we can now do this, the result being as follows:

THEOREM 1.20. *Assuming that $f, g : X \to \mathbb{R}$ are independent, the measures*

$$\mu_{f+g} \quad , \quad \mu_f * \mu_g$$

have the same moments, and so, they coincide.

PROOF. We have the following computation, using the independence of f, g:

$$\begin{aligned} M_k(f+g) &= E((f+g)^k) \\ &= \sum_r \binom{k}{r} E(f^r g^{k-r}) \\ &= \sum_r \binom{k}{r} M_r(f) M_{k-r}(g) \end{aligned}$$

On the other hand, we have as well the following computation:

$$\begin{aligned} \int_X x^k d(\mu_f * \mu_g)(x) &= \int_{X \times X} (x+y)^k d\mu_f(x) d\mu_g(y) \\ &= \sum_r \binom{k}{r} \int_X x^r d\mu_f(x) \int_X y^{k-r} d\mu_g(y) \\ &= \sum_r \binom{k}{r} M_r(f) M_{k-r}(g) \end{aligned}$$

Thus, job done, and theorem proved, or rather Theorem 1.18 reproved. □

Getting back now to the basic theory of independence, here is now a second result, coming as a continuation of Theorem 1.18, which is something more advanced:

THEOREM 1.21. *Assuming that $f, g : X \to \mathbb{R}$ are independent, we have*

$$F_{f+g} = F_f F_g$$

where $F_f(x) = E(e^{ixf})$ is the Fourier transform.

PROOF. We have the following computation, using Theorem 1.18:

$$\begin{aligned} F_{f+g}(x) &= \int_X e^{ixz} d\mu_{f+g}(z) \\ &= \int_X e^{ixz} d(\mu_f * \mu_g)(z) \\ &= \int_{X\times X} e^{ix(z+t)} d\mu_f(z) d\mu_g(t) \\ &= \int_X e^{ixz} d\mu_f(z) \int_X e^{ixt} d\mu_g(t) \\ &= F_f(x) F_g(x) \end{aligned}$$

Thus, we are led to the conclusion in the statement. □

As a comment here, you might wonder what that $i \in \mathbb{C}$ number in the definition of the Fourier transform is good for. Good question, which will be answered, in due time.

1d. Binomial laws

Let us do now some computations. We recall from the above that the k-th binomial law of parameter $p \in (0,1)$, with $k \in \mathbb{N}$, is given by the following formula:

$$P(s) = p^s (1-p)^{k-s} \binom{k}{s}$$

As a first concrete result about these laws, we have:

THEOREM 1.22. *The mean of the k-th binomial law of parameter $p \in (0,1)$ is:*

$$E = kp$$

As for the variance and higher moments, these are given by similar formulae.

PROOF. In what regards the mean, this can be computed as follows:

$$\begin{aligned}
E &= \sum_{s=0}^{k} P(s)s \\
&= \sum_{s=0}^{k} p^s(1-p)^{k-s}\binom{k}{s}s \\
&= \sum_{s=1}^{k} p^s(1-p)^{k-s}\binom{k}{s}s \\
&= \sum_{s=1}^{k} p^s(1-p)^{k-s}\frac{k!}{(s-1)!(k-s)!} \\
&= k\sum_{s=1}^{k} p^s(1-p)^{k-s}\frac{(k-1)!}{(s-1)!(k-s)!} \\
&= k\sum_{r=0}^{k-1} p^{r+1}(1-p)^{k-r-1}\frac{(k-1)!}{r!(k-r-1)!} \\
&= kp\sum_{r=0}^{k-1} p^{r}(1-p)^{k-r-1}\frac{(k-1)!}{r!(k-r-1)!} \\
&= kp(p+(1-p))^{k-1} \\
&= kp
\end{aligned}$$

As for the higher moments, these can be computed in a similar way. □

1e. Exercises

Exercises:

EXERCISE 1.23.

EXERCISE 1.24.

EXERCISE 1.25.

EXERCISE 1.26.

EXERCISE 1.27.

EXERCISE 1.28.

EXERCISE 1.29.

EXERCISE 1.30.

Bonus exercise.

CHAPTER 2

Poisson laws

2a. Poisson laws

At a more advanced level, we have the Poisson Limit Theorem (PLT), that we would like to explain now. Let us start with the following definition:

Definition 2.1. *The Poisson law of parameter* 1 *is the following measure,*

$$p_1=\frac{1}{e}\sum_{k\in\mathbb N}\frac{\delta_k}{k!}$$

and the Poisson law of parameter $t>0$ *is the following measure,*

$$p_t=e^{-t}\sum_{k\in\mathbb N}\frac{t^k}{k!}\,\delta_k$$

with the letter "p" standing for Poisson.

As a first observation, the above laws have indeed mass 1, as they should, due to the following key formula, which is actually the key formula of all mathematics:

$$e^t=\sum_{k\in\mathbb N}\frac{t^k}{k!}$$

We will see in the moment why these measures appear a bit everywhere, in discrete contexts, the reasons for this coming from the Poisson Limit Theorem (PLT). Let us first develop some general theory. We first have the following result:

Theorem 2.2. *We have the following formula, for any* $s,t>0$*,*

$$p_s*p_t=p_{s+t}$$

so the Poisson laws form a convolution semigroup.

PROOF. By using $\delta_k * \delta_l = \delta_{k+l}$ and the binomial formula, we obtain:

$$\begin{aligned}
p_s * p_t &= e^{-s}\sum_k \frac{s^k}{k!}\,\delta_k * e^{-t}\sum_l \frac{t^l}{l!}\,\delta_l \\
&= e^{-s-t}\sum_n \delta_n \sum_{k+l=n}\frac{s^k t^l}{k!l!} \\
&= e^{-s-t}\sum_n \frac{\delta_n}{n!}\sum_{k+l=n}\frac{n!}{k!l!}s^k t^l \\
&= e^{-s-t}\sum_n \frac{(s+t)^n}{n!}\,\delta_n \\
&= p_{s+t}
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Next in line, we have the following result, which is fundamental as well:

THEOREM 2.3. *The Poisson laws appear as formal exponentials*

$$p_t = \sum_k \frac{t^k(\delta_1 - \delta_0)^{*k}}{k!}$$

with respect to the convolution of measures $*$.

PROOF. By using the binomial formula, the measure on the right is:

$$\begin{aligned}
\mu &= \sum_k \frac{t^k}{k!}\sum_{r+s=k}(-1)^s\frac{k!}{r!s!}\delta_r \\
&= \sum_k t^k \sum_{r+s=k}(-1)^s\frac{\delta_r}{r!s!} \\
&= \sum_r \frac{t^r\delta_r}{r!}\sum_s \frac{(-1)^s}{s!} \\
&= \frac{1}{e}\sum_r \frac{t^r\delta_r}{r!} \\
&= p_t
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

2b. Poisson limits

Regarding now the Fourier transform computation, this is as follows:

THEOREM 2.4. *The Fourier transform of p_t is given by*

$$F_{p_t}(y)=\exp\left((e^{iy}-1)t\right)$$

for any $t>0$.

PROOF. We have indeed the following computation:

$$\begin{aligned}F_{p_t}(y)&=e^{-t}\sum_k\frac{t^k}{k!}F_{\delta_k}(y)\\&=e^{-t}\sum_k\frac{t^k}{k!}\,e^{iky}\\&=e^{-t}\sum_k\frac{(e^{iy}t)^k}{k!}\\&=\exp(-t)\exp(e^{iy}t)\\&=\exp\left((e^{iy}-1)t\right)\end{aligned}$$

Thus, we obtain the formula in the statement. □

Observe that the above formula gives an alternative proof for Theorem 2.2, by using the fact that the logarithm of the Fourier transform linearizes the convolution. As another application, we can now establish the Poisson Limit Theorem, as follows:

THEOREM 2.5 (PLT). *We have the following convergence, in moments,*

$$\left(\left(1-\frac{t}{n}\right)\delta_0+\frac{t}{n}\,\delta_1\right)^{*n}\to p_t$$

for any $t>0$.

PROOF. Let us denote by ν_n the measure under the convolution sign, namely:

$$\nu_n=\left(1-\frac{t}{n}\right)\delta_0+\frac{t}{n}\,\delta_1$$

We have the following computation, for the Fourier transform of the limit:

$$\begin{aligned}F_{\delta_r}(y)=e^{iry}\quad&\implies\quad F_{\nu_n}(y)=\left(1-\frac{t}{n}\right)+\frac{t}{n}\,e^{iy}\\&\implies\quad F_{\nu_n^{*n}}(y)=\left(\left(1-\frac{t}{n}\right)+\frac{t}{n}\,e^{iy}\right)^n\\&\implies\quad F_{\nu_n^{*n}}(y)=\left(1+\frac{(e^{iy}-1)t}{n}\right)^n\\&\implies\quad F(y)=\exp\left((e^{iy}-1)t\right)\end{aligned}$$

Thus, we obtain indeed the Fourier transform of p_t, as desired. □

2c. Moments, partitions

At the level of moments now, things are quite subtle for Poisson laws. We first have the following result, dealing with the simplest case, where the parameter is $t = 1$:

THEOREM 2.6. *The moments of p_1 are the Bell numbers,*

$$M_k(p_1) = |P(k)|$$

where $P(k)$ is the set of partitions of $\{1, \ldots, k\}$.

PROOF. The moments of p_1 are given by the following formula:

$$M_k = \frac{1}{e}\sum_r \frac{r^k}{r!}$$

We therefore have the following recurrence formula for these moments:

$$\begin{aligned}
M_{k+1} &= \frac{1}{e}\sum_r \frac{(r+1)^{k+1}}{(r+1)!}\\
&= \frac{1}{e}\sum_r \frac{r^k}{r!}\left(1+\frac{1}{r}\right)^k\\
&= \frac{1}{e}\sum_r \frac{r^k}{r!}\sum_s \binom{k}{s} r^{-s}\\
&= \sum_s \binom{k}{s}\cdot\frac{1}{e}\sum_r \frac{r^{k-s}}{r!}\\
&= \sum_s \binom{k}{s} M_{k-s}
\end{aligned}$$

With this done, let us try now to find a recurrence for the Bell numbers:

$$B_k = |P(k)|$$

A partition of $\{1, \ldots, k+1\}$ appears by choosing s neighbors for 1, among the k numbers available, and then partitioning the $k - s$ elements left. Thus, we have:

$$B_{k+1} = \sum_s \binom{k}{s} B_{k-s}$$

Thus, our moments M_k satisfy the same recurrence as the numbers B_k. Regarding now the initial values, in what concerns the first moment of p_1, we have:

$$M_1 = \frac{1}{e}\sum_r \frac{r}{r!} = 1$$

Also, by using the above recurrence for the numbers M_k, we obtain from this:

$$M_2 = \sum_s \binom{1}{s} M_{k-s} = 1 + 1 = 2$$

On the other hand, $B_1 = 1$ and $B_2 = 2$. Thus we obtain $M_k = B_k$, as claimed. □

More generally now, we have the following result, dealing with the case $t > 0$:

THEOREM 2.7. *The moments of p_t with $t > 0$ are given by*

$$M_k(p_t) = \sum_{\pi \in P(k)} t^{|\pi|}$$

where $|.|$ is the number of blocks.

PROOF. The moments of the Poisson law p_t with $t > 0$ are given by:

$$M_k = e^{-t} \sum_r \frac{t^r r^k}{r!}$$

We have the following recurrence formula for these moments:

$$\begin{aligned} M_{k+1} &= e^{-t} \sum_r \frac{t^{r+1}(r+1)^{k+1}}{(r+1)!} \\ &= e^{-t} \sum_r \frac{t^{r+1} r^k}{r!} \left(1 + \frac{1}{r}\right)^k \\ &= e^{-t} \sum_r \frac{t^{r+1} r^k}{r!} \sum_s \binom{k}{s} r^{-s} \\ &= \sum_s \binom{k}{s} \cdot e^{-t} \sum_r \frac{t^{r+1} r^{k-s}}{r!} \\ &= t \sum_s \binom{k}{s} M_{k-s} \end{aligned}$$

Regarding now the initial values, the first moment of p_t is given by:

$$M_1 = e^{-t} \sum_r \frac{t^r r}{r!} = e^{-t} \sum_r \frac{t^r}{(r-1)!} = t$$

Now by using the above recurrence we obtain from this:

$$M_2 = t \sum_s \binom{1}{s} M_{k-s} = t(1 + t) = t + t^2$$

On the other hand, consider the numbers in the statement, namely:

$$S_k=\sum_{\pi\in P(k)}t^{|\pi|}$$

Since a partition of $\{1,\ldots,k+1\}$ appears by choosing s neighbors for 1, among the k numbers available, and then partitioning the $k-s$ elements left, we have:

$$S_{k+1}=t\sum_s\binom{k}{s}S_{k-s}$$

As for the initial values of these numbers, these are $S_1=t$, $S_2=t+t^2$. Thus the initial values coincide, and so these numbers are the moments of p_t, as stated. □

Summarizing, we have so far a quite good understanding of discrete probability theory. Of course, this is just the beginning of things, and we will be back to this, later.

2d. Cumulants, inversion

We have seen a lot of interesting combinatorics in this chapter, but this is not the end of the story. Following Rota, let us formulate now the following definition:

Definition 2.8. *Associated to any real probability measure $\mu=\mu_f$ is the following modification of the logarithm of the Fourier transform $F_\mu(\xi)=E(e^{i\xi f})$,*

$$K_\mu(\xi)=\log E(e^{\xi f})$$

called cumulant-generating function. The Taylor coefficients $k_n(\mu)$ of this series, given by

$$K_\mu(\xi)=\sum_{n=1}^\infty k_n(\mu)\,\frac{\xi^n}{n!}$$

are called cumulants of the measure μ. We also use the notations k_f,K_f for these cumulants and their generating series, where f is a variable following the law μ.

In other words, the cumulants are more or less the coefficients of the logarithm of the Fourier transform $\log F_\mu$, up to some normalizations. To be more precise, we have $K_\mu(\xi)=\log F_\mu(-i\xi)$, so the formula relating $\log F_\mu$ to the cumulants $k_n(\mu)$ is:

$$\log F_\mu(-i\xi)=\sum_{n=1}^\infty k_n(\mu)\,\frac{\xi^n}{n!}$$

Equivalently, the formula relating $\log F_\mu$ to the cumulants $k_n(\mu)$ is:

$$\log F_\mu(\xi)=\sum_{n=1}^\infty k_n(\mu)\,\frac{(i\xi)^n}{n!}$$

We will see in a moment the reasons for the above normalizations, namely change of variables $\xi\to-i\xi$, and Taylor coefficients instead of plain coefficients, the idea being that for simple laws like g_t, p_t, we will obtain in this way very simple quantities. Let us also mention that there is a reason for indexing the cumulants by $n = 1, 2, 3, \ldots$ instead of $n = 0, 1, 2, \ldots$, and more on this later, once we will have some theory and examples.

As a first observation, the sequence of cumulants $k_1, k_2, k_3, \ldots$ appears as a modification of the sequence of moments $M_1, M_2, M_3, \ldots$, the numerics being as follows:

PROPOSITION 2.9. *The sequence of cumulants $k_1, k_2, k_3, \ldots$ appears as a modification of the sequence of moments $M_1, M_2, M_3, \ldots$, and uniquely determines μ. We have*

$$\begin{aligned} k_1 &= M_1 \\ k_2 &= -M_1^2 + M_2 \\ k_3 &= 2M_1^3 - 3M_1M_2 + M_3 \\ k_4 &= -6M_1^4 + 12M_1^2M_2 - 3M_2^2 - 4M_1M_3 + M_4 \\ &\vdots \end{aligned}$$

in one sense, and in the other sense we have

$$\begin{aligned} M_1 &= k_1 \\ M_2 &= k_1^2 + k_2 \\ M_3 &= k_1^3 + 3k_1k_2 + k_3 \\ M_4 &= k_1^4 + 6k_1^2k_2 + 3k_2^2 + 4k_1k_3 + k_4 \\ &\vdots \end{aligned}$$

with in both cases the correspondence being polynomial, with integer coefficients.

PROOF. We know from Definition 2.8 that the cumulants are given by:

$$\log E(e^{\xi f}) = \sum_{s=1}^\infty k_s(f)\,\frac{\xi^s}{s!}$$

By exponentiating, we obtain from this the following formula:

$$E(e^{\xi f}) = \exp\left(\sum_{s=1}^\infty k_s(f)\,\frac{\xi^s}{s!}\right)$$

Now by looking at the terms of order $1, 2, 3, 4$, this gives the above formulae. $\square$

The interest in cumulants comes from the fact that $\log F_\mu$, and so the cumulants $k_n(\mu)$ too, linearize the convolution. To be more precise, we have the following result:

THEOREM 2.10. *The cumulants have the following properties:*

(1) $k_n(cf) = c^n k_n(f)$.
(2) $k_1(f + d) = k_1(f) + d$, *and* $k_n(f + d) = k_n(f)$ *for* $n > 1$.
(3) $k_n(f + g) = k_n(f) + k_n(g)$, *if* f, g *are independent.*

PROOF. Here (1) and (2) are both clear from definitions, because we have:

$$\begin{aligned} K_{cf+d}(\xi) &= \log E(e^{\xi(cf+d)}) \\ &= \log[e^{\xi d} \cdot E(e^{\xi cf})] \\ &= \xi d + K_f(c\xi) \end{aligned}$$

As for (3), this follows from the fact that the Fourier transform $F_f(\xi) = E(e^{i\xi f})$ satisfies the following formula, whenever f, g are independent random variables:

$$F_{f+g}(\xi) = F_f(\xi)F_g(\xi)$$

Indeed, by applying the logarithm, we obtain the following formula:

$$\log F_{f+g}(\xi) = \log F_f(\xi) + \log F_g(\xi)$$

With the change of variables $\xi \to -i\xi$, we obtain the following formula:

$$K_{f+g}(\xi) = K_f(\xi) + K_g(\xi)$$

Thus, at the level of coefficients, we obtain $k_n(f+g) = k_n(f) + k_n(g)$, as claimed. □

In order to get familiar with the cumulants, let us work out some examples. In what regards the basic probability measures, that we know so far, the cumulants are always given by simple formulae, as shown by the following result:

THEOREM 2.11. *The sequence of cumulants $k_1, k_2, k_3, \ldots$ is as follows:*

1. *For $\mu = \delta_c$ the cumulants are $c, 0, 0, \ldots$*
2. *For $\mu = g_t$ the cumulants are $0, t, 0, 0, \ldots$*
3. *For $\mu = p_t$ the cumulants are $t, t, t, \ldots$*

PROOF. We have 3 computations to be done, the idea being as follows:

(1) For $\mu = \delta_c$ we have the following computation:

$$\begin{aligned} K_\mu(\xi) &= \log E(e^{c\xi}) \\ &= \log(e^{c\xi}) \\ &= c\xi \end{aligned}$$

But the plain coefficients of this series are the numbers $c, 0, 0, \ldots$, and so the Taylor coefficients of this series are these same numbers $c, 0, 0, \ldots$, as claimed.

(2) For $\mu = g_t$ we have the following computation:

$$\begin{aligned} K_\mu(\xi) &= \log F_\mu(-i\xi) \\ &= \log \exp\left[-t(-i\xi)^2/2\right] \\ &= t\xi^2/2 \end{aligned}$$

But the plain coefficients of this series are the numbers $0, t/2, 0, 0, \ldots$, and so the Taylor coefficients of this series are the numbers $0, t, 0, 0, \ldots$, as claimed.

(3) For $\mu = p_t$ we have the following computation:

$$\begin{aligned}K_\mu(\xi) &= \log F_\mu(-i\xi)\\ &= \log\exp\left[(e^{i(-i\xi)}-1)t\right]\\ &= (e^\xi-1)t\end{aligned}$$

But the plain coefficients of this series are the numbers $t/n!$, and so the Taylor coefficients of this series are the numbers $t, t, t, \ldots$, as claimed. $\square$

Getting back now to general theory, the sequence of cumulants $k_1, k_2, k_3, \ldots$ appears as a modification of the sequence of moments $M_1, M_2, M_3, \ldots$, and understanding the relation between moments and cumulants will be our next task. We recall from Proposition 2.9 that we have the following formulae, for the cumulants in terms of moments:

$$k_1 = M_1$$

$$k_2 = -M_1^2 + M_2$$

$$k_3 = 2M_1^3 - 3M_1M_2 + M_3$$

$$k_4 = -6M_1^4 + 12M_1^2M_2 - 3M_2^2 - 4M_1M_3 + M_4$$

$$\vdots$$

Also, we have the following formulae, for the moments in terms of cumulants:

$$M_1 = k_1$$

$$M_2 = k_1^2 + k_2$$

$$M_3 = k_1^3 + 3k_1k_2 + k_3$$

$$M_4 = k_1^4 + 6k_1^2k_2 + 3k_2^2 + 4k_1k_3 + k_4$$

$$\vdots$$

In order to understand what exactly is going on, with moments and cumulants, which reminds a bit the Möbius inversion formula, we need to do some combinatorics, in relation with the set-theoretic partitions. We first have the following definition:

Definition 2.12. *The Möbius function of any lattice, and so of P, is given by*

$$\mu(\pi,\nu) = \begin{cases}1 & \text{if } \pi = \nu\\ -\sum_{\pi\leq\tau<\nu}\mu(\pi,\tau) & \text{if } \pi < \nu\\ 0 & \text{if } \pi \not\leq \nu\end{cases}$$

with the construction being performed by recurrence.

As an illustration here, for $P(2)=\{||,\sqcap\}$, we have by definition:

$$\mu(||,||)=\mu(\sqcap,\sqcap)=1$$

Also, $||<\sqcap$, with no intermediate partition in between, so we obtain:

$$\mu(||,\sqcap)=-\mu(||,||)=-1$$

Finally, we have $\sqcap\not\leq||$, and so we have as well the following formula:

$$\mu(\sqcap,||)=0$$

Thus, the Möbius matrix $M_{\pi\nu}=\mu(\pi,\nu)$ of the lattice $P(2)=\{||,\sqcap\}$ is as follows:

$$M=\begin{pmatrix}1&-1\\0&1\end{pmatrix}$$

At $k=3$ now, we have the following formula for the Möbius matrix $M_{\pi\nu}=\mu(\pi,\nu)$, once again written with the indices picked increasing in $P(3)=\{|||,\sqcap|,\sqcap\hskip-3.2mm{\ }_|\hskip0.5mm,|\sqcap,\sqcap\hskip-0.7mm\sqcap\}$:

$$M=\begin{pmatrix}1&-1&-1&-1&2\\0&1&0&0&-1\\0&0&1&0&-1\\0&0&0&1&-1\\0&0&0&0&1\end{pmatrix}$$

The main interest in the Möbius function comes from the Möbius inversion formula, which in linear algebra terms can be stated and proved as follows:

THEOREM 2.13. *We have the following implication,*

$$f(\pi)=\sum_{\nu\leq\pi}g(\nu)\quad\implies\quad g(\pi)=\sum_{\nu\leq\pi}\mu(\nu,\pi)f(\nu)$$

valid for any two functions $f,g:P(n)\to\mathbb{C}$.

PROOF. Consider the adjacency matrix of P, given by the following formula:

$$A_{\pi\nu}=\begin{cases}1&\text{if }\pi\leq\nu\\0&\text{if }\pi\not\leq\nu\end{cases}$$

Our claim is that the inverse of this matrix is the Möbius matrix of P, given by:

$$M_{\pi\nu}=\mu(\pi,\nu)$$

Indeed, the above matrix A is upper triangular, and when trying to invert it, we are led to the recurrence in Definition 2.12, so to the Möbius matrix M. Thus we have:

$$M=A^{-1}$$

Thus, in practice, we are led to the inversion formula in the statement. $\square$

As a first illustration, for $P(2)$ the formula $M = A^{-1}$ appears as follows:

$$\begin{pmatrix}1&-1\\0&1\end{pmatrix}=\begin{pmatrix}1&1\\0&1\end{pmatrix}^{-1}$$

At $k = 3$ now, the formula $M = A^{-1}$ for $P(3)$ reads:

$$\begin{pmatrix}1&-1&-1&-1&2\\0&1&0&0&-1\\0&0&1&0&-1\\0&0&0&1&-1\\0&0&0&0&1\end{pmatrix}=\begin{pmatrix}1&1&1&1&1\\0&1&0&0&1\\0&0&1&0&1\\0&0&0&1&1\\0&0&0&0&1\end{pmatrix}^{-1}$$

In general, the inversion formula $M = A^{-1}$ looks quite similar.

With these ingredients in hand, let us go back to probability. We first have:

Definition 2.14. *We define quantities $M_\pi(f), k_\pi(f)$, depending on partitions*

$$\pi \in P(k)$$

by starting with $M_n(f), k_n(f)$, and using multiplicativity over the blocks.

To be more precise, the convention here is that for the one-block partition $1_n \in P(n)$, the corresponding moment and cumulant are the usual ones, namely:

$$M_{1_n}(f) = M_n(f) \quad , \quad k_{1_n}(f) = k_n(f)$$

Then, for an arbitrary partition $\pi \in P(k)$, we decompose this partition into blocks, having sizes $b_1, \ldots, b_s$, and we set, by multiplicativity over blocks:

$$M_\pi(f) = M_{b_1}(f) \ldots M_{b_s}(f) \quad , \quad k_\pi(f) = k_{b_1}(f) \ldots k_{b_s}(f)$$

With this convention, following Rota and others, we can now formulate a key result, fully clarifying the relation between moments and cumulants, as follows:

Theorem 2.15. *We have the moment-cumulant formulae*

$$M_n(f) = \sum_{\nu \in P(n)} k_\nu(f) \quad , \quad k_n(f) = \sum_{\nu \in P(n)} \mu(\nu, 1_n) M_\nu(f)$$

or, equivalently, we have the moment-cumulant formulae

$$M_\pi(f) = \sum_{\nu \leq \pi} k_\nu(f) \quad , \quad k_\pi(f) = \sum_{\nu \leq \pi} \mu(\nu, \pi) M_\nu(f)$$

where μ is the Möbius function of $P(n)$.

Proof. There are several things going on here, the idea being as follows:

(1) According to our conventions above, the first set of formulae is equivalent to the second set of formulae. Also, due to the Möbius inversion formula, in the second set of formulae, the two formulae there are in fact equivalent. Thus, the 4 formulae in the statement are all equivalent. In what follows we will focus on the first 2 formulae.

(2) Let us first work out some examples. At $n = 1, 2, 3$ the moment formula gives the following equalities, which are in tune with the findings from Proposition 2.9:

$$M_1 = k_{|} = k_1$$

$$M_2 = k_{||} + k_{\sqcap} = k_1^2 + k_2$$

$$M_3 = k_{|||} + k_{\sqcap|} + k_{\overline{|\,|}\!\!\!\!\;|} + k_{|\sqcap} + k_{\sqcap\!\sqcap} = k_1^3 + 3k_1k_2 + k_3$$

At $n = 4$ now, which is a case which is of particular interest for certain considerations to follow, the computation is as follows, again in tune with Proposition 2.9:

$$\begin{aligned} M_4 &= k_{||||} + (\underbrace{k_{\sqcap||} + \ldots}_{6\ terms}) + (\underbrace{k_{\sqcap\sqcap} + \ldots}_{3\ terms}) + (\underbrace{k_{\sqcap\!\sqcap|} + \ldots}_{4\ terms}) + k_{\sqcap\!\sqcap\!\sqcap} \\ &= k_1^4 + 6k_1^2k_2 + 3k_2^2 + 4k_1k_3 + k_4 \end{aligned}$$

As for the cumulant formula, at $n = 1, 2, 3$ this gives the following formulae for the cumulants, again in tune with the findings from Proposition 2.9:

$$k_1 = M_{|} = M_1$$

$$k_2 = (-1)M_{||} + M_{\sqcap} = -M_1^2 + M_2$$

$$k_3 = 2M_{|||} + (-1)M_{\sqcap|} + (-1)M_{\overline{|\,|}\!\!\!\!\;|} + (-1)M_{|\sqcap} + M_{\sqcap\!\sqcap} = 2M_1^3 - 3M_1M_2 + M_3$$

Finally, at $n = 4$, after computing the Möbius function of $P(4)$, we obtain the following formula for the fourth cumulant, again in tune with Proposition 2.9:

$$\begin{aligned} k_4 &= (-6)M_{||||} + 2(\underbrace{M_{\sqcap||} + \ldots}_{6\ terms}) + (-1)(\underbrace{M_{\sqcap\sqcap} + \ldots}_{3\ terms}) + (-1)(\underbrace{M_{\sqcap\!\sqcap|} + \ldots}_{4\ terms}) + M_{\sqcap\!\sqcap\!\sqcap} \\ &= -6M_1^4 + 12M_1^2M_2 - 3M_2^2 - 4M_1M_3 + M_4 \end{aligned}$$

(3) Time now to get to work, and prove the result. As mentioned above, the formulae in the statement are all equivalent, and it is enough to prove the first one, namely:

$$M_n(f) = \sum_{\nu \in P(n)} k_\nu(f)$$

In order to do this, we use the very definition of the cumulants, namely:

$$\log E(e^{\xi f}) = \sum_{s=1}^\infty k_s(f)\,\frac{\xi^s}{s!}$$

By exponentiating, we obtain from this the following formula:

$$E(e^{\xi f})=\exp\left(\sum_{s=1}^\infty k_s(f)\,\frac{\xi^s}{s!}\right)$$

(4) Let us first compute the function on the left. This is easily done, as follows:

$$E(e^{\xi f})=E\left(\sum_{n=0}^\infty\frac{(\xi f)^n}{n!}\right)=\sum_{n=0}^\infty M_n(f)\,\frac{\xi^n}{n!}$$

(5) Regarding now the function on the right, this is given by:

$$\begin{aligned}\exp\left(\sum_{s=1}^\infty k_s(f)\,\frac{\xi^s}{s!}\right) &= \sum_{p=0}^\infty\frac{\left(\sum_{s=1}^\infty k_s(f)\,\frac{\xi^s}{s!}\right)^p}{p!}\\ &= \sum_{p=0}^\infty\frac{1}{p!}\sum_{s_1=1}^\infty k_{s_1}(f)\,\frac{\xi^{s_1}}{s_1!}\ldots\ldots\sum_{s_p=1}^\infty k_{s_p}(f)\,\frac{\xi^{s_p}}{s_p!}\\ &= \sum_{p=0}^\infty\frac{1}{p!}\sum_{s_1=1}^\infty\ldots\sum_{s_p=1}^\infty k_{s_1}(f)\ldots k_{s_p}(f)\,\frac{\xi^{s_1+\ldots+s_p}}{s_1!\ldots s_p!}\end{aligned}$$

But the point now is that all this leads us into partitions. Indeed, we are summing over indices $s_1,\ldots,s_p\in\mathbb{N}$, which can be thought of as corresponding to a partition of $n=s_1+\ldots+s_p$. So, let us rewrite our sum, as a sum over partitions. For this purpose, recall that the number of partitions $\nu\in P(n)$ having blocks of sizes $s_1,\ldots,s_p$ is:

$$\binom{n}{s_1,\ldots,s_p}=\frac{n!}{p_1!\ldots p_s!}$$

Also, when resumming over partitions, there will be a $p!$ factor as well, coming from the permutations of $s_1,\ldots,s_p$. Thus, our sum can be rewritten as follows:

$$\begin{aligned}\exp\left(\sum_{s=1}^\infty k_s(f)\,\frac{\xi^s}{s!}\right) &= \sum_{n=0}^\infty\sum_{p=0}^\infty\frac{1}{p!}\sum_{s_1+\ldots+s_p=n}k_{s_1}(f)\ldots k_{s_p}(f)\,\frac{\xi^n}{s_1!\ldots s_p!}\\ &= \sum_{n=0}^\infty\frac{\xi^n}{n!}\sum_{p=0}^\infty\frac{1}{p!}\sum_{s_1+\ldots+s_p=n}\binom{n}{s_1,\ldots,s_p}k_{s_1}(f)\ldots k_{s_p}(f)\\ &= \sum_{n=0}^\infty\frac{\xi^n}{n!}\sum_{\nu\in P(n)}k_\nu(f)\end{aligned}$$

(6) We are now in position to conclude. According to (3,4,5), we have:

$$\sum_{n=0}^\infty M_n(f)\,\frac{\xi^n}{n!}=\sum_{n=0}^\infty\frac{\xi^n}{n!}\sum_{\nu\in P(n)}k_\nu(f)$$

Thus, we have the following formula, valid for any $n \in \mathbb{N}$:

$$M_n(f) = \sum_{\nu \in P(n)} k_\nu(f)$$

We are therefore led to the conclusions in the statement. □

2e. Exercises

Exercises:

Exercise 2.16.

Exercise 2.17.

Exercise 2.18.

Exercise 2.19.

Exercise 2.20.

Exercise 2.21.

Exercise 2.22.

Exercise 2.23.

Bonus exercise.

CHAPTER 3

Advanced laws

3a. Pascal distributions

We would like to discuss now some technical generalizations of the main laws that we saw so far, namely the binomial ones and the Poisson ones. Let us start with:

THEOREM 3.1. *We have the generalized binomial formula*

$$(1+x)^a = \sum_{k=0}^{\infty} \binom{a}{k} x^k$$

with the generalized binomial coefficients being given by

$$\binom{a}{k} = \frac{a(a-1)\ldots(a-k+1)}{k!}$$

valid for any exponent $a \in \mathbb{Z}$, and any $|x| < 1$.

PROOF. This is something quite tricky, the idea being as follows:

(1) For exponents $a \in \mathbb{N}$, this is something that we know well, and which is valid for any $x \in \mathbb{R}$, coming from the usual binomial formula, namely:

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$$

(2) For the exponent $a = -1$ this is something that we know well too, coming from the following formula, valid for any $|x| < 1$:

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + \ldots$$

Indeed, this is exactly our generalized binomial formula at $a = -1$, because:

$$\binom{-1}{k} = \frac{(-1)(-2)\ldots(-k)}{k!} = (-1)^k$$

(3) Let us discuss now the general case $a \in -\mathbb{N}$. With $a = -n$, and $n \in \mathbb{N}$, the generalized binomial coefficients are given by the following formula:

$$\begin{aligned}\binom{-n}{k} &= \frac{(-n)(-n-1)\ldots(-n-k+1)}{k!}\\ &= (-1)^k\frac{n(n+1)\ldots(n+k-1)}{k!}\\ &= (-1)^k\frac{(n+k-1)!}{(n-1)!k!}\\ &= (-1)^k\binom{n+k-1}{n-1}\end{aligned}$$

Thus, our generalized binomial formula at $a = -n$, and $n \in \mathbb{N}$, reads:

$$\frac{1}{(1+t)^n} = \sum_{k=0}^{\infty}(-1)^k\binom{n+k-1}{n-1}t^k$$

(4) In order to prove this formula, it is convenient to write it with $-t$ instead of t, in order to get rid of signs. The formula to be proved becomes:

$$\frac{1}{(1-t)^n} = \sum_{k=0}^{\infty}\binom{n+k-1}{n-1}t^k$$

We prove this by recurrence on n. At $n = 1$ this formula definitely holds, as explained in (2) above. So, assume that the formula holds at $n \in \mathbb{N}$. We have then:

$$\begin{aligned}\frac{1}{(1-t)^{n+1}} &= \frac{1}{1-t}\cdot\frac{1}{(1-t)^n}\\ &= \sum_{k=0}^{\infty}t^k\sum_{l=0}^{\infty}\binom{n+l-1}{n-1}t^l\\ &= \sum_{s=0}^{\infty}t^s\sum_{l=0}^{s}\binom{n+l-1}{n-1}\end{aligned}$$

On the other hand, the formula that we want to prove is:

$$\frac{1}{(1-t)^{n+1}} = \sum_{s=0}^{\infty}\binom{n+s}{n}t^k$$

Thus, in order to finish, we must prove the following formula:

$$\sum_{l=0}^{s}\binom{n+l-1}{n-1} = \binom{n+s}{n}$$

(5) In order to prove this latter formula, we proceed by recurrence on $s \in \mathbb{N}$. At $s = 0$ the formula is trivial, $1 = 1$. So, assume that the formula holds at $s \in \mathbb{N}$. In order to prove the formula at $s+1$, we are in need of the following formula:

$$\binom{n+s}{n} + \binom{n+s}{n-1} = \binom{n+s+1}{n}$$

But this is the Pascal formula, that we know well, and we are done. □

Getting now to probability, we can talk about Pascal laws, and their properties.

3b. Compound Poisson

In relation with Poisson laws, we have work to do too. Indeed, we have the following notion, extending the Poisson limit theory developed in the previous section:

Definition 3.2. *Associated to any compactly supported positive measure ν on $\mathbb{C}$, not necessarily of mass 1, is the probability measure*

$$p_\nu = \lim_{n\to\infty} \left(\left(1 - \frac{t}{n}\right)\delta_0 + \frac{1}{n}\nu \right)^{*n}$$

where $t = mass(\nu)$, called compound Poisson law.

In what follows we will be mainly interested in the case where the measure ν is discrete, as is for instance the case for $\nu = t\delta_1$ with $t > 0$, which produces the Poisson laws. The following standard result allows one to detect compound Poisson laws:

Proposition 3.3. *For $\nu = \sum_{i=1}^s t_i \delta_{z_i}$ with $t_i > 0$ and $z_i \in \mathbb{C}$, we have*

$$F_{p_\nu}(y) = \exp\left(\sum_{i=1}^s t_i (e^{iyz_i} - 1) \right)$$

where F denotes the Fourier transform.

Proof. Let η_n be the measure in Definition 3.2, under the convolution sign:

$$\eta_n = \left(1 - \frac{t}{n}\right)\delta_0 + \frac{1}{n}\nu$$

We have then the following computation:

$$F_{\eta_n}(y) = \left(1 - \frac{t}{n}\right) + \frac{1}{n}\sum_{i=1}^s t_i e^{iyz_i} \implies F_{\eta_n^{*n}}(y) = \left(\left(1 - \frac{t}{n}\right) + \frac{1}{n}\sum_{i=1}^s t_i e^{iyz_i} \right)^n$$

$$\implies F_{p_\nu}(y) = \exp\left(\sum_{i=1}^s t_i (e^{iyz_i} - 1) \right)$$

Thus, we have obtained the formula in the statement. □

We have as well the following result, providing an alternative to Definition 3.2, and which will be our formulation here of the Compound Poisson Limit Theorem:

THEOREM 3.4 (CPLT). *For $\nu=\sum_{i=1}^s t_i\delta_{z_i}$ with $t_i>0$ and $z_i\in\mathbb C$, we have*

$$p_\nu=\mathrm{law}\left(\sum_{i=1}^s z_i\alpha_i\right)$$

where the variables α_i are Poisson (t_i), independent.

PROOF. Let α be the sum of Poisson variables in the statement, namely:

$$\alpha=\sum_{i=1}^s z_i\alpha_i$$

By using some standard Fourier transform formulae, we have:

$$F_{\alpha_i}(y)=\exp(t_i(e^{iy}-1))\implies F_{z_i\alpha_i}(y)=\exp(t_i(e^{iyz_i}-1))$$
$$\implies F_\alpha(y)=\exp\left(\sum_{i=1}^s t_i(e^{iyz_i}-1)\right)$$

Thus we have indeed the same formula as in Proposition 3.3, as desired. □

At the level of main examples of compound Poisson laws, we have:

DEFINITION 3.5. *The Bessel law of level $s\in\mathbb N\cup\{\infty\}$ and parameter $t>0$ is*

$$b_t^s=p_{t\varepsilon_s}$$

with ε_s being the uniform measure on the s-th roots of unity. The measures

$$b_t=b_t^2\quad,\quad B_t=b_t^\infty$$

are called real Bessel law, and complex Bessel law.

In practice now, we can study the above measures b_t^s in our standard way, meaning density, moments, Fourier, semigroup property, limiting theorems, and other aspects. In what regards limiting theorems, the measures b_t^s appear by definition via the CPLT, so done with that. As a consequence of this, however, let us record the following fact:

PROPOSITION 3.6. *The Bessel laws are given by*

$$b_t^s=\mathrm{law}\left(\sum_{k=1}^s w^ka_k\right)$$

where $a_1,\ldots,a_s$ are Poisson (t) independent, and $w=e^{2\pi i/s}$.

PROOF. This follows indeed from Theorem 3.4. □

As a first basic theoretical result about the Bessel laws, we have:

THEOREM 3.7. *The generalized Bessel laws b_t^s have the property*

$$b_t^s * b_{t'}^s = b_{t+t'}^s$$

so they form a truncated one-parameter semigroup with respect to convolution.

PROOF. This follows indeed from the Fourier transform formula from Proposition 3.3, because for the Bessel laws, the log of this Fourier transform is linear in t. □

Regarding now the moments, the result here is as follows:

THEOREM 3.8. *The moments of the Bessel law b_t^s are the numbers*

$$M_k = |P^s(k)|$$

where $P^s(k)$ is the set of partitions of $\{1,\ldots,k\}$ satisfying

$$\#\circ = \#\bullet\,(s)$$

as a weighted sum, in each block.

PROOF. We already know that the formula in the statement holds indeed at $s=1$, where $b_t^1 = p_t$ is the Poisson law of parameter $t>0$, and where $P^1 = P$ is the set of all partitions. At $s=2$ we have $P^2 = P_{even}$, and the result is elementary as well, from what we have in the above. In general, this follows by doing some standard combinatorics. □

We would like to develop now some more theory for the Bessel laws. First, it is convenient to introduce as well modified versions of these laws, as follows:

DEFINITION 3.9. *The Bessel and modified Bessel laws are given by*

$$b_t^s = \mathrm{law}\left(\sum_{k=1}^s w^k a_k\right) \quad , \quad \tilde{b}_t^s = \mathrm{law}\left(\sum_{k=1}^s w^k a_k\right)^s$$

where $a_1,\ldots,a_s$ are independent random variables, each of them following the Poisson law of parameter t/s, and $w = e^{2\pi i/s}$.

As a first remark, at $s=1$ we get the Poisson law of parameter t:

$$b_t^1 = \tilde{b}_t^1 = e^{-t}\sum_{r=0}^\infty \frac{t^r}{r!}\,\delta_r$$

We will need in our computations the level s exponential function, given by:

$$\exp_s z = \sum_{k=0}^\infty \frac{z^{sk}}{(sk)!}$$

We have the following formula, in terms of root of unity $w = e^{2\pi i/s}$:

$$\exp_s z = \frac{1}{s}\sum_{k=1}^s \exp(w^k z)$$

Observe also that at $s=1,2$ we have the following formulae:

$$\exp_1=\exp\quad,\quad\exp_2=\cosh$$

We have the following result, regarding both the plain and modified Bessel laws, which is a more explicit version of Proposition 3.3, for the Bessel laws:

THEOREM 3.10. *The Fourier transform of b_t^s is given by*

$$\log F_t^s(z)=t\,(\exp_s z-1)$$

so in particular the measures b_t^s are additive with respect to t.

PROOF. Consider, as in Proposition 3.6, the following variable:

$$a=\sum_{k=1}^s w^k a_k$$

We have the following computation, for the corresponding Fourier transform:

$$\begin{aligned}\log F_a(z)&=\sum_{k=1}^s\log F_{a_k}(w^kz)\\&=\sum_{k=1}^s\frac{t}{s}\big(\exp(w^kz)-1\big)\end{aligned}$$

But this gives the following formula, in terms of the above function $\exp_s$:

$$\begin{aligned}\log F_a(z)&=t\left(\left(\frac{1}{s}\sum_{k=1}^s\exp(w^kz)\right)-1\right)\\&=t\,(\exp_s(z)-1)\end{aligned}$$

Now since b_t^s is the law of a, this gives the formula in the statement. □

Let us study now the densities of $b_t^s,\tilde{b}_t^s$. We have here the following result:

THEOREM 3.11. *We have the formulae*

$$b_t^s=e^{-t}\sum_{p_1=0}^\infty\ldots\sum_{p_s=0}^\infty\frac{1}{p_1!\ldots p_s!}\left(\frac{t}{s}\right)^{p_1+\ldots+p_s}\delta\left(\sum_{k=1}^s w^kp_k\right)$$

$$\tilde{b}_t^s=e^{-t}\sum_{p_1=0}^\infty\ldots\sum_{p_s=0}^\infty\frac{1}{p_1!\ldots p_s!}\left(\frac{t}{s}\right)^{p_1+\ldots+p_s}\delta\left(\sum_{k=1}^s w^kp_k\right)^s$$

where $w=e^{2\pi i/s}$, and the δ symbol is a Dirac mass.

PROOF. It is enough to prove the formula for b_t^s. For this purpose, we compute the Fourier transform of the measure on the right. This is given by:

$$\begin{aligned}
F(z) &= e^{-t}\sum_{p_1=0}^\infty\ldots\sum_{p_s=0}^\infty\frac{1}{p_1!\ldots p_s!}\left(\frac{t}{s}\right)^{p_1+\ldots+p_s}F\delta\left(\sum_{k=1}^s w^kp_k\right)(z)\\
&= e^{-t}\sum_{p_1=0}^\infty\ldots\sum_{p_s=0}^\infty\frac{1}{p_1!\ldots p_s!}\left(\frac{t}{s}\right)^{p_1+\ldots+p_s}\exp\left(\sum_{k=1}^s w^kp_kz\right)\\
&= e^{-t}\sum_{r=0}^\infty\left(\frac{t}{s}\right)^r\sum_{\Sigma p_i=r}\frac{\exp\left(\sum_{k=1}^s w^kp_kz\right)}{p_1!\ldots p_s!}
\end{aligned}$$

We multiply by e^t, and we compute the derivative with respect to t:

$$\begin{aligned}
(e^tF(z))' &= \sum_{r=1}^\infty\frac{r}{s}\left(\frac{t}{s}\right)^{r-1}\sum_{\Sigma p_i=r}\frac{\exp\left(\sum_{k=1}^s w^kp_kz\right)}{p_1!\ldots p_s!}\\
&= \frac{1}{s}\sum_{r=1}^\infty\left(\frac{t}{s}\right)^{r-1}\sum_{\Sigma p_i=r}\left(\sum_{l=1}^s p_l\right)\frac{\exp\left(\sum_{k=1}^s w^kp_kz\right)}{p_1!\ldots p_s!}\\
&= \frac{1}{s}\sum_{r=1}^\infty\left(\frac{t}{s}\right)^{r-1}\sum_{\Sigma p_i=r}\sum_{l=1}^s\frac{\exp\left(\sum_{k=1}^s w^kp_kz\right)}{p_1!\ldots p_{l-1}!(p_l-1)!p_{l+1}!\ldots p_s!}
\end{aligned}$$

By using the variable $u=r-1$, we get:

$$\begin{aligned}
(e^tF(z))' &= \frac{1}{s}\sum_{u=0}^\infty\left(\frac{t}{s}\right)^u\sum_{\Sigma q_i=u}\sum_{l=1}^s\frac{\exp\left(w^lz+\sum_{k=1}^s w^kq_kz\right)}{q_1!\ldots q_s!}\\
&= \left(\frac{1}{s}\sum_{l=1}^s\exp(w^lz)\right)\left(\sum_{u=0}^\infty\left(\frac{t}{s}\right)^u\sum_{\Sigma q_i=u}\frac{\exp\left(\sum_{k=1}^s w^kq_kz\right)}{q_1!\ldots q_s!}\right)\\
&= (\exp_s z)(e^tF(z))
\end{aligned}$$

On the other hand, consider the following function:

$$\Phi(t)=\exp(t\exp_s z)$$

This function satisfies as well the equation found above, namely:

$$\Phi'(t)=(\exp_s z)\Phi(t)$$

We conclude from this that we have the following equality of functions:

$$e^tF(z)=\Phi(t)$$

But this gives the following formula, for the logarithm of the Fourier transform:

$$\begin{aligned}\log F &= \log(e^{-t}\exp(t\exp_s z))\\ &= \log(\exp(t(\exp_s z - 1)))\\ &= t(\exp_s z - 1)\end{aligned}$$

Thus, we are led to the formulae in the statement. □

3c. Hypergeometric laws

We can talk about hypergeometric laws. Again, we will be back to this.

3d. Beta distributions

Finally, we can talk about beta distributions. We will be back to this.

3e. Exercises

Exercises:

Exercise 3.12.

Exercise 3.13.

Exercise 3.14.

Exercise 3.15.

Exercise 3.16.

Exercise 3.17.

Exercise 3.18.

Exercise 3.19.

Bonus exercise.

CHAPTER 4

Central limits

4a. Central limits

We have seen that some interesting theory can be developed for the discrete measures, notably with a lot of exciting results regarding the Poisson laws, and their versions.

However, we cannot leave basic probability without talking, in one form or another, about central limits. You have certainly heard about bell-shaped curves, and perhaps even observed them in physics or chemistry class, because any routine measurement leads to such curves. Mathematically, here is the question that we would like to solve:

QUESTION 4.1. *Given random variables $f_1, f_2, f_3, \ldots$, say taken discrete, which are i.i.d., centered, and with common variance $t > 0$, do we have*

$$\frac{1}{\sqrt{n}}\sum_{i=1}^n f_i \sim g_t$$

in the $n \to \infty$ limit, for some bell-shaped density g_t? And, what is the formula of g_t?

Observe that this question perfectly makes sense, with the probability theory that we know, by assuming that our random variables $f_1, f_2, f_3, \ldots$ are discrete, as said above. As for the $1/\sqrt{n}$ factor, there is certainly need for a normalization factor there, as for things to have a chance to converge, and the good factor is $1/\sqrt{n}$, as shown by:

PROPOSITION 4.2. *In order for a sum of the following type to have a chance to converge, with $f_1, f_2, f_3, \ldots$ being i.i.d., centered, and with common variance $t > 0$,*

$$S = \sum_{i=1}^n f_i$$

we must normalize this sum by a $1/\sqrt{n}$ factor, as in Question 4.1.

PROOF. The idea here is to look at the moments of S. Since all variables f_i are centered, $E(f_i) = 0$, so is their sum, $E(S) = 0$, and no contradiction here. However, when looking at the variance of S, which equals the second moment, due to $E(S) = 0$, things become interesting, due to the following computation:

$$\begin{aligned} V(S) &= E(S^2) \\ &= E\left(\sum_{ij} f_i f_j\right) \\ &= \sum_{ij} E(f_i f_j) \\ &= \sum_i E(f_i^2) + \sum_{i\neq j} E(f_i)E(f_j) \\ &= \sum_i E(f_i^2) \\ &= nt \end{aligned}$$

Thus, we are in need a normalization factor α, in order for our sum to have a chance to converge. But, repeating the computation with S replaced by αS gives:

$$V(\alpha S) = \alpha^2 nt$$

Thus, the good normalization factor is $\alpha = 1/\sqrt{n}$, as claimed. □

So far, so good, we have a nice problem above, and time now to make a plan, in order to solve it. With the tools that we have, from this book so far, here is such a plan:

PLAN 4.3. *In order to solve our central limiting question, we have to:*

(1) *Apply Fourier and let $n \to \infty$, as to compute the Fourier transform of g_t.*
(2) *Do some combinatorics and calculus, as to compute the moments of g_t.*
(3) *Recover g_t out of its moments, again via combinatorics and calculus.*

Getting to work now, let us start with (1). Things are quickly done here, by using the standard linearization results for convolution, which lead to:

THEOREM 4.4. *Given discrete variables $f_1, f_2, f_3, \ldots$, which are i.i.d., centered, and with common variance $t > 0$, we have*

$$\frac{1}{\sqrt{n}} \sum_{i=1}^n f_i \sim g_t$$

with $n \to \infty$, with g_t being the law having $F(x) = e^{-tx^2/2}$ as Fourier transform.

PROOF. There are several things going on here, the idea being as follows:

(1) Observe first that in terms of moments, the Fourier transform of an arbitrary random variable $f : X \to \mathbb{R}$ is given by the following formula:

$$\begin{aligned} F_f(x) &= E(e^{ixf}) \\ &= E\left(\sum_{k=0}^\infty \frac{(ixf)^k}{k!}\right) \\ &= \sum_{k=0}^\infty \frac{(ix)^k E(f^k)}{k!} \\ &= \sum_{k=0}^\infty \frac{i^k M_k(f)}{k!}\, x^k \end{aligned}$$

(2) In particular, in the case of a centered variable, $E(f) = 0$, as those that we are interested in, the Fourier transform formula that we get is as follows:

$$F_f(x) = 1 - \frac{M_2(f)}{2} \cdot x^2 - i\,\frac{M_3(f)}{6} \cdot x^3 + \ldots$$

Moreover, by further assuming that the Fourier variable is small, $x \simeq 0$, the Fourier transform formula that we get, that we will use in what follows, becomes:

$$F_f(x) = 1 - \frac{M_2(f)}{2} \cdot x^2 + O(x^2)$$

(3) In addition to this, we will also need to know what happens to the Fourier transform when rescaling. But the formula here is very easy to find, as follows:

$$\begin{aligned} F_{\alpha f}(x) &= E(e^{ix\alpha f}) \\ &= E(e^{i\alpha x f}) \\ &= F_f(\alpha x) \end{aligned}$$

(4) Good news, we can now do our computation. By using the above formulae in (2) and (3), the Fourier transform of the variable in the statement is given by:

$$\begin{aligned} F(x) &= \left[F_f\left(\frac{x}{\sqrt{n}}\right)\right]^n \\ &= \left[1 - \frac{M_2(f)}{2} \cdot \frac{x^2}{n} + O(n^{-2})\right]^n \\ &= \left[1 - \frac{tx^2}{2n} + O(n^{-2})\right]^n \\ &\simeq \left[1 - \frac{tx^2}{2n}\right]^n \\ &\simeq e^{-tx^2/2} \end{aligned}$$

(3) We are therefore led to the conclusion in the statement, modulo the fact that we do not know yet that a density g_t having as Fourier transform $F(x) = e^{-tx^2/2}$ really exists, plus perhaps some other abstract issues, related to the continuous measures, to be discussed too. But too late to go back, both cat and sailors are happy, we will go ahead. So, theorem proved, modulo finding that law g_t, which still remains to be done. $\square$

Getting now to step (2) of our Plan 4.3, that is easy to work out too, via some elementary one-variable calculus, with the result here being as follows:

THEOREM 4.5. *The "normal" law g_t, having as Fourier transform*

$$F(x) = e^{-tx^2/2}$$

must have all odd moments zero, and its even moments must be the numbers

$$M_k(g_t) = t^{k/2} \times k!!$$

where $k!! = (k-1)(k-3)(k-5)\ldots$, for $k \in 2\mathbb{N}$.

PROOF. Again, several things going on here, the idea being as follows:

(1) To start with, at the level of formalism and notations, in view of Question 4.1 and of Theorem 4.4, we have adopted the term "normal" for the mysterious law g_t that we are looking for, the one having $F(x) = e^{-tx^2/2}$ as Fourier transform.

(2) Getting towards the computation of the moments, as a first useful observation, according to Theorem 4.4 this normal law g_t must be centered, as shown by:

$$\begin{aligned} f_i = \text{centered} \quad &\implies \quad \sum_{i=1}^n f_i = \text{centered} \\ &\implies \quad \frac{1}{\sqrt{n}} \sum_{i=1}^n f_i = \text{centered} \\ &\implies \quad g_t = \text{centered} \end{aligned}$$

Moreover, the same argument works by replacing "centered" with "having an even function as density", and this shows, via some standard calculus, that we will leave here as an exercise, that the odd moments of our normal law must vanish:

$$M_{2l+1}(g_t) = 0$$

Thus, first assertion proved, and we only have to care about the even moments.

(3) As a comment here, as we will see in a moment, our study below of the moments computes in fact the odd moments too, as being all equal to 0, this time without making reference to Theorem 4.4. Thus, definitely no worries with the odd moments.

(4) Getting to work now, we must reformulate the equation $F(x)=e^{-tx^2/2}$, in terms of moments. We know from the proof of Theorem 4.4 that we have:

$$F(x)=\sum_{k=0}^\infty\frac{i^kM_k(g_t)}{k!}\,x^k$$

On the other hand, we have the following formula, for the exponential:

$$e^{-tx^2/2}=\sum_{r=0}^\infty(-1)^r\frac{t^rx^{2r}}{2^rr!}$$

Thus, our equation $F(x)=e^{-tx^2/2}$ takes the following form:

$$\sum_{k=0}^\infty\frac{i^kM_k(g_t)}{k!}\,x^k=\sum_{r=0}^\infty(-1)^r\frac{t^rx^{2r}}{2^rr!}$$

(5) As a first observation, the odd moments must vanish, as said in (2) above. As for the even moments, these can be computed as follows:

$$\begin{aligned}
M_k(g_t)&=k!\times\frac{t^{k/2}}{2^{k/2}(k/2)!}\\
&=t^{k/2}\times\frac{k!}{2^{k/2}(k/2)!}\\
&=t^{k/2}\times\frac{2\cdot3\cdot4\ldots(k-1)\cdot k}{2\cdot4\cdot6\ldots(k-2)\cdot k}\\
&=t^{k/2}\times3\cdot5\ldots(k-3)(k-1)\\
&=t^{k/2}\times k!!
\end{aligned}$$

Thus, we are led to the formula in the statement. □

The moment formula that we found is quite interesting, and before going ahead with step (3) of our Plan 4.3, let us look a bit at this, and see what we can further say.

To be more precise, in analogy with what we know about the Poisson laws, and about the Bessel laws too, making reference to interesting combinatorics and partitions, when it comes to moments, we have the following result, regarding the normal laws:

THEOREM 4.6. *The moments of the normal law g_t are given by*

$$M_k(g_t)=t^{k/2}|P_2(k)|$$

for any $k\in\mathbb N$, with $P_2(k)$ standing for the pairings of $\{1,\ldots,k\}$.

Proof. This is a reformulation of Theorem 4.5, the idea being as follows:

(1) We know from Theorem 4.5 that the moments of the normal law $M_k = M_k(g_t)$ that we are interested in are given by the following formula, with the convention $k!! = 0$ for k odd, and $k!! = (k-1)(k-3)(k-5)\ldots$ for k even, for the double factorials:

$$M_k(g_t) = t^{k/2} \times k!!$$

Now observe that, according to our above convention for the double factorials, these are subject to the following recurrence relation, with initial data $1!! = 0, 2!! = 1$:

$$k!! = (k-1)(k-2)!!$$

We conclude that the moments of the normal law $M_k = M_k(g_t)$ are subject to the following recurrence relation, with initial data $M_1 = 0, M_2 = t$:

$$M_k = t(k-1)M_{k-2}$$

(2) On the other hand, let us first count the pairings of the set $\{1, \ldots, k\}$. In order to have such a pairing, we must pair 1 with one of the numbers $2, \ldots, k$, and then use a pairing of the remaining $k-2$ numbers. Thus, we have the following recurrence formula for the number P_k of such pairings, with the initial data $P_1 = 0, P_2 = 1$:

$$P_k = (k-1)P_{k-2}$$

Now by multiplying by $t^{k/2}$, the resulting numbers $N_k = t^{k/2}P_k$ will be subject to the following recurrence relation, with initial data $N_1 = 0, N_2 = t$:

$$N_k = t(k-1)N_{k-2}$$

(3) Thus, the moments $M_k = M_k(g_t)$ and the numbers $N_k = t^{k/2}P_k$ are subject to the same recurrence relation, with the same initial data, so they are equal, as claimed. □

Still in analogy with what we know about the Poisson laws, and about the Bessel laws too, we can further process what we found in Theorem 4.6, and we are led to:

Theorem 4.7. *The moments of the normal law g_t are given by*

$$M_k(g_t) = \sum_{\pi \in P_2(k)} t^{|\pi|}$$

where $P_2(k)$ is the set of pairings of $\{1, \ldots, k\}$, and $|.|$ is the number of blocks.

Proof. This is a quick reformulation of Theorem 4.6, with the number of blocks of a pairing of $\{1, \ldots, k\}$ being trivially $k/2$, independently of the pairing. □

It is possible to do some more combinatorics here, again in relation with what we know about the Poisson laws, for instance by looking at cumulants, and we have:

Theorem 4.8. *The cumulants of the normal law g_t are the following numbers:*

$$0, t, 0, 0, \ldots$$

In particular, the normal laws satisfy $g_s * g_t = g_{s+t}$, for any $s, t > 0$.

Proof. We have two assertions here, the idea being as follows:

(1) For the normal law g_t we have the following computation:

$$\begin{aligned} K_\mu(\xi) &= \log F_\mu(-i\xi) \\ &= \log \exp\left[-t(-i\xi)^2/2\right] \\ &= t\xi^2/2 \end{aligned}$$

But the plain coefficients of this series are the numbers $0, t/2, 0, 0, \ldots$, and so the Taylor coefficients of this series are the numbers $0, t, 0, 0, \ldots$, as claimed.

(2) As for the last assertion, regarding the semigroup property of the normal laws, this actually follows from Theorem 4.4, the log of the Fourier transform being linear in t, but is best seen by looking at the cumulants, which are obviously linear in t.

(3) However, as a technical remark here, the linearization results for the convolution that we have, be them in terms of the Fourier transform, or of the cumulants, were formally established before only for the discrete measures. So, instead of further thinking at all this, let us pull out a third, elementary proof for $g_s * g_t = g_{s+t}$.

(4) In order to do this, consider, as in Theorem 4.4, on one hand i.i.d. centered variables $f_1, f_2, f_3, \ldots$ having variance $s > 0$, and on the other hand i.i.d. centered variables $h_1, h_2, h_3, \ldots$ having variance $t > 0$. According to Theorem 16.4, we have:

$$\frac{1}{\sqrt{n}}\sum_{i=1}^n f_i \sim g_s \quad , \quad \frac{1}{\sqrt{n}}\sum_{i=1}^n h_i \sim g_t$$

Now let us sum these formulae. Assuming that the variables $f_1, f_2, f_3, \ldots$ that we used were independent from the variables $h_1, h_2, h_3, \ldots$, we obtain in this way:

$$\frac{1}{\sqrt{n}}\sum_{i=1}^n (f_i + h_i) \sim g_s * g_t$$

On the other hand, yet another application of Theorem 4.4, with the remark that by independence, the variance of $f_i + h_i$ is indeed $s + t$, gives the following formula:

$$\frac{1}{\sqrt{n}}\sum_{i=1}^n (f_i + h_i) \sim g_{s+t}$$

Thus, we are led to the semigroup formula $g_s * g_t = g_{s+t}$, as desired. □

As a philosophical conclusion now to all this, let us formulate:

CONCLUSION 4.9. *The normal laws g_t have properties which are quite similar to those of the Poisson laws p_t, and combinatorially, the passage*

$$p_t \to g_t$$

appears by replacing the partitions with the pairings.

Which sounds quite conceptual, and promising, hope you agree with me. In the meantime, however, we still need to know what the density of g_t is.

4b. Normal laws

So, let us get now to step (3) of our Plan 4.3. This does not look obvious at all, but some partial integration know-how leads us to the following statement:

THEOREM 4.10. *The normal laws are given by*

$$g_t = \frac{1}{\sqrt{2t} \cdot I} \, e^{-x^2/2t} dx$$

with the constant on the bottom being $I = \int_{\mathbb{R}} e^{-x^2} dx$.

PROOF. This comes from partial integration, as follows:

(1) Let us first do a naive computation. Consider the following quantities:

$$M_k = \int_{\mathbb{R}} x^k e^{-x^2} dx$$

It is quite obvious that by partial integration we will get a recurrence formula for these numbers, similar to the one that we have for the moments of the normal laws. So, let us do this. By partial integration we obtain the following formula, for any $k \in \mathbb{N}$:

$$\begin{aligned} M_k &= -\frac{1}{2} \int_{\mathbb{R}} x^{k-1} \left(e^{-x^2} \right)' dx \\ &= \frac{1}{2} \int_{\mathbb{R}} (k-1) x^{k-2} e^{-x^2} dx \\ &= \frac{k-1}{2} \cdot M_{k-2} \end{aligned}$$

(2) Thus, we are on the good way, with the recurrence formula that we got being the same as that for the moments of $g_{1/2}$. Now let us fine-tune this, as to reach to the same recurrence as for the moments of g_t. Consider the following quantities:

$$N_k = \int_{\mathbb{R}} x^k e^{-x^2/2t} dx$$

By partial integration as before, we obtain the following formula:

$$\begin{aligned} N_k &= \int_{\mathbb{R}} (tx^{k-1}) \left(-e^{-x^2/2t}\right)' dx \\ &= \int_{\mathbb{R}} t(k-1)x^{k-2}e^{-x^2/2t}dx \\ &= t(k-1)\int_{\mathbb{R}} x^{k-2}e^{-x^2/2t}dx \\ &= t(k-1)N_{k-2} \end{aligned}$$

(3) Thus, almost done, and it remains to discuss normalization. We know from the above that we must have a formula as follows, with I_t being a certain constant:

$$g_t = \frac{1}{I_t} \cdot e^{-x^2/2t}\, dx$$

But the constant I_t must be the one making g_t of mass 1, and so:

$$\begin{aligned} I_t &= \int_{\mathbb{R}} e^{-x^2/2t}\, dx \\ &= \int_{\mathbb{R}} e^{-2ty^2/2t}\sqrt{2t}dy \\ &= \sqrt{2t}\int_{\mathbb{R}} e^{-y^2}dy \end{aligned}$$

Thus, we are led to the formula in the statement. □

What we did in the above is good work, and it remains to compute the constant I appearing in Theorem 4.10, given by the following formula, and called Gauss integral:

$$I = \int_{\mathbb{R}} e^{-x^2}dx$$

With some advanced integration know-how, this can be done, as follows:

THEOREM 4.11. *We have the following formula,*

$$\int_{\mathbb{R}} e^{-x^2}dx = \sqrt{\pi}$$

called Gauss integral formula.

PROOF. As already mentioned, this is something which is nearly impossible to prove, with bare hands. However, this can be proved by using two dimensions, as follows:

$$\begin{aligned}
\int_{\mathbb{R}}\int_{\mathbb{R}} e^{-x^2-y^2}dxdy &= 4\int_0^\infty\int_0^\infty e^{-x^2-y^2}dxdy \\
&= 4\int_0^\infty\int_0^\infty e^{-t^2y^2-y^2}ydtdy \\
&= 4\int_0^\infty\int_0^\infty ye^{-y^2(1+t^2)}dydt \\
&= 2\int_0^\infty\int_0^\infty\left(-\frac{e^{-y^2(1+t^2)}}{1+t^2}\right)'dydt \\
&= 2\int_0^\infty\frac{dt}{1+t^2} \\
&= 2\int_0^\infty(\arctan t)'dt \\
&= \pi
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Very nice, so as a final conclusion to our study, started long ago, in the beginning of this chapter, we can now formulate the Central Limit Theorem (CLT), as follows:

THEOREM 4.12 (CLT). *Given discrete random variables $f_1, f_2, f_3, \ldots$, which are i.i.d., centered, and with common variance $t > 0$, we have*

$$\frac{1}{\sqrt{n}}\sum_{i=1}^n f_i \sim g_t$$

in the $n \to \infty$ limit, in moments, with the limiting mesure being

$$g_t = \frac{1}{\sqrt{2\pi t}}e^{-x^2/2t}dx$$

called normal, or Gaussian law of parameter $t > 0$.

PROOF. This follows indeed from our various results above, and more specifically from Theorem 4.4, Theorem 4.5 for the terminology, Theorem 4.10 and Theorem 4.11. □

Let us study now more in detail the laws that we found. Normally we already have everything that is needed, but it is instructive at this point to do some computations, based on the explicit formula of g_t found above, and on Theorem 4.11. We first have:

PROPOSITION 4.13. *We have the variance formula*

$$V(g_t) = t$$

valid for any $t > 0$.

PROOF. We already know this, but we can establish this as well directly, starting from our formula of g_t from Theorem 4.12. Indeed, the first moment is 0, because our normal law g_t is centered. As for the second moment, this can be computed as follows:

$$\begin{aligned} M_2 &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} x^2 e^{-x^2/2t}dx \\ &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} (tx)\left(-e^{-x^2/2t}\right)' dx \\ &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} te^{-x^2/2t}dx \\ &= t \end{aligned}$$

We conclude from this that the variance is $V = M_2 = t$, as claimed. □

More generally, we can recover in this way the computation of all moments:

THEOREM 4.14. *The even moments of the normal law are the numbers*

$$M_k(g_t) = t^{k/2} \times k!!$$

where $k!! = (k-1)(k-3)(k-5)\ldots$, *and the odd moments vanish.*

PROOF. Again, we already know this, but we can establish this as well directly, starting from our formula above of g_t. Indeed, we have the following computation:

$$\begin{aligned} M_k &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} y^k e^{-y^2/2t}dy \\ &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} (ty^{k-1})\left(-e^{-y^2/2t}\right)' dy \\ &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} t(k-1)y^{k-2}e^{-y^2/2t}dy \\ &= t(k-1)\times\frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} y^{k-2}e^{-y^2/2t}dy \\ &= t(k-1)M_{k-2} \end{aligned}$$

Thus by recurrence, we are led to the formula in the statement. □

Here is another result, which is the key one for the study of the normal laws:

THEOREM 4.15. *We have the following formula, valid for any* $t > 0$*:*

$$F_{g_t}(x) = e^{-tx^2/2}$$

In particular, the normal laws satisfy $g_s * g_t = g_{s+t}$, *for any* $s, t > 0$.

PROOF. As before, we already know this, but we can establish now the Fourier transform formula as well directly, by using the explicit formula of g_t, as follows:

$$\begin{aligned} F_{g_t}(x) &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} e^{-y^2/2t+ixy}dy \\ &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} e^{-(y/\sqrt{2t}-\sqrt{t/2}ix)^2-tx^2/2}dy \\ &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} e^{-z^2-tx^2/2}\sqrt{2t}dz \\ &= \frac{1}{\sqrt{\pi}}e^{-tx^2/2}\int_{\mathbb{R}} e^{-z^2}dz \\ &= e^{-tx^2/2} \end{aligned}$$

As for the last assertion, this follows from the fact that $\log F_{g_t}$ is linear in t. □

Observe that, thinking retrospectively, the above computation formally solves the question raised by Theorem 4.4, and so could have been used there, afterwards. However, and here comes the point, all this is based on Theorem 4.11, and also, crucially, on our work from Theorem 4.10, which in turn was based on moments and so on.

4c. Complex variables

Let us discuss now the complex analogues of all the above, with a notion of complex normal, or Gaussian law. To start with, we have the following definition:

DEFINITION 4.16. *A complex random variable is a variable $f : X \to \mathbb{C}$. In the discrete case, the law of such a variable is the complex probability measure*

$$\mu = \sum_i \alpha_i \delta_{z_i} \quad , \quad \alpha_i \geq 0 \quad , \quad \sum_i \alpha_i = 1 \quad , \quad z_i \in \mathbb{C}$$

given by the following formula, with P being the probability over X,

$$\mu = \sum_{z \in \mathbb{C}} P(f = z)\delta_z$$

with the sum being finite or countable, as per our discreteness assumption.

In order to understand the precise relation with the real theory, that we know well, we can decompose any complex variable $f : X \to \mathbb{C}$ as a sum, as follows:

$$f = g + ih \quad , \quad g = Re(f), \ h = Im(f)$$

With this done, we have the following computation, for the corresponding law:

$$\begin{aligned}\mu &= \sum_{z\in\mathbb{C}} P(f=z)\delta_z\\ &= \sum_{x,y\in\mathbb{R}} P(f=x+iy)\delta_{x+iy}\\ &= \sum_{x,y\in\mathbb{R}} P(g+ih=x+iy)\delta_{x+iy}\\ &= \sum_{x,y\in\mathbb{R}} P(g=x,h=y)\delta_{x+iy}\end{aligned}$$

In the case where the real and imaginary parts $g,h:X\to\mathbb{R}$ are independent, we can say more about this, with the above computation having the following continuation:

$$\begin{aligned}\mu &= \sum_{x,y\in\mathbb{R}} P(g=x,h=y)\delta_{x+iy}\\ &= \sum_{x,y\in\mathbb{R}} P(g=x)P(h=y)\delta_{x+iy}\\ &= \sum_{x,y\in\mathbb{R}} P(g=x)P(h=y)\delta_x*\delta_{iy}\\ &= \left(\sum_{x\in\mathbb{R}} P(g=x)\delta_x\right)*\left(\sum_{y\in\mathbb{R}} P(h=y)\delta_{iy}\right)\\ &= \mu_g * i\mu_h\end{aligned}$$

To be more precise, we have used here in the beginning the independence of the variables $h,g:X\to\mathbb{R}$, and at the end we have denoted the measure on the right, which is obtained from μ_h by putting this measure on the imaginary axis, by $i\mu_h$.

All this is quite interesting, going beyond what we know so far about basic probability, in the real case, so let us record this finding, along with a bit more, as follows:

THEOREM 4.17. *For a discrete complex random variable $f:X\to\mathbb{C}$, decomposed into real and imaginary parts as $f=g+ih$, and with g,h assumed independent, we have*

$$\mu_f=\mu_g*i\mu_h$$

with $*$ being the usual convolution operation, $\delta_z*\delta_t=\delta_{z+t}$, and with $\mu\to i\mu$ denoting the rotated version, $\mathbb{R}\to i\mathbb{R}$. If g,h are not independent, this formula does not hold.

PROOF. We already know that the first assertion holds, as explained in the above. As for the second assertion, this follows by carefully examining the above computation.

Indeed, we have used only at one point the independence of g, h, so for the formula $\mu_f = \mu_g * i\mu_h$ to hold, the equality used at that point, which is as follows, must hold:

$$\sum_{x,y\in\mathbb{R}} P(g = x, h = y)\delta_{x+iy} = \sum_{x,y\in\mathbb{R}} P(g = x)P(h = y)\delta_{x+iy}$$

But this is the same as saying that the following must hold, for any x, y:

$$P(g = x, h = y) = P(g = x)P(h = y)$$

We conclude that, in order for the decomposition formula $\mu_f = \mu_g * i\mu_h$ to hold, the real and imaginary parts $g, h : X \to \mathbb{R}$ must be independent, as stated. □

Going now to the point, probabilistic limiting theorems, let us discuss the complex analogue of the CLT. We have the following statement, to start with:

THEOREM 4.18. *Given discrete complex variables $f_1, f_2, f_3, \ldots$ whose real and imaginary parts are i.i.d., centered, and with common variance $t > 0$, we have*

$$\frac{1}{\sqrt{n}}\sum_{i=1}^{n} f_i \sim C_t$$

with $n \to \infty$, in moments, where C_t is the law of a complex variable whose real and imaginary parts are independent, and each following the law g_t.

PROOF. This follows indeed from the real CLT, established in Theorem 4.12, simply by taking the real and imaginary parts of all the variables involved. □

It is tempting at this point to call Theorem 4.18 the complex CLT, or CCLT, but before doing that, let us study a bit more all this. We would like to have a better understanding of the limiting law C_t at the end, and for this purpose, let us look at a sum as follows, with a, b being real independent variables, both following the normal law g_t:

$$c = a + ib$$

To start with, this variable is centered, in a complex sense, because we have:

$$\begin{aligned} E(c) &= E(a + ib) \\ &= E(a) + iE(b) \\ &= 0 + i \cdot 0 \\ &= 0 \end{aligned}$$

Regarding now the variance, things are more complicated, because the usual variance formula from the real case, which is $V(c) = E(c^2)$ in the centered case, will not provide us with a positive number, in the case where our variable is not real. So, in order to have a variance which is real, and positive too, we must rather use a formula of type

$V(c) = E(|c|^2)$, in the centered case. And, with this convention for the variance, we have then the following computation, for the variance of the above variable c:

$$\begin{aligned} V(c) &= E(|c|^2) \\ &= E(a^2 + b^2) \\ &= E(a^2) + E(b^2) \\ &= V(a^2) + V(b^2) \\ &= t + t \\ &= 2t \end{aligned}$$

But this suggests to divide everything by $\sqrt{2}$, as to have in the end a variable having complex variance t, in our sense, and we are led in this way into:

Definition 4.19. *The complex normal, or Gaussian law of parameter $t > 0$ is*

$$G_t = law\left(\frac{1}{\sqrt{2}}(a + ib)\right)$$

where a, b are real and independent, each following the law g_t.

In short, the complex normal laws appear as natural complexifications of the real normal laws. As in the real case, these measures form convolution semigroups:

Proposition 4.20. *The complex Gaussian laws have the property*

$$G_s * G_t = G_{s+t}$$

for any $s, t > 0$, and so they form a convolution semigroup.

Proof. This follows indeed from the real result, namely $g_s * g_t = g_{s+t}$, established in Theorem 4.8, simply by taking real and imaginary parts. □

We have as well the following complex analogue of the CLT:

Theorem 4.21 (CCLT). *Given discrete complex variables $f_1, f_2, f_3, \ldots$ whose real and imaginary parts are i.i.d. and centered, and having variance $t > 0$, we have*

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} f_i \sim G_t$$

with $n \to \infty$, in moments.

Proof. This follows indeed from our previous CCLT result, from Theorem 4.18, by dividing everything by $\sqrt{2}$, as explained in the above. □

4d. Wick formula

Regarding now the moments, the situation here is more complicated than in the real case, because in order to have good results, we have to deal with both the complex variables, and their conjugates. Let us formulate the following definition:

DEFINITION 4.22. *The moments a complex variable $f \in L^\infty(X)$ are the numbers*

$$M_k = E(f^k)$$

depending on colored integers $k = \circ \bullet \bullet \circ \ldots$, with the conventions

$$f^\emptyset = 1 \quad , \quad f^\circ = f \quad , \quad f^\bullet = \bar{f}$$

and multiplicativity, in order to define the colored powers f^k.

As an illustration for this notion, which is something very intuitive, here are the formulae of the four possible order 2 moments of a complex variable f:

$$M_{\circ\circ} = E(f^2) \quad , \quad M_{\circ\bullet} = E(f\bar{f})$$

$$M_{\bullet\circ} = E(\bar{f}f) \quad , \quad M_{\bullet\bullet} = E(\bar{f}^2)$$

Observe that, since $f, \bar{f}$ commute, we have the following identity, which shows that there is a bit of redundancy in our above definition, as formulated:

$$M_{\circ\bullet} = M_{\bullet\circ}$$

In fact, again since $f, \bar{f}$ commute, we can permute terms, in the general context of Definition 4.22, and restrict the attention to exponents of the following type:

$$k = \ldots \circ \circ \circ \bullet \bullet \bullet \bullet \ldots$$

However, our results about the complex Gaussian laws, and other complex laws, later on, not to talk about laws of matrices, random matrices and other noncommuting variables, that will appear later too, will look better without doing this. So, we will use Definition 4.22 as stated. Getting to work now, we first have the following result:

THEOREM 4.23. *The moments of the complex normal law are given by*

$$M_k(G_t) = \begin{cases} t^p p! & (k \text{ uniform, of length } 2p) \\ 0 & (k \text{ not uniform}) \end{cases}$$

where $k = \circ \bullet \bullet \circ \ldots$ is called uniform when it contains the same number of $\circ$ and $\bullet$.

PROOF. We must compute the moments, with respect to colored integer exponents $k = \circ \bullet \bullet \circ \ldots$ as above, of the variable from Definition 4.19, namely:

$$f = \frac{1}{\sqrt{2}}(a + ib)$$

We can assume that we are in the case $t = 1$, and the proof here goes as follows:

(1) As a first observation, in the case where our exponent $k=\circ\bullet\bullet\circ\ldots$ is not uniform, a standard rotation argument shows that the corresponding moment of f vanishes. To be more precise, the variable $f'=wf$ is complex Gaussian too, for any complex number $w\in\mathbb{T}$, and from $M_k(f)=M_k(f')$ we obtain $M_k(f)=0$, in this case.

(2) In the uniform case now, where the exponent $k=\circ\bullet\bullet\circ\ldots$ consists of p copies of $\circ$ and p copies of $\bullet$, the corresponding moment can be computed as follows:

$$\begin{aligned}
M_k &= \int (f\bar{f})^p\\
&= \frac{1}{2^p}\int (a^2+b^2)^p\\
&= \frac{1}{2^p}\sum_r \binom{p}{r}\int a^{2r}\int b^{2p-2r}\\
&= \frac{1}{2^p}\sum_r \binom{p}{r}(2r)!!(2p-2r)!!\\
&= \frac{1}{2^p}\sum_r \frac{p!}{r!(p-r)!}\cdot\frac{(2r)!}{2^r r!}\cdot\frac{(2p-2r)!}{2^{p-r}(p-r)!}\\
&= \frac{p!}{4^p}\sum_r \binom{2r}{r}\binom{2p-2r}{p-r}
\end{aligned}$$

(3) In order to finish now the computation, let us recall that we have the following formula, coming from the generalized binomial formula, or from the Taylor formula:

$$\frac{1}{\sqrt{1+t}}=\sum_{q=0}^\infty \binom{2q}{q}\left(\frac{-t}{4}\right)^q$$

By taking the square of this series, we obtain the following formula:

$$\frac{1}{1+t}=\sum_p \left(\frac{-t}{4}\right)^p\sum_r \binom{2r}{r}\binom{2p-2r}{p-r}$$

Now by looking at the coefficient of t^p on both sides, we conclude that the sum on the right equals 4^p. Thus, we can finish the moment computation in (2), as follows:

$$M_k=\frac{p!}{4^p}\times 4^p=p!$$

We are therefore led to the conclusion in the statement. □

As before with the real Gaussian laws, or even before with the Poisson and Bessel laws, a better-looking statement regarding the moments is in terms of partitions.

Indeed, given a colored integer $k = \circ\bullet\bullet\circ\ldots$, let us say that $\pi \in P_2(k)$ is matching when it pairs $\circ - \bullet$ symbols. With this convention, we have the following result:

THEOREM 4.24. *The moments of the complex normal law are the numbers*

$$M_k(G_t) = \sum_{\pi\in\mathcal{P}_2(k)} t^{|\pi|}$$

where $\mathcal{P}_2(k)$ are the matching pairings of $\{1,\ldots,k\}$, and $|.|$ is the number of blocks.

PROOF. This is a reformulation of Theorem 4.23. Indeed, we can assume that we are in the case $t = 1$, and here we know from Theorem 4.23 that the moments are:

$$M_k = \begin{cases} (|k|/2)! & (k \text{ uniform})\\ 0 & (k \text{ not uniform})\end{cases}$$

On the other hand, the numbers $|\mathcal{P}_2(k)|$ are given by exactly the same formula. Indeed, in order to have a matching pairing of k, our exponent $k = \circ\bullet\bullet\circ\ldots$ must be uniform, consisting of p copies of $\circ$ and p copies of $\bullet$, with $p = |k|/2$. But then the matching pairings of k correspond to the permutations of the $\bullet$ symbols, as to be matched with $\circ$ symbols, and so we have $p!$ such pairings. Thus, we have the same formula as for the moments of f, and we are led to the conclusion in the statement. □

In practice, we also need to know how to compute joint moments. We have here:

THEOREM 4.25 (Wick formula). *Given independent variables f_i, each following the complex normal law G_t, with $t > 0$ being a fixed parameter, we have the formula*

$$E\left(f_{i_1}^{k_1}\ldots f_{i_s}^{k_s}\right) = t^{s/2}\#\left\{\pi\in\mathcal{P}_2(k)\Big|\pi\leq\ker i\right\}$$

where $k = k_1\ldots k_s$ and $i = i_1\ldots i_s$, for the joint moments of these variables, where $\pi \leq \ker i$ means that the indices of i must fit into the blocks of π, in the obvious way.

PROOF. This is something well-known, which can be proved as follows:

(1) Let us first discuss the case where we have a single variable f, which amounts in taking $f_i = f$ for any i in the formula in the statement. What we have to compute here are the moments of f, with respect to colored integer exponents $k = \circ\bullet\bullet\circ\ldots$, and the formula in the statement tells us that these moments must be:

$$E(f^k) = t^{|k|/2}|\mathcal{P}_2(k)|$$

But this is the formula in Theorem 4.24, so we are done with this case.

(2) In general now, when expanding the product $f_{i_1}^{k_1}\ldots f_{i_s}^{k_s}$ and rearranging the terms, we are left with doing a number of computations as in (1), and then making the product of the expectations that we found. But this amounts in counting the partitions in the statement, with the condition $\pi \leq \ker i$ there standing for the fact that we are doing the various type (1) computations independently, and then making the product. □

The above statement is one of the possible formulations of the Wick formula, and there are many more formulations, which are all useful. For instance, we have:

THEOREM 4.26 (Wick formula 2). *Given independent variables f_i, each following the complex normal law G_t, with $t > 0$ being a fixed parameter, we have the formula*

$$E\left(f_{i_1}\dots f_{i_k}f_{j_1}^*\dots f_{j_k}^*\right)=t^k\#\left\{\pi\in S_k\Big|i_{\pi(r)}=j_r,\forall r\right\}$$

for the non-vanishing joint moments of these variables.

PROOF. This follows from the usual Wick formula, from Theorem 4.25. With some changes in the indices and notations, the formula there reads:

$$E\left(f_{I_1}^{K_1}\dots f_{I_s}^{K_s}\right)=t^{s/2}\#\left\{\sigma\in\mathcal{P}_2(K)\Big|\sigma\leq\ker I\right\}$$

Now observe that we have $\mathcal{P}_2(K)=\emptyset$, unless the colored integer $K=K_1\dots K_s$ is uniform, in the sense that it contains the same number of $\circ$ and $\bullet$ symbols. Up to permutations, the non-trivial case, where the moment is non-vanishing, is the case where the colored integer $K=K_1\dots K_s$ is of the following special form:

$$K=\underbrace{\circ\circ\dots\circ}_{k}\ \underbrace{\bullet\bullet\dots\bullet}_{k}$$

So, let us focus on this case, which is the non-trivial one. Here we have $s=2k$, and we can write the multi-index $I=I_1\dots I_s$ in the following way:

$$I=i_1\dots i_k\ j_1\dots j_k$$

With these changes made, the above usual Wick formula reads:

$$E\left(f_{i_1}\dots f_{i_k}f_{j_1}^*\dots f_{j_k}^*\right)=t^k\#\left\{\sigma\in\mathcal{P}_2(K)\Big|\sigma\leq\ker(ij)\right\}$$

The point now is that the matching pairings $\sigma\in\mathcal{P}_2(K)$, with $K=\circ\dots\circ\bullet\dots\bullet$, of length $2k$, as above, correspond to the permutations $\pi\in S_k$, in the obvious way. With this identification made, the above modified usual Wick formula becomes:

$$E\left(f_{i_1}\dots f_{i_k}f_{j_1}^*\dots f_{j_k}^*\right)=t^k\#\left\{\pi\in S_k\Big|i_{\pi(r)}=j_r,\forall r\right\}$$

Thus, we have reached to the formula in the statement, and we are done. □

Finally, here is one more formulation of the Wick formula, useful as well:

THEOREM 4.27 (Wick formula 3). *Given independent variables f_i, each following the complex normal law G_t, with $t > 0$ being a fixed parameter, we have the formula*

$$E\left(f_{i_1}f_{j_1}^*\dots f_{i_k}f_{j_k}^*\right)=t^k\#\left\{\pi\in S_k\Big|i_{\pi(r)}=j_r,\forall r\right\}$$

for the non-vanishing joint moments of these variables.

PROOF. This follows from our second Wick formula, from Theorem 4.26, simply by permuting the terms, as to have an alternating sequence of plain and conjugate variables. Alternatively, we can start with Theorem 4.25, and then perform the same manipulations as in the proof of Theorem 4.26, but with the exponent being this time as follows:

$$K = \underbrace{\circ\bullet\circ\bullet\ldots\ldots\circ\bullet}_{2k}$$

Thus, we are led to the conclusion in the statement. □

4e. Exercises

Exercises:

EXERCISE 4.28.

EXERCISE 4.29.

EXERCISE 4.30.

EXERCISE 4.31.

EXERCISE 4.32.

EXERCISE 4.33.

EXERCISE 4.34.

EXERCISE 4.35.

Bonus exercise.

Part II

Laws of matrices

CHAPTER 5

Linear algebra

5a. Linear maps

According to various findings in physics, starting with those of Heisenberg from the early 1920s, basic quantum mechanics involves linear operators $T : H \to H$ from a complex Hilbert space H to itself. The space H is typically infinite dimensional, a basic example being the Schrödinger space $H = L^2(\mathbb{R}^3)$ of the wave functions $\psi : \mathbb{R}^3 \to \mathbb{C}$ of the electron. In fact, in what regards the electron, this space $H = L^2(\mathbb{R}^3)$ is basically the correct one, with the only adjustment needed, due to Pauli and others, being that of tensoring with a copy of $K = \mathbb{C}^2$, in order to account for the electron spin.

But more on this later. Let us start this Part II more modestly, as follows:

Fact 5.1. *We are interested in quantum mechanics, taking place in infinite dimensions, but as a main source of inspiration we will have $H = \mathbb{C}^N$, with scalar product*

$$< x, y >= \sum_i x_i \bar{y}_i$$

with the linearity at left being the standard mathematical convention. More specifically, we will be interested in the mathematics of the linear operators $T : H \to H$.

The point now, that you surely know about, is that the above operators $T : H \to H$ correspond to the square matrices $A \in M_N(\mathbb{C})$. Thus, as a preliminary to what we want to do in this book, we need a good knowledge of linear algebra over $\mathbb{C}$.

You probably know well linear algebra, but always good to recall this, and this will be the purpose of the present chapter. Let us start with the very basics:

Theorem 5.2. *The linear maps $T : \mathbb{C}^N \to \mathbb{C}^N$ are in correspondence with the square matrices $A \in M_N(\mathbb{C})$, with the linear map associated to such a matrix being*

$$Tx = Ax$$

and with the matrix associated to a linear map being $A_{ij} =< Te_j, e_i >$.

Proof. The first assertion is clear, because a linear map $T : \mathbb{C}^N \to \mathbb{C}^N$ must send a vector $x \in \mathbb{C}^N$ to a certain vector $Tx \in \mathbb{C}^N$, all whose components are linear combinations of the components of x. Thus, we can write, for certain complex numbers $A_{ij} \in \mathbb{C}$:

$$T\begin{pmatrix}x_1\\ \vdots\\ \vdots\\ x_N\end{pmatrix}=\begin{pmatrix}A_{11}x_1+\ldots+A_{1N}x_N\\ \vdots\\ \vdots\\ A_{N1}x_1+\ldots+A_{NN}x_N\end{pmatrix}$$

Now the parameters $A_{ij} \in \mathbb{C}$ can be regarded as being the entries of a square matrix $A \in M_N(\mathbb{C})$, and with the usual convention for matrix multiplication, we have:

$$Tx = Ax$$

Regarding the second assertion, with $Tx = Ax$ as above, if we denote by $e_1, \ldots, e_N$ the standard basis of $\mathbb{C}^N$, then we have the following formula:

$$Te_j=\begin{pmatrix}A_{1j}\\ \vdots\\ \vdots\\ A_{Nj}\end{pmatrix}$$

But this gives the second formula, $< Te_j, e_i >= A_{ij}$, as desired. □

Our claim now is that, no matter what we want to do with T or A, of advanced type, we will run at some point into their adjoints T^* and A^*, constructed as follows:

Theorem 5.3. *The adjoint operator $T^* : \mathbb{C}^N \to \mathbb{C}^N$, which is given by*

$$< Tx, y >=< x, T^*y >$$

corresponds to the adjoint matrix $A^* \in M_N(\mathbb{C})$, given by

$$(A^*)_{ij} = \bar{A}_{ji}$$

via the correspondence between linear maps and matrices constructed above.

Proof. Given a linear map $T : \mathbb{C}^N \to \mathbb{C}^N$, fix $y \in \mathbb{C}^N$, and consider the linear form $\varphi(x) =< Tx, y >$. This form must be as follows, for a certain vector $T^*y \in \mathbb{C}^N$:

$$\varphi(x) =< x, T^*y >$$

Thus, we have constructed a map $y \to T^*y$ as in the statement, which is obviously linear, and that we can call T^*. Now by taking the vectors $x, y \in \mathbb{C}^N$ to be elements of the standard basis of $\mathbb{C}^N$, our defining formula for T^* reads:

$$< Te_i, e_j >=< e_i, T^*e_j >$$

By reversing the scalar product on the right, this formula can be written as:

$$< T^*e_j, e_i >=\overline{< Te_i, e_j >}$$

But this means that the matrix of T^* is given by $(A^*)_{ij} = \bar{A}_{ji}$, as desired. □

Getting back to our claim, the adjoints $*$ are indeed ubiquitous, as shown by:

THEOREM 5.4. *The following happen:*

(1) $T(x) = Ux$ *with* $U \in M_N(\mathbb{C})$ *is an isometry precisely when* $U^* = U^{-1}$.
(2) $T(x) = Px$ *with* $P \in M_N(\mathbb{C})$ *is a projection precisely when* $P^2 = P^* = P$.

PROOF. Let us first recall that the lengths, or norms, of the vectors $x \in \mathbb{C}^N$ can be recovered from the knowledge of the scalar products, as follows:

$$||x|| = \sqrt{< x, x >}$$

Conversely, we can recover the scalar products out of norms, by using the following difficult to remember formula, called complex polarization identity:

$$4 < x, y >= ||x + y||^2 - ||x - y||^2 + i||x + iy||^2 - i||x - iy||^2$$

The proof of this latter formula is indeed elementary, as follows:

$$\begin{aligned} & ||x + y||^2 - ||x - y||^2 + i||x + iy||^2 - i||x - iy||^2 \\ = & ||x||^2 + ||y||^2 - ||x||^2 - ||y||^2 + i||x||^2 + i||y||^2 - i||x||^2 - i||y||^2 \\ & +2Re(< x, y >) + 2Re(< x, y >) + 2iIm(< x, y >) + 2iIm(< x, y >) \\ = & 4 < x, y > \end{aligned}$$

Finally, we will use Theorem 5.3, and more specifically the following formula coming from there, valid for any matrix $A \in M_N(\mathbb{C})$ and any two vectors $x, y \in \mathbb{C}^N$:

$$< Ax, y >=< x, A^*y >$$

(1) Given a matrix $U \in M_N(\mathbb{C})$, we have indeed the following equivalences, with the first one coming from the polarization identity, and the other ones being clear:

$$\begin{aligned} ||Ux|| = ||x|| & \iff < Ux, Uy >=< x, y > \\ & \iff < x, U^*Uy >=< x, y > \\ & \iff U^*Uy = y \\ & \iff U^*U = 1 \\ & \iff U^* = U^{-1} \end{aligned}$$

(2) Given a matrix $P \in M_N(\mathbb{C})$, in order for $x \to Px$ to be an oblique projection, we must have $P^2 = P$. Now observe that this projection is orthogonal when:

$$\begin{aligned} < Px - x, Py >= 0 & \iff < P^*Px - P^*x, y >= 0 \\ & \iff P^*Px - P^*x = 0 \\ & \iff P^*P - P^* = 0 \\ & \iff P^*P = P^* \end{aligned}$$

The point now is that by conjugating the last formula, we obtain $P^*P = P$. Thus we must have $P = P^*$, and this gives the result. $\square$

Summarizing, the linear operators come in pairs T, T^*, and the associated matrices come as well in pairs A, A^*. This is something quite interesting, philosophically speaking, and will keep this in mind, and come back to it later, on numerous occasions.

5b. Diagonalization

Let us discuss now the diagonalization question for the linear maps and matrices. Again, we will be quite brief here, and for more, we refer to any standard linear algebra book. By the way, there will be some complex analysis involved too, and here we refer to Rudin [78]. Which book of Rudin will be in fact the one and only true prerequisite for reading the present book, but more on references and reading later.

The basic diagonalization theory, formulated in terms of matrices, is as follows:

Proposition 5.5. *A vector $v \in \mathbb{C}^N$ is called eigenvector of $A \in M_N(\mathbb{C})$, with corresponding eigenvalue λ, when A multiplies by λ in the direction of v:*

$$Av = \lambda v$$

In the case where $\mathbb{C}^N$ has a basis $v_1, \ldots, v_N$ formed by eigenvectors of A, with corresponding eigenvalues $\lambda_1, \ldots, \lambda_N$, in this new basis A becomes diagonal, as follows:

$$A \sim \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{pmatrix}$$

Equivalently, if we denote by $D = diag(\lambda_1, \ldots, \lambda_N)$ the above diagonal matrix, and by $P = [v_1 \ldots v_N]$ the square matrix formed by the eigenvectors of A, we have:

$$A = PDP^{-1}$$

In this case we say that the matrix A is diagonalizable.

Proof. This is something which is clear, the idea being as follows:

(1) The first assertion is clear, because the matrix which multiplies each basis element v_i by a number λ_i is precisely the diagonal matrix $D = diag(\lambda_1, \ldots, \lambda_N)$.

(2) The second assertion follows from the first one, by changing the basis. We can prove this by a direct computation as well, because we have $Pe_i = v_i$, and so:

$$\begin{aligned} PDP^{-1}v_i &= PDe_i \\ &= P\lambda_i e_i \\ &= \lambda_i Pe_i \\ &= \lambda_i v_i \end{aligned}$$

Thus, the matrices A and PDP^{-1} coincide, as stated. □

Let us recall as well that the basic example of a non diagonalizable matrix, over the complex numbers as above, is the following matrix:

$$J = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Indeed, we have $J\binom{x}{y} = \binom{y}{0}$, so the eigenvectors are the vectors of type $\binom{x}{0}$, all with eigenvalue 0. Thus, we have not enough eigenvectors for constructing a basis of $\mathbb{C}^2$.

In general, in order to study the diagonalization problem, the idea is that the eigenvectors can be grouped into linear spaces, called eigenspaces, as follows:

THEOREM 5.6. *Let $A \in M_N(\mathbb{C})$, and for any eigenvalue $\lambda \in \mathbb{C}$ define the corresponding eigenspace as being the vector space formed by the corresponding eigenvectors:*

$$E_\lambda = \left\{ v \in \mathbb{C}^N \Big| Av = \lambda v \right\}$$

These eigenspaces E_λ are then in a direct sum position, in the sense that given vectors $v_1 \in E_{\lambda_1}, \ldots, v_k \in E_{\lambda_k}$ corresponding to different eigenvalues $\lambda_1, \ldots, \lambda_k$, we have:

$$\sum_i c_i v_i = 0 \implies c_i = 0$$

In particular we have the following estimate, with sum over all the eigenvalues,

$$\sum_\lambda \dim(E_\lambda) \leq N$$

and our matrix is diagonalizable precisely when we have equality.

PROOF. We prove the first assertion by recurrence on $k \in \mathbb{N}$. Assume by contradiction that we have a formula as follows, with the scalars $c_1, \ldots, c_k$ being not all zero:

$$c_1 v_1 + \ldots + c_k v_k = 0$$

By dividing by one of these scalars, we can assume that our formula is:

$$v_k = c_1 v_1 + \ldots + c_{k-1} v_{k-1}$$

Now let us apply A to this vector. On the left we obtain:

$$Av_k = \lambda_k v_k = \lambda_k c_1 v_1 + \ldots + \lambda_k c_{k-1} v_{k-1}$$

On the right we obtain something different, as follows:

$$\begin{aligned} A(c_1 v_1 + \ldots + c_{k-1} v_{k-1}) &= c_1 A v_1 + \ldots + c_{k-1} A v_{k-1} \\ &= c_1 \lambda_1 v_1 + \ldots + c_{k-1} \lambda_{k-1} v_{k-1} \end{aligned}$$

We conclude from this that the following equality must hold:

$$\lambda_k c_1 v_1 + \ldots + \lambda_k c_{k-1} v_{k-1} = c_1 \lambda_1 v_1 + \ldots + c_{k-1} \lambda_{k-1} v_{k-1}$$

On the other hand, we know by recurrence that the vectors $v_1, \ldots, v_{k-1}$ must be linearly independent. Thus, the coefficients must be equal, at right and at left:

$$\lambda_k c_1 = c_1 \lambda_1$$

$$\vdots$$

$$\lambda_k c_{k-1} = c_{k-1} \lambda_{k-1}$$

Now since at least one of the numbers c_i must be nonzero, from $\lambda_k c_i = c_i \lambda_i$ we obtain $\lambda_k = \lambda_i$, which is a contradiction. Thus our proof by recurrence of the first assertion is complete. As for the second assertion, this follows from the first one. □

In order to reach now to more advanced results, we can use the characteristic polynomial, which appears via the following fundamental result:

THEOREM 5.7. *Given a matrix $A \in M_N(\mathbb{C})$, consider its characteristic polynomial:*

$$P(x) = \det(A - x 1_N)$$

The eigenvalues of A are then the roots of P. Also, we have the inequality

$$\dim(E_\lambda) \leq m_\lambda$$

where m_λ is the multiplicity of λ, as root of P.

PROOF. The first assertion follows from the following computation, using the fact that a linear map is bijective when the determinant of the associated matrix is nonzero:

$$\begin{aligned} \exists v, Av = \lambda v &\iff \exists v, (A - \lambda 1_N) v = 0 \\ &\iff \det(A - \lambda 1_N) = 0 \end{aligned}$$

Regarding now the second assertion, given an eigenvalue λ of our matrix A, consider the dimension $d_\lambda = \dim(E_\lambda)$ of the corresponding eigenspace. By changing the basis of $\mathbb{C}^N$, as for the eigenspace E_λ to be spanned by the first d_λ basis elements, our matrix becomes as follows, with B being a certain smaller matrix:

$$A \sim \begin{pmatrix} \lambda 1_{d_\lambda} & 0 \\ 0 & B \end{pmatrix}$$

We conclude that the characteristic polynomial of A is of the following form:

$$P_A = P_{\lambda 1_{d_\lambda}} P_B = (\lambda - x)^{d_\lambda} P_B$$

Thus the multiplicity m_λ of our eigenvalue λ, as a root of P, satisfies $m_\lambda \geq d_\lambda$, and this leads to the conclusion in the statement. □

Now recall that we are over $\mathbb{C}$, which is something that we have not used yet, in our last two statements. And the point here is that we have the following key result:

THEOREM 5.8. *Any polynomial $P\in\mathbb C[X]$ decomposes as*

$$P=c(X-a_1)\ldots(X-a_N)$$

with $c\in\mathbb C$ and with $a_1,\ldots,a_N\in\mathbb C$.

PROOF. It is enough to prove that P has one root, and we do this by contradiction. Assume that P has no roots, and pick a number $z\in\mathbb C$ where $|P|$ attains its minimum:

$$|P(z)|=\min_{x\in\mathbb C}|P(x)|>0$$

Since $Q(t)=P(z+t)-P(z)$ is a polynomial which vanishes at $t=0$, this polynomial must be of the form ct^k + higher terms, with $c\neq0$, and with $k\geq1$ being an integer. We obtain from this that, with $t\in\mathbb C$ small, we have the following estimate:

$$P(z+t)\simeq P(z)+ct^k$$

Now let us write $t=rw$, with $r>0$ small, and with $|w|=1$. Our estimate becomes:

$$P(z+rw)\simeq P(z)+cr^kw^k$$

Now recall that we have assumed $P(z)\neq0$. We can therefore choose $w\in\mathbb T$ such that cw^k points in the opposite direction to that of $P(z)$, and we obtain in this way:

$$|P(z+rw)|\simeq|P(z)+cr^kw^k|=|P(z)|(1-|c|r^k)$$

Now by choosing $r>0$ small enough, as for the error in the first estimate to be small, and overcame by the negative quantity $-|c|r^k$, we obtain from this:

$$|P(z+rw)|<|P(z)|$$

But this contradicts our definition of $z\in\mathbb C$, as a point where $|P|$ attains its minimum. Thus P has a root, and by recurrence it has N roots, as stated. □

Now by putting everything together, we obtain the following result:

THEOREM 5.9. *Given a matrix $A\in M_N(\mathbb C)$, consider its characteristic polynomial*

$$P(X)=\det(A-X1_N)$$

then factorize this polynomial, by computing the complex roots, with multiplicities,

$$P(X)=(-1)^N(X-\lambda_1)^{n_1}\ldots(X-\lambda_k)^{n_k}$$

and finally compute the corresponding eigenspaces, for each eigenvalue found:

$$E_i=\left\{v\in\mathbb C^N\Big|Av=\lambda_iv\right\}$$

The dimensions of these eigenspaces satisfy then the following inequalities,

$$\dim(E_i)\leq n_i$$

and A is diagonalizable precisely when we have equality for any i.

Proof. This follows by combining Theorem 5.6, Theorem 5.7 and Theorem 5.8. Indeed, the statement is well formulated, thanks to Theorem 5.8. By summing the inequalities $\dim(E_\lambda) \leq m_\lambda$ from Theorem 5.7, we obtain an inequality as follows:

$$\sum_\lambda \dim(E_\lambda) \leq \sum_\lambda m_\lambda \leq N$$

On the other hand, we know from Theorem 5.6 that our matrix is diagonalizable when we have global equality. Thus, we are led to the conclusion in the statement. $\square$

This was for the main result of linear algebra. There are countless applications of this, and generally speaking, advanced linear algebra consists in building on Theorem 5.9.

In practice, diagonalizing a matrix remains something quite complicated. Let us record a useful algorithmic version of the above result, as follows:

Theorem 5.10. *The square matrices $A \in M_N(\mathbb{C})$ can be diagonalized as follows:*
(1) *Compute the characteristic polynomial.*
(2) *Factorize the characteristic polynomial.*
(3) *Compute the eigenvectors, for each eigenvalue found.*
(4) *If there are no N eigenvectors, A is not diagonalizable.*
(5) *Otherwise, A is diagonalizable, $A = PDP^{-1}$.*

Proof. This is an informal reformulation of Theorem 5.9, with (4) referring to the total number of linearly independent eigenvectors found in (3), and with $A = PDP^{-1}$ in (5) being the usual diagonalization formula, with P, D being as before. $\square$

As an illustration for all this, which is a must-know computation, we have:

Theorem 5.11. *The rotation of angle $t \in \mathbb{R}$ in the plane diagonalizes as:*

$$\begin{pmatrix}\cos t & -\sin t\\ \sin t & \cos t\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1 & 1\\ i & -i\end{pmatrix}\begin{pmatrix}e^{-it} & 0\\ 0 & e^{it}\end{pmatrix}\begin{pmatrix}1 & -i\\ 1 & i\end{pmatrix}$$

Over the reals this is impossible, unless $t = 0, \pi$, where the rotation is diagonal.

Proof. Observe first that, as indicated, unlike we are in the case $t = 0, \pi$, where our rotation is $\pm 1_2$, our rotation is a "true" rotation, having no eigenvectors in the plane. Fortunately the complex numbers come to the rescue, via the following computation:

$$\begin{pmatrix}\cos t & -\sin t\\ \sin t & \cos t\end{pmatrix}\begin{pmatrix}1\\ i\end{pmatrix} = \begin{pmatrix}\cos t - i\sin t\\ i\cos t + \sin t\end{pmatrix} = e^{-it}\begin{pmatrix}1\\ i\end{pmatrix}$$

We have as well a second complex eigenvector, coming from:

$$\begin{pmatrix}\cos t & -\sin t\\ \sin t & \cos t\end{pmatrix}\begin{pmatrix}1\\ -i\end{pmatrix} = \begin{pmatrix}\cos t + i\sin t\\ -i\cos t + \sin t\end{pmatrix} = e^{it}\begin{pmatrix}1\\ -i\end{pmatrix}$$

Thus, we are led to the conclusion in the statement. $\square$

As another basic illustration, we have the following result:

THEOREM 5.12. *The all-one, or flat matrix, namely*

$$\mathbb{I}_N = \begin{pmatrix}1&\ldots&1\\ \vdots&&\vdots\\ 1&\ldots&1\end{pmatrix}$$

diagonalizes as follows, over the complex numbers,

$$\mathbb{I}_N = \frac{1}{N}F_NQF_N^*$$

with $F_N = (w^{ij})_{ij}$ with $w = e^{2\pi i/N}$ being the Fourier matrix, and $Q = diag(N, 0, \ldots, 0)$.

PROOF. It is clear that we have $\mathbb{I}_N = NP_N$, with P_N being the projection on the all-1 vector $\xi = (1)_i \in \mathbb{R}^N$. Thus, $\mathbb{I}_N$ diagonalizes over $\mathbb{R}$, as follows:

$$\mathbb{I}_N \sim \begin{pmatrix}N&&&\\&0&&\\&&\ddots&\\&&&0\end{pmatrix}$$

The problem, however, is that when looking for 0-eigenvectors, in order to have an explicit diagonalization formula, we must solve the following equation:

$$x_1 + \ldots + x_N = 0$$

And this is not an easy task, if we want a nice basis for the space of solutions. Fortunately, complex numbers come to the rescue, and we are led to the conclusion in the statement. We will leave the verifications here as an instructive exercise. □

5c. Matrix tricks

At the level of basic examples of diagonalizable matrices, we first have the following result, which provides us with the "generic" examples:

THEOREM 5.13. *For a matrix $A \in M_N(\mathbb{C})$ the following conditions are equivalent,*

(1) *The eigenvalues are different, $\lambda_i \neq \lambda_j$,*
(2) *The characteristic polynomial P has simple roots,*
(3) *The characteristic polynomial satisfies $(P, P') = 1$,*
(4) *The resultant of P, P' is nonzero, $R(P, P') \neq 0$,*
(5) *The discriminant of P is nonzero, $\Delta(P) \neq 0$,*

and in this case, the matrix is diagonalizable.

PROOF. The last assertion holds indeed, due to Theorem 5.9. As for the equivalences in the statement, these are all standard, the idea for their proofs, along with some more theory, needed for using in practice the present result, being as follows:

(1) $\iff$ (2) This follows from Theorem 5.9.

(2) $\iff$ (3) This is standard, the double roots of P being roots of P'.

(3) $\iff$ (4) The idea here is that associated to any two polynomials P,Q is their resultant $R(P,Q)$, which checks whether P,Q have a common root. Let us write:

$$P = c(X-a_1)\ldots(X-a_k)$$

$$Q = d(X-b_1)\ldots(X-b_l)$$

We can define then the resultant as being the following quantity:

$$R(P,Q) = c^l d^k \prod_{ij}(a_i - b_j)$$

The point now, that we will explain as well, is that this is a polynomial in the coefficients of P,Q, with integer coefficients. Indeed, this can be checked as follows:

– We can expand the formula of $R(P,Q)$, and in what regards $a_1,\ldots,a_k$, which are the roots of P, we obtain in this way certain symmetric functions in these variables, which will be therefore polynomials in the coefficients of P, with integer coefficients.

– We can then look what happens with respect to the remaining variables $b_1,\ldots,b_l$, which are the roots of Q. Once again what we have here are certain symmetric functions, and so polynomials in the coefficients of Q, with integer coefficients.

– Thus, we are led to the above conclusion, that $R(P,Q)$ is a polynomial in the coefficients of P,Q, with integer coefficients, and with the remark that the $c^l d^k$ factor is there for these latter coefficients to be indeed integers, instead of rationals.

Alternatively, let us write our two polynomials in usual form, as follows:

$$P = p_k X^k + \ldots + p_1 X + p_0$$

$$Q = q_l X^l + \ldots + q_1 X + q_0$$

The corresponding resultant appears then as the determinant of an associated matrix, having size $k+l$, and having 0 coefficients at the blank spaces, as follows:

$$R(P,Q) = \begin{vmatrix} p_k & & & q_l & & \\ \vdots & \ddots & & \vdots & \ddots & \\ p_0 & & p_k & q_0 & & q_l \\ & \ddots & \vdots & & \ddots & \vdots \\ & & p_0 & & & q_0 \end{vmatrix}$$

(4) $\iff$ (5) Once again this is something standard, the idea here being that the discriminant $\Delta(P)$ of a polynomial $P \in \mathbb{C}[X]$ is, modulo scalars, the resultant $R(P, P')$. To be more precise, let us write our polynomial as follows:

$$P(X) = cX^N + dX^{N-1} + \ldots$$

Its discriminant is then defined as being the following quantity:

$$\Delta(P) = \frac{(-1)^{\binom{N}{2}}}{c} R(P, P')$$

This is a polynomial in the coefficients of P, with integer coefficients, with the division by c being indeed possible, under $\mathbb{Z}$, and with the sign being there for various reasons, including the compatibility with some well-known formulae, at small values of N. $\square$

All the above might seem a bit complicated, so as an illustration, let us work out an example. Consider the case of a polynomial of degree 2, and a polynomial of degree 1:

$$P = ax^2 + bx + c \quad , \quad Q = dx + e$$

In order to compute the resultant, let us factorize our polynomials:

$$P = a(x - p)(x - q) \quad , \quad Q = d(x - r)$$

The resultant can be then computed as follows, by using the two-step method:

$$\begin{aligned} R(P, Q) &= ad^2(p - r)(q - r) \\ &= ad^2(pq - (p + q)r + r^2) \\ &= cd^2 + bd^2 r + ad^2 r^2 \\ &= cd^2 - bde + ae^2 \end{aligned}$$

Observe that $R(P, Q) = 0$ corresponds indeed to the fact that P, Q have a common root. Indeed, the root of Q is $r = -e/d$, and we have:

$$P(r) = \frac{ae^2}{d^2} - \frac{be}{d} + c = \frac{R(P, Q)}{d^2}$$

We can recover as well the resultant as a determinant, as follows:

$$R(P, Q) = \begin{vmatrix} a & d & 0 \\ b & e & d \\ c & 0 & e \end{vmatrix} = ae^2 - bde + cd^2$$

Finally, in what regards the discriminant, let us see what happens in degree 2. Here we must compute the resultant of the following two polynomials:

$$P = aX^2 + bX + c \quad , \quad P' = 2aX + b$$

The resultant is then given by the following formula:

$$\begin{aligned} R(P,P') &= ab^2-b(2a)b+c(2a)^2 \\ &= 4a^2c-ab^2 \\ &= -a(b^2-4ac) \end{aligned}$$

Now by doing the discriminant normalizations, we obtain, as we should:

$$\Delta(P)=b^2-4ac$$

As already mentioned, one can prove that the matrices having distinct eigenvalues are "generic", and so the above result basically captures the whole situation. We have in fact the following collection of density results, which are quite advanced:

Theorem 5.14. *The following happen, inside $M_N(\mathbb{C})$:*

1. *The invertible matrices are dense.*
2. *The matrices having distinct eigenvalues are dense.*
3. *The diagonalizable matrices are dense.*

Proof. These are quite advanced results, which can be proved as follows:

(1) This is clear, intuitively speaking, because the invertible matrices are given by the condition $\det A\neq 0$. Thus, the set formed by these matrices appears as the complement of the hypersurface $\det A=0$, and so must be dense inside $M_N(\mathbb{C})$, as claimed.

(2) Here we can use a similar argument, this time by saying that the set formed by the matrices having distinct eigenvalues appears as the complement of the hypersurface given by $\Delta(P_A)=0$, and so must be dense inside $M_N(\mathbb{C})$, as claimed.

(3) This follows from (2), via the fact that the matrices having distinct eigenvalues are diagonalizable, that we know from Theorem 5.13. There are of course some other proofs as well, for instance by putting the matrix in Jordan form. □

As an application of the above results, and of our methods in general, we have:

Theorem 5.15. *The following happen:*

1. *We have $P_{AB}=P_{BA}$, for any two matrices $A,B\in M_N(\mathbb{C})$.*
2. *AB,BA have the same eigenvalues, with the same multiplicities.*
3. *If A has eigenvalues $\lambda_1,\ldots,\lambda_N$, then $f(A)$ has eigenvalues $f(\lambda_1),\ldots,f(\lambda_N)$.*

Proof. These results can be deduced by using Theorem 5.14, as follows:

(1) It follows from definitions that the characteristic polynomial of a matrix is invariant under conjugation, in the sense that we have the following formula:

$$P_C=P_{ACA^{-1}}$$

Now observe that, when assuming that A is invertible, we have:

$$AB=A(BA)A^{-1}$$

Thus, we have the result when A is invertible. By using now Theorem 5.14 (1), we conclude that this formula holds for any matrix A, by continuity.

(2) This is a reformulation of (1), via the fact that P encodes the eigenvalues, with multiplicities, which is hard to prove with bare hands.

(3) This is something quite informal, clear for the diagonal matrices D, then for the diagonalizable matrices PDP^{-1}, and finally for all matrices, by using Theorem 5.14 (3), provided that f has suitable regularity properties. We will be back to this. □

Let us go back to the main problem raised by the diagonalization procedure, namely the computation of the roots of characteristic polynomials. We have here:

THEOREM 5.16. *The complex eigenvalues of a matrix $A \in M_N(\mathbb{C})$, counted with multiplicities, have the following properties:*

1. *Their sum is the trace.*
2. *Their product is the determinant.*

PROOF. Consider indeed the characteristic polynomial P of the matrix:

$$\begin{aligned} P(X) &= \det(A - X1_N) \\ &= (-1)^N X^N + (-1)^{N-1} Tr(A) X^{N-1} + \ldots + \det(A) \end{aligned}$$

We can factorize this polynomial, by using its N complex roots, and we obtain:

$$\begin{aligned} P(X) &= (-1)^N (X - \lambda_1) \ldots (X - \lambda_N) \\ &= (-1)^N X^N + (-1)^{N-1} \left(\sum_i \lambda_i \right) X^{N-1} + \ldots + \prod_i \lambda_i \end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Regarding now the intermediate terms, we have here:

THEOREM 5.17. *Assume that $A \in M_N(\mathbb{C})$ has eigenvalues $\lambda_1, \ldots, \lambda_N \in \mathbb{C}$, counted with multiplicities. The basic symmetric functions of these eigenvalues, namely*

$$c_k = \sum_{i_1 < \ldots < i_k} \lambda_{i_1} \ldots \lambda_{i_k}$$

are then given by the fact that the characteristic polynomial of the matrix is:

$$P(X) = (-1)^N \sum_{k=0}^N (-1)^k c_k X^k$$

Moreover, all symmetric functions of the eigenvalues, such as the sums of powers

$$d_s = \lambda_1^s + \ldots + \lambda_N^s$$

appear as polynomials in these characteristic polynomial coefficients c_k.

Proof. These results can be proved by doing some algebra, as follows:

(1) Consider indeed the characteristic polynomial P of the matrix, factorized by using its N complex roots, taken with multiplicities. By expanding, we obtain:

$$\begin{aligned} P(X) &= (-1)^N(X-\lambda_1)\ldots(X-\lambda_N) \\ &= (-1)^N X^N + (-1)^{N-1}\left(\sum_i \lambda_i\right) X^{N-1} + \ldots + \prod_i \lambda_i \\ &= (-1)^N X^N + (-1)^{N-1} c_1 X^{N-1} + \ldots + (-1)^0 c_N \\ &= (-1)^N \left(X^N - c_1 X^{N-1} + \ldots + (-1)^N c_N\right) \end{aligned}$$

With the convention $c_0 = 1$, we are led to the conclusion in the statement.

(2) This is something standard, coming by doing some abstract algebra. Working out the formulae for the sums of powers $d_s = \sum_i \lambda_i^s$, at small values of the exponent $s \in \mathbb{N}$, is an excellent exercise, which shows how to proceed in general, by recurrence. □

5d. Spectral theorems

Let us go back now to the diagonalization question. Here is a key result:

Theorem 5.18. *Any matrix $A \in M_N(\mathbb{C})$ which is self-adjoint, $A = A^*$, is diagonalizable, with the diagonalization being of the following type,*

$$A = UDU^*$$

with $U \in U_N$, and with $D \in M_N(\mathbb{R})$ diagonal. The converse holds too.

Proof. As a first remark, the converse trivially holds, because if we take a matrix of the form $A = UDU^*$, with U unitary and D diagonal and real, then we have:

$$\begin{aligned} A^* &= (UDU^*)^* \\ &= UD^*U^* \\ &= UDU^* \\ &= A \end{aligned}$$

In the other sense now, assume that A is self-adjoint, $A = A^*$. Our first claim is that the eigenvalues are real. Indeed, assuming $Av = \lambda v$, we have:

$$\begin{aligned} \lambda < v, v > &= < \lambda v, v > \\ &= < Av, v > \\ &= < v, Av > \\ &= < v, \lambda v > \\ &= \bar{\lambda} < v, v > \end{aligned}$$

Thus we obtain $\lambda \in \mathbb{R}$, as claimed. Our next claim now is that the eigenspaces corresponding to different eigenvalues are pairwise orthogonal. Assume indeed that:

$$Av = \lambda v \quad , \quad Aw = \mu w$$

We have then the following computation, using $\lambda, \mu \in \mathbb{R}$:

$$\begin{aligned} \lambda < v, w > &= < \lambda v, w > \\ &= < Av, w > \\ &= < v, Aw > \\ &= < v, \mu w > \\ &= \mu < v, w > \end{aligned}$$

Thus $\lambda \neq \mu$ implies $v \perp w$, as claimed. In order now to finish the proof, it remains to prove that the eigenspaces of A span the whole space $\mathbb{C}^N$. For this purpose, we will use a recurrence method. Let us pick an eigenvector of our matrix:

$$Av = \lambda v$$

Assuming now that we have a vector w orthogonal to it, $v \perp w$, we have:

$$\begin{aligned} < Aw, v > &= < w, Av > \\ &= < w, \lambda v > \\ &= \lambda < w, v > \\ &= 0 \end{aligned}$$

Thus, if v is an eigenvector, then the vector space $v^\perp$ is invariant under A. Moreover, since a matrix A is self-adjoint precisely when $< Av, v > \in \mathbb{R}$ for any vector $v \in \mathbb{C}^N$, as one can see by expanding the scalar product, the restriction of A to the subspace $v^\perp$ is self-adjoint. Thus, we can proceed by recurrence, and we obtain the result. □

As basic examples of self-adjoint matrices, we have the orthogonal projections. The diagonalization result regarding them is as follows:

PROPOSITION 5.19. *The matrices $P \in M_N(\mathbb{C})$ which are projections,*

$$P^2 = P^* = P$$

are precisely those which diagonalize as follows,

$$P = UDU^*$$

with $U \in U_N$, and with $D \in M_N(0,1)$ being diagonal.

PROOF. The equation for the projections being $P^2 = P^* = P$, the eigenvalues λ are real, and we have as well the following condition, coming from $P^2 = P$:

$$\begin{aligned}\lambda < v, v > &= < \lambda v, v >\\ &= < Pv, v >\\ &= < P^2 v, v >\\ &= < Pv, Pv >\\ &= < \lambda v, \lambda v >\\ &= \lambda^2 < v, v >\end{aligned}$$

Thus we obtain $\lambda \in \{0, 1\}$, as claimed, and as a final conclusion here, the diagonalization of the self-adjoint matrices is as follows, with $e_i \in \{0, 1\}$:

$$P \sim \begin{pmatrix} e_1 & & \\ & \ddots & \\ & & e_N \end{pmatrix}$$

To be more precise, the number of 1 values is the dimension of the image of P, and the number of 0 values is the dimension of space of vectors sent to 0 by P. □

An important class of self-adjoint matrices, which includes for instance all the projections, are the positive matrices. The theory here is as follows:

THEOREM 5.20. *For a matrix $A \in M_N(\mathbb{C})$ the following conditions are equivalent, and if they are satisfied, we say that A is positive:*

1. *$A = B^2$, with $B = B^*$.*
2. *$A = CC^*$, for some $C \in M_N(\mathbb{C})$.*
3. *$< Ax, x > \geq 0$, for any vector $x \in \mathbb{C}^N$.*
4. *$A = A^*$, and the eigenvalues are positive, $\lambda_i \geq 0$.*
5. *$A = UDU^*$, with $U \in U_N$ and with $D \in M_N(\mathbb{R}_+)$ diagonal.*

PROOF. The idea is that the equivalences in the statement basically follow from some elementary computations, with only Theorem 5.18 needed, at some point:

(1) $\implies$ (2) This is clear, because we can take $C = B$.

(2) $\implies$ (3) This follows from the following computation:

$$\begin{aligned}< Ax, x > &= < CC^* x, x >\\ &= < C^* x, C^* x >\\ &\geq 0\end{aligned}$$

(3) $\implies$ (4) By using the fact that $< Ax, x >$ is real, we have:

$$\begin{aligned}< Ax, x > &= < x, A^* x >\\ &= < A^* x, x >\end{aligned}$$

Thus we have $A=A^*$, and the remaining assertion, regarding the eigenvalues, follows from the following computation, assuming $Ax=\lambda x$:

$$\begin{aligned} < Ax,x > &= < \lambda x,x > \\ &= \lambda < x,x > \\ &\geq 0 \end{aligned}$$

(4) $\implies$ (5) This follows indeed by using Theorem 5.18.

(5) $\implies$ (1) Assuming $A=UDU^*$, with $U\in U_N$, and with $D\in M_N(\mathbb{R}_+)$ being diagonal, we can set $B=U\sqrt{D}U^*$. Then B is self-adjoint, and its square is given by:

$$\begin{aligned} B^2 &= U\sqrt{D}U^*\cdot U\sqrt{D}U^* \\ &= UDU^* \\ &= A \end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Let us record as well the following technical version of the above result:

Theorem 5.21. *For a matrix $A\in M_N(\mathbb{C})$ the following conditions are equivalent, and if they are satisfied, we say that A is strictly positive:*

1. *$A=B^2$, with $B=B^*$, invertible.*
2. *$A=CC^*$, for some $C\in M_N(\mathbb{C})$ invertible.*
3. *$< Ax,x >> 0$, for any nonzero vector $x\in\mathbb{C}^N$.*
4. *$A=A^*$, and the eigenvalues are strictly positive, $\lambda_i>0$.*
5. *$A=UDU^*$, with $U\in U_N$ and with $D\in M_N(\mathbb{R}_+^*)$ diagonal.*

Proof. This follows either from Theorem 5.20, by adding the various extra assumptions in the statement, or from the proof of Theorem 5.20, by modifying where needed. □

Let us discuss now the case of the unitary matrices. We have here:

Theorem 5.22. *Any matrix $U\in M_N(\mathbb{C})$ which is unitary, $U^*=U^{-1}$, is diagonalizable, with the eigenvalues on $\mathbb{T}$. More precisely we have*

$$U=VDV^*$$

with $V\in U_N$, and with $D\in M_N(\mathbb{T})$ diagonal. The converse holds too.

PROOF. As a first remark, the converse trivially holds, because given a matrix of type $U = VDV^*$, with $V \in U_N$, and with $D \in M_N(\mathbb{T})$ being diagonal, we have:

$$\begin{aligned} U^* &= (VDV^*)^* \\ &= VD^*V^* \\ &= VD^{-1}V^{-1} \\ &= (V^*)^{-1}D^{-1}V^{-1} \\ &= (VDV^*)^{-1} \\ &= U^{-1} \end{aligned}$$

Let us prove now the first assertion, stating that the eigenvalues of a unitary matrix $U \in U_N$ belong to $\mathbb{T}$. Indeed, assuming $Uv = \lambda v$, we have:

$$\begin{aligned} < v, v > &= < U^*Uv, v > \\ &= < Uv, Uv > \\ &= < \lambda v, \lambda v > \\ &= |\lambda|^2 < v, v > \end{aligned}$$

Thus we obtain $\lambda \in \mathbb{T}$, as claimed. Our next claim now is that the eigenspaces corresponding to different eigenvalues are pairwise orthogonal. Assume indeed that:

$$Uv = \lambda v \quad , \quad Uw = \mu w$$

We have then the following computation, using $U^* = U^{-1}$ and $\lambda, \mu \in \mathbb{T}$:

$$\begin{aligned} \lambda < v, w > &= < \lambda v, w > \\ &= < Uv, w > \\ &= < v, U^*w > \\ &= < v, U^{-1}w > \\ &= < v, \mu^{-1}w > \\ &= \mu < v, w > \end{aligned}$$

Thus $\lambda \neq \mu$ implies $v \perp w$, as claimed. In order now to finish the proof, it remains to prove that the eigenspaces of U span the whole space $\mathbb{C}^N$. For this purpose, we will use a recurrence method. Let us pick an eigenvector of our matrix:

$$Uv = \lambda v$$

Assuming that we have a vector w orthogonal to it, $v \perp w$, we have:

$$\begin{aligned}< Uw, v > &= < w, U^*v > \\ &= < w, U^{-1}v > \\ &= < w, \lambda^{-1}v > \\ &= \lambda < w, v > \\ &= 0\end{aligned}$$

Thus, if v is an eigenvector, then the vector space $v^\perp$ is invariant under U. Now since U is an isometry, so is its restriction to this space $v^\perp$. Thus this restriction is a unitary, and so we can proceed by recurrence, and we obtain the result. □

The self-adjoint matrices and the unitary matrices are particular cases of the general notion of a "normal matrix", and we have here:

THEOREM 5.23. *Any matrix $A \in M_N(\mathbb{C})$ which is normal, $AA^* = A^*A$, is diagonalizable, with the diagonalization being of the following type,*

$$A = UDU^*$$

with $U \in U_N$, and with $D \in M_N(\mathbb{C})$ diagonal. The converse holds too.

PROOF. As a first remark, the converse trivially holds, because if we take a matrix of the form $A = UDU^*$, with U unitary and D diagonal, then we have:

$$\begin{aligned}AA^* &= UDU^* \cdot UD^*U^* \\ &= UDD^*U^* \\ &= UD^*DU^* \\ &= UD^*U^* \cdot UDU^* \\ &= A^*A\end{aligned}$$

In the other sense now, this is something more technical. Our first claim is that a matrix A is normal precisely when the following happens, for any vector v:

$$||Av|| = ||A^*v||$$

Indeed, the above equality can be written as follows:

$$< AA^*v, v >=< A^*Av, v >$$

But this is equivalent to $AA^* = A^*A$, by expanding the scalar products. Our next claim is that A, A^* have the same eigenvectors, with conjugate eigenvalues:

$$Av = \lambda v \implies A^*v = \bar{\lambda}v$$

Indeed, this follows from the following computation, and from the trivial fact that if A is normal, then so is any matrix of type $A-\lambda 1_N$:

$$\begin{aligned}||(A^*-\bar{\lambda}1_N)v|| &= ||(A-\lambda 1_N)^*v||\\ &= ||(A-\lambda 1_N)v||\\ &= 0\end{aligned}$$

Let us prove now, by using this, that the eigenspaces of A are pairwise orthogonal. Assume that we have two eigenvectors, corresponding to different eigenvalues, $\lambda\neq\mu$:

$$Av=\lambda v \quad , \quad Aw=\mu w$$

We have the following computation, which shows that $\lambda\neq\mu$ implies $v\perp w$:

$$\begin{aligned}\lambda<v,w> &= <\lambda v,w>\\ &= <Av,w>\\ &= <v,A^*w>\\ &= <v,\bar{\mu}w>\\ &= \mu<v,w>\end{aligned}$$

In order to finish, it remains to prove that the eigenspaces of A span the whole $\mathbb{C}^N$. This is something that we have already seen for the self-adjoint matrices, and for unitaries, and we will use here these results, in order to deal with the general normal case. As a first observation, given an arbitrary matrix A, the matrix AA^* is self-adjoint:

$$(AA^*)^*=AA^*$$

Thus, we can diagonalize this matrix AA^*, as follows, with the passage matrix being a unitary, $V\in U_N$, and with the diagonal form being real, $E\in M_N(\mathbb{R})$:

$$AA^*=VEV^*$$

Now observe that, for matrices of type $A=UDU^*$, which are those that we supposed to deal with, we have the following formulae:

$$V=U \quad , \quad E=D\bar{D}$$

In particular, the matrices A and AA^* have the same eigenspaces. So, this will be our idea, proving that the eigenspaces of AA^* are eigenspaces of A. In order to do so, let us pick two eigenvectors v,w of the matrix AA^*, corresponding to different eigenvalues, $\lambda\neq\mu$. The eigenvalue equations are then as follows:

$$AA^*v=\lambda v \quad , \quad AA^*w=\mu w$$

We have the following computation, using the normality condition $AA^* = A^*A$, and the fact that the eigenvalues of AA^*, and in particular μ, are real:

$$\begin{aligned}\lambda < Av, w > &= < \lambda Av, w >\\ &= < A\lambda v, w >\\ &= < AAA^*v, w >\\ &= < AA^*Av, w >\\ &= < Av, AA^*w >\\ &= < Av, \mu w >\\ &= \mu < Av, w >\end{aligned}$$

We conclude that we have $< Av, w >= 0$. But this reformulates as follows:

$$\lambda \neq \mu \implies A(E_\lambda) \perp E_\mu$$

Now since the eigenspaces of AA^* are pairwise orthogonal, and span the whole $\mathbb{C}^N$, we deduce from this that these eigenspaces are invariant under A:

$$A(E_\lambda) \subset E_\lambda$$

But with this result in hand, we can finish. Indeed, we can decompose the problem, and the matrix A itself, following these eigenspaces of AA^*, which in practice amounts in saying that we can assume that we only have 1 eigenspace. Now by rescaling, this is the same as assuming that we have $AA^* = 1$. But with this, we are now into the unitary case, that we know how to solve, as explained in Theorem 5.22, and so done. □

As a first application, we have the following result:

THEOREM 5.24. *Given a matrix $A \in M_N(\mathbb{C})$, we can construct a matrix $|A|$ as follows, by using the fact that A^*A is diagonalizable, with positive eigenvalues:*

$$|A| = \sqrt{A^*A}$$

This matrix $|A|$ is then positive, and its square is $|A|^2 = A^*A$. In the case $N = 1$, we obtain in this way the usual absolute value of the complex numbers.

PROOF. Consider indeed the matrix A^*A, which is normal. According to Theorem 5.23, we can diagonalize this matrix as follows, with $U \in U_N$, and with D diagonal:

$$A = UDU^*$$

From $A^*A \geq 0$ we obtain $D \geq 0$. But this means that the entries of D are real, and positive. Thus we can extract the square root $\sqrt{D}$, and then set:

$$\sqrt{A^*A} = U\sqrt{D}U^*$$

Thus, we are basically done. Indeed, if we call this latter matrix $|A|$, then we are led to the conclusions in the statement. Finally, the last assertion is clear from definitions. □

We can now formulate a first polar decomposition result, as follows:

THEOREM 5.25. *Any invertible matrix $A\in M_N(\mathbb C)$ decomposes as*

$$A=U|A|$$

with $U\in U_N$, and with $|A|=\sqrt{A^*A}$ as above.

PROOF. This is routine, and follows by comparing the actions of $A,|A|$ on the vectors $v\in\mathbb C^N$, and deducing from this the existence of a unitary $U\in U_N$ as above. We will be back to this, later on, directly in the case of the linear operators on Hilbert spaces. □

Observe that at $N=1$ we obtain in this way the usual polar decomposition of the nonzero complex numbers. More generally now, we have the following result:

THEOREM 5.26. *Any square matrix $A\in M_N(\mathbb C)$ decomposes as*

$$A=U|A|$$

with U being a partial isometry, and with $|A|=\sqrt{A^*A}$ as above.

PROOF. Again, this follows by comparing the actions of $A,|A|$ on the vectors $v\in\mathbb C^N$, and deducing from this the existence of a partial isometry U as above. Alternatively, we can get this from Theorem 5.25, applied on the complement of the 0-eigenvectors. □

This was for our basic presentation of linear algebra. There are of course many other things that can be said, but we will come back to some of them in what follows, directly in the case of the linear operators on the arbitrary Hilbert spaces.

5e. Exercises

This was a very standard linear chapter, and as exercises here, we have:

EXERCISE 5.27. *Compute the matrices of all basic linear maps $f:\mathbb R^2\to\mathbb R^2$.*

EXERCISE 5.28. *Compute the matrix of the rank one projection on $\xi\in\mathbb C^N$.*

EXERCISE 5.29. *Diagonalize 50 matrices, and even better, 500 matrices.*

EXERCISE 5.30. *Check the details for the diagonalization of the flat matrix.*

EXERCISE 5.31. *Learn more about the resultant, and the discriminant.*

EXERCISE 5.32. *Learn also about the Cardano formulae, in degree 3, and 4.*

EXERCISE 5.33. *What can you say about the diagonalization of orthogonal matrices?*

EXERCISE 5.34. *Work out some explicit polar decomposition results.*

As bonus exercise, learn some more specialized results too, such as the Jordan form.

CHAPTER 6

Laws of matrices

6a. Diagonal matrices

We would like to discuss now some interesting applications of our various spectral theorems to probability theory. Let us start with something basic, as follows:

DEFINITION 6.1. *Let X be a probability space, that is, a space with a probability measure, and with the corresponding integration denoted E, and called expectation.*

1. *The random variables are the real functions $f\in L^\infty(X)$.*
2. *The moments of such a variable are the numbers $M_k(f)=E(f^k)$.*
3. *The law of such a variable is the measure given by $M_k(f)=\int_\mathbb{R}x^kd\mu_f(x)$.*

Here, and in what follows, we use the term "law" for "probability distribution", which means exactly the same thing, and is more convenient. Regarding now the fact that the law μ_f exists indeed, this is true, but not exactly trivial. By linearity, we would like to have a probability measure making hold the following formula, for any $P\in\mathbb{C}[X]$:

$$E(P(f))=\int_\mathbb{R}P(x)d\mu_f(x)$$

By using a standard continuity argument, it is enough to have this formula for the characteristic functions χ_I of the arbitrary measurable sets of real numbers $I\subset\mathbb{R}$:

$$E(\chi_I(f))=\int_\mathbb{R}\chi_I(x)d\mu_f(x)$$

But this latter formula, which reads $P(f\in I)=\mu_f(I)$, can serve as a definition for μ_f, and we are done. Alternatively, assuming some familiarity with measure theory, μ_f is the push-forward of the probability measure on X, via the function $f:X\to\mathbb{R}$.

Let us summarize this discussion in the form of a theorem, as follows:

THEOREM 6.2. *The law μ_f of a random variable f exists indeed, and we have*

$$E(\varphi(f))=\int_\mathbb{R}\varphi(x)d\mu_f(x)$$

for any integrable function $\varphi:\mathbb{R}\to\mathbb{C}$.

PROOF. This follows from the above discussion, and with the precise assumption on $\varphi : \mathbb{R} \to \mathbb{C}$, which is its integrability, in the abstract mathematical sense, being in fact something that we will not really need, in what follows. In fact, for most purposes we will get away with polynomials $\varphi \in \mathbb{C}[X]$, and by linearity this means that we can get away with monomials $\varphi(x) = x^k$, which brings us back to Definition 6.1 (3), as stated. □

Getting now to the case of the matrices $A \in M_N(\mathbb{C})$, here it is quite tricky to figure out what the law of A should mean, based on intuition only. So, in the lack of a bright idea, let us just reproduce Definition 6.1, with a few modifications, as follows:

DEFINITION 6.3. *Let $N \in \mathbb{N}$, and consider the algebra $M_N(\mathbb{C})$ of complex $N \times N$ matrices, with its normalized trace $tr : M_N(\mathbb{C}) \to \mathbb{C}$, given by $tr(A) = Tr(A)/N$.*

1. *We call random variables the self-adjoint matrices $A \in M_N(\mathbb{C})$.*
2. *The moments of such a variable are the numbers $M_k(A) = tr(A^k)$.*
3. *The law of such a variable is the measure given by $M_k(A) = \int_{\mathbb{R}} x^k d\mu_A(x)$.*

Here we have normalized the trace, as to have $tr(1) = 1$, in analogy with the formula $E(1) = 1$ from usual probability. By the way, as a piece of advice here, many confusions appear from messing up tr and Tr, and it is better ot forget about Tr, and always use tr. With the drawback that if you're a physicist, tr might get messed up in quick handwriting with the reduced Planck constant $\hbar = h/2\pi$. However, shall you ever face this problem, I have an advice here too, namely forgetting about h, and using h instead of $\hbar$.

Another comment is that we assumed in (1) that our matrix is self-adjoint, $A = A^*$, with the adjoint matrix being given, as usual, by the formula $(A^*)_{ij} = \bar{A}_{ji}$. Why this, because for instance at $N = 1$ we would like our matrix, which in the case $N = 1$ is a number, to be real, and so we must assume $A = A^*$. Of course there is still some discussion here, for instance because you might argue that why not assuming instead that the entries of A are real. But let us leave this for later, and in the meantime, just trust me. Or perhaps, let us trust Heisenberg, who used self-adjoint matrices. More later.

Back to work now, what we have in Definition 6.1 looks quite reasonable, but as before with the usual random variables $f \in L^\infty(X)$, some discussion is needed, in order to understand if the law μ_A exists indeed, and by which mechanism. And, good news here, in the case of the simplest matrices, the real diagonal ones, we have:

THEOREM 6.4. *For any diagonal matrix $A \in M_N(\mathbb{R})$ we have the formula*

$$tr(P(A)) = \frac{1}{N}(P(\lambda_1) + \ldots + P(\lambda_N))$$

where $\lambda_1, \ldots, \lambda_N \in \mathbb{R}$ are the diagonal entries of A. Thus the measure

$$\mu_A = \frac{1}{N}(\delta_{\lambda_1} + \ldots + \delta_{\lambda_N})$$

can be regarded as being the law of A, in the sense of Definition 6.3.

PROOF. Assume indeed that we have a real diagonal matrix, as follows, with the convention that the matrix entries which are missing are by definition 0 entries:

$$A=\begin{pmatrix}\lambda_1\\&\ddots\\&&\lambda_N\end{pmatrix}$$

The powers of A are then diagonal too, given by the following formula:

$$A^k=\begin{pmatrix}\lambda_1^k\\&\ddots\\&&\lambda_N^k\end{pmatrix}$$

In fact, given any polynomial $P\in\mathbb C[X]$, we have the following formula:

$$P(A)=\begin{pmatrix}P(\lambda_1)\\&\ddots\\&&P(\lambda_N)\end{pmatrix}$$

Thus, the first formula in the statement holds indeed. In particular, we conclude that the moments of A are given by the following formula:

$$M_k(A)=tr(A^k)=\frac{1}{N}\sum_i\lambda_i^k$$

On the other hand, with $\mu_A=\frac{1}{N}(\delta_{\lambda_1}+\ldots+\delta_{\lambda_N})$ as in the statement, we have:

$$\begin{aligned}\int_{\mathbb R}x^kd\mu_A(x)&=\frac{1}{N}\sum_i\int_{\mathbb R}x^kd\delta_{\lambda_i}(x)\\&=\frac{1}{N}\sum_i\lambda_i^k\end{aligned}$$

Thus that the law of A exists indeed, and is the measure μ_A, as claimed. □

6b. Self-adjoint matrices

The point now is that, by using the spectral theorem for self-adjoint matrices, we have the following generalization of Theorem 6.4, dealing with the general case:

THEOREM 6.5. *For a self-adjoint matrix $A\in M_N(\mathbb C)$ we have the formula*

$$tr(P(A))=\frac{1}{N}(P(\lambda_1)+\ldots+P(\lambda_N))$$

where $\lambda_1,\ldots,\lambda_N\in\mathbb R$ are the eigenvalues of A. Thus the measure

$$\mu_A=\frac{1}{N}(\delta_{\lambda_1}+\ldots+\delta_{\lambda_N})$$

can be regarded as being the law of A, in the sense of Definition 6.3.

Proof. We already know, from Theorem 6.4, that the result holds indeed for the diagonal matrices. In the general case now, that of an arbitrary self-adjoint matrix, we know from chapter 5 that our matrix is diagonalizable, as follows:

$$A = UDU^*$$

Now observe that the moments of A are given by the following formula:

$$\begin{aligned} tr(A^k) &= tr(UDU^* \cdot UDU^* \ldots UDU^*) \\ &= tr(UD^kU^*) \\ &= tr(D^k) \end{aligned}$$

We conclude from this, by reasoning by linearity, that the matrices A, D have the same law, $\mu_A = \mu_D$, and this gives all the assertions in the statement. □

6c. Normal matrices

Let us start with the complex variables $f \in L^\infty(X)$. The main difference with respect to the real case comes from the fact that we have now a pair of variables instead of one, namely $f : X \to \mathbb{C}$ itself, and its conjugate $\bar{f} : X \to \mathbb{C}$. Thus, we are led to:

Definition 6.6. *The moments a complex variable $f \in L^\infty(X)$ are the numbers*

$$M_k(f) = E(f^k)$$

depending on colored integers $k = \circ \bullet \bullet \circ \ldots$, with the conventions

$$f^\emptyset = 1 \quad , \quad f^\circ = f \quad , \quad f^\bullet = \bar{f}$$

and multiplicativity, in order to define the colored powers f^k.

Observe that, since $f, \bar{f}$ commute, we can permute terms, and restrict the attention to exponents of type $k = \ldots \circ \circ \circ \bullet \bullet \bullet \bullet \ldots$, if we want to. However, our various results below will look better without doing this, so we will use Definition 6.6 as stated.

Regarding now the notion of law, this extends too, the result being as follows:

Theorem 6.7. *Each complex variable $f \in L^\infty(X)$ has a law, which is by definition a complex probability measure μ_f making the following formula hold,*

$$M_k(f) = \int_{\mathbb{C}} z^k d\mu_f(z)$$

for any colored integer k. Moreover, we have in fact the formula

$$E(\varphi(f)) = \int_{\mathbb{C}} \varphi(x) d\mu_f(x)$$

valid for any integrable function $\varphi : \mathbb{C} \to \mathbb{C}$.

PROOF. The first assertion follows exactly as in the real case, and with z^k being defined exactly as f^k, namely by the following formulae, and multiplicativity:

$$z^\emptyset = 1 \quad , \quad z^\circ = z \quad , \quad z^\bullet = \bar{z}$$

As for the second assertion, this basically follows from this by linearity and continuity, by using standard measure theory, again as in the real case. □

Moving ahead towards matrices, all this leads to a mixture of easy and complicated problems. First, Definition 6.6 has the following straightforward analogue:

DEFINITION 6.8. *The moments a matrix $A \in M_N(\mathbb{C})$ are the numbers*

$$M_k(A) = tr(A^k)$$

depending on colored integers $k = \circ\bullet\bullet\circ\ldots$, with the usual conventions

$$A^\emptyset = 1 \quad , \quad A^\circ = A \quad , \quad A^\bullet = A^*$$

and multiplicativity, in order to define the colored powers A^k.

As a first observation about this, unless the matrix is normal, $AA^* = A^*A$, we cannot switch to exponents of type $k = \ldots\circ\circ\circ\bullet\bullet\bullet\bullet\ldots$, as it was theoretically possible for the complex variables $f \in L^\infty(X)$. Here is an explicit counterexample for this:

PROPOSITION 6.9. *The following matrix, which is not normal,*

$$J = \begin{pmatrix}0&1\\0&0\end{pmatrix}$$

has the property $tr(JJ^*JJ^*) \neq tr(JJJ^*J^*)$.

PROOF. We have the following formulae, which show that J is not normal:

$$JJ^* = \begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix} = \begin{pmatrix}1&0\\0&0\end{pmatrix}$$

$$J^*J = \begin{pmatrix}0&0\\1&0\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix} = \begin{pmatrix}0&0\\0&1\end{pmatrix}$$

Let us compute now the quantities in the statement. We first have:

$$tr(JJ^*JJ^*) = tr((JJ^*)^2) = tr\begin{pmatrix}1&0\\0&0\end{pmatrix} = \frac{1}{2}$$

On the other hand, we have as well the following formula:

$$tr(JJJ^*J^*) = tr\left(\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix}\right) = tr\begin{pmatrix}0&0\\0&0\end{pmatrix} = 0$$

Thus, we are led to the conclusion in the statement. □

The above counterexample makes it quite clear that things will be complicated, when attempting to talk about the law of an arbitrary matrix $A \in M_N(\mathbb{C})$. But, there is solution to everything. By being a bit smart, we can formulate things as follows:

DEFINITION 6.10. *The law of a complex matrix $A \in M_N(\mathbb{C})$ is the following functional, on the algebra of polynomials in two noncommuting variables X, X^*:*

$$\mu_A : \mathbb{C} < X, X^* > \to \mathbb{C} \quad , \quad P \to tr(P(A))$$

In the case where we have a complex probability measure $\mu_A \in \mathcal{P}(\mathbb{C})$ such that

$$tr(P(A)) = \int_{\mathbb{C}} P(x)\, d\mu_A(x)$$

we identify this complex measure with the law of A.

As mentioned above, this is something smart, that will take us some time to understand. As a first observation, knowing the law is the same as knowing the moments, because if we write our polynomial as $P = \sum_k c_k X^k$, then we have:

$$tr(P(A)) = tr\left(\sum_k c_k A^k\right) = \sum_k c_k M_k(A)$$

Let us try now to compute some matrix laws, and see what we get. We already did some computations in the real case, and then for the basic 2×2 Jordan block J too, and based on all this, we can formulate the following result, with mixed conclusions:

THEOREM 6.11. *The following happen:*

(1) *If $A = A^*$ then $\mu_A = \frac{1}{N}(\lambda_1 + \ldots + \lambda_N)$, with $\lambda_i \in \mathbb{R}$ being the eigenvalues.*
(2) *If A is diagonal, $\mu_A = \frac{1}{N}(\lambda_1 + \ldots + \lambda_N)$, with $\lambda_i \in \mathbb{C}$ being the eigenvalues.*
(3) *For the basic Jordan block J, the law μ_J is not a complex measure.*
(4) *In fact, assuming $AA^* \neq A^*A$, the law μ_A is not a complex measure.*

PROOF. This follows from the above, with only (4) being new. Assuming $AA^* \neq A^*A$, in order to show that μ_A is not a measure, we can use a positivity trick, as follows:

$$\begin{aligned}
AA^* - A^*A \neq 0 \quad &\Longrightarrow \quad (AA^* - A^*A)^2 > 0\\
&\Longrightarrow \quad AA^*AA^* - AA^*A^*A - A^*AAA^* + A^*AA^*A > 0\\
&\Longrightarrow \quad tr(AA^*AA^* - AA^*A^*A - A^*AAA^* + A^*AA^*A) > 0\\
&\Longrightarrow \quad tr(AA^*AA^* + A^*AA^*A) > tr(AA^*A^*A + A^*AAA^*)\\
&\Longrightarrow \quad tr(AA^*AA^*) > tr(AAA^*A^*)
\end{aligned}$$

Thus, we can conclude as in the proof for J, the point being that we cannot obtain both the above numbers by integrating $|z|^2$ with respect to a measure $\mu_A \in \mathcal{P}(\mathbb{C})$. □

Fortunately, by using the spectral theorem for normal matrices, we have:

Theorem 6.12. *Given a matrix $A \in M_N(\mathbb{C})$ which is normal, $AA^* = A^*A$, we have the following formula, valid for any polynomial $P \in \mathbb{C} < X, X^* >$,*

$$tr(P(A)) = \frac{1}{N}(P(\lambda_1) + \ldots + P(\lambda_N))$$

where $\lambda_1, \ldots, \lambda_N \in \mathbb{C}$ are the eigenvalues of A. Thus the complex measure

$$\mu_A = \frac{1}{N}(\delta_{\lambda_1} + \ldots + \delta_{\lambda_N})$$

is the law of A. In the non-normal case, the law μ_A is not a measure.

Proof. As before in the diagonal case, since our matrix is normal, $AA^* = A^*A$, knowing its law in the abstract sense of generalized probability is the same as knowing the restriction of this abstract distribution to the usual polynomials in two variables:

$$\mu_A : \mathbb{C}[X, X^*] \to \mathbb{C} \quad , \quad P \to tr(P(A))$$

In order now to compute this functional, we can write $A = UDU^*$, as in chapter 5, and then change the basis via U, which in practice means that we can simply assume $U = 1$. Thus if we denote by $\lambda_1, \ldots, \lambda_N$ the diagonal entries of D, which are the eigenvalues of A, the law that we are looking for is the following functional:

$$\mu_A : \mathbb{C}[X, X^*] \to \mathbb{C} \quad , \quad P \to \frac{1}{N}(P(\lambda_1) + \ldots + P(\lambda_N))$$

But this functional corresponds to integrating P with respect to the following complex measure, that we agree to still denote by μ_A, and call distribution of A:

$$\mu_A = \frac{1}{N}(\delta_{\lambda_1} + \ldots + \delta_{\lambda_N})$$

Thus, we are led to the conclusion in the statement. □

6d. Some speculations

Good news, with our linear algebra knowledge, we have now enough ingredients for developing a "baby theory" of quantum spaces. Let us start in the following way:

Speculation 6.13. *Since the algebra $A = M_n(\mathbb{C})$ is isomorphic as vector space with $\mathbb{C}^{n^2} = C(1, \ldots, n^2)$, we can think of it as being of the following form, with M_n being some sort of "quantum space", and with $\sim$ standing for some sort of "twisting":*

$$A = C(M_n) \quad , \quad M_n \sim \{1, \ldots, n^2\}$$

And this quantum space M_n might be useful in dealing with quantum mechanics, where things are a bit "fuzzy", with the particles having undefined positions and speeds.

And take this as this comes, with this depending on your physics knowledge. To be more precise, you surely know that in quantum mechanics things are a bit "fuzzy", as said above, and so anything mathematical of classical type, be that usual curves, surfaces, manifolds $X \subset \mathbb{R}^N$, or even finite spaces like $\{1, \ldots, N\}$, which were originally designed in order to help with classical mechanics, will normally fail in that setting. Thus, we are genuinely interested in all sorts of crazy mathematical "quantum spaces", any idea being welcome, in the hope that such spaces can help us in quantum mechanics.

In a word, Speculation 6.13, and anything similar, is definitely welcome. But then, thinking a bit more at all this, the above space M_n is not that crazy as in seems, I mean come up if you can with a mathematical construction of a "quantum space" which is less crazy. So, as a conclusion, Speculation 6.13 is not only welcome, but warmly welcome, if the gods of quantum mechanics are with us, spaces like M_n might be the answer.

Less speculatively now, and assuming that you know some physics, at $n = 2$, which is of particular interest, you surely know that talking about the electron spin requires the Pauli matrices, which look as follows, and form a basis of the algebra $M_2(\mathbb{C})$:

$$c_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad c_2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad , \quad c_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad , \quad c_4 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Thus, Speculation 6.13 at $n = 2$ is in fact something corresponding to a deep finding in physics, and worth a Nobel Prize, the one won by Pauli for his work.

In any case, beginner level or not, you must agree with me that Speculation 6.13 is something to be taken seriously. So, let us further speculate on that. We have:

SPECULATION 6.14. *Regarding M_n, we can even have a geometric picture of it,*

$$\begin{matrix} \bullet_{11} & \bullet_{12} & \cdots & \bullet_{1n} \\ \bullet_{21} & \bullet_{22} & \cdots & \bullet_{2n} \\ \vdots & & & \vdots \\ \bullet_{n1} & \bullet_{n2} & \cdots & \bullet_{nn} \end{matrix}$$

with each formal point $\bullet_{ij}$ standing for the corresponding elementary matrix

$$e_{ij} : e_j \to e_i$$

based on the observation that these matrices form a basis of $A = C(M_n)$.

To be more precise here, let us first examine the classical space $X = \{1, \ldots, n^2\}$. We can represent this space by a series of n^2 points, as everyone does, as follows:

$$\bullet_1 \quad \bullet_2 \quad \cdots \quad \bullet_{n^2}$$

Now if we look at the algebra of functions $C(X) = \mathbb{C}^{n^2}$, this is spanned by the Dirac masses δ_i, one for each of the points $\bullet_i$. Thus, we can say that "spaces are described by the functions on them", and we are led in this way to the above picture of M_n.

All this is quite interesting, we have some beginning of mathematics here, for our mysterious space M_n. And we can further speculate on this, in the following way:

SPECULATION 6.15. *The twisting operation $\{1,\ldots,n^2\} \to M_n$, which reads*

$$\bullet_1 \quad \bullet_2 \quad \ldots \quad \bullet_{n^2} \qquad \rightsquigarrow \qquad \begin{matrix} \bullet_{11} & \ldots & \bullet_{1n} \\ \vdots & & \vdots \\ \bullet_{n1} & \ldots & \bullet_{nn} \end{matrix}$$

amounts in changing the multiplication rule on the vector space $\mathbb{C}^{n^2}$, as follows,

$$e_ie_j = \delta_{ij}e_i \qquad \rightsquigarrow \qquad e_{ij}e_{kl} = \delta_{jk}e_{il}$$

at the level of the standard basis, in each case.

To be more precise, here we are using the same philosophy as for Speculation 6.14, namely that "spaces are described by the functions on them", and in what regards the multiplication formulae, we first have $e_ie_j = \delta_{ij}e_i$, which is the familiar multiplication rule for the Dirac masses on $\{1,\ldots,n^2\}$, and then we have $e_{ij}e_{kl} = \delta_{jk}e_{il}$, which is the familiar multiplication rule for the matrix units $e_{ij} : e_j \to e_i$, from Speculation 6.14.

More in detail now, we would like to have a formula as follows, with the operation $A \to A^\sigma$ being something that destroys the commutativity of the multiplication:

$$C(M_n) = C(1,\ldots,n^2)^\sigma$$

In more familiar terms, with usual complex matrices on the left, and with a better-looking product of sets being used on the right, this formula reads:

$$M_n(\mathbb{C}) = C\Big(\{1,\ldots,n\} \times \{1,\ldots,n\}\Big)^\sigma$$

In order to establish this formula, consider the algebra on the right. As a complex vector space, this algebra has the standard basis $\{f_{ij}\}$ formed by the Dirac masses at the points (i,j), and the multiplicative structure of this algebra is given by:

$$f_{ij}f_{kl} = \delta_{ij,kl}$$

Now let us twist this multiplication, according to the formula $e_{ij}e_{kl} = \delta_{jk}e_{il}$. We obtain in this way the usual combination formulae for the standard matrix units $e_{ij} : e_j \to e_i$ of the algebra $M_n(\mathbb{C})$, and so we have our twisting result, as claimed.

As a further comment, at $n=2$, coming as a continuation of our previous comment on the Pauli matrices, in case you are familiar with these, you might argue that why using e_{ij} instead of these Pauli matrices. Good point, and we will be back to this, later.

Very nice all this, and as a natural question now, we have:

QUESTION 6.16. *How to unify the theory of classical finite spaces $\{1,\ldots,N\}$ with the theory of quantum finite spaces of type M_n, that we are currently building?*

In answer, we can look at multimatrix algebras, and we have:

SPECULATION 6.17. *We can call finite quantum spaces the spaces of type*

$$X = M_{n_1} \sqcup \ldots \sqcup M_{n_k}$$

coming according to the following formula, for the associated algebras of functions:

$$C(X) = M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_k}(\mathbb{C})$$

The cardinality $|X|$ of such a space is by definition $N = n_1^2 + \ldots + n_k^2$.

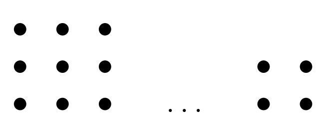
To be more precise, we are saying this in view of the following formula, valid for any two finite sets X, Y, and which is something very elementary:

$$C(X \sqcup Y) = C(X) \oplus C(Y)$$

Indeed, staying a bit speculatory, of course, we can take this as a definition for the disjoint union of finite quantum spaces, and with this in hand, we have the following computation, fully justifying what was said in the above:

$$\begin{aligned} C(M_{n_1} \sqcup \ldots \sqcup M_{n_k}) &= C(M_{n_1}) \oplus \ldots \oplus C(M_{n_k}) \\ &= M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_k}(\mathbb{C}) \end{aligned}$$

In any case, Speculation 6.17 looks very good, and fully answers Question 6.16. And as further good news here, we even have pictures for these general finite quantum spaces, generalizing our previous pictures for M_n and for $\{1,\ldots,N\}$. Indeed, given a direct sum of matrix algebras, $A = M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_k}(\mathbb{C})$, we can represent each matrix block as a square, and we end up with a picture like this, representing A:



But looking at this picture, we can say that this represents the space X itself. For instance the number of points is the correct one, $|X| = \dim A$. Also, in the case $A = \mathbb{C}^N$, the picture that we get, $\bullet\ \bullet\ \ldots\ \bullet$, is the correct picture of X, as a space of points. More generally, when $n_i = 1$, the associated point $\bullet$ is a true point of X. And so on.

As a related speculation now, we can talk as well about products of finite quantum spaces, defined according to the following formula:

$$C(X \times Y) = C(X) \otimes C(Y)$$

To be more precise, this is something well-known, and elementary, for any two finite sets X, Y, and in view of this, we can take it as a definition for $X \times Y$, in general. And again, all this is compatible with what we previously knew about M_n and $\{1, \ldots, N\}$.

Very nice all this. As a last topic of discussion, we must still extend what we have to the case of the multimatrix algebras, and the result here, including what we knew from before, of algebraic nature, regarding the multimatrix algebras, is as follows:

SPECULATION 6.18. *We can call finite quantum spaces the spaces of type*

$$X = M_{n_1} \sqcup \ldots \sqcup M_{n_k}$$

coming according to the following formula, for the associated algebras of functions:

$$C(X) = M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_k}(\mathbb{C})$$

The cardinality $|X|$ of such a space is by definition the following number,

$$N = n_1^2 + \ldots + n_k^2$$

and the possible traces are as follows, with $\lambda_i > 0$ summing up to 1:

$$tr = \lambda_1 tr_1 \oplus \ldots \oplus \lambda_k tr_k$$

Among these traces, we have the canonical trace, appearing as

$$tr : C(X) \subset \mathcal{L}(C(X)) \to \mathbb{C}$$

via the left regular representation, having weights $\lambda_i = n_i^2/N$.

To be more precise, these are things that we already know from before, save for the last assertion, which is new, and needs some explanations. Consider the left regular representation of our algebra $A = C(X)$, which is given by the following formula:

$$\pi : A \subset \mathcal{L}(A) \quad , \quad \pi(a) : b \to ab$$

We know that the algebra $\mathcal{L}(A)$ of linear operators $T : A \to A$ is isomorphic to a matrix algebra, and more specifically to $M_N(\mathbb{C})$, with $N = |X|$ being as before:

$$\mathcal{L}(A) \simeq M_N(\mathbb{C})$$

Thus, this algebra has a trace $tr : \mathcal{L}(A) \to \mathbb{C}$, and by composing this trace with the representation π, we obtain a certain trace $tr : A \to \mathbb{C}$, that we can call "canonical":

$$tr : A \subset \mathcal{L}(A) \to \mathbb{C}$$

In practice now, and in order to avoid too much abstraction, we can compute the weights of this trace by using a multimatrix basis of A, formed by matrix units e^i_{ab}, with $i \in \{1, \ldots, k\}$ and with $a, b \in \{1, \ldots, n_i\}$, and we obtain, as claimed:

$$\lambda_i = \frac{n_i^2}{N}$$

It is possible to speculate some more, along the same lines, but enough work done for the day, let us formulate our conclusions, which are quite good, as follows:

CONCLUSION 6.19. *Spaces like M_n are the simplest possible "quantum spaces", mathematically speaking, and we definitely have tools, including pictures, for dealing with them. With a bit of luck, these might help in quantum physics, which needs such spaces.*

Of course, all this was a bit subjective, and many things remain to be clarified. But no worries, we will be back to this soon, with full mathematical details.

6e. Exercises

Exercises:

EXERCISE 6.20.

EXERCISE 6.21.

EXERCISE 6.22.

EXERCISE 6.23.

EXERCISE 6.24.

EXERCISE 6.25.

EXERCISE 6.26.

EXERCISE 6.27.

Bonus exercise.

CHAPTER 7

Basic examples

7a. Basic examples

Basic examples.

7b. Further examples

Further examples.

7c. Advanced theory

Advanced theory.

7d. Some conclusions

Some conclusions.

7e. Exercises

Exercises:

Exercise 7.1.

Exercise 7.2.

Exercise 7.3.

Exercise 7.4.

Exercise 7.5.

Exercise 7.6.

Exercise 7.7.

Exercise 7.8.

Bonus exercise.

CHAPTER 8

Beyond normality

8a. Jordan blocks

Jordan blocks.

8b. Into combinatorics

Into combinatorics.

8c. Further computations

Further computations.

8d. Discrete distributions

Discrete distributions.

8e. Exercises

Exercises:

Exercise 8.1.

Exercise 8.2.

Exercise 8.3.

Exercise 8.4.

Exercise 8.5.

Exercise 8.6.

Exercise 8.7.

Exercise 8.8.

Bonus exercise.

Part III

Random matrices

CHAPTER 9

Spectral theory

9a. Linear operators

We would like to first discuss the theory of linear operators $T : H \to H$ over a complex Hilbert space H, usually taken separable. Let us start with a basic result, as follows:

THEOREM 9.1. *Given a Hilbert space H, consider the linear operators $T : H \to H$, and for each such operator define its norm by the following formula:*

$$||T|| = \sup_{||x||=1} ||Tx||$$

The operators which are bounded, $||T|| < \infty$, form then a complex algebra $B(H)$, which is complete with respect to $||.||$. When H comes with a basis $\{e_i\}_{i\in I}$, we have

$$B(H) \subset M_I(\mathbb{C})$$

with the correspondence $T \to M$ coming via the usual linear algebra formulae, namely:

$$T(x) = Mx \quad , \quad M_{ij} = < Te_j, e_i >$$

In infinite dimensions, the inclusion $B(H) \subset M_I(\mathbb{C})$ is not an equality.

PROOF. This is something straightforward, the idea being as follows:

(1) The fact that we have indeed an algebra, satisfying the product condition in the statement, follows from the following estimates, which are all elementary:

$$||S + T|| \leq ||S|| + ||T||$$

$$||\lambda T|| = |\lambda| \cdot ||T||$$

$$||ST|| \leq ||S|| \cdot ||T||$$

(2) Regarding now the completness assertion, if $\{T_n\} \subset B(H)$ is Cauchy then $\{T_n x\}$ is Cauchy for any $x \in H$, so we can define the limit $T = \lim_{n\to\infty} T_n$ by setting:

$$Tx = \lim_{n\to\infty} T_n x$$

Let us first check that the application $x \to Tx$ is linear. We have:

$$\begin{aligned} T(x+y) &= \lim_{n\to\infty} T_n(x+y) \\ &= \lim_{n\to\infty} T_n(x)+T_n(y) \\ &= \lim_{n\to\infty} T_n(x)+\lim_{n\to\infty} T_n(y) \\ &= T(x)+T(y) \end{aligned}$$

Similarly, we have $T(\lambda x) = \lambda T(x)$, and we conclude that $T \in \mathcal{L}(H)$.

(3) With this done, it remains to prove now that we have $T \in B(H)$, and that $T_n \to T$ in norm. For this purpose, observe that we have:

$$\begin{aligned} ||T_n - T_m|| \leq \varepsilon\ ,\ \forall n,m \geq N &\implies ||T_n x - T_m x|| \leq \varepsilon\ ,\ \forall ||x|| = 1\ ,\ \forall n,m \geq N \\ &\implies ||T_n x - Tx|| \leq \varepsilon\ ,\ \forall ||x|| = 1\ ,\ \forall n \geq N \\ &\implies ||T_N x - Tx|| \leq \varepsilon\ ,\ \forall ||x|| = 1 \\ &\implies ||T_N - T|| \leq \varepsilon \end{aligned}$$

But this gives both $T \in B(H)$, and $T_N \to T$ in norm, and we are done.

(4) Regarding the embedding, the correspondence $T \to M$ in the statement is indeed linear, and its kernel is $\{0\}$, so we have indeed an embedding as follows, as claimed:

$$B(H) \subset M_I(\mathbb{C})$$

In finite dimensions we have an isomorphism, because any $M \in M_N(\mathbb{C})$ determines an operator $T : \mathbb{C}^N \to \mathbb{C}^N$, given by $< Te_j, e_i >= M_{ij}$. However, in infinite dimensions, we have matrices not producing operators, as for instance the all-one matrix. □

As a second basic result regarding the operators, we will need:

Theorem 9.2. *Each operator $T \in B(H)$ has an adjoint $T^* \in B(H)$, given by:*

$$< Tx, y >=< x, T^*y >$$

The operation $T \to T^*$ is antilinear, antimultiplicative, involutive, and satisfies:

$$||T|| = ||T^*|| \quad , \quad ||TT^*|| = ||T||^2$$

When H comes with a basis $\{e_i\}_{i\in I}$, the operation $T \to T^*$ corresponds to

$$(M^*)_{ij} = \overline{M}_{ji}$$

at the level of the associated matrices $M \in M_I(\mathbb{C})$.

Proof. This is standard too, and can be proved in 3 steps, as follows:

(1) The existence of the adjoint operator T^*, given by the formula in the statement, comes from the fact that the function $\varphi(x) =< Tx, y >$ being a linear map $H \to \mathbb{C}$, we must have a formula as follows, for a certain vector $T^*y \in H$:

$$\varphi(x) =< x, T^*y >$$

Moreover, since this vector is unique, T^* is unique too, and we have as well:

$$(S+T)^* = S^* + T^* \quad , \quad (\lambda T)^* = \bar{\lambda} T^* \quad , \quad (ST)^* = T^*S^* \quad , \quad (T^*)^* = T$$

Observe also that we have indeed $T^* \in B(H)$, because:

$$\begin{aligned} ||T|| &= \sup_{||x||=1} \sup_{||y||=1} < Tx, y > \\ &= \sup_{||y||=1} \sup_{||x||=1} < x, T^*y > \\ &= ||T^*|| \end{aligned}$$

(2) Regarding now $||TT^*|| = ||T||^2$, which is a key formula, observe that we have:

$$||TT^*|| \leq ||T|| \cdot ||T^*|| = ||T||^2$$

On the other hand, we have as well the following estimate:

$$\begin{aligned} ||T||^2 &= \sup_{||x||=1} | < Tx, Tx > | \\ &= \sup_{||x||=1} | < x, T^*Tx > | \\ &\leq ||T^*T|| \end{aligned}$$

By replacing $T \to T^*$ we obtain from this $||T||^2 \leq ||TT^*||$, as desired.

(3) Finally, when H comes with a basis, the formula $< Tx, y >=< x, T^*y >$ applied with $x = e_i$, $y = e_j$ translates into the formula $(M^*)_{ij} = \overline{M}_{ji}$, as desired. □

Let us discuss now the diagonalization problem for the operators $T \in B(H)$, in analogy with the diagonalization problem for the usual matrices $A \in M_N(\mathbb{C})$. As a first observation, we can talk about eigenvalues and eigenvectors, as follows:

Definition 9.3. *Given an operator $T \in B(H)$, assuming that we have*

$$Tx = \lambda x$$

we say that $x \in H$ is an eigenvector of T, with eigenvalue $\lambda \in \mathbb{C}$.

We know many things about eigenvalues and eigenvectors, in the finite dimensional case. However, most of these will not extend to the infinite dimensional case, or at least not extend in a straightforward way, due to a number of reasons:

(1) Most of basic linear algebra is based on the fact that $Tx = \lambda x$ is equivalent to $(T-\lambda)x = 0$, so that λ is an eigenvalue when $T-\lambda$ is not invertible. In the infinite dimensional setting $T-\lambda$ might be injective and not surjective, or vice versa, or invertible with $(T-\lambda)^{-1}$ not bounded, and so on.

(2) Also, in linear algebra $T-\lambda$ is not invertible when $\det(T-\lambda)=0$, and with this leading to most of the advanced results about eigenvalues and eigenvectors. In infinite dimensions, however, it is impossible to construct a determinant function $\det : B(H) \to \mathbb{C}$, and this even for the diagonal operators on $l^2(\mathbb{N})$.

Summarizing, we are in trouble. Forgetting about (2), which obviously leads nowhere, let us focus on the difficulties in (1). In order to cut short the discussion there, regarding the various properties of $T-\lambda$, we can just say that $T-\lambda$ is either invertible with bounded inverse, the "good case", or not. We are led in this way to the following definition:

Definition 9.4. *The spectrum of an operator $T \in B(H)$ is the set*

$$\sigma(T) = \left\{\lambda \in \mathbb{C}\Big| T-\lambda \notin B(H)^{-1}\right\}$$

where $B(H)^{-1} \subset B(H)$ is the set of invertible operators.

As a basic example, in the finite dimensional case, $H = \mathbb{C}^N$, the spectrum of a usual matrix $A \in M_N(\mathbb{C})$ is the collection of its eigenvalues, taken without multiplicities. We will see many other examples. In general, the spectrum has the following properties:

Proposition 9.5. *The spectrum of $T \in B(H)$ contains the eigenvalue set*

$$\varepsilon(T) = \left\{\lambda \in \mathbb{C}\Big| \ker(T-\lambda) \neq \{0\}\right\}$$

and $\varepsilon(T) \subset \sigma(T)$ is an equality in finite dimensions, but not in infinite dimensions.

Proof. We have several assertions here, the idea being as follows:

(1) First of all, the eigenvalue set is indeed the one in the statement, because $Tx = \lambda x$ tells us precisely that $T-\lambda$ must be not injective. The fact that we have $\varepsilon(T) \subset \sigma(T)$ is clear as well, because if $T-\lambda$ is not injective, it is not bijective.

(2) In finite dimensions we have $\varepsilon(T) = \sigma(T)$, because $T-\lambda$ is injective if and only if it is bijective, with the boundedness of the inverse being automatic.

(3) In infinite dimensions we can assume $H = l^2(\mathbb{N})$, and the shift operator $S(e_i) = e_{i+1}$ is injective but not surjective. Thus $0 \in \sigma(T) - \varepsilon(T)$. □

Philosophically, the best way of thinking at this is as follows: the numbers $\lambda \notin \sigma(T)$ are good, because we can invert $T-\lambda$, the numbers $\lambda \in \sigma(T) - \varepsilon(T)$ are bad, because so they are, and the eigenvalues $\lambda \in \varepsilon(T)$ are evil. Welcome to operator theory.

Let us develop now some general theory. As a first goal, we would like to prove that the spectra are non-empty. This is something quite tricky, the result being as follows:

THEOREM 9.6. *The spectrum of a bounded operator $T \in B(H)$ is:*
(1) *Compact.*
(2) *Contained in the disc $D_0(||T||)$.*
(3) *Non-empty.*

PROOF. This can be proved by using some complex analysis, as follows:

(1) In view of (2) below, it is enough to prove that $\sigma(T)$ is closed. But this follows from the following computation, with $|\varepsilon|$ being small:

$$\begin{aligned}\lambda \notin \sigma(T) &\implies T - \lambda \in B(H)^{-1}\\ &\implies T - \lambda - \varepsilon \in B(H)^{-1}\\ &\implies \lambda + \varepsilon \notin \sigma(T)\end{aligned}$$

(2) This follows indeed from the following computation:

$$\begin{aligned}\lambda > ||T|| &\implies \left|\left|\frac{T}{\lambda}\right|\right| < 1\\ &\implies 1 - \frac{T}{\lambda} \in B(H)^{-1}\\ &\implies \lambda - T \in B(H)^{-1}\\ &\implies \lambda \notin \sigma(T)\end{aligned}$$

(3) Assume by contradiction $\sigma(T) = \emptyset$. Given a linear form $f \in B(H)^*$, consider the following map, which is well-defined, due to our assumption $\sigma(T) = \emptyset$:

$$\varphi : \mathbb{C} \to \mathbb{C} \quad , \quad \lambda \to f((T - \lambda)^{-1})$$

By using the fact that $T \to T^{-1}$ is differentiable, which is something elementary, we conclude that this map is differentiable, and so holomorphic. Also, we have:

$$\begin{aligned}\lambda \to \infty &\implies T - \lambda \to \infty\\ &\implies (T - \lambda)^{-1} \to 0\\ &\implies f((T - \lambda))^{-1} \to 0\end{aligned}$$

Thus by the Liouville theorem we obtain $\varphi = 0$. But, in view of the definition of φ, this gives $(T - \lambda)^{-1} = 0$, which is a contradiction, as desired. □

Here is now a second basic result regarding the spectra, inspired from what happens in finite dimensions, for the usual complex matrices, and which shows that things do not necessarily extend without troubles to the infinite dimensional setting:

THEOREM 9.7. *We have the following formula, valid for any operators S, T:*

$$\sigma(ST) \cup \{0\} = \sigma(TS) \cup \{0\}$$

In finite dimensions we have $\sigma(ST) = \sigma(TS)$, but this fails in infinite dimensions.

PROOF. There are several assertions here, the idea being as follows:

(1) This is something that we know in finite dimensions, coming from the fact that the characteristic polynomials of the associated matrices A, B coincide:

$$P_{AB} = P_{BA}$$

Thus we obtain $\sigma(ST) = \sigma(TS)$ in this case, as claimed. Observe that this improves twice the general formula in the statement, first because we have no issues at 0, and second because what we obtain is actually an equality of sets with mutiplicities.

(2) In general now, let us first prove the main assertion, stating that $\sigma(ST), \sigma(TS)$ coincide outside 0. We first prove that we have the following implication:

$$1 \notin \sigma(ST) \implies 1 \notin \sigma(TS)$$

Assume indeed that $1 - ST$ is invertible, with inverse denoted R:

$$R = (1 - ST)^{-1}$$

We have then the following formulae, relating our variables R, S, T:

$$RST = STR = R - 1$$

By using $RST = R - 1$, we have the following computation:

$$\begin{aligned}(1 + TRS)(1 - TS) &= 1 + TRS - TS - TRSTS \\ &= 1 + TRS - TS - TRS + TS \\ &= 1\end{aligned}$$

A similar computation, using $STR = R - 1$, shows that we have:

$$(1 - TS)(1 + TRS) = 1$$

Thus $1 - TS$ is invertible, with inverse $1 + TRS$, which proves our claim. Now by multiplying by scalars, we deduce from this that for any $\lambda \in \mathbb{C} - \{0\}$ we have:

$$\lambda \notin \sigma(ST) \implies \lambda \notin \sigma(TS)$$

But this leads to the conclusion in the statement.

(3) Regarding now the counterexample to the formula $\sigma(ST) = \sigma(TS)$, in general, let us take S to be the shift on $H = L^2(\mathbb{N})$, given by the following formula:

$$S(e_i) = e_{i+1}$$

As for T, we can take it to be the adjoint of S, and we have:

$$S^*S = 1 \implies 0 \notin \sigma(SS^*)$$

$$SS^* = Proj(e_0^\perp) \implies 0 \in \sigma(SS^*)$$

Thus, the spectra do not match on 0, and so we have our counterexample. □

9b. Spectral radius

Let us develop now some systematic theory for the computation of the spectra, based on what we know about the eigenvalues of the usual complex matrices. As a first result, which is well-known for the usual matrices, and extends well, we have:

THEOREM 9.8. *We have the "polynomial functional calculus" formula*

$$\sigma(P(T)) = P(\sigma(T))$$

valid for any polynomial $P \in \mathbb{C}[X]$, and any operator $T \in B(H)$.

PROOF. We pick a scalar $\lambda \in \mathbb{C}$, and we decompose the polynomial $P - \lambda$:

$$P(X) - \lambda = c(X - r_1) \ldots (X - r_n)$$

We have then the following equivalences:

$$\begin{aligned} \lambda \notin \sigma(P(T)) &\iff P(T) - \lambda \in B(H)^{-1} \\ &\iff c(T - r_1) \ldots (T - r_n) \in B(H)^{-1} \\ &\iff T - r_1, \ldots, T - r_n \in B(H)^{-1} \\ &\iff r_1, \ldots, r_n \notin \sigma(T) \\ &\iff \lambda \notin P(\sigma(T)) \end{aligned}$$

Thus, we are led to the formula in the statement. □

The above result is something very useful, and generalizing it will be our next task. As a first ingredient here, assuming that $A \in M_N(\mathbb{C})$ is invertible, we have:

$$\sigma(A^{-1}) = \sigma(A)^{-1}$$

It is possible to extend this formula to the arbitrary operators, and we will do this in a moment. Before starting, however, we have to find a class of functions generalizing both the polynomials $P \in \mathbb{C}[X]$ and the inverse function $x \to x^{-1}$. The answer to this question is provided by the rational functions, which are as follows:

DEFINITION 9.9. *A rational function $f \in \mathbb{C}(X)$ is a quotient of polynomials:*

$$f = \frac{P}{Q}$$

Assuming that P, Q are prime to each other, we can regard f as a usual function,

$$f : \mathbb{C} - X \to \mathbb{C}$$

with X being the set of zeros of Q, also called poles of f.

Now that we have our class of functions, the next step consists in applying them to operators. Here we cannot expect $f(T)$ to make sense for any f and any T, for instance because T^{-1} is defined only when T is invertible. We are led in this way to:

Definition 9.10. *Given an operator $T\in B(H)$, and a rational function $f=P/Q$ having poles outside $\sigma(T)$, we can construct the following operator,*

$$f(T)=P(T)Q(T)^{-1}$$

that we can denote as a usual fraction, as follows,

$$f(T)=\frac{P(T)}{Q(T)}$$

due to the fact that $P(T),Q(T)$ commute, so that the order is irrelevant.

To be more precise, $f(T)$ is indeed well-defined, and the fraction notation is justified too. In more formal terms, we can say that we have a morphism of complex algebras as follows, with $\mathbb{C}(X)^T$ standing for the rational functions having poles outside $\sigma(T)$:

$$\mathbb{C}(X)^T\to B(H)\quad,\quad f\to f(T)$$

Summarizing, we have now a good class of functions, generalizing both the polynomials and the inverse map $x\to x^{-1}$. We can now extend Theorem 9.8, as follows:

Theorem 9.11. *We have the "rational functional calculus" formula*

$$\sigma(f(T))=f(\sigma(T))$$

valid for any rational function $f\in\mathbb{C}(X)$ having poles outside $\sigma(T)$.

Proof. We pick a scalar $\lambda\in\mathbb{C}$, we write $f=P/Q$, and we set:

$$F=P-\lambda Q$$

By using now Theorem 9.9, for this polynomial, we obtain:

$$\begin{aligned}\lambda\in\sigma(f(T))&\iff F(T)\notin B(H)^{-1}\\&\iff 0\in\sigma(F(T))\\&\iff 0\in F(\sigma(T))\\&\iff \exists\mu\in\sigma(T),F(\mu)=0\\&\iff \lambda\in f(\sigma(T))\end{aligned}$$

Thus, we are led to the formula in the statement. □

As an application of the above methods, we can investigate certain special classes of operators, such as the self-adjoint ones, and the unitary ones. Let us start with:

Proposition 9.12. *The following happen:*

1. *We have $\sigma(T^*)=\overline{\sigma(T)}$, for any $T\in B(H)$.*
2. *If $T=T^*$ then $X=\sigma(T)$ satisfies $X=\overline{X}$.*
3. *If $U^*=U^{-1}$ then $X=\sigma(U)$ satisfies $X^{-1}=\overline{X}$.*

PROOF. We have several assertions here, the idea being as follows:

(1) The spectrum of the adjoint operator T^* can be computed as follows:

$$\begin{aligned}\sigma(T^*) &= \left\{\lambda\in\mathbb{C}\Big|T^*-\lambda\notin B(H)^{-1}\right\}\\ &= \left\{\lambda\in\mathbb{C}\Big|T-\bar{\lambda}\notin B(H)^{-1}\right\}\\ &= \overline{\sigma(T)}\end{aligned}$$

(2) This is clear indeed from (1).

(3) For a unitary operator, $U^*=U^{-1}$, Theorem 9.11 and (1) give:

$$\sigma(U)^{-1}=\sigma(U^{-1})=\sigma(U^*)=\overline{\sigma(U)}$$

Thus, we are led to the conclusion in the statement. □

In analogy with what happens for the usual matrices, we would like to improve now (2,3) above, with results stating that the spectrum $X=\sigma(T)$ satisfies $X\subset\mathbb{R}$ for self-adjoints, and $X\subset\mathbb{T}$ for unitaries. This will be tricky. Let us start with:

THEOREM 9.13. *The spectrum of a unitary operator*

$$U^*=U^{-1}$$

is on the unit circle, $\sigma(U)\subset\mathbb{T}$.

PROOF. Assuming $U^*=U^{-1}$, we have the following norm computation:

$$||U||=\sqrt{||UU^*||}=\sqrt{1}=1$$

Now if we denote by D the unit disk, we obtain from this:

$$\sigma(U)\subset D$$

On the other hand, once again by using $U^*=U^{-1}$, we have as well:

$$||U^{-1}||=||U^*||=||U||=1$$

Thus, as before with D being the unit disk in the complex plane, we have:

$$\sigma(U^{-1})\subset D$$

Now by using Theorem 9.11, we obtain $\sigma(U)\subset D\cap D^{-1}=\mathbb{T}$, as desired. □

We have as well a similar result for the self-adjoints, as follows:

THEOREM 9.14. *The spectrum of a self-adjoint operator*

$$T=T^*$$

consists of real numbers, $\sigma(T)\subset\mathbb{R}$.

PROOF. The idea is that we can deduce the result from Theorem 9.13, by using the following remarkable rational function, depending on a parameter $r\in\mathbb{R}$:

$$f(z)=\frac{z+ir}{z-ir}$$

Indeed, for $r>>0$ the operator $f(T)$ is well-defined, and we have:

$$\left(\frac{T+ir}{T-ir}\right)^*=\frac{T-ir}{T+ir}=\left(\frac{T+ir}{T-ir}\right)^{-1}$$

Thus $f(T)$ is unitary, and by using Theorem 9.13 we obtain:

$$\begin{aligned}\sigma(T)&\subset f^{-1}(f(\sigma(T)))\\&=f^{-1}(\sigma(f(T)))\\&\subset f^{-1}(\mathbb{T})\\&=\mathbb{R}\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

One key thing that we know about matrices, which is clear for the diagonalizable matrices, and then in general follows by density, is the following formula:

$$\sigma(e^A)=e^{\sigma(A)}$$

We would like to have such formulae for the general operators $T\in B(H)$, but this is something quite technical. Consider the rational calculus morphism from Definition 9.10, which is as follows, with the exponent standing for "having poles outside $\sigma(T)$":

$$\mathbb{C}(X)^T\to B(H)\quad,\quad f\to f(T)$$

As mentioned before, the rational functions are holomorphic outside their poles, and this raises the question of extending this morphism, as follows:

$$Hol(\sigma(T))\to B(H)\quad,\quad f\to f(T)$$

But for this, we can use the Cauchy formula. Indeed, given a function $f\in\mathbb{C}(X)^T$, the operator $f(T)\in B(H)$ from Definition 9.10 can be recaptured as follows:

$$f(T)=\frac{1}{2\pi i}\int_\gamma\frac{f(z)}{z-T}\,dz$$

Now given an arbitrary function $f\in Hol(\sigma(T))$, we can define $f(T)\in B(H)$ by the exactly same formula, and we obtain in this way the desired correspondence:

$$Hol(\sigma(T))\to B(H)\quad,\quad f\to f(T)$$

This was for the plan. In practice now, all this needs a bit of care, with many verifications needed, and with the technical remark that a winding number must be added to the above Cauchy formulae, for things to be correct. The result is as follows:

THEOREM 9.15. *Given $T\in B(H)$, we have a morphism of algebras as follows, where $Hol(\sigma(T))$ is the algebra of functions which are holomorphic around $\sigma(T)$,*

$$Hol(\sigma(T))\to B(H)\quad,\quad f\to f(T)$$

which extends the previous rational functional calculus $f\to f(T)$. We have:

$$\sigma(f(T))=f(\sigma(T))$$

Moreover, if $\sigma(T)$ is contained in an open set U and $f_n,f:U\to\mathbb{C}$ are holomorphic functions such that $f_n\to f$ uniformly on compact subsets of U then $f_n(T)\to f(T)$.

PROOF. This follows indeed by reasoning along the above lines, by making a heavy use of the Cauchy formula, and for full details here, we refer to any specialized operator theory book. In what follows, we will not really need this result. □

In order to formulate now our next result, we will need the following notion:

DEFINITION 9.16. *Given an operator $T\in B(H)$, its spectral radius*

$$\rho(T)\in\big[0,||T||\big]$$

is the radius of the smallest disk centered at 0 containing $\sigma(T)$.

Now with this notion in hand, we have the following key result, improving our key theoretical result so far about spectra, namely $\sigma(T)\neq\emptyset$, from Theorem 9.6:

THEOREM 9.17. *The spectral radius of an operator $T\in B(H)$ is given by*

$$\rho(T)=\lim_{n\to\infty}||T^n||^{1/n}$$

and in this formula, we can replace the limit by an inf.

PROOF. We have several things to be proved, the idea being as follows:

(1) Our first claim is that the numbers $u_n=||T^n||^{1/n}$ satisfy:

$$(n+m)u_{n+m}\leq nu_n+mu_m$$

Indeed, we have the following estimate, using the Young inequality $ab\leq a^p/p+b^q/q$, with exponents $p=(n+m)/n$ and $q=(n+m)/m$:

$$\begin{aligned}
u_{n+m}&=||T^{n+m}||^{1/(n+m)}\\
&\leq||T^n||^{1/(n+m)}||T^m||^{1/(n+m)}\\
&\leq||T^n||^{1/n}\cdot\frac{n}{n+m}+||T^m||^{1/m}\cdot\frac{m}{n+m}\\
&=\frac{nu_n+mu_m}{n+m}
\end{aligned}$$

(2) Our second claim is that the second assertion holds, namely:

$$\lim_{n\to\infty}||T^n||^{1/n}=\inf_n||T^n||^{1/n}$$

For this purpose, we just need the inequality found in (1). Indeed, fix $m \geq 1$, let $n \geq 1$, and write $n = lm + r$ with $0 \leq r \leq m - 1$. By using twice $u_{ab} \leq u_b$, we get:

$$\begin{aligned} u_n &\leq \frac{1}{n}(lmu_{lm} + ru_r) \\ &\leq \frac{1}{n}(lmu_m + ru_1) \\ &\leq u_m + \frac{r}{n}u_1 \end{aligned}$$

It follows that we have $\limsup_n u_n \leq u_m$, which proves our claim.

(3) Summarizing, we are left with proving the main formula, which is as follows, and with the remark that we already know that the sequence on the right converges:

$$\rho(T) = \lim_{n\to\infty} ||T^n||^{1/n}$$

In one sense, we can use the polynomial calculus formula $\sigma(T^n) = \sigma(T)^n$. Indeed, this gives the following estimate, valid for any n, as desired:

$$\begin{aligned} \rho(T) &= \sup_{\lambda\in\sigma(T)} |\lambda| \\ &= \sup_{\rho\in\sigma(T)^n} |\rho|^{1/n} \\ &= \sup_{\rho\in\sigma(T^n)} |\rho|^{1/n} \\ &= \rho(T^n)^{1/n} \\ &\leq ||T^n||^{1/n} \end{aligned}$$

(4) For the reverse inequality, we fix a number $\rho > \rho(T)$, and we want to prove that we have $\rho \geq \lim_{n\to\infty} ||T^n||^{1/n}$. By using the Cauchy formula, we have:

$$\begin{aligned} \frac{1}{2\pi i}\int_{|z|=\rho} \frac{z^n}{z-T}\,dz &= \frac{1}{2\pi i}\int_{|z|=\rho} \sum_{k=0}^\infty z^{n-k-1}T^k\,dz \\ &= \sum_{k=0}^\infty \frac{1}{2\pi i}\left(\int_{|z|=\rho} z^{n-k-1}dz\right)T^k \\ &= \sum_{k=0}^\infty \delta_{n,k+1}T^k \\ &= T^{n-1} \end{aligned}$$

By applying the norm we obtain from this formula:

$$||T^{n-1}|| \leq \frac{1}{2\pi}\int_{|z|=\rho} \left|\left|\frac{z^n}{z-T}\right|\right| dz \leq \rho^n \cdot \sup_{|z|=\rho} \left|\left|\frac{1}{z-T}\right|\right|$$

Since the sup does not depend on n, by taking n-th roots, we obtain in the limit:

$$\rho \geq \lim_{n\to\infty} ||T^n||^{1/n}$$

Now recall that ρ was by definition an arbitrary number satisfying $\rho > \rho(T)$. Thus, we have obtained the following estimate, valid for any $T \in B(H)$:

$$\rho(T) \geq \lim_{n\to\infty} ||T^n||^{1/n}$$

Thus, we are led to the conclusion in the statement. □

In the case of the normal elements, we have the following finer result:

THEOREM 9.18. *The spectral radius of a normal element,*

$$TT^* = T^*T$$

is equal to its norm.

PROOF. We can proceed in two steps, as follows:

Step 1. In the case $T = T^*$ we have $||T^n|| = ||T||^n$ for any exponent of the form $n = 2^k$, by using the formula $||TT^*|| = ||T||^2$, and by taking n-th roots we get:

$$\rho(T) \geq ||T||$$

Thus, we are done with the self-adjoint case, with the result $\rho(T) = ||T||$.

Step 2. In the general normal case $TT^* = T^*T$ we have $T^n(T^n)^* = (TT^*)^n$, and by using this, along with the result from Step 1, applied to TT^*, we obtain:

$$\begin{aligned}
\rho(T) &= \lim_{n\to\infty} ||T^n||^{1/n} \\
&= \sqrt{\lim_{n\to\infty} ||T^n(T^n)^*||^{1/n}} \\
&= \sqrt{\lim_{n\to\infty} ||(TT^*)^n||^{1/n}} \\
&= \sqrt{\rho(TT^*)} \\
&= \sqrt{||T||^2} \\
&= ||T||
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

9c. Normal operators

By using Theorem 9.18 we can say a number of non-trivial things about the normal operators, commonly known as "spectral theorem for normal operators". As a first result here, we can improve the polynomial functional calculus formula, as follows:

THEOREM 9.19. *Given $T \in B(H)$ normal, we have a morphism of algebras*

$$\mathbb{C}[X] \to B(H) \quad , \quad P \to P(T)$$

having the properties $||P(T)|| = ||P_{|\sigma(T)}||$, and $\sigma(P(T)) = P(\sigma(T))$.

PROOF. This is an improvement of Theorem 9.8 in the normal case, with the extra assertion being the norm estimate. But the element $P(T)$ being normal, we can apply to it the spectral radius formula for normal elements, and we obtain:

$$\begin{aligned} ||P(T)|| &= \rho(P(T)) \\ &= \sup_{\lambda \in \sigma(P(T))} |\lambda| \\ &= \sup_{\lambda \in P(\sigma(T))} |\lambda| \\ &= ||P_{|\sigma(T)}|| \end{aligned}$$

Thus, we are led to the conclusions in the statement. □

We can improve as well the rational calculus formula, and the holomorphic calculus formula, in the same way. Importantly now, at a more advanced level, we have:

THEOREM 9.20. *Given $T \in B(H)$ normal, we have a morphism of algebras*

$$C(\sigma(T)) \to B(H) \quad , \quad f \to f(T)$$

which is isometric, $||f(T)|| = ||f||$, and has the property $\sigma(f(T)) = f(\sigma(T))$.

PROOF. The idea here is to "complete" the morphism in Theorem 9.19, namely:

$$\mathbb{C}[X] \to B(H) \quad , \quad P \to P(T)$$

Indeed, we know from Theorem 9.19 that this morphism is continuous, and is in fact isometric, when regarding the polynomials $P \in \mathbb{C}[X]$ as functions on $\sigma(T)$:

$$||P(T)|| = ||P_{|\sigma(T)}||$$

Thus, by Stone-Weierstrass, we have a unique isometric extension, as follows:

$$C(\sigma(T)) \to B(H) \quad , \quad f \to f(T)$$

It remains to prove $\sigma(f(T)) = f(\sigma(T))$, and we can do this by double inclusion:

"$\subset$" Given a continuous function $f \in C(\sigma(T))$, we must prove that we have:

$$\lambda \notin f(\sigma(T)) \implies \lambda \notin \sigma(f(T))$$

For this purpose, consider the following function, which is well-defined:

$$\frac{1}{f - \lambda} \in C(\sigma(T))$$

We can therefore apply this function to T, and we obtain:

$$\left(\frac{1}{f-\lambda}\right)T=\frac{1}{f(T)-\lambda}$$

In particular $f(T)-\lambda$ is invertible, so $\lambda\notin\sigma(f(T))$, as desired.

"$\supset$" Given a continuous function $f\in C(\sigma(T))$, we must prove that we have:

$$\lambda\in f(\sigma(T))\implies\lambda\in\sigma(f(T))$$

But this is the same as proving that we have:

$$\mu\in\sigma(T)\implies f(\mu)\in\sigma(f(T))$$

For this purpose, we approximate our function by polynomials, $P_n\to f$, and we examine the following convergence, which follows from $P_n\to f$:

$$P_n(T)-P_n(\mu)\to f(T)-f(\mu)$$

We know from polynomial functional calculus that we have:

$$P_n(\mu)\in P_n(\sigma(T))=\sigma(P_n(T))$$

Thus, the operators $P_n(T)-P_n(\mu)$ are not invertible. On the other hand, we know that the set formed by the invertible operators is open, so its complement is closed. Thus the limit $f(T)-f(\mu)$ is not invertible either, and so $f(\mu)\in\sigma(f(T))$, as desired. □

As an important comment, Theorem 9.20 is not exactly in final form, because it misses an important point, namely that our correspondence maps:

$$\bar{z}\to T^*$$

However, this is something non-trivial, and we will be back to this later. Observe however that Theorem 9.20 is fully powerful for the self-adjoint operators, $T=T^*$, where the spectrum is real, so where $z=\bar{z}$ on the spectrum. We will be back to this.

As a second result now, along the same lines, we can further extend Theorem 9.20 into a measurable functional calculus theorem, as follows:

THEOREM 9.21. *Given $T\in B(H)$ normal, we have a morphism of algebras as follows, with L^∞ standing for abstract measurable functions, or Borel functions,*

$$L^\infty(\sigma(T))\to B(H)\quad,\quad f\to f(T)$$

which is isometric, $||f(T)||=||f||$, and has the property $\sigma(f(T))=f(\sigma(T))$.

PROOF. As before, the idea will be that of "completing" what we have. To be more precise, we can use the Riesz theorem and a polarization trick, as follows:

(1) Given a vector $x\in H$, consider the following functional:

$$C(\sigma(T))\to\mathbb{C}\quad,\quad g\to<g(T)x,x>$$

By the Riesz theorem, this functional must be the integration with respect to a certain measure μ on the space $\sigma(T)$. Thus, we have a formula as follows:

$$< g(T)x, x >= \int_{\sigma(T)} g(z) d\mu(z)$$

Now given an arbitrary Borel function $f \in L^\infty(\sigma(T))$, as in the statement, we can define a number $< f(T)x, x > \in \mathbb{C}$, by using exactly the same formula, namely:

$$< f(T)x, x >= \int_{\sigma(T)} f(z) d\mu(z)$$

Thus, we have managed to define numbers $< f(T)x, x > \in \mathbb{C}$, for all vectors $x \in H$, and in addition we can recover these numbers as follows, with $g_n \in C(\sigma(T))$:

$$< f(T)x, x >= \lim_{g_n \to f} < g_n(T)x, x >$$

(2) In order to define now numbers $< f(T)x, y > \in \mathbb{C}$, for all vectors $x, y \in H$, we can use a polarization trick. Indeed, for any operator $S \in B(H)$ we have:

$$\begin{aligned} < S(x+y), x+y > &= < Sx, x > + < Sy, y > \\ &\quad + < Sx, y > + < Sy, x > \end{aligned}$$

By replacing $y \to iy$, we have as well the following formula:

$$\begin{aligned} < S(x+iy), x+iy > &= < Sx, x > + < Sy, y > \\ &\quad -i < Sx, y > +i < Sy, x > \end{aligned}$$

By multiplying this latter formula by i, we obtain the following formula:

$$\begin{aligned} i < S(x+iy), x+iy > &= i < Sx, x > +i < Sy, y > \\ &\quad + < Sx, y > - < Sy, x > \end{aligned}$$

Now by summing this latter formula with the first one, we obtain:

$$\begin{aligned} < S(x+y), x+y > +i < S(x+iy), x+iy > &= (1+i)[< Sx, x > + < Sy, y >] \\ &\quad +2 < Sx, y > \end{aligned}$$

(3) But with this, we can now finish. Indeed, by combining (1,2), given a Borel function $f \in L^\infty(\sigma(T))$, we can define numbers $< f(T)x, y > \in \mathbb{C}$ for any $x, y \in H$, and it is routine to check, by using approximation by continuous functions $g_n \to f$ as in (1), that we obtain in this way an operator $f(T) \in B(H)$, having all the desired properties. □

As a comment here, the above result and its proof provide us with more than a Borel functional calculus, because what we got is a certain measure on the spectrum $\sigma(T)$, along with a functional calculus for the L^∞ functions with respect to this measure. We will be back to this later, and for the moment we will only need Theorem 9.21 as formulated, with $L^\infty(\sigma(T))$ standing, a bit abusively, for the Borel functions on $\sigma(T)$.

9d. Diagonalization

Let us discuss now some useful decomposition results for the bounded linear operators $T\in B(H)$, that we can now establish, by using the above measurable calculus technology. We know that any $z\in\mathbb C$ can be written as follows, with $a,b\in\mathbb R$:

$$z=a+ib$$

Also, we know that both the real and imaginary parts $a,b\in\mathbb R$, and more generally any real number $c\in\mathbb R$, can be written as follows, with $r,s\geq 0$:

$$c=r-s$$

In order to discuss now the operator theoretic generalizations of these results, which by the way covers the usual matrix case too, let us start with the following basic fact:

Theorem 9.22. *Any operator $T\in B(H)$ can be written as*

$$T=Re(T)+iIm(T)$$

with $Re(T),Im(T)\in B(H)$ being self-adjoint, and this decomposition is unique.

Proof. This is something elementary, the idea being as follows:

(1) As a first observation, in the case $H=\mathbb C$ our operators are usual complex numbers, and the formula in the statement corresponds to the following basic fact:

$$z=Re(z)+iIm(z)$$

(2) In general now, we can use the same formulae for the real and imaginary part as in the complex number case, the decomposition formula being as follows:

$$T=\frac{T+T^*}{2}+i\cdot\frac{T-T^*}{2i}$$

To be more precise, both the operators on the right are self-adjoint, and the summing formula holds indeed, and so we have our decomposition result, as desired.

(3) Regarding now the uniqueness, by linearity it is enough to show that $R+iS=0$ with R,S both self-adjoint implies $R=S=0$. But this follows by applying the adjoint to $R+iS=0$, which gives $R-iS=0$, and so $R=S=0$, as desired. □

More generally now, as a continuation of this, and as an answer to some of the questions raised above, in relation with the complex numbers, we have the following result:

Theorem 9.23. *Given an operator $T\in B(H)$, the following happen:*

(1) *We can write $T=A+iB$, with $A,B\in B(H)$ being self-adjoint.*
(2) *When $T=T^*$, we can write $T=R-S$, with $R,S\in B(H)$ being positive.*
(3) *Thus, we can write any T as a linear combination of 4 positive elements.*

PROOF. All this follows from basic spectral theory, as follows:

(1) This is something that we already know, from Theorem 9.22, with the decomposition formula there being something straightforward, as follows:

$$T=\frac{T+T^*}{2}+i\cdot\frac{T-T^*}{2i}$$

(2) This follows from the measurable functional calculus. Indeed, assuming $T=T^*$ we have $\sigma(T)\subset\mathbb{R}$, so we can use the following decomposition formula on $\mathbb{R}$:

$$1=\chi_{[0,\infty)}+\chi_{(-\infty,0)}$$

To be more precise, let us multiply by z, and rewrite this formula as follows:

$$z=\chi_{[0,\infty)}z-\chi_{(-\infty,0)}(-z)$$

Now by applying these measurable functions to T, we obtain as formula as follows, with both the operators $T_+,T_-\in B(H)$ being positive, as desired:

$$T=T_+-T_-$$

(3) This follows indeed by combining the results in (1) and (2) above. □

Going ahead with our decomposition results, another basic thing that we know about complex numbers is that any $z\in\mathbb{C}$ appears as a real multiple of a unitary:

$$z=re^{it}$$

Finding the correct operator theoretic analogue of this is quite tricky, and this even for the usual matrices $A\in M_N(\mathbb{C})$. As a basic result here, we have:

THEOREM 9.24. *Given an operator $T\in B(H)$, the following happen:*

(1) *When $T=T^*$ and $||T||\leq 1$, we can write T as an average of 2 unitaries:*

$$T=\frac{U+V}{2}$$

(2) *In the general $T=T^*$ case, we can write T as a rescaled sum of unitaries:*

$$T=\lambda(U+V)$$

(3) *Thus, in general, we can write T as a rescaled sum of 4 unitaries.*

PROOF. This follows from the results that we have, as follows:

(1) Assuming $T=T^*$ and $||T||\leq 1$ we have $1-T^2\geq 0$, and the decomposition that we are looking for is as follows, with both the components being unitaries:

$$T=\frac{T+i\sqrt{1-T^2}}{2}+\frac{T-i\sqrt{1-T^2}}{2}$$

To be more precise, the square root can be extracted by using the continuous functional calculus, and the check of the unitarity of the components goes as follows:

$$\begin{aligned}(T+i\sqrt{1-T^2})(T-i\sqrt{1-T^2}) &= T^2+(1-T^2)\\ &= 1\end{aligned}$$

(2) This simply follows by applying (1) to the operator $T/||T||$.

(3) Assuming first that we have $||T||\leq 1$, we know from Theorem 9.23 (1) that we can write $T=A+iB$, with A,B being self-adjoint, and satisfying $||A||,||B||\leq 1$. Now by applying (1) to both A and B, we obtain a decomposition of T as follows:

$$T=\frac{U+V+W+X}{2}$$

In general, we can apply this to the operator $T/||T||$, and we obtain the result. □

Good news, we can now diagonalize the normal operators. We will do this in 3 steps, first for the self-adjoint operators, then for the families of commuting self-adjoint operators, and finally for the general normal operators, by using the following trick:

$$T=Re(T)+iIm(T)$$

However, and coming somehow as bad news, all this will be quite technical. Indeed, the diagonalization in infinite dimensions is more tricky than in finite dimensions, and instead of writing a formula of type $T=UDU^*$, with $U,D\in B(H)$ being respectively unitary and diagonal, we will express our operator as $T=U^*MU$, with $U:H\to K$ being a certain unitary, and $M\in B(K)$ being a certain diagonal operator. The point indeed is that this is how the spectral theorem is used in practice, for concrete applications.

But probably too much talking, let us get to work. We first have:

THEOREM 9.25. *Any self-adjoint operator $T\in B(H)$ can be diagonalized,*

$$T=U^*M_fU$$

with $U:H\to L^2(X)$ being a unitary operator from H to a certain L^2 space associated to T, with $f:X\to\mathbb{R}$ being a certain function, once again associated to T, and with

$$M_f(g)=fg$$

being the usual multiplication operator by f, on the Hilbert space $L^2(X)$.

PROOF. The construction of U,f can be done in several steps, as follows:

(1) We first prove the result in the special case where our operator T has a cyclic vector $x\in H$, with this meaning that the following holds:

$$\overline{span\left(T^kx\Big|n\in\mathbb{N}\right)}=H$$

For this purpose, let us go back to the proof of Theorem 9.21. We will use the following formula from there, with μ being the measure on $X=\sigma(T)$ associated to x:

$$<g(T)x,x>=\int_{\sigma(T)}g(z)d\mu(z)$$

Our claim is that we can define a unitary $U:H\to L^2(X)$, first on the dense part spanned by the vectors T^kx, by the following formula, and then by continuity:

$$U[g(T)x]=g$$

Indeed, the following computation shows that U is well-defined, and isometric:

$$\begin{aligned}||g(T)x||^2&=<g(T)x,g(T)x>\\&=<g(T)^*g(T)x,x>\\&=<|g|^2(T)x,x>\\&=\int_{\sigma(T)}|g(z)|^2d\mu(z)\\&=||g||_2^2\end{aligned}$$

We can then extend U by continuity into a unitary $U:H\to L^2(X)$, as claimed. Now observe that we have the following formula:

$$\begin{aligned}UTU^*g&=U[Tg(T)x]\\&=U[(zg)(T)x]\\&=zg\end{aligned}$$

Thus our result is proved in the present case, with U as above, and with $f(z)=z$.

(2) We discuss now the general case. Our first claim is that H has a decomposition as follows, with each H_i being invariant under T, and admitting a cyclic vector x_i:

$$H=\bigoplus_i H_i$$

Indeed, this is something elementary, the construction being by recurrence in finite dimensions, in the obvious way, and by using the Zorn lemma in general. Now with this decomposition in hand, we can make a direct sum of the diagonalizations obtained in (1), for each of the restrictions $T_{|H_i}$, and we obtain the formula in the statement. □

The above result is very nice, closing more or less the discussion regarding the self-adjoint operators. At the theoretical level, however, there are still a number of comments that can be made, about this, and we will be back to this, at the end of this chapter.

We have the following technical generalization of the above result:

THEOREM 9.26. *Any family of commuting self-adjoint operators $T_i \in B(H)$ can be jointly diagonalized,*

$$T_i = U^* M_{f_i} U$$

with $U : H \to L^2(X)$ being a unitary operator from H to a certain L^2 space associated to $\{T_i\}$, with $f_i : X \to \mathbb{R}$ being certain functions, once again associated to T_i, and with

$$M_{f_i}(g) = f_i g$$

being the usual multiplication operator by f_i, on the Hilbert space $L^2(X)$.

PROOF. This is similar to the proof of Theorem 9.25, by suitably modifying the measurable calculus formula, and μ itself, as to have this working for all operators T_i. □

We can now discuss the case of the arbitrary normal operators, as follows:

THEOREM 9.27. *Any normal operator $T \in B(H)$ can be diagonalized,*

$$T = U^* M_f U$$

with $U : H \to L^2(X)$ being a unitary operator from H to a certain L^2 space associated to T, with $f : X \to \mathbb{C}$ being a certain function, once again associated to T, and with

$$M_f(g) = fg$$

being the usual multiplication operator by f, on the Hilbert space $L^2(X)$.

PROOF. This is our main diagonalization theorem, the idea being as follows:

(1) Consider the decomposition of T into its real and imaginary parts, namely:

$$T = \frac{T + T^*}{2} + i \cdot \frac{T - T^*}{2i}$$

We know that the real and imaginary parts are self-adjoint operators. Now since T was assumed to be normal, $TT^* = T^*T$, these real and imaginary parts commute:

$$\left[\frac{T + T^*}{2}, \frac{T - T^*}{2i}\right] = 0$$

Thus Theorem 9.26 applies to these real and imaginary parts, and gives the result. □

This was for our series of diagonalization theorems. There is of course one more result here, regarding the families of commuting normal operators, as follows:

THEOREM 9.28. *Any family of commuting normal operators $T_i \in B(H)$ can be jointly diagonalized,*

$$T_i = U^* M_{f_i} U$$

with $U : H \to L^2(X)$ being a unitary operator from H to a certain L^2 space associated to $\{T_i\}$, with $f_i : X \to \mathbb{C}$ being certain functions, once again associated to T_i, and with

$$M_{f_i}(g) = f_i g$$

being the usual multiplication operator by f_i, on the Hilbert space $L^2(X)$.

Proof. This is similar to the proof of Theorem 9.26 and Theorem 9.27, by combining the arguments there. To be more precise, this follows as Theorem 9.26, by using the decomposition trick from the proof of Theorem 9.27. □

With the above diagonalization results in hand, we can now "fix" the continuous and measurable functional calculus theorems, with a key complement, as follows:

Theorem 9.29. *Given a normal operator $T \in B(H)$, the following hold, for both the functional calculus and the measurable calculus morphisms:*

(1) *These morphisms are $*$-morphisms.*
(2) *The function $\bar{z}$ gets mapped to T^*.*
(3) *The functions $Re(z), Im(z)$ get mapped to $Re(T), Im(T)$.*
(4) *The function $|z|^2$ gets mapped to $TT^* = T^*T$.*
(5) *If f is real, then $f(T)$ is self-adjoint.*

Proof. These assertions are more or less equivalent, with (1) being the main one, which obviously implies everything else. But this assertion (1) follows from the diagonalization result for normal operators, from Theorem 9.27. □

9e. Exercises

Exercises:

Exercise 9.30.

Exercise 9.31.

Exercise 9.32.

Exercise 9.33.

Exercise 9.34.

Exercise 9.35.

Exercise 9.36.

Exercise 9.37.

Bonus exercise.

CHAPTER 10

Wigner matrices

10a. Gaussian matrices

We have now all the needed ingredients for launching some explicit random matrix computations. Our goal will be that of computing the asymptotic moments, and then the asymptotic laws, with $N \to \infty$, for the main classes of large random matrices.

Let us begin by specifying the precise classes of matrices that we are interested in. First we have the complex Gaussian matrices, which are constructed as follows:

DEFINITION 10.1. *A complex Gaussian matrix is a random matrix of type*

$$Z \in M_N(L^\infty(X))$$

which has i.i.d. centered complex normal entries.

Here we use the notion of complex normal variable, introduced and studied in chapter 4. To be more precise, the complex Gaussian law of parameter $t > 0$ is by definition the following law, with a, b being independent, each following the normal law g_t:

$$G_t = law\left(\frac{1}{\sqrt{2}}(a+ib)\right)$$

With this notion in hand, the assumption in the above definition is that all the matrix entries Z_{ij} are independent, and follow this law G_t, for a fixed value of $t > 0$. We will see that the above matrices have an interesting, and "central" combinatorics, among all kinds of random matrices, with the study of the other random matrices being usually obtained as a modification of the study of the Gaussian matrices.

As a somewhat surprising remark, using real normal variables in Definition 10.1, instead of the complex ones appearing there, leads nowhere. The correct real versions of the Gaussian matrices are the Wigner random matrices, constructed as follows:

DEFINITION 10.2. *A Wigner matrix is a random matrix of type*

$$Z \in M_N(L^\infty(X))$$

which has i.i.d. centered complex normal entries, up to the constraint $Z = Z^*$.

This definition is something a bit compacted, and to be more precise, a Wigner matrix is by definition a random matrix as follows, with the diagonal entries being real normal variables, $a_i \sim g_t$, for some $t > 0$, the upper diagonal entries being complex normal variables, $b_{ij} \sim G_t$, the lower diagonal entries being the conjugates of the upper diagonal entries, as indicated, and with all the variables a_i, b_{ij} being independent:

$$Z = \begin{pmatrix} a_1 & b_{12} & \dots & \dots & b_{1N} \\ \bar{b}_{12} & a_2 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & a_{N-1} & b_{N-1,N} \\ \bar{b}_{1N} & \dots & \dots & \bar{b}_{N-1,N} & a_N \end{pmatrix}$$

As a comment here, for many concrete applications the Wigner matrices are in fact the central objects in random matrix theory, and in particular, they are often more important than the Gaussian matrices. In fact, these are the random matrices which were first considered and investigated, a long time ago, by Wigner himself [**100**].

However, as we will soon discover, the Gaussian matrices are somehow more fundamental than the Wigner matrices, at least from an abstract point of view, and this will be the point of view that we will follow here, with the Gaussian matrices coming first.

Finally, we will be interested as well in the complex Wishart matrices, which are the positive versions of the above random matrices, constructed as follows:

Definition 10.3. *A complex Wishart matrix is a random matrix of type*

$$Z = YY^* \in M_N(L^\infty(X))$$

with Y being a complex Gaussian matrix.

As before with the Gaussian and Wigner matrices, there are many possible comments that can be made here, of technical or historical nature, as follows:

(1) First, using real Gaussian variables instead of complex Gaussian variables in the above definition leads to a less interesting combinatorics, and we will not do this.

(2) The complex Wishart matrices were introduced and studied by Marchenko and Pastur not long after Wigner, in [**67**], and so historically came second.

(3) Finally, in what regards their combinatorics and applications, the Wishart matrices quite often come first, before both the Gaussian and the Wigner ones.

So long for random matrix definitions and general talk about this, with all this being at this point quite subjective, but we will soon get to work, and prove results motivating all the above. Let us summarize this preliminary discussion in the following way:

Conclusion 10.4. *There are three main types of random matrices, as follows:*

1. *The Gaussian matrices, which can be thought of as being "complex".*
2. *The Wigner matrices, which can be thought of as being "real".*
3. *The Wishart matrices, which can be thought of as being "positive".*

We will study these three types of matrices in what follows, in the above precise order, with this order being the one that, technically, best fits us here. Let us also mention that there are many other interesting classes of random matrices, which are more specialized, usually appearing as modifications of the above. More on these later.

In order to compute the asymptotic laws of the Gaussian, Wigner and Wishart matrices, we use the moment method. Given a colored integer $k = \circ\bullet\bullet\circ\ldots$, we say that a pairing $\pi \in P_2(k)$ is matching when it pairs $\circ - \bullet$ symbols. With this convention, we have the following result, which will be our main tool for computing moments:

Theorem 10.5 (Wick formula). *Given independent variables X_i, each following the complex normal law G_t, with $t > 0$ being a fixed parameter, we have the formula*

$$E\left(X_{i_1}^{k_1}\ldots X_{i_s}^{k_s}\right) = t^{s/2}\#\left\{\pi\in\mathcal{P}_2(k)\Big|\pi\leq\ker i\right\}$$

where $k = k_1\ldots k_s$ and $i = i_1\ldots i_s$, for the joint moments of these variables.

Proof. This is something that we know from chapter 4, the idea being as follows:

(1) In the case where we have a single complex normal variable X, which amounts in taking $X_i = X$ for any i in the formula in the statement, what we have to compute are the moments of X, with respect to colored integer exponents $k = \circ\bullet\bullet\circ\ldots$, and the formula in the statement tells us that these moments must be:

$$E(X^k) = t^{|k|/2}|\mathcal{P}_2(k)|$$

(2) But this is something that we know from chapter 4, the idea being that at $t = 1$ this follows by doing some combinatorics and calculus, in analogy with the combinatorics and calculus from the real case, where the moment formula is identical, save for the matching pairings $\mathcal{P}_2$ being replaced by the usual pairings P_2, and then that the general case $t > 0$ follows from this, by rescaling. Thus, we are done with this case.

(3) In general now, with several variables as in the statement, when expanding the product $X_{i_1}^{k_1}\ldots X_{i_s}^{k_s}$ and rearranging the terms, we are left with doing a number of computations as in (1), and then making the product of the expectations that we found.

(4) But this amounts in counting the partitions in the statement, with the condition $\pi\leq\ker i$ there standing for the fact that we are doing the various type (1) computations independently, and then making the product. Thus, we obtain the result. ∎

The above statement is one of the possible formulations of the Wick formula, and there are in fact many more formulations, which are all useful. Here is an alternative such formulation, which is quite popular, and that we will often use in what follows:

THEOREM 10.6 (Wick formula 2). *Given independent variables f_i, each following the complex normal law G_t, with $t > 0$ being a fixed parameter, we have the formula*

$$E\left(f_{i_1}\dots f_{i_k}f_{j_1}^*\dots f_{j_k}^*\right)=t^k\#\left\{\pi\in S_k\Big|i_{\pi(r)}=j_r,\forall r\right\}$$

for the non-vanishing joint moments of these variables.

PROOF. This follows from the usual Wick formula, from Theorem 10.5. With some changes in the indices and notations, the formula there reads:

$$E\left(f_{I_1}^{K_1}\dots f_{I_s}^{K_s}\right)=t^{s/2}\#\left\{\sigma\in\mathcal{P}_2(K)\Big|\sigma\leq\ker I\right\}$$

Now observe that we have $\mathcal{P}_2(K)=\emptyset$, unless the colored integer $K=K_1\dots K_s$ is uniform, in the sense that it contains the same number of $\circ$ and $\bullet$ symbols. Up to permutations, the non-trivial case, where the moment is non-vanishing, is the case where the colored integer $K=K_1\dots K_s$ is of the following special form:

$$K=\underbrace{\circ\circ\dots\circ}_k\ \underbrace{\bullet\bullet\dots\bullet}_k$$

So, let us focus on this case, which is the non-trivial one. Here we have $s=2k$, and we can write the multi-index $I=I_1\dots I_s$ in the following way:

$$I=i_1\dots i_k\ j_1\dots j_k$$

With these changes made, the above usual Wick formula reads:

$$E\left(f_{i_1}\dots f_{i_k}f_{j_1}^*\dots f_{j_k}^*\right)=t^k\#\left\{\sigma\in\mathcal{P}_2(K)\Big|\sigma\leq\ker(ij)\right\}$$

The point now is that the matching pairings $\sigma\in\mathcal{P}_2(K)$, with $K=\circ\dots\circ\bullet\dots\bullet$, of length $2k$, as above, correspond to the permutations $\pi\in S_k$, in the obvious way. With this identification made, the above modified usual Wick formula becomes:

$$E\left(f_{i_1}\dots f_{i_k}f_{j_1}^*\dots f_{j_k}^*\right)=t^k\#\left\{\pi\in S_k\Big|i_{\pi(r)}=j_r,\forall r\right\}$$

Thus, we have reached to the formula in the statement, and we are done. □

Finally, here is one more formulation of the Wick formula, which is useful as well:

THEOREM 10.7 (Wick formula 3). *Given independent variables f_i, each following the complex normal law G_t, with $t > 0$ being a fixed parameter, we have the formula*

$$E\left(f_{i_1}f_{j_1}^*\dots f_{i_k}f_{j_k}^*\right)=t^k\#\left\{\pi\in S_k\Big|i_{\pi(r)}=j_r,\forall r\right\}$$

for the non-vanishing joint moments of these variables.

Proof. This follows from our second Wick formula, from Theorem 10.6, simply by permuting the terms, as to have an alternating sequence of plain and conjugate variables. Alternatively, we can start with Theorem 10.5, and then perform the same manipulations as in the proof of Theorem 10.6, but with the exponent being this time as follows:

$$K=\underbrace{\circ\bullet\circ\bullet\ldots\ldots\circ\bullet}_{2k}$$

Thus, we are led to the conclusion in the statement. □

Now by getting back to the Gaussian matrices, we have the following result:

Theorem 10.8. *Given a sequence of Gaussian random matrices*

$$Z_N\in M_N(L^\infty(X))$$

having independent G_t variables as entries, for some $t>0$, we have

$$M_k\left(\frac{Z_N}{\sqrt{N}}\right)\simeq t^{|k|/2}|\mathcal{NC}_2(k)|$$

for any colored integer $k=\circ\bullet\bullet\circ\ldots$, in the $N\to\infty$ limit.

Proof. This is something standard, which can be done as follows:

(1) We fix $N\in\mathbb N$, and we let $Z=Z_N$. Let us first compute the trace of Z^k. With $k=k_1\ldots k_s$, and with the convention $(ij)^\circ=ij,(ij)^\bullet=ji$, we have:

$$\begin{aligned}Tr(Z^k)&=Tr(Z^{k_1}\ldots Z^{k_s})\\&=\sum_{i_1=1}^N\ldots\sum_{i_s=1}^N(Z^{k_1})_{i_1i_2}(Z^{k_2})_{i_2i_3}\ldots(Z^{k_s})_{i_si_1}\\&=\sum_{i_1=1}^N\ldots\sum_{i_s=1}^N(Z_{(i_1i_2)^{k_1}})^{k_1}(Z_{(i_2i_3)^{k_2}})^{k_2}\ldots(Z_{(i_si_1)^{k_s}})^{k_s}\end{aligned}$$

(2) Next, we rescale our variable Z by a $\sqrt N$ factor, as in the statement, and we also replace the usual trace by its normalized version, $tr=Tr/N$. Our formula becomes:

$$tr\left(\left(\frac{Z}{\sqrt N}\right)^k\right)=\frac{1}{N^{s/2+1}}\sum_{i_1=1}^N\ldots\sum_{i_s=1}^N(Z_{(i_1i_2)^{k_1}})^{k_1}(Z_{(i_2i_3)^{k_2}})^{k_2}\ldots(Z_{(i_si_1)^{k_s}})^{k_s}$$

Thus, the moment that we are interested in is given by:

$$M_k\left(\frac{Z}{\sqrt N}\right)=\frac{1}{N^{s/2+1}}\sum_{i_1=1}^N\ldots\sum_{i_s=1}^N\int_X(Z_{(i_1i_2)^{k_1}})^{k_1}(Z_{(i_2i_3)^{k_2}})^{k_2}\ldots(Z_{(i_si_1)^{k_s}})^{k_s}$$

(3) Let us apply now the Wick formula, from Theorem 10.5. We conclude that the moment that we are interested in is given by:

$$\begin{aligned} & M_k\left(\frac{Z}{\sqrt{N}}\right) \\ = & \frac{t^{s/2}}{N^{s/2+1}}\sum_{i_1=1}^N\ldots\sum_{i_s=1}^N\#\left\{\pi\in\mathcal{P}_2(k)\Big|\pi\leq\ker\left((i_1i_2)^{k_1},(i_2i_3)^{k_2},\ldots,(i_si_1)^{k_s}\right)\right\} \\ = & t^{s/2}\sum_{\pi\in\mathcal{P}_2(k)}\frac{1}{N^{s/2+1}}\#\left\{i\in\{1,\ldots,N\}^s\Big|\pi\leq\ker\left((i_1i_2)^{k_1},(i_2i_3)^{k_2},\ldots,(i_si_1)^{k_s}\right)\right\} \end{aligned}$$

(4) Our claim now is that in the $N\to\infty$ limit the combinatorics of the above sum simplifies, with only the noncrossing partitions contributing to the sum, and with each of them contributing precisely with a 1 factor, so that we will have, as desired:

$$\begin{aligned} M_k\left(\frac{Z}{\sqrt{N}}\right) &= t^{s/2}\sum_{\pi\in\mathcal{P}_2(k)}\left(\delta_{\pi\in NC_2(k)}+O(N^{-1})\right) \\ &\simeq t^{s/2}\sum_{\pi\in\mathcal{P}_2(k)}\delta_{\pi\in NC_2(k)} \\ &= t^{s/2}|\mathcal{NC}_2(k)| \end{aligned}$$

(5) In order to prove this, the first observation is that when k is not uniform, in the sense that it contains a different number of $\circ,\bullet$ symbols, we have $\mathcal{P}_2(k)=\emptyset$, and so:

$$M_k\left(\frac{Z}{\sqrt{N}}\right)=t^{s/2}|\mathcal{NC}_2(k)|=0$$

(6) Thus, we are left with the case where k is uniform. Let us examine first the case where k consists of an alternating sequence of $\circ$ and $\bullet$ symbols, as follows:

$$k=\underbrace{\circ\bullet\circ\bullet\ldots\ldots\circ\bullet}_{2p}$$

In this case it is convenient to relabel our multi-index $i=(i_1,\ldots,i_s)$, with $s=2p$, in the form $(j_1,l_1,j_2,l_2,\ldots,j_p,l_p)$. With this done, our moment formula becomes:

$$M_k\left(\frac{Z}{\sqrt{N}}\right)=t^p\sum_{\pi\in\mathcal{P}_2(k)}\frac{1}{N^{p+1}}\#\left\{j,l\in\{1,\ldots,N\}^p\Big|\pi\leq\ker\left(j_1l_1,j_2l_1,j_2l_2,\ldots,j_1l_p\right)\right\}$$

Now observe that, with k being as above, we have an identification $\mathcal{P}_2(k)\simeq S_p$, obtained in the obvious way. With this done too, our moment formula becomes:

$$M_k\left(\frac{Z}{\sqrt{N}}\right)=t^p\sum_{\pi\in S_p}\frac{1}{N^{p+1}}\#\left\{j,l\in\{1,\ldots,N\}^p\Big|j_r=j_{\pi(r)+1},l_r=l_{\pi(r)},\forall r\right\}$$

(7) We are now ready to do our asymptotic study, and prove the claim in (4). Let indeed $\gamma \in S_p$ be the full cycle, which is by definition the following permutation:

$$\gamma = (1\,2\,\ldots\,p)$$

In terms of γ, the conditions $j_r = j_{\pi(r)+1}$ and $l_r = l_{\pi(r)}$ found above read:

$$\gamma\pi \leq \ker j \quad , \quad \pi \leq \ker l$$

Counting the number of free parameters in our moment formula, we obtain:

$$\begin{aligned} M_k\left(\frac{Z}{\sqrt{N}}\right) &= \frac{t^p}{N^{p+1}}\sum_{\pi\in S_p} N^{|\pi|+|\gamma\pi|} \\ &= t^p \sum_{\pi\in S_p} N^{|\pi|+|\gamma\pi|-p-1} \end{aligned}$$

(8) The point now is that the last exponent is well-known to be ≤ 0, with equality precisely when the permutation $\pi \in S_p$ is geodesic, which in practice means that π must come from a noncrossing partition. Thus we obtain, in the $N \to \infty$ limit, as desired:

$$M_k\left(\frac{Z}{\sqrt{N}}\right) \simeq t^p |\mathcal{NC}_2(k)|$$

This finishes the proof in the case of the exponents k which are alternating, and the case where k is an arbitrary uniform exponent is similar, by permuting everything. $\square$

This was for the computation, but in what regards now the interpretation of what we found, things are more complicated. The precise question is as follows:

QUESTION 10.9. *What is the abstract asymptotic distribution that we found, having as moments the numbers*

$$M_k = t^{|k|/2} |\mathcal{NC}_2(k)|$$

for any colored integer $k = \circ\bullet\bullet\circ\ldots$?

As a first observation, the above moment formula is very similar to the one for the usual complex Gaussian variables G_t, from chapter 4, which was as follows:

$$N_k = t^{|k|/2} |\mathcal{P}_2(k)|$$

It is possible to make many speculations here, for instance in relation with the combinatorics from chapters 3-4, but we will do this later, once we will know more. Let us record however our observation as a partial answer to Question 10.9, as follows:

ANSWER 10.10. *The abstract asymptotic distribution that we found appears as some sort of "free analogue" of the usual complex normal law G_t, with the underlying matching pairings being now replaced by underlying matching noncrossing pairings.*

Obviously, some interesting things are going on here. We will see in a moment, after doing some more combinatorics, this time in connection with the Wigner matrices, that there are some good reasons for calling this mysterious law "circular".

Thus, for ending with our present study with a nice conclusion, we can say that the Gaussian matrices become "asymptotically circular", with this meaning by definition that the $N \to \infty$ moments are those computed above. This is of course something quite vague, and we will be back to it in Part IV, when doing free probability.

10b. Wigner matrices

Moving ahead now, let us investigate the second class of random matrices that we are interested in, namely the Wigner matrices, which are by definition self-adjoint. Here our results will be far more complete than those for the Gaussian matrices.

Let us first recall from the above that a Wigner matrix is by definition a random matrix which has i.i.d. centered complex normal entries, up to the constraint $Z = Z^*$. In practice, this means that our matrix is as follows, with the diagonal entries being real normal variables, $a_i \sim g_t$, for some $t > 0$, the upper diagonal entries being complex normal variables, $b_{ij} \sim G_t$, the lower diagonal entries being the conjugates of the upper diagonal entries, as indicated, and with all the variables a_i, b_{ij} being independent:

$$Z = \begin{pmatrix} a_1 & b_{12} & \ldots & \ldots & b_{1N} \\ \bar{b}_{12} & a_2 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & a_{N-1} & b_{N-1,N} \\ \bar{b}_{1N} & \ldots & \ldots & \bar{b}_{N-1,N} & a_N \end{pmatrix}$$

As a starting point for the study of these matrices, we have the following simple fact, making the connection with the theory of Gaussian matrices developed above:

PROPOSITION 10.11. *Given a Gaussian matrix Z, with independent entries following the centered complex normal law G_t, with $t > 0$, if we write*

$$Z = \frac{1}{\sqrt{2}}(X + iY)$$

with X, Y being self-adjoint, then both X, Y are Wigner matrices, of parameter t.

PROOF. This is something elementary, which can be done in two steps, as follows:

(1) As a first observation, the result holds at $N = 1$. Indeed, here our Gaussian matrix Z is just a random variable, subject to the condition $Z \sim G_t$. But recall that the law G_t

is by definition as follows, with X, Y being independent, each following the law g_t:

$$G_t = law\left(\frac{1}{\sqrt{2}}(X+iY)\right)$$

Thus in this case, $N=1$, the variables X, Y that we obtain in the statement, as rescaled real and imaginary parts of Z, are subject to the condition $X, Y \sim g_t$, and so are Wigner matrices of size $N=1$ and parameter $t>0$, as in Definition 10.2.

(2) In the general case now, $N \in \mathbb{N}$, the proof is similar, by using the basic behavior of the real and complex normal variables with respect to sums. □

The above result is quite interesting for us, because it shows that, in order to investigate the Wigner matrices, we are basically not in need of some new computations, starting from the Wick formula, and doing combinatorics afterwards, but just of some manipulations on the results that we already have, regarding the Gaussian matrices.

To be more precise, by using this method, we obtain the following result, coming by combining the observation in Proposition 10.11 with the formula in Theorem 10.8:

THEOREM 10.12. *Given a sequence of Wigner random matrices*

$$Z_N \in M_N(L^\infty(X))$$

having independent G_t variables as entries, with $t>0$, up to $Z_N = Z_N^*$, we have

$$M_k\left(\frac{Z_N}{\sqrt{N}}\right) \simeq t^{k/2}|NC_2(k)|$$

for any integer $k \in \mathbb{N}$, in the $N \to \infty$ limit.

PROOF. This can be deduced from a direct computation based on the Wick formula, similar to that from the proof of Theorem 10.8, but the best is to deduce this result from Theorem 10.8 itself. Indeed, we know from there that for Gaussian matrices $Y_N \in M_N(L^\infty(X))$ we have the following formula, valid for any colored integer $K = \circ\bullet\bullet\circ\ldots$, in the $N \to \infty$ limit, with $\mathcal{NC}_2$ standing for noncrossing matching pairings:

$$M_K\left(\frac{Y_N}{\sqrt{N}}\right) \simeq t^{|K|/2}|\mathcal{NC}_2(K)|$$

By doing some combinatorics, we deduce from this that we have the following formula for the moments of the matrices $Re(Y_N)$, with respect to usual exponents, $k \in \mathbb{N}$:

$$\begin{aligned}
M_k\left(\frac{Re(Y_N)}{\sqrt{N}}\right) &= 2^{-k} \cdot M_k\left(\frac{Y_N}{\sqrt{N}} + \frac{Y_N^*}{\sqrt{N}}\right) \\
&= 2^{-k} \sum_{|K|=k} M_K\left(\frac{Y_N}{\sqrt{N}}\right) \\
&\simeq 2^{-k} \sum_{|K|=k} t^{k/2} |\mathcal{NC}_2(K)| \\
&= 2^{-k} \cdot t^{k/2} \cdot 2^{k/2} |\mathcal{NC}_2(k)| \\
&= 2^{-k/2} \cdot t^{k/2} |NC_2(k)|
\end{aligned}$$

Now since the matrices $Z_N = \sqrt{2} Re(Y_N)$ are of Wigner type, this gives the result. □

Summarizing, all this brings us into counting noncrossing pairings. But here, let us recall from Part I that we have the following well-known result:

THEOREM 10.13. *The Catalan numbers $C_k = |NC_2(2k)|$ are as follows:*

(1) *They satisfy $C_{k+1} = \sum_{a+b=k} C_a C_b$.*
(2) *The series $f(z) = \sum_{k \geq 0} C_k z^k$ satisfies $zf^2 - f + 1 = 0$.*
(3) *This series is given by $f(z) = \frac{1-\sqrt{1-4z}}{2z}$.*
(4) *We have the formula $C_k = \frac{1}{k+1}\binom{2k}{k}$.*

PROOF. This is something that we know well from Part I, with (1) coming from the definition of C_k, and with (1) $\implies$ (2) $\implies$ (3) $\implies$ (4) being routine, using standard calculus. Alternatively, and also explained in Part I, the formula in (4) can be established as well via a bijective proof, by counting Dyck paths in the plane. □

Getting back now to the Wigner matrices, we can convert the main result that we have about them, Theorem 10.12, into something more concrete, as follows:

THEOREM 10.14. *Given a sequence of Wigner random matrices*

$$Z_N \in M_N(L^\infty(X))$$

having independent G_t variables as entries, with $t > 0$, up to $Z_N = Z_N^*$, we have

$$M_{2k}\left(\frac{Z_N}{\sqrt{N}}\right) \simeq t^k C_k$$

in the $N \to \infty$ limit. As for the asymptotic odd moments, these all vanish.

PROOF. This follows from Theorem 10.12 and Theorem 10.13. Indeed, according to the results there, the asymptotic even moments are given by:

$$M_{2k}\left(\frac{Z_N}{\sqrt{N}}\right)\simeq t^k|NC_2(2k)|=t^kC_k$$

As for the asymptotic odd moments, once again from Theorem 10.12, we know that these all vanish. Thus, we are led to the conclusion in the statement. □

Summarizing, we are done with the moment computations, and with the asymptotic study, for both the Gaussian and the Wigner matrices. It remains now to interpret the results that we have, with the computation of the corresponding laws. As explained before, for the Gaussian matrices this is something quite complicated, with the technology that we presently have, and this will have to wait a bit, until we do some free probability.

Regarding the Wigner matrices, however, the problems left here are very explicit, and quite elementary, and we will solve them next, in the remainder of this chapter.

10c. Semicircle laws

In order to recapture the asymptotic measure of the Wigner matrices out of the moments, which are the Catalan numbers, there are several methods available, namely:

(1) Stieltjes inversion.

(2) Knowledge of SU_2.

(3) Cheating.

The first method, which is straightforward, without any trick, is based on the Stieltjes inversion formula, that we know well. In fact, we have already applied that formula to the Catalan numbers, with the following conclusion:

PROPOSITION 10.15. *The real measure having as even moments the Catalan numbers, $C_k=\frac{1}{k+1}\binom{2k}{k}$, and having all odd moments 0 is the measure*

$$\gamma_1=\frac{1}{2\pi}\sqrt{4-x^2}dx$$

called Wigner semicircle law on $[-2,2]$.

PROOF. This is something that we know, but since we will need the proof in what follows, in view of some generalizations, let us briefly recall it. The starting point is the formula in Theorem 10.13 for the generating series of the Catalan numbers, namely:

$$\sum_{k=0}^\infty C_kz^k=\frac{1-\sqrt{1-4z}}{2z}$$

By using this formula with $z=\xi^{-2}$, we obtain the following formula, for the Cauchy transform of the real measure that we want to compute:

$$\begin{aligned}G(\xi) &= \xi^{-1}\sum_{k=0}^\infty C_k\xi^{-2k}\\ &= \xi^{-1}\cdot\frac{1-\sqrt{1-4\xi^{-2}}}{2\xi^{-2}}\\ &= \frac{\xi}{2}\left(1-\sqrt{1-4\xi^{-2}}\right)\\ &= \frac{\xi}{2}-\frac{1}{2}\sqrt{\xi^2-4}\end{aligned}$$

Now let us apply the Stieltjes inversion formula, namely:

$$d\mu(x)=\lim_{t\searrow 0}-\frac{1}{\pi}\,Im\,(G(x+it))\cdot dx$$

The study of the limit on the right is then straightforward, going as follows:

(1) According to the general philosophy of the Stieltjes formula, the first term in the formula of $G(\xi)$, namely $\xi/2$, which is "trivial", will not contribute to the density.

(2) As for the second term, which is something non-trivial, this will contribute to the density, the rule here being that the square root $\sqrt{\xi^2-4}$ will be replaced by the "dual" square root $\sqrt{4-x^2}\,dx$, and that we have to multiply everything by $-1/\pi$.

(3) As a conclusion, by Stieltjes inversion we obtain the following density:

$$d\mu(x)=-\frac{1}{\pi}\cdot-\frac{1}{2}\sqrt{4-x^2}\,dx=\frac{1}{2\pi}\sqrt{4-x^2}dx$$

Thus, we have obtained the mesure in the statement, and we are done. □

More generally now, we have the following result:

Proposition 10.16. *Given $t>0$, the real measure having as even moments the numbers $M_{2k}=t^kC_k$ and having all odd moments 0 is the measure*

$$\gamma_t=\frac{1}{2\pi t}\sqrt{4t-x^2}dx$$

called Wigner semicircle law on $[-2\sqrt{t},2\sqrt{t}]$.

Proof. This follows by redoing the above Stieltjes inversion computation, with a parameter $t>0$ added. To be more precise, as before, the starting point is the formula from Theorem 10.13 for the generating series of the Catalan numbers, namely:

$$\sum_{k=0}^\infty C_kz^k=\frac{1-\sqrt{1-4z}}{2z}$$

By using this formula with $z = t\xi^{-2}$, we obtain the following formula, for the Cauchy transform of the real measure that we want to compute:

$$\begin{aligned} G(\xi) &= \xi^{-1}\sum_{k=0}^\infty t^kC_k\xi^{-2k} \\ &= \xi^{-1}\cdot\frac{1-\sqrt{1-4t\xi^{-2}}}{2t\xi^{-2}} \\ &= \frac{\xi}{2t}\left(1-\sqrt{1-4t\xi^{-2}}\right) \\ &= \frac{\xi}{2t}-\frac{1}{2t}\sqrt{\xi^2-4t} \end{aligned}$$

Thus, by Stieltjes inversion we obtain the following density, as claimed:

$$d\mu(x) = \frac{1}{2\pi t}\sqrt{4t-x^2}\,dx$$

But simplest is in fact, perhaps a bit by cheating, simply using the result at $t = 1$, from Proposition 10.15, along with a change of variables. Indeed, by using Proposition 10.15, the even moments of the measure in the statement are given by:

$$\begin{aligned} M_{2k} &= \frac{1}{2\pi t}\int_{-2\sqrt{t}}^{2\sqrt{t}}\sqrt{4t-x^2}\,x^{2k}\,dx \\ &= \frac{1}{2\pi t}\int_{-1}^1\sqrt{4t-ty^2}\,(\sqrt{t}y)^{2k}\,\sqrt{t}\,dy \\ &= \frac{t^k}{2\pi}\int_{-1}^1\sqrt{4-y^2}\,y^{2k}\,dy \\ &= t^kC_k \end{aligned}$$

As for the odd moments, these all vanish, because the density of γ_t is an even function. Thus, one way or another, we are led to the conclusion in the statement. □

Talking cheating, another way of recovering Proposition 10.15, this time without using the Stieltjes inversion formula, but by knowing instead the answer to the question, namely the semicircle law, in advance, which is of course cheating, is as follows:

PROPOSITION 10.17. *The Catalan numbers are the even moments of*

$$\gamma_1 = \frac{1}{2\pi}\sqrt{4-x^2}dx$$

called Wigner semicircle law. As for the odd moments of γ_1, these all vanish.

PROOF. The even moments of the Wigner law can be computed with the change of variable $x = 2\cos t$, and we are led to the following formula:

$$\begin{aligned}
M_{2k} &= \frac{1}{\pi}\int_0^2 \sqrt{4-x^2}x^{2k}\,dx \\
&= \frac{1}{\pi}\int_0^{\pi/2} \sqrt{4-4\cos^2 t}\,(2\cos t)^{2k} 2\sin t\,dt \\
&= \frac{4^{k+1}}{\pi}\int_0^{\pi/2} \cos^{2k} t\sin^2 t\,dt \\
&= \frac{4^{k+1}}{\pi}\cdot\frac{\pi}{2}\cdot\frac{(2k)!!2!!}{(2k+3)!!} \\
&= 2\cdot 4^k\cdot\frac{(2k)!/2^k k!}{2^{k+1}(k+1)!} \\
&= C_k
\end{aligned}$$

As for the odd moments, these all vanish, because the density of γ_1 is an even function. Thus, we are led to the conclusion in the statement. □

More generally, we have the following result, involving a parameter $t > 0$:

PROPOSITION 10.18. *The numbers $t^k C_k$ are the even moments of*

$$\gamma_t = \frac{1}{2\pi t}\sqrt{4t - x^2}dx$$

called semicircle law on $[-2\sqrt{t}, 2\sqrt{t}]$. As for the odd moments of γ_t, these all vanish.

PROOF. This follows indeed from what we have in Proposition 10.17, via a quick change of variables, as explained at the end of the proof of Proposition 10.16. □

In any case, one way or another, we have our semicircle measures, and by putting now everything together, we obtain the Wigner theorem, as follows:

THEOREM 10.19. *Given a sequence of Wigner random matrices*

$$Z_N \in M_N(L^\infty(X))$$

having independent G_t variables as entries, with $t > 0$, up to $Z_N = Z_N^*$, we have

$$\frac{Z_N}{\sqrt{N}} \sim \frac{1}{2\pi t}\sqrt{4t - x^2}dx$$

in the $N \to \infty$ limit, with the limiting measure being the Wigner semicircle law γ_t.

PROOF. This follows indeed by combining Theorem 10.14 either with Proposition 10.16, and doing here an honest job, or with Proposition 10.18. □

There are many other things that can be said about the Wigner matrices, which appear as variations of the above, and we refer here to the standard random matrix books [2], [68], [71], [90]. We will be back to them later on in this book, in Part IV.

10d. Unitary groups

We discuss here an alternative interpretation of the limiting laws γ_t that we found above, by using Lie groups, the idea being that the standard semicircle law γ_1, and more generally all the laws γ_t, naturally appear in connection with the group SU_2.

This is something quite natural, and good to know, and will be useful for us later on. In relation with the above, the knowledge of this fact can be used as an alternative to both Stieltjes inversion, and cheating, in order to establish the Wigner theorem.

Let us start with the following fundamental group theory result, coming as a complement to the standard general theory for the compact groups:

THEOREM 10.20. *We have the following formula,*

$$SU_2 = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \Big| \ |\alpha|^2 + |\beta|^2 = 1 \right\}$$

which makes SU_2 isomorphic to the unit sphere $S^1_{\mathbb{C}} \subset \mathbb{C}^2$.

PROOF. Consider an arbitrary 2×2 matrix, written as follows:

$$U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

Assuming that we have $\det U = 1$, the inverse of this matrix is then given by:

$$U^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$$

On the other hand, assuming $U \in U_2$, the inverse must be the adjoint:

$$U^{-1} = \begin{pmatrix} \bar{\alpha} & \bar{\gamma} \\ \bar{\beta} & \bar{\delta} \end{pmatrix}$$

We conclude that our matrix must be of the following special form:

$$U = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}$$

Now since the determinant is 1, we must have $|\alpha|^2 + |\beta|^2 = 1$, so we are done with one direction. As for the converse, this is clear, the matrices in the statement being unitaries, and of determinant 1, and so being elements of SU_2. Finally, we have:

$$S^1_{\mathbb{C}} = \left\{ (\alpha, \beta) \in \mathbb{C}^2 \Big| \ |\alpha|^2 + |\beta|^2 = 1 \right\}$$

Thus, the final assertion in the statement holds as well. □

Next, we have the following useful reformulation of Theorem 10.20:

THEOREM 10.21. *We have the formula*

$$SU_2=\left\{\begin{pmatrix}p+iq&r+is\\ -r+is&p-iq\end{pmatrix}\Big|\,p^2+q^2+r^2+s^2=1\right\}$$

which makes SU_2 isomorphic to the unit real sphere $S^3_\mathbb{R}\subset\mathbb{R}^3$.

PROOF. We recall from Theorem 10.20 that we have:

$$SU_2=\left\{\begin{pmatrix}\alpha&\beta\\ -\bar{\beta}&\bar{\alpha}\end{pmatrix}\Big|\,|\alpha|^2+|\beta|^2=1\right\}$$

Now let us write our parameters $\alpha,\beta\in\mathbb{C}$, which belong to the complex unit sphere $S^1_\mathbb{C}\subset\mathbb{C}^2$, in terms of their real and imaginary parts, as follows:

$$\alpha=p+iq\quad,\quad\beta=r+is$$

In terms of $p,q,r,s\in\mathbb{R}$, our formula for a generic matrix $U\in SU_2$ reads:

$$U=\begin{pmatrix}p+iq&r+is\\ -r+is&p-iq\end{pmatrix}$$

As for the condition to be satisfied by the parameters $p,q,r,s\in\mathbb{R}$, this comes the condition $|\alpha|^2+|\beta|^2=1$ to be satisfied by $\alpha,\beta\in\mathbb{C}$, which reads:

$$p^2+q^2+r^2+s^2=1$$

Thus, we are led to the conclusion in the statement. Regarding now the last assertion, recall that the unit sphere $S^3_\mathbb{R}\subset\mathbb{R}^4$ is given by:

$$S^3_\mathbb{R}=\left\{(p,q,r,s)\,\Big|\,p^2+q^2+r^2+s^2=1\right\}$$

Thus, we have an isomorphism of compact spaces $SU_2\simeq S^3_\mathbb{R}$, as claimed. □

Here is yet another useful reformulation of our main result so far, regarding SU_2, obtained by further building on the parametrization from Theorem 10.21:

THEOREM 10.22. *We have the following formula,*

$$SU_2=\left\{p\beta_1+q\beta_2+r\beta_3+s\beta_4\,\Big|\,p^2+q^2+r^2+s^2=1\right\}$$

where $\beta_1,\beta_2,\beta_3,\beta_4$ are the following matrices,

$$\beta_1=\begin{pmatrix}1&0\\0&1\end{pmatrix}\quad,\quad\beta_2=\begin{pmatrix}i&0\\0&-i\end{pmatrix}\quad,\quad\beta_3=\begin{pmatrix}0&1\\-1&0\end{pmatrix}\quad,\quad\beta_4=\begin{pmatrix}0&i\\i&0\end{pmatrix}$$

called Pauli spin matrices.

PROOF. We recall from Theorem 10.21 that the group SU_2 can be parametrized by the real sphere $S^3_\mathbb{R}\subset\mathbb{R}^4$, in the following way:

$$SU_2=\left\{\begin{pmatrix}p+iq&r+is\\-r+is&p-iq\end{pmatrix}\Big|\,p^2+q^2+r^2+s^2=1\right\}$$

But this gives the formula in the statement, with the Pauli matrices $\beta_1,\beta_2,\beta_3,\beta_4$ being the coefficients of p,q,r,s, in this parametrization. □

The above result is often the most convenient one, when dealing with SU_2. This is because the Pauli matrices have a number of remarkable properties, as follows:

PROPOSITION 10.23. *The Pauli matrices multiply according to the following formulae,*

$$\beta_2^2=\beta_3^2=\beta_4^2=-1$$

$$\beta_2\beta_3=-\beta_3\beta_2=\beta_4$$

$$\beta_3\beta_4=-\beta_4\beta_3=\beta_2$$

$$\beta_4\beta_2=-\beta_2\beta_4=\beta_3$$

they conjugate according to the following rules,

$$\beta_1^*=\beta_1,\ \beta_2^*=-\beta_2,\ \beta_3^*=-\beta_3,\ \beta_4^*=-\beta_4$$

and they form an orthonormal basis of $M_2(\mathbb{C})$, with respect to the scalar product

$$<x,y>=tr(xy^*)$$

with $tr:M_2(\mathbb{C})\to\mathbb{C}$ being the normalized trace of 2×2 matrices, $tr=Tr/2$.

PROOF. The first two assertions, regarding the multiplication and conjugation rules for the Pauli matrices, follow from some elementary computations. As for the last assertion, this follows by using these rules. Indeed, the fact that the Pauli matrices are pairwise orthogonal follows from computations of the following type, for $i\neq j$:

$$<\beta_i,\beta_j>=tr(\beta_i\beta_j^*)=tr(\pm\beta_i\beta_j)=tr(\pm\beta_k)=0$$

As for the fact that the Pauli matrices have norm 1, this follows from:

$$<\beta_i,\beta_i>=tr(\beta_i\beta_i^*)=tr(\pm\beta_i^2)=tr(\beta_1)=1$$

Thus, we are led to the conclusion in the statement. □

Now back to probability, we can recover our semicircular measures, as follows:

THEOREM 10.24. *The main character of SU_2 follows the following law,*

$$\gamma_1=\frac{1}{2\pi}\sqrt{4-x^2}dx$$

which is the Wigner law of parameter 1.

Proof. This follows from Theorem 10.21, by identifying SU_2 with the sphere $S^3_\mathbb{R}$, the variable $\chi = 2Re(p)$ being semicircular. Indeed, let us write, as in Theorem 10.21:

$$SU_2 = \left\{ \begin{pmatrix} p+iq & r+is \\ -p+iq & r-is \end{pmatrix} \Big| \, p^2+q^2+r^2+s^2=1 \right\}$$

In this picture, the main character is given by the following formula:

$$\chi \begin{pmatrix} p+iq & r+is \\ -r+is & p-iq \end{pmatrix} = 2p$$

We are therefore left with computing the law of the following variable:

$$p \in C(S^3_\mathbb{R})$$

For this purpose, we can use the moment method. Let us recall from chapter 1 that the polynomial integrals over the real spheres are given by the following formula:

$$\int_{S^{N-1}_\mathbb{R}} x_1^{k_1} \ldots x_N^{k_N} \, dx = \frac{(N-1)!!k_1!! \ldots k_N!!}{(N+\Sigma k_i - 1)!!}$$

In our case, where $N = 4$, we obtain the following moment formula:

$$\begin{aligned}
\int_{S^3_\mathbb{R}} p^{2k} &= \frac{3!!(2k)!!}{(2k+3)!!} \\
&= 2 \cdot \frac{3 \cdot 5 \cdot 7 \ldots (2k-1)}{2 \cdot 4 \cdot 6 \ldots (2k+2)} \\
&= 2 \cdot \frac{(2k)!}{2^k k! 2^{k+1}(k+1)!} \\
&= \frac{1}{4^k} \cdot \frac{1}{k+1} \binom{2k}{k} \\
&= \frac{C_k}{4^k}
\end{aligned}$$

Thus the variable $2p \in C(S^3_\mathbb{R})$ follows the Wigner semicircle law γ_1, as claimed. □

Summarizing, we have managed to recover the Wigner semicircle law γ_1 out of purely geometric considerations, involving the real sphere $S^3_\mathbb{R}$ and the special complex rotation group SU_2. Moreover, with a change of variable, our results extend to γ_t with $t > 0$. And this is quite interesting, philosophically, and also makes an interesting connection with the standard Lie group material, which remains to be further investigated.

Finally, as the physicists say, there is no SU_2 without SO_3, so let us discuss as well the computation for SO_3, that we will certainly need later. Let us start with:

PROPOSITION 10.25. *The adjoint action $SU_2 \curvearrowright M_2(\mathbb{C})$, given by $T_U(A) = UAU^*$, leaves invariant the following real vector subspace of $M_2(\mathbb{C})$,*

$$\mathbb{R}^4 = span(\beta_1, \beta_2, \beta_3, \beta_4)$$

and we obtain in this way a group morphism $SU_2 \to GL_4(\mathbb{R})$.

PROOF. We have two assertions to be proved, as follows:

(1) We must first prove that, with $E \subset M_2(\mathbb{C})$ being the real vector space in the statement, we have the following implication:

$$U \in SU_2, A \in E \implies UAU^* \in E$$

But this is clear from the multiplication rules for the Pauli matrices, from Proposition 10.23. Indeed, let us write our matrices U, A as follows:

$$U = x\beta_1 + y\beta_2 + z\beta_3 + t\beta_4$$

$$A = a\beta_1 + b\beta_2 + c\beta_3 + d\beta_4$$

We know that the coefficients x, y, z, t and a, b, c, d are all real, due to $U \in SU_2$ and $A \in E$. The point now is that when computing UAU^*, by using the various rules from Proposition 10.23, we obtain a matrix of the same type, namely a combination of $\beta_1, \beta_2, \beta_3, \beta_4$, with real coefficients. Thus, we have $UAU^* \in E$, as desired.

(2) In order to conclude, let us identify $E \simeq \mathbb{R}^4$, by using the basis $\beta_1, \beta_2, \beta_3, \beta_4$. The result found in (1) shows that we have a correspondence as follows:

$$SU_2 \to M_4(\mathbb{R}) \quad , \quad U \to (T_U)_{|E}$$

Now observe that for any $U \in SU_2$ and any $A \in M_2(\mathbb{C})$ we have:

$$T_{U^*}T_U(A) = U^*UAU^*U = A$$

Thus $T_{U^*} = T_U^{-1}$, and so the correspondence that we found can be written as:

$$SU_2 \to GL_4(\mathbb{R}) \quad , \quad U \to (T_U)_{|E}$$

But this a group morphism, due to the following computation:

$$T_UT_V(A) = UVAV^*U^* = T_{UV}(A)$$

Thus, we are led to the conclusion in the statement. □

The point now is that Proposition 10.25 can be improved as follows:

PROPOSITION 10.26. *The adjoint action $SU_2 \curvearrowright M_2(\mathbb{C})$, given by*

$$T_U(A) = UAU^*$$

leaves invariant the following real vector subspace of $M_2(\mathbb{C})$,

$$F = span_{\mathbb{R}}(\beta_2, \beta_3, \beta_4)$$

and we obtain in this way a group morphism $SU_2 \to SO_3$.

PROOF. We can do this in several steps, as follows:

(1) Our first claim is that the group morphism $SU_2 \to GL_4(\mathbb{R})$ constructed in Proposition 10.25 is in fact a morphism $SU_2 \to O_4$. In order to prove this, recall the following formula, valid for any $U \in SU_2$, from the proof of Proposition 10.25:

$$T_{U^*} = T_U^{-1}$$

We want to prove that the matrices $T_U \in GL_4(\mathbb{R})$ are orthogonal, and in view of the above formula, it is enough to prove that we have:

$$T_U^* = (T_U)^t$$

So, let us prove this. For any two matrices $A, B \in E$, we have:

$$\begin{aligned} < T_{U^*}(A), B > &= < U^*AU, B > \\ &= tr(U^*AUB) \\ &= tr(AUBU^*) \end{aligned}$$

On the other hand, we have as well the following formula:

$$\begin{aligned} < (T_U)^t(A), B > &= < A, T_U(B) > \\ &= < A, UBU^* > \\ &= tr(AUBU^*) \end{aligned}$$

Thus we have indeed $T_U^* = (T_U)^t$, which proves our $SU_2 \to O_4$ claim.

(2) In order now to finish, recall that we have by definition $\beta_1 = 1$, as a matrix. Thus, the action of SU_2 on the vector $\beta_1 \in E$ is given by:

$$T_U(\beta_1) = U\beta_1U^* = UU^* = 1 = \beta_1$$

We conclude that $\beta_1 \in E$ is invariant under SU_2, and by orthogonality the following subspace of E must be invariant as well under the action of SU_2:

$$\beta_1^\perp = span_{\mathbb{R}}(\beta_2, \beta_3, \beta_4)$$

Now if we call this subspace F, and we identify $F \simeq \mathbb{R}^3$ by using the basis $\beta_2, \beta_3, \beta_4$, we obtain by restriction to F a morphism of groups as follows:

$$SU_2 \to O_3$$

But since this morphism is continuous and SU_2 is connected, its image must be connected too. Now since the target group decomposes as $O_3 = SO_3 \sqcup (-SO_3)$, and $1 \in SU_2$ gets mapped to $1 \in SO_3$, the whole image must lie inside SO_3, and we are done. □

The above result is quite interesting, because we will see in a moment that the morphism $SU_2 \to SO_3$ constructed there is surjective. Thus, we will have a way of parametrizing the elements $V \in SO_3$ by elements $U \in SU_2$, and so ultimately by parameters

$(x,y,z,t)\in S^3_{\mathbb{R}}$. In order to work out all this, let us start with the following result, coming as a continuation of Proposition 10.25, independently of Proposition 10.26:

PROPOSITION 10.27. *With respect to the standard basis $\beta_1,\beta_2,\beta_3,\beta_4$ of the vector space $\mathbb{R}^4=span(\beta_1,\beta_2,\beta_3,\beta_4)$, the morphism $T:SU_2\to GL_4(\mathbb{R})$ is given by:*

$$T_U=\begin{pmatrix}1&0&0&0\\0&p^2+q^2-r^2-s^2&2(qr-ps)&2(pr+qs)\\0&2(ps+qr)&p^2+r^2-q^2-s^2&2(rs-pq)\\0&2(qs-pr)&2(pq+rs)&p^2+s^2-q^2-r^2\end{pmatrix}$$

Thus, when looking at T as a group morphism $SU_2\to O_4$, what we have in fact is a group morphism $SU_2\to O_3$, and even $SU_2\to SO_3$.

PROOF. With notations from Proposition 10.25 and its proof, let us first look at the action $L:SU_2\curvearrowright\mathbb{R}^4$ by left multiplication, $L_U(A)=UA$. We have:

$$L_U=\begin{pmatrix}p&-q&-r&-s\\q&p&-s&r\\r&s&p&-q\\s&-r&q&p\end{pmatrix}$$

Similarly, in what regards now the action $R:SU_2\curvearrowright\mathbb{R}^4$ by right multiplication, $R_U(A)=AU^*$, the corresponding matrix is given by:

$$R_U=\begin{pmatrix}p&q&r&s\\-q&p&-s&r\\-r&s&p&-q\\-s&-r&q&p\end{pmatrix}$$

Now by composing, the matrix of the adjoint matrix in the statement is:

$$\begin{aligned}T_U&=R_UL_U\\&=\begin{pmatrix}p&q&r&s\\-q&p&-s&r\\-r&s&p&-q\\-s&-r&q&p\end{pmatrix}\begin{pmatrix}p&-q&-r&-s\\q&p&-s&r\\r&s&p&-q\\s&-r&q&p\end{pmatrix}\\&=\begin{pmatrix}1&0&0&0\\0&p^2+q^2-r^2-s^2&2(qr-ps)&2(pr+qs)\\0&2(ps+qr)&p^2+r^2-q^2-s^2&2(rs-pq)\\0&2(qs-pr)&2(pq+rs)&p^2+s^2-q^2-r^2\end{pmatrix}\end{aligned}$$

Thus, we have the formula in the statement, and this gives the result. $\square$

We can now formulate a famous result, due to Euler-Rodrigues, as follows:

THEOREM 10.28. *We have the Euler-Rodrigues formula*

$$U=\begin{pmatrix}p^2+q^2-r^2-s^2&2(qr-ps)&2(pr+qs)\\2(ps+qr)&p^2+r^2-q^2-s^2&2(rs-pq)\\2(qs-pr)&2(pq+rs)&p^2+s^2-q^2-r^2\end{pmatrix}$$

with $p^2+q^2+r^2+s^2=1$, for the generic elements of SO_3.

PROOF. We know from the above that we have a group morphism $SU_2\to SO_3$, given by the formula in the statement, and the problem now is that of proving that this is a double cover map, in the sense that it is surjective, and with kernel $\{\pm1\}$.

(1) Regarding the kernel, this is elementary to compute, as follows:

$$\begin{aligned}\ker(SU_2\to SO_3)&=\left\{U\in SU_2\Big|T_U(A)=A,\forall A\in E\right\}\\&=\left\{U\in SU_2\Big|UA=AU,\forall A\in E\right\}\\&=\left\{U\in SU_2\Big|U\beta_i=\beta_iU,\forall i\right\}\\&=\{\pm1\}\end{aligned}$$

(2) Thus, we are done with this, and as a side remark here, this result shows that our morphism $SU_2\to SO_3$ is ultimately a morphism as follows:

$$PU_2\subset SO_3\quad,\quad PU_2=SU_2/\{\pm1\}$$

Here P stands for "projective", and it is possible to say more about the construction $G\to PG$, which can be performed for any subgroup $G\subset U_N$. But we will not get here into this, our next goal being anyway that of proving that we have $PU_2=SO_3$.

(3) We must prove now that the morphism $SU_2\to SO_3$ is surjective. This is something non-trivial, and there are several proofs for this, as follows:

– A first proof is by using Lie theory. To be more precise, the tangent spaces at 1 of both SU_2 and SO_3 can be explicitly computed, by doing some linear algebra, and the morphism $SU_2\to SO_3$ follows to be surjective around 1, and then globally.

– Another proof is via representation theory. Indeed, the representations of SU_2 and SO_3 can be explicitly computed, and follow to be subject to very similar formulae, called Clebsch-Gordan rules, and this shows that $SU_2\to SO_3$ is surjective.

– Yet another advanced proof, which is actually quite bordeline for what can be called "proof", is by using the ADE/McKay classification of the subgroups $G\subset SO_3$, which shows that there is no room strictly inside SO_3 for something as big as PU_2.

(4) Thus, done with this, one way or another. Alternatively, a more pedestrian proof for the surjectivity of the morphism $SU_2\to SO_3$ is based on the fact that any rotation $U\in SO_3$ has an axis, and we will leave the computations here as an instructive exercise. □

Now back to probability, let us formulate the following definition:

DEFINITION 10.29. *The standard Marchenko-Pastur law π_1 is given by:*

$$f \sim \gamma_1 \implies f^2 \sim \pi_1$$

That is, π_1 is the law of the square of a variable following the semicircle law γ_1.

Here the fact that π_1 is indeed well-defined comes from the fact that a measure is uniquely determined by its moments. More explicitly now, we have:

PROPOSITION 10.30. *The density of the Marchenko-Pastur law is*

$$\pi_1 = \frac{1}{2\pi}\sqrt{4x^{-1}-1}\,dx$$

and the moments of this measure are the Catalan numbers.

PROOF. There are several proofs here, the simplest being by cheating. Indeed, the moments of π_1 can be computed with the change of variable $x = 4\cos^2 t$, as follows:

$$\begin{aligned}
M_k &= \frac{1}{2\pi}\int_0^4 \sqrt{4x^{-1}-1}\,x^k dx\\
&= \frac{1}{2\pi}\int_0^{\pi/2} \frac{\sin t}{\cos t}\cdot (4\cos^2 t)^k \cdot 2\cos t \sin t\,dt\\
&= \frac{4^{k+1}}{\pi}\int_0^{\pi/2} \cos^{2k} t \sin^2 t\,dt\\
&= \frac{4^{k+1}}{\pi}\cdot\frac{\pi}{2}\cdot\frac{(2k)!!2!!}{(2k+3)!!}\\
&= 2\cdot 4^k\cdot\frac{(2k)!/2^k k!}{2^{k+1}(k+1)!}\\
&= C_k
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

We can do now the character computation for SO_3, as follows:

THEOREM 10.31. *The main character of SO_3, modified by adding 1 to it, given in standard Euler-Rodrigues coordinates by*

$$\chi = 4p^2$$

follows a squared semicircle law, or Marchenko-Pastur law π_1.

PROOF. This follows by using the quotient map $SU_2 \to SO_3$, and the result for SU_2. Indeed, by using the Euler-Rodrigues formula, in the context of Theorem 10.24 and its proof, the main character of SO_3, modified by adding 1 to it, is given by:

$$\chi = (3p^2 - q^2 - r^2 - s^2) + 1 = 4p^2$$

Now recall from the proof of Theorem 10.24 that we have:

$$2p \sim \gamma_1$$

On the other hand, a quick comparison between the moment formulae for the Wigner and Marchenko-Pastur laws, which are very similar, shows that we have:

$$f \sim \gamma_1 \implies f^2 \sim \pi_1$$

Thus, with $f = 2p$, we obtain the result in the statement. □

10e. Exercises

Exercises:

Exercise 10.32.

Exercise 10.33.

Exercise 10.34.

Exercise 10.35.

Exercise 10.36.

Exercise 10.37.

Exercise 10.38.

Exercise 10.39.

Bonus exercise.

CHAPTER 11

Wishart matrices

11a. Positive matrices

We discuss in this chapter the complex Wishart matrices, which are the positive analogues of the Gaussian and Wigner matrices. These matrices were introduced and studied by Marchenko and Pastur in [**67**], not long after Wigner's paper [**100**], and are of interest in connection with many questions. They are constructed as follows:

Definition 11.1. *A complex Wishart matrix is a random matrix of type*

$$W = YY^* \in M_N(L^\infty(X))$$

with Y being a complex Gaussian matrix, with entries following the law G_t.

Due to the formula $W = YY^*$, the Wishart matrices are positive, in the general positivity sense of chapter 9. Before getting into their study, let us first develop some more theory for the positive matrices and operators. As a starting point, we have:

Theorem 11.2. *For an operator $T \in B(H)$, the following are equivalent:*

1. $<Tx, x> \geq 0$, *for any $x \in H$.*
2. *T is normal, and $\sigma(T) \subset [0, \infty)$.*
3. *$T = S^2$, for some $S \in B(H)$ satisfying $S = S^*$.*
4. *$T = R^*R$, for some $R \in B(H)$.*

If these conditions are satisfied, we call T positive, and write $T \geq 0$.

Proof. We have already seen some implications in chapter 9, but the best is to forget the few partial results that we know, and prove everything, as follows:

(1) $\implies$ (2) Assuming $<Tx, x> \geq 0$, with $S = T - T^*$ we have:

$$\begin{aligned} <Sx, x> &= <Tx, x> - <T^*x, x> \\ &= <Tx, x> - <x, Tx> \\ &= <Tx, x> - \overline{<Tx, x>} \\ &= 0 \end{aligned}$$

The next step is to use a polarization trick, as follows:

$$\begin{aligned} < Sx, y > &= < S(x+y), x+y > - < Sx, x > - < Sy, y > - < Sy, x > \\ &= - < Sy, x > \\ &= < y, Sx > \\ &= \overline{< Sx, y >} \end{aligned}$$

Thus we must have $< Sx, y > \in \mathbb{R}$, and with $y \to iy$ we obtain $< Sx, y > \in i\mathbb{R}$ too, and so $< Sx, y >= 0$. Thus $S = 0$, which gives $T = T^*$. Now since T is self-adjoint, it is normal as claimed. Moreover, by self-adjointness, we have:

$$\sigma(T) \subset \mathbb{R}$$

In order to prove now that we have indeed $\sigma(T) \subset [0, \infty)$, as claimed, we must invert $T + \lambda$, for any $\lambda > 0$. For this purpose, observe that we have:

$$\begin{aligned} < (T+\lambda)x, x > &= < Tx, x > + < \lambda x, x > \\ &\geq < \lambda x, x > \\ &= \lambda ||x||^2 \end{aligned}$$

But this shows that $T + \lambda$ is injective. In order to prove now the surjectivity, and the boundedness of the inverse, observe first that we have:

$$\begin{aligned} Im(T+\lambda)^\perp &= \ker(T+\lambda)^* \\ &= \ker(T+\lambda) \\ &= \{0\} \end{aligned}$$

Thus $Im(T + \lambda)$ is dense. On the other hand, observe that we have:

$$\begin{aligned} ||(T+\lambda)x||^2 &= < Tx + \lambda x, Tx + \lambda x > \\ &= ||Tx||^2 + 2\lambda < Tx, x > + \lambda^2 ||x||^2 \\ &\geq \lambda^2 ||x||^2 \end{aligned}$$

Thus for any vector in the image $y \in Im(T + \lambda)$ we have:

$$||y|| \geq \lambda \Big|\Big|(T+\lambda)^{-1} y\Big|\Big|$$

As a conclusion to what we have so far, $T + \lambda$ is bijective and invertible as a bounded operator from H onto its image, with the following norm bound:

$$||(T+\lambda)^{-1}|| \leq \lambda^{-1}$$

But this shows that $Im(T + \lambda)$ is complete, hence closed, and since we already knew that $Im(T + \lambda)$ is dense, our operator $T + \lambda$ is surjective, and we are done.

(2) $\implies$ (3) Since T is normal, and with spectrum contained in $[0, \infty)$, we can use the continuous functional calculus formula for the normal operators from chapter 9, with the function $f(x) = \sqrt{x}$, as to construct a square root $S = \sqrt{T}$.

(3) $\implies$ (4) This is trivial, because we can set $R = S$.

(4) $\implies$ (1) This is clear, because we have the following computation:

$$< R^*Rx, x >=< Rx, Rx >= ||Rx||^2$$

Thus, we have the equivalences in the statement. □

In analogy with what happens in finite dimensions, where among the positive matrices $A \geq 0$ we have the strictly positive ones, $A > 0$, given by the fact that the eigenvalues are strictly positive, we have as well a "strict" version of the above result, as follows:

THEOREM 11.3. *For an operator $T \in B(H)$, the following are equivalent:*

(1) *T is positive and invertible.*
(2) *T is normal, and $\sigma(T) \subset (0, \infty)$.*
(3) *$T = S^2$, for some $S \in B(H)$ invertible, satisfying $S = S^*$.*
(4) *$T = R^*R$, for some $R \in B(H)$ invertible.*

If these conditions are satisfied, we call T strictly positive, and write $T > 0$.

PROOF. Our claim is that the above conditions (1-4) are precisely the conditions (1-4) in Theorem 11.2, with the assumption "T is invertible" added. Indeed:

(1) This is clear by definition.

(2) In the context of Theorem 11.2 (2), namely when T is normal, and $\sigma(T) \subset [0, \infty)$, the invertibility of T, which means $0 \notin \sigma(T)$, gives $\sigma(T) \subset (0, \infty)$, as desired.

(3) In the context of Theorem 11.2 (3), namely when $T = S^2$, with $S = S^*$, by using the basic properties of the functional calculus for normal operators, the invertibility of T is equivalent to the invertibility of its square root $S = \sqrt{T}$, as desired.

(4) In the context of Theorem 11.2 (4), namely when $T = RR^*$, the invertibility of T is equivalent to the invertibility of R. This can be either checked directly, or deduced via the equivalence (3) $\iff$ (4) from Theorem 11.2, by using the above argument (3). □

As a subtlety now, we have the following complement to the above result:

PROPOSITION 11.4. *For a strictly positive operator, $T > 0$, we have*

$$< Tx, x >> 0 \quad , \quad \forall x \neq 0$$

but the converse of this fact is not true, unless we are in finite dimensions.

PROOF. We have several things to be proved, the idea being as follows:

(1) Regarding the main assertion, the inequality can be deduced as follows, by using the fact that the operator $S=\sqrt{T}$ is invertible, and in particular injective:

$$\begin{aligned}<Tx,x> &= <S^2x,x>\\ &= <Sx,S^*x>\\ &= <Sx,Sx>\\ &= ||Sx||^2\\ &> 0\end{aligned}$$

(2) In finite dimensions, assuming $<Tx,x>>0$ for any $x\neq 0$, we know from Theorem 11.2 that we have $T\geq 0$. Thus we have $\sigma(T)\subset[0,\infty)$, and assuming by contradiction $0\in\sigma(T)$, we obtain that T has $\lambda=0$ as eigenvalue, and the corresponding eigenvector $x\neq 0$ has the property $<Tx,x>=0$, contradiction. Thus $T>0$, as claimed.

(3) Finally, regarding the counterexample for the converse, we can use here:

$$T=\begin{pmatrix}1\\&\frac{1}{2}\\&&\frac{1}{3}\\&&&\ddots\end{pmatrix}$$

Indeed, T is well-defined and bounded, and we have $<Tx,x>>0$, for any vector $x\neq 0$. However, T is not invertible, and so the converse does not hold, as stated. □

With the above results in hand, let us discuss now some decomposition results for the bounded operators $T\in B(H)$, in analogy with what we know about the usual complex numbers $z\in\mathbb{C}$. We know that any $z\in\mathbb{C}$ can be written as follows, with $a,b\in\mathbb{R}$:

$$z=a+ib$$

Also, we know that both the real and imaginary parts $a,b\in\mathbb{R}$, and more generally any real number $c\in\mathbb{R}$, can be written as follows, with $r,s\geq 0$:

$$c=r-s$$

Here is the operator theoretic generalization of these results:

Proposition 11.5. *Given an operator $T\in B(H)$, the following happen:*

1. *We can write $T=A+iB$, with $A,B\in B(H)$ self-adjoint.*
2. *When $T=T^*$, we can write $T=R-S$, with $R,S\in B(H)$ positive.*
3. *Thus, we can write any T as a linear combination of 4 positive elements.*

Proof. All this follows from basic spectral theory, as follows:

(1) We can use here the same formula as for complex numbers, namely:

$$T=\frac{T+T^*}{2}+i\cdot\frac{T-T^*}{2i}$$

(2) This follows from the measurable functional calculus. Indeed, assuming $T = T^*$ we have $\sigma(T) \subset \mathbb{R}$, so we can use the following decomposition formula on $\mathbb{R}$:

$$z = \chi_{[0,\infty)} z - \chi_{(-\infty,0)}(-z)$$

Now by applying these measurable functions to T, we obtain as formula as follows, with both the operators $T_+, T_- \in B(H)$ being positive, as desired:

$$T = T_+ - T_-$$

(3) This follows by combining the results in (1) and (2) above. □

Going ahead with our decomposition results, another basic thing that we know about complex numbers is that any $z \in \mathbb{C}$ appears as a real multiple of a unitary:

$$z = re^{it}$$

Finding the correct operator theoretic analogue of this is quite tricky, and this even for the usual matrices $A \in M_N(\mathbb{C})$. As a basic result here, we have:

Proposition 11.6. *Given an operator $T \in B(H)$, the following happen:*

1. *If $T = T^*$ and $||T|| \leq 1$, we can write $T = (U + V)/2$, with U, V unitaries.*
2. *If $T = T^*$, we can write $T = \lambda(U + V)$, with U, V unitaries.*
3. *In general, we can write T as a rescaled sum of 4 unitaries.*

Proof. This follows from the results that we have, as follows:

(1) Assuming $T = T^*$ and $||T|| \leq 1$ we have $1 - T^2 \geq 0$, and the decomposition that we are looking for is as follows, with both the components being unitaries:

$$T = \frac{T + i\sqrt{1 - T^2}}{2} + \frac{T - i\sqrt{1 - T^2}}{2}$$

To be more precise, the square root can be extracted as in Theorem 11.2 (3), and the check of the unitarity of the components goes as follows:

$$(T + i\sqrt{1 - T^2})(T - i\sqrt{1 - T^2}) = T^2 + (1 - T^2) = 1$$

(2) This simply follows by applying (1) to the operator $T/||T||$.

(3) Assuming first $||T|| \leq 1$, we know from Proposition 11.5 (1) that we can write $T = A + iB$, with A, B being self-adjoint, and satisfying $||A||, ||B|| \leq 1$. Now by applying (1) to both A and B, we obtain a decomposition of T as follows:

$$T = \frac{U + V + X + Y}{2}$$

In general, we can apply this to the operator $T/||T||$, and we obtain the result. □

All this gets us into the multiplicative theory of the complex numbers, that we will attempt to generalize now. As a first construction, that we would like to generalize to the bounded operator setting, we have the construction of the modulus, as follows:

$$|z|=\sqrt{z\bar{z}}$$

The point now is that we can indeed generalize this construction, as follows:

PROPOSITION 11.7. *Given an operator $T\in B(H)$, we can construct a positive operator $|T|\in B(H)$, satisfying $|T|^2=T^*T$, as follows, by using the fact that T^*T is positive:*

$$|T|=\sqrt{T^*T}$$

In the case $H=\mathbb{C}$, this gives the usual absolute value of the complex numbers:

$$|z|=\sqrt{z\bar{z}}$$

More generally, in the case where $H=\mathbb{C}^N$ is finite dimensional, we obtain in this way the usual moduli of the complex matrices $A\in M_N(\mathbb{C})$.

PROOF. We have several things to be proved, the idea being as follows:

(1) The first assertion follows from Theorem 11.2. Indeed, according to (4) there the operator T^*T is indeed positive, and then according to (2) there we can extract the square root of this latter positive operator, by applying to it the function $\sqrt{z}$.

(2) By functional calculus we have then $|T|^2=T^*T$, as desired.

(3) In the case $H=\mathbb{C}$, we obtain indeed the absolute value of complex numbers.

(4) In the case where the space H is finite dimensional, $H=\mathbb{C}^N$, we obtain indeed the usual moduli of the complex matrices $A\in M_N(\mathbb{C})$. □

As a comment here, it is possible to talk as well about the operator $\sqrt{TT^*}$, which is in general different from $\sqrt{T^*T}$. Observe that when T is normal, we have:

$$\sqrt{TT^*}=\sqrt{T^*T}$$

Regarding now the polar decomposition formula, let us start with a weak version of this statement, regarding the invertible operators, as follows:

THEOREM 11.8. *We have the polar decomposition formula*

$$T=U\sqrt{T^*T}$$

with U being a unitary, for any $T\in B(H)$ invertible.

PROOF. According to our definition of $|T|=\sqrt{T^*T}$, we have:

$$\begin{aligned}<|T|x,|T|y> &= <x,|T|^2y>\\ &= <x,T^*Ty>\\ &= <Tx,Ty>\end{aligned}$$

Thus we can define a unitary operator $U\in B(H)$ as follows:

$$U(|T|x)=Tx$$

But this formula shows that we have $T=U|T|$, as desired. □

Observe that we have uniqueness in the above result, in what regards the choice of the unitary $U\in B(H)$, due to the fact that we can write this unitary as follows:

$$U=T(\sqrt{T^*T})^{-1}$$

More generally now, we have the following result:

THEOREM 11.9. *We have the polar decomposition formula*

$$T=U\sqrt{T^*T}$$

with U being a partial isometry, for any $T\in B(H)$.

PROOF. As before, in the proof of Theorem 11.8, we have the following equality, valid for any two vectors $x,y\in H$:

$$<|T|x,|T|y>=<Tx,Ty>$$

We conclude that the following linear application is well-defined, and isometric:

$$U:Im|T|\to Im(T)\quad,\quad |T|x\to Tx$$

By continuity we can extend this map U into an isometry, as follows:

$$U:\overline{Im|T|}\to\overline{Im(T)}\quad,\quad |T|x\to Tx$$

Moreover, we can further extend U into a partial isometry $U:H\to H$, by setting $Ux=0$, for any $x\in\overline{Im|T|}^\perp$, and with this convention, the result follows. □

Summarizing, as a first application of our spectral theory methods, we have now a full generalization of the polar decomposition result for the usual matrices.

11b. Marchenko-Pastur

Let us discuss now the complex Wishart matrices, which are the positive analogues of the Gaussian and Wigner matrices. These matrices were introduced and studied by Marchenko-Pastur in [67], not long after Wigner's paper [100], and are of interest in connection with many questions. They are constructed as follows:

DEFINITION 11.10. *A complex Wishart matrix is a random matrix of type*

$$W=YY^*\in M_N(L^\infty(X))$$

with Y being a complex Gaussian matrix, with entries following the law G_t.

There are in fact several possible definitions for the complex Wishart matrices, with some being more clever and useful that some other. To start with, we will use the above definition, which comes naturally out of what we know about the Gaussian and Wigner matrices. Once such matrices studied, we will talk about their versions, too.

Observe that, due to the defining formula $W = YY^*$, the complex Wishart matrices are obviously positive, $W \geq 0$, in the sense of the general positivity notion discussed above. Due to this key positivity property, and to the otherwise "randomness" of W, such matrices are useful in many down-to-earth contexts. More on this later.

As usual with the random matrices, we will be interested in computing the asymptotic laws of our Wishart matrices W, suitably rescaled, in the $N \to \infty$ limit. Quite surprisingly, the computation here leads to the Catalan numbers, but not exactly in the same way as for the Wigner matrices, the precise result being as follows:

Theorem 11.11. *Given a sequence of complex Wishart matrices*

$$W_N = Y_N Y_N^* \in M_N(L^\infty(X))$$

with Y_N being $N \times N$ complex Gaussian of parameter $t > 0$, we have

$$M_k\left(\frac{W_N}{N}\right) \simeq t^k C_k$$

for any exponent $k \in \mathbb{N}$, in the $N \to \infty$ limit.

Proof. There are several possible proofs for this result, as follows:

(1) A first method is by using the result that we have from chapter 10, for the Gaussian matrices Y_N. Indeed, we know from there that we have the following formula, valid for any colored integer $K = \circ\bullet\bullet\circ\ldots$, in the $N \to \infty$ limit:

$$M_K\left(\frac{Y_N}{\sqrt{N}}\right) \simeq t^{|K|/2}|\mathcal{NC}_2(K)|$$

With $K = \circ\bullet\circ\bullet\ldots$, alternating word of length $2k$, with $k \in \mathbb{N}$, this gives:

$$M_k\left(\frac{Y_N Y_N^*}{N}\right) \simeq t^k|\mathcal{NC}_2(K)|$$

Thus, in terms of the Wishart matrix $W_N = Y_N Y_N^*$ we have, for any $k \in \mathbb{N}$:

$$M_k\left(\frac{W_N}{N}\right) \simeq t^k|\mathcal{NC}_2(K)|$$

The point now is that, by doing some combinatorics, we have:

$$|\mathcal{NC}_2(K)| = |NC_2(2k)| = C_k$$

Thus, we are led to the formula in the statement.

(2) A second method, that we will explain now as well, is by proving the result directly, starting from definitions. The matrix entries of our matrix $W = W_N$ are given by:

$$W_{ij} = \sum_{r=1}^N Y_{ir}\bar{Y}_{jr}$$

Thus, the normalized traces of powers of W are given by the following formula:

$$\begin{aligned} tr(W^k) &= \frac{1}{N}\sum_{i_1=1}^N\ldots\sum_{i_k=1}^N W_{i_1i_2}W_{i_2i_3}\ldots W_{i_ki_1} \\ &= \frac{1}{N}\sum_{i_1=1}^N\ldots\sum_{i_k=1}^N\sum_{r_1=1}^N\ldots\sum_{r_k=1}^N Y_{i_1r_1}\bar{Y}_{i_2r_1}Y_{i_2r_2}\bar{Y}_{i_3r_2}\ldots Y_{i_kr_k}\bar{Y}_{i_1r_k}\end{aligned}$$

By rescaling now W by a $1/N$ factor, as in the statement, we obtain:

$$tr\left(\left(\frac{W}{N}\right)^k\right) = \frac{1}{N^{k+1}}\sum_{i_1=1}^N\ldots\sum_{i_k=1}^N\sum_{r_1=1}^N\ldots\sum_{r_k=1}^N Y_{i_1r_1}\bar{Y}_{i_2r_1}Y_{i_2r_2}\bar{Y}_{i_3r_2}\ldots Y_{i_kr_k}\bar{Y}_{i_1r_k}$$

By using now the Wick rule, we obtain the following formula for the moments, with $K = \circ\bullet\circ\bullet\ldots$, alternating word of length $2k$, and with $I = (i_1r_1, i_2r_1, \ldots, i_kr_k, i_1r_k)$:

$$\begin{aligned} M_k\left(\frac{W}{N}\right) &= \frac{t^k}{N^{k+1}}\sum_{i_1=1}^N\ldots\sum_{i_k=1}^N\sum_{r_1=1}^N\ldots\sum_{r_k=1}^N \#\left\{\pi\in\mathcal{P}_2(K)\Big|\pi\leq\ker I\right\} \\ &= \frac{t^k}{N^{k+1}}\sum_{\pi\in\mathcal{P}_2(K)}\#\left\{i,r\in\{1,\ldots,N\}^k\Big|\pi\leq\ker I\right\}\end{aligned}$$

In order to compute this quantity, we use the standard bijection $\mathcal{P}_2(K)\simeq S_k$. By identifying the pairings $\pi\in\mathcal{P}_2(K)$ with their counterparts $\pi\in S_k$, we obtain:

$$M_k\left(\frac{W}{N}\right) = \frac{t^k}{N^{k+1}}\sum_{\pi\in S_k}\#\left\{i,r\in\{1,\ldots,N\}^k\Big|i_s = i_{\pi(s)+1}, r_s = r_{\pi(s)}, \forall s\right\}$$

Now let $\gamma\in S_k$ be the full cycle, which is by definition the following permutation:

$$\gamma = (1\,2\,\ldots\,k)$$

The general factor in the product computed above is then 1 precisely when following two conditions are simultaneously satisfied:

$$\gamma\pi\leq\ker i \quad , \quad \pi\leq\ker r$$

Counting the number of free parameters in our moment formula, we obtain:

$$M_k\left(\frac{W}{N}\right) = t^k\sum_{\pi\in S_k}N^{|\pi|+|\gamma\pi|-k-1}$$

The point now is that the last exponent is well-known to be ≤ 0, with equality precisely when the permutation $\pi \in S_k$ is geodesic, which in practice means that π must come from a noncrossing partition. Thus we obtain, in the $N \to \infty$ limit:

$$M_k\left(\frac{W}{N}\right) \simeq t^k C_k$$

Thus, we are led to the conclusion in the statement. □

As a consequence of the above result, we have a new look on the Catalan numbers, which is more adapted to our present Wishart matrix considerations, as follows:

PROPOSITION 11.12. *The Catalan numbers $C_k = |NC_2(2k)|$ appear as well as*

$$C_k = |NC(k)|$$

where $NC(k)$ is the set of all noncrossing partitions of $\{1, \ldots, k\}$.

PROOF. This follows indeed from the proof of Theorem 11.11. □

The direct explanation for the above formula, relating noncrossing partitions and pairings, comes form the following result, which is very useful, and good to know:

PROPOSITION 11.13. *We have a bijection between noncrossing partitions and pairings*

$$NC(k) \simeq NC_2(2k)$$

which is constructed as follows:

(1) *The application $NC(k) \to NC_2(2k)$ is the "fattening" one, obtained by doubling all the legs, and doubling all the strings as well.*
(2) *Its inverse $NC_2(2k) \to NC(k)$ is the "shrinking" application, obtained by collapsing pairs of consecutive neighbors.*

PROOF. The fact that the two operations in the statement are indeed inverse to each other is clear, by computing the corresponding two compositions, with the remark that the construction of the fattening operation requires the partitions to be noncrossing. □

As a comment here, the above result is something quite remarkable, in view of the total lack of relation between $P(k)$ and $P_2(2k)$. Thus, taking for granted that "classical probability is about partitions, and free probability is about noncrossing partitions", a general principle that emerges from our study so far, and that we will fully justify later on, we have in Proposition 11.13 an endless source of things to be done, in the free case, having no classical counterpart. We will keep this discovery in our pocket, and have it pulled out of there, for some magic, on several occasions, in what follows.

Getting back now to Wishart matrices, at $t = 1$ we are led to the question of finding the law having the Catalan numbers as moments. We already know the answer to this question from chapter 10, and more specifically from our considerations there at the end, regarding SO_3, but here is as well an independent, pedestian solution to this question:

PROPOSITION 11.14. *The real measure having the Catalan numbers as moments is*

$$\pi_1 = \frac{1}{2\pi}\sqrt{4x^{-1}-1}\,dx$$

called Marchenko-Pastur law of parameter 1.

PROOF. As already mentioned, this is something that we already know, because we came upon this when talking about SO_3. Here are two alternative proofs:

(1) By using the Stieltjes inversion formula. In order to apply this formula, we need a simple formula for the Cauchy transform. For this purpose, our starting point will be the well-known formula for the generating series of the Catalan numbers, namely:

$$\sum_{k=0}^\infty C_k z^k = \frac{1-\sqrt{1-4z}}{2z}$$

By using this formula with $z=\xi^{-1}$, we obtain the following formula:

$$\begin{aligned}
G(\xi) &= \xi^{-1}\sum_{k=0}^\infty C_k\xi^{-k}\\
&= \xi^{-1}\cdot\frac{1-\sqrt{1-4\xi^{-1}}}{2\xi^{-1}}\\
&= \frac{1}{2}\left(1-\sqrt{1-4\xi^{-1}}\right)\\
&= \frac{1}{2}-\frac{1}{2}\sqrt{1-4\xi^{-1}}
\end{aligned}$$

With this formula in hand, let us apply now the Stieltjes inversion formula. The first term, namely 1/2, which is trivial, will not contribute to the density. As for the second term, which is something non-trivial, this will contribute to the density, the rule here being that the square root $\sqrt{1-4\xi^{-1}}$ will be replaced by the "dual" square root $\sqrt{4x^{-1}-1}\,dx$, and that we have to multiply everything by $-1/\pi$. Thus, by Stieltjes inversion we obtain the density in the statement, namely:

$$\begin{aligned}
d\mu(x) &= -\frac{1}{\pi}\cdot -\frac{1}{2}\sqrt{4x^{-1}-1}\,dx\\
&= \frac{1}{2\pi}\sqrt{4x^{-1}-1}\,dx
\end{aligned}$$

(2) Alternatively, if the above was too complicated, we can simply cheat, as we actually did in chapter 10, when talking about SO_3. Indeed, the moments of the law π_1 in the

statement can be computed with the change of variable $x = 4\cos^2 t$, as follows:

$$\begin{aligned}
M_k &= \frac{1}{2\pi}\int_0^4 \sqrt{4x^{-1}-1}\,x^k dx\\
&= \frac{1}{2\pi}\int_0^{\pi/2} \frac{\sin t}{\cos t}\cdot(4\cos^2 t)^k\cdot 2\cos t\sin t\,dt\\
&= \frac{4^{k+1}}{\pi}\int_0^{\pi/2}\cos^{2k} t\sin^2 t\,dt\\
&= \frac{4^{k+1}}{\pi}\cdot\frac{\pi}{2}\cdot\frac{(2k)!!2!!}{(2k+3)!!}\\
&= 2\cdot 4^k\cdot\frac{(2k)!/2^k k!}{2^{k+1}(k+1)!}\\
&= C_k
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Now back to the Wishart matrices, we are led to the following result:

THEOREM 11.15. *Given a sequence of complex Wishart matrices*

$$W_N = Y_N Y_N^* \in M_N(L^\infty(X))$$

with Y_N being $N\times N$ complex Gaussian of parameter 1, we have

$$\frac{W_N}{N} \sim \frac{1}{2\pi}\sqrt{4x^{-1}-1}\,dx$$

with $N\to\infty$, with the limiting measure being the Marchenko-Pastur law π_1.

PROOF. This follows indeed from the asymptotic moment computation that we have, for these matrices, from Theorem 11.11, coupled with Proposition 11.14. □

More generally now, we have as well a straightforward parametric version of the above result, involving a parameter $t>0$ as in Definition 11.10, as follows:

THEOREM 11.16. *Given a sequence of complex Wishart matrices*

$$W_N = Y_N Y_N^* \in M_N(L^\infty(X))$$

with Y_N being $N\times N$ complex Gaussian of parameter $t>0$, we have

$$\frac{W_N}{tN} \sim \frac{1}{2\pi}\sqrt{4x^{-1}-1}\,dx$$

with $N\to\infty$, with the limiting measure being the Marchenko-Pastur law π_1.

Proof. This follows again from Theorem 11.11 and Proposition 11.14. To be more precise, recall the main formula from Theorem 11.11, for the matrices as above, namely:

$$M_k\left(\frac{W_N}{N}\right)\simeq t^kC_k$$

By dividing by t^k, this formula can be written as follows:

$$M_k\left(\frac{W_N}{tN}\right)\simeq C_k$$

Now by using Proposition 11.14, we are led to the conclusion in the statement. □

Summarizing, we have deduced the Marchenko-Pastur theorem from the result for Gaussian matrices, via some moment combinatorics. It is possible as well to be a bit more direct here, by passing through the Wigner theorem, and then recovering the Marchenko-Pastur law directly from the Wigner semicircle law, by performing a kind of square operation. But this is more or less the same thing as we did above.

11c. Parametric version

We discuss now a generalization of the above results, motivated by a whole array of concrete questions, and bringing into the picture a "true" parameter $t>0$, which is different from the parameter $t>0$ used above, which is something quite trivial.

For this purpose, let us go back to the definition of the Wishart matrices. There were as follows, with Y being a $N\times N$ matrix with i.i.d. entries, each following the law G_t:

$$W=YY^*$$

The point now is that, more generally, we can use in this $W=YY^*$ construction a $N\times M$ matrix Y with i.i.d. entries, each following the law G_t, with $M\in\mathbb N$ being arbitrary. Thus, we have a new parameter, and by ditching the old parameter $t>0$, which was something not very interesting, we are led to the following definition, which is the "true" definition of the Wishart matrices, from [67] and the subsequent literature:

Definition 11.17. *A complex Wishart matrix is a $N\times N$ matrix of the form*

$$W=YY^*$$

where Y is a $N\times M$ matrix with i.i.d. entries, each following the law G_1.

As before with our previous Wishart matrices, that the new ones generalize, up to setting $t=1$, we have $W\geq 0$, by definition. Due to this property, and to the otherwise "randomness" of W, these matrices are useful in many contexts. More on this later.

In order to see what is going on, combinatorially, let us compute moments. The result here is substantially more interesting than that for the previous Wishart matrices, with the new revelant numeric parameter being now the number $t=M/N$, as follows:

THEOREM 11.18. *Given a sequence of complex Wishart matrices*

$$W_N = Y_N Y_N^* \in M_N(L^\infty(X))$$

with Y_N being $N \times M$ complex Gaussian of parameter 1, we have

$$M_k\left(\frac{W_N}{N}\right) \simeq \sum_{\pi \in NC(k)} t^{|\pi|}$$

for any exponent $k \in \mathbb{N}$, in the $M = tN \to \infty$ limit.

PROOF. This is something which is very standard, as follows:

(1) Before starting, let us clarify the relation with our previous Wishart matrix results. In the case $M = N$ we have $t = 1$, and the formula in the statement reads:

$$M_k\left(\frac{W_N}{N}\right) \simeq |NC(k)|$$

Thus, what we have here is the previous Wishart matrix formula, in full generality, at the value $t = 1$ of our old parameter $t > 0$.

(2) Observe also that by rescaling, we can obtain if we want from this the previous Wishart matrix formula, in full generality, at any value $t > 0$ of our old parameter. Thus, things fine, we are indeed generalizing what we did before.

(3) In order to prove now the formula in the statement, we proceed as usual, by using the Wick formula. The matrix entries of our Wishart matrix $W = W_N$ are given by:

$$W_{ij} = \sum_{r=1}^{M} Y_{ir} \bar{Y}_{jr}$$

Thus, the normalized traces of powers of W are given by the following formula:

$$\begin{aligned} tr(W^k) &= \frac{1}{N} \sum_{i_1=1}^{N} \ldots \sum_{i_k=1}^{N} W_{i_1 i_2} W_{i_2 i_3} \ldots W_{i_k i_1} \\ &= \frac{1}{N} \sum_{i_1=1}^{N} \ldots \sum_{i_k=1}^{N} \sum_{r_1=1}^{M} \ldots \sum_{r_k=1}^{M} Y_{i_1 r_1} \bar{Y}_{i_2 r_1} Y_{i_2 r_2} \bar{Y}_{i_3 r_2} \ldots Y_{i_k r_k} \bar{Y}_{i_1 r_k} \end{aligned}$$

By rescaling now W by a $1/N$ factor, as in the statement, we obtain:

$$tr\left(\left(\frac{W}{N}\right)^k\right) = \frac{1}{N^{k+1}} \sum_{i_1=1}^{N} \ldots \sum_{i_k=1}^{N} \sum_{r_1=1}^{M} \ldots \sum_{r_k=1}^{M} Y_{i_1 r_1} \bar{Y}_{i_2 r_1} Y_{i_2 r_2} \bar{Y}_{i_3 r_2} \ldots Y_{i_k r_k} \bar{Y}_{i_1 r_k}$$

(4) By using now the Wick rule, we obtain the following formula for the moments, with $K=\circ\bullet\circ\bullet\ldots$, alternating word of lenght $2k$, and $I=(i_1r_1,i_2r_1,\ldots,i_kr_k,i_1r_k)$:

$$\begin{aligned}M_k\left(\frac{W}{N}\right)&=\frac{1}{N^{k+1}}\sum_{i_1=1}^N\ldots\sum_{i_k=1}^N\sum_{r_1=1}^M\ldots\sum_{r_k=1}^M\#\left\{\pi\in\mathcal{P}_2(K)\Big|\pi\leq\ker I\right\}\\&=\frac{1}{N^{k+1}}\sum_{\pi\in\mathcal{P}_2(K)}\#\left\{i\in\{1,\ldots,N\}^k,r\in\{1,\ldots,M\}^k\Big|\pi\leq\ker I\right\}\end{aligned}$$

(5) In order to compute this quantity, we use the standard bijection $\mathcal{P}_2(K)\simeq S_k$. By identifying the pairings $\pi\in\mathcal{P}_2(K)$ with their counterparts $\pi\in S_k$, we obtain:

$$M_k\left(\frac{W}{N}\right)=\frac{1}{N^{k+1}}\sum_{\pi\in S_k}\#\left\{i\in\{1,\ldots,N\}^k,r\in\{1,\ldots,M\}^k\Big|i_s=i_{\pi(s)+1},r_s=r_{\pi(s)}\right\}$$

Now let $\gamma\in S_k$ be the full cycle, which is by definition the following permutation:

$$\gamma=(1\,2\,\ldots\,k)$$

The general factor in the product computed above is then 1 precisely when following two conditions are simultaneously satisfied:

$$\gamma\pi\leq\ker i\quad,\quad\pi\leq\ker r$$

Counting the number of free parameters in our expectation formula, we obtain:

$$M_k\left(\frac{W}{N}\right)=\frac{1}{N^{k+1}}\sum_{\pi\in S_k}N^{|\gamma\pi|}M^{|\pi|}=\sum_{\pi\in S_k}N^{|\gamma\pi|-k-1}M^{|\pi|}$$

(6) Now by using the same arguments as in the case $M=N$, from the proof of Theorem 7.11, we conclude that in the $M=tN\to\infty$ limit the permutations $\pi\in S_k$ which matter are those coming from noncrossing partitions, and so that we have:

$$M_k\left(\frac{W}{N}\right)\simeq\sum_{\pi\in NC(k)}N^{-|\pi|}M^{|\pi|}=\sum_{\pi\in NC(k)}t^{|\pi|}$$

We are therefore led to the conclusion in the statement. □

In order to recapture now the density out of the moments, we can of course use the Stieltjes inversion formula, but the computations here are a bit opaque. So, inspired from what happens at $t=1$, let us cheat a bit, and formulate a nice definition, as follows:

Definition 11.19. *The Marchenko-Pastur law π_t of parameter $t>0$ is given by:*

$$a\sim\gamma_t\implies a^2\sim\pi_t$$

That is, π_t the law of the square of a variable following the law γ_t.

This is certainly very nice, and we know from chapter 10 that at $t=1$ we obtain indeed the Marchenko-Pastur law π_1, as constructed above. In general, we have:

Proposition 11.20. *The Marchenko-Pastur law of parameter $t>0$ is*

$$\pi_t=\max(1-t,0)\delta_0+\frac{\sqrt{4t-(x-1-t)^2}}{2\pi x}\,dx$$

the support being $[0,4t^2]$, and the moments of this measure are

$$M_k=\sum_{\pi\in NC(k)}t^{|\pi|}$$

exactly as for the asymptotic moments of the complex Wishart matrices.

Proof. This follows as usual, by doing some computations, either combinatorics, or calculus. To be more precise, we have three formulae for π_t to be connected, namely the one in Definition 11.19, and the two ones from the present statement, and the connections between them can be established exactly as we did before, at $t=1$. □

Summarizing, we have now a definition for the Marchenko-Pastur law π_t, which is quite elegant, via Definition 11.19, but which still requires some computations, performed in the proof of Proposition 11.20. We will see later on, in Part IV, an even more elegant definition for π_t, out of its particular case π_1 which was well understood, simply obtained by considering the corresponding 1-parameter free convolution semigroup. We will also see that π_t appears as the "free version" of the Poisson law p_t, and that this can be even taken as a definition for π_t, if we really want to. More on this later.

Now back to the complex Wishart matrices that we are interested in, in this chapter, we can now formulate a final result regarding them, as follows:

Theorem 11.21. *Given a sequence of complex Wishart matrices*

$$W_N=Y_NY_N^*\in M_N(L^\infty(X))$$

with Y_N being $N\times M$ complex Gaussian of parameter 1, we have

$$\frac{W_N}{N}\sim\max(1-t,0)\delta_0+\frac{\sqrt{4t-(x-1-t)^2}}{2\pi x}\,dx$$

with $M=tN\to\infty$, with the limiting measure being the Marchenko-Pastur law π_t.

Proof. This follows indeed from Theorem 11.18 and Proposition 11.20. □

As it was the case with the Gaussian and Wigner matrices, there are many other things that can be said about the complex Wishart matrices, as variations of the above. We refer here to the standard random matrix literature [2], [68], [71], [90]. We will be back to this right below, in the remainder of this chapter, with some wizarding computations from [5], and then more systematically in Part IV, when doing free probability.

11d. Shifted semicircles

Our goal now, in the remainder of this chapter, will be that of explaining a surprising result, due to Aubrun [5], stating that when suitably block-transposing the entries of a complex Wishart matrix, we obtain as asymptotic distribution a shifted version of Wigner's semicircle law. Following [5], [11], let us start with the following definition:

Definition 11.22. *The partial transpose of a complex Wishart matrix W of parameters (dn, dm) is the matrix*

$$\widetilde{W} = (id \otimes t)W$$

where id is the identity of $M_d(\mathbb{C})$, and t is the transposition of $M_n(\mathbb{C})$.

In more familiar terms of bases and indices, the standard decomposition $\mathbb{C}^{dn} = \mathbb{C}^d \otimes \mathbb{C}^n$ induces an algebra decomposition $M_{dn}(\mathbb{C}) = M_d(\mathbb{C}) \otimes M_n(\mathbb{C})$, and with this convention made, the partial transpose matrix $\widetilde{W}$ constructed above has entries as follows:

$$\widetilde{W}_{ia,jb} = W_{ib,ja}$$

Our goal in what follows will be that of computing the law of $\widetilde{W}$, first when d, n, m are fixed, and then in the $d \to \infty$ regime. For this purpose, we will need a number of standard facts regarding the noncrossing partitions. Let us start with:

Proposition 11.23. *For a permutation $\sigma \in S_p$, we have the formula*

$$|\sigma| + \#\sigma = p$$

where $|\sigma|$ is the number of cycles of σ, and $\#\sigma$ is the minimal $k \in \mathbb{N}$ such that σ is a product of k transpositions. Also, the following formula defines a distance on S_p,

$$(\sigma, \pi) \to \#(\sigma^{-1}\pi)$$

and the set of permutations $\sigma \in S_p$ which saturate the triangular inequality

$$\#\sigma + \#(\sigma^{-1}\gamma) = \#\gamma = p - 1$$

where $\gamma \in S_p$ is a full cycle, is in bijection with the set $NC(p)$.

Proof. All this is standard combinatorics, that we will leave as an exercise. □

We use the standard bijection $NC(p) \simeq NC_2(2p)$, denoted $\pi \to \widetilde{\pi}$, obtained by fattening the partitions. We have the following formula, where $\vee$ is the join operation on $NC_2(2p)$, and $\rho_{12} = (12)(34)\ldots(2p-1, 2p)$ is the fattened identity permutation:

$$|\pi| = |\widetilde{\pi} \vee \rho_{12}|$$

Similarly, we have the formula $|\pi\gamma| = |\widetilde{\pi} \vee \rho_{14}|$, where ρ_{14} is the pairing corresponding to the fattening of the inverse full cycle $\gamma^{-1}(i) = i - 1$, which pairs an element $2i$ with $2(i-1) - 1 = 2i - 3$, or, equivalently, an element $i \in \{1, \ldots, 2p\}$ with $i + (-1)^{i+1}3$.

We will need the following well-known result:

Proposition 11.24. *The number $||\pi||$ of blocks having even size is given by*

$$1+||\pi||=|\pi\gamma|$$

for every noncrossing partition $\pi\in NC(p)$.

Proof. We use a recurrence over the number of blocks of π. If π has just one block, its associated geodesic permutation is γ and we have:

$$|\gamma^2|=\begin{cases}1 & (p\text{ odd})\\ 2 & (p\text{ even})\end{cases}$$

For the partitions π having more than one block, we can assume without loss of generality that $\pi=\hat{1}_k\sqcup\pi'$, where $\hat{1}_k$ is a contiguous block of size k. Recall that the number of blocks of the permutation $\pi\gamma$ is given by the following formula, where $\rho_{14}\in P_2(2p)$ is the pair partition which pairs an element i with $i+(-1)^{i+1}3$:

$$|\pi\gamma|=|\widetilde{\pi}\vee\rho_{14}|$$

If k is an even number, $k=2r$, consider the following partition, which contains the block $(1\,4\,5\,8\ldots 4r-3\,4r)$, along with the blocks coming from the elements of the form $4i+2,4i+3$ from $\{1,\ldots,4r\}$ and from π':

$$\sigma=\widetilde{\hat{1}_{2r}\sqcup\pi'}\vee\rho_{14}$$

We can count the blocks of the join of two partitions by drawing them one beneath the other and counting the number of connected components of the curve, without taking into account the possible crossings. We conclude that we have the following formula, where ρ_{14}' is ρ_{14} restricted to the set $\{2k+1,2k+2\ldots,2p\}$:

$$|\widetilde{\pi}\vee\rho_{14}|=1+|\widetilde{\pi'}\vee\rho_{14}'|$$

If k is odd, $k=2r+1$, there is no extra block appearing, so we have:

$$|\widetilde{\pi}\vee\rho_{14}|=|\widetilde{\pi'}\vee\rho_{14}'|$$

Thus, we are led to the conclusion in the statement. □

We can now investigate the block-transposed Wishart matrices, and we have:

Theorem 11.25. *For any $p\geq 1$ we have the formula*

$$\lim_{d\to\infty}(E\circ tr)\big(m\widetilde{W}\big)^p=\sum_{\pi\in NC(p)}m^{|\pi|}n^{||\pi||}$$

where $|.|$ and $||.||$ are the number of blocks, and the number of blocks of even size.

Proof. The matrix elements of the partial transpose matrix are given by:

$$\widetilde{W}_{ia,jb}=W_{ib,ja}=(dm)^{-1}\sum_{k=1}^d\sum_{c=1}^m G_{ib,kc}\bar{G}_{ja,kc}$$

This gives the following formula:

$$\begin{aligned}tr(\widetilde{W}^p) &= (dn)^{-1}(dm)^{-p}\sum_{i_1,\ldots,i_p=1}^d\sum_{a_1,\ldots,a_p=1}^n\prod_{s=1}^p W_{i_sa_{s+1},i_{s+1}a_s}\\ &= (dn)^{-1}(dm)^{-p}\sum_{i_1,\ldots,i_p=1}^d\sum_{a_1,\ldots,a_p=1}^n\prod_{s=1}^p\sum_{j_1,\ldots,j_p=1}^d\sum_{b_1,\ldots,b_p=1}^m G_{i_sa_{s+1},j_sb_s}\bar{G}_{i_{s+1}a_s,j_sb_s}\end{aligned}$$

After interchanging the product with the last two sums, the average of the general term can be computed by the Wick rule, namely:

$$E\left(\prod_{s=1}^p G_{i_sa_{s+1},j_sb_s}\bar{G}_{i_{s+1}a_s,j_sb_s}\right)=\sum_{\pi\in S_p}\prod_{s=1}^p\delta_{i_s,i_{\pi(s)+1}}\delta_{a_{s+1},a_{\pi(s)}}\delta_{j_s,j_{\pi(s)}}\delta_{b_s,b_{\pi(s)}}$$

Let $\gamma\in S_p$ be the full cycle $\gamma=(1\,2\,\ldots\,p)^{-1}$. The general factor in the above product is 1 if and only if the following four conditions are simultaneously satisfied:

$$\gamma^{-1}\pi\leq\ker i\quad,\quad\pi\gamma\leq\ker a\quad,\quad\pi\leq\ker j\quad,\quad\pi\leq\ker b$$

Counting the number of free parameters in the above equation, we obtain:

$$\begin{aligned}(E\circ tr)(\widetilde{W}^p) &= (dn)^{-1}(dm)^{-p}\sum_{\pi\in S_p}d^{|\pi|+|\gamma^{-1}\pi|}m^{|\pi|}n^{|\pi\gamma|}\\ &= \sum_{\pi\in S_p}d^{|\pi|+|\gamma^{-1}\pi|-p-1}m^{|\pi|-p}n^{|\pi\gamma|-1}\end{aligned}$$

The exponent of d in the last expression on the right is:

$$\begin{aligned}N(\pi) &= |\pi|+|\gamma^{-1}\pi|-p-1\\ &= p-1-(\#\pi+\#(\gamma^{-1}\pi))\\ &= p-1-(\#\pi+\#(\pi^{-1}\gamma))\end{aligned}$$

As explained in the beginning of this section, this quantity is known to be ≤ 0, with equality iff π is geodesic, hence associated to a noncrossing partition. Thus:

$$(E\circ tr)(\widetilde{W}^p)=(1+O(d^{-1}))m^{-p}n^{-1}\sum_{\pi\in NC(p)}m^{|\pi|}n^{|\pi\gamma|}$$

Together with $|\pi\gamma|=||\pi||+1$, this gives the result. □

We would like now to find an equation for the moment generating function of the asymptotic law of $m\widetilde{W}$. This moment generating function is defined by:

$$F(z)=\lim_{d\to\infty}(E\circ tr)\left(\frac{1}{1-zm\widetilde{W}}\right)$$

We have the following result, regarding this moment generating function:

THEOREM 11.26. *The moment generating function of $m\widetilde{W}$ satisfies the equation*

$$(F-1)(1-z^2F^2)=mzF(1+nzF)$$

in the $d\to\infty$ limit.

PROOF. We use the formula in Theorem 11.25. If we denote by $N(p,b,e)$ the number of partitions in $NC(p)$ having b blocks and e even blocks, we have:

$$\begin{aligned}F&=1+\sum_{p=1}^\infty\sum_{\pi\in NC(p)}z^pm^{|\pi|}n^{||\pi||}\\&=1+\sum_{p=1}^\infty\sum_{b=0}^\infty\sum_{e=0}^\infty z^pm^bn^eN(p,b,e)\end{aligned}$$

Let us try to find a recurrence formula for the numbers $N(p,b,e)$. If we look at the block containing 1, this block must have $r\geq 0$ other legs, and we get:

$$\begin{aligned}N(p,b,e)&=\sum_{r\in2\mathbb{N}}\sum_{p=\Sigma p_i+r+1}\sum_{b=\Sigma b_i+1}\sum_{e=\Sigma e_i}N(p_1,b_1,e_1)\ldots N(p_{r+1},b_{r+1},e_{r+1})\\&+\sum_{r\in2\mathbb{N}+1}\sum_{p=\Sigma p_i+r+1}\sum_{b=\Sigma b_i+1}\sum_{e=\Sigma e_i+1}N(p_1,b_1,e_1)\ldots N(p_{r+1},b_{r+1},e_{r+1})\end{aligned}$$

Here $p_1,\ldots,p_{r+1}$ are the number of points between the legs of the block containing 1, so that we have $p=(p_1+\ldots+p_{r+1})+r+1$, and the whole sum is split over two cases, r even or odd, because the parity of r affects the number of even blocks of our partition. Now by multiplying everything by a $z^pm^bn^e$ factor, and by carefully distributing the various powers of z,m,b on the right, we obtain the following formula:

$$\begin{aligned}z^pm^bn^eN(p,b,e)&=m\sum_{r\in2\mathbb{N}}z^{r+1}\sum_{p=\Sigma p_i+r+1}\sum_{b=\Sigma b_i+1}\sum_{e=\Sigma e_i}\prod_{i=1}^{r+1}z^{p_i}m^{b_i}n^{e_i}N(p_i,b_i,e_i)\\&+mn\sum_{r\in2\mathbb{N}+1}z^{r+1}\sum_{p=\Sigma p_i+r+1}\sum_{b=\Sigma b_i+1}\sum_{e=\Sigma e_i+1}\prod_{i=1}^{r+1}z^{p_i}m^{b_i}n^{e_i}N(p_i,b_i,e_i)\end{aligned}$$

Let us sum now all these equalities, over all $p\geq 1$ and over all $b,e\geq 0$. According to the definition of F, at left we obtain $F-1$. As for the two sums appearing on the right, that is, at right of the two z^{r+1} factors, when summing them over all $p \geq 1$ and over all $b, e \geq 0$, we obtain in both cases F^{r+1}. So, we have the following formula:

$$\begin{aligned} F-1 &= m\sum_{r\in 2\mathbb{N}}(zF)^{r+1}+mn\sum_{r\in 2\mathbb{N}+1}(zF)^{r+1} \\ &= m\,\frac{zF}{1-z^2F^2}+mn\,\frac{z^2F^2}{1-z^2F^2} \\ &= mzF\,\frac{1+nzF}{1-z^2F^2} \end{aligned}$$

But this gives the formula in the statement, and we are done. □

Our goal now will be that of further processing the formula in Theorem 11.26, as to reach to a formula for the density of the corresponding law. This is something quite tricky, and as a first result here, we can reformulate Theorem 11.26 as follows:

THEOREM 11.27. *The Cauchy transform of $m\widetilde{W}$ satisfies the equation*

$$(\xi G-1)(1-G^2)=mG(1+nG)$$

in the $d\to\infty$ limit. Moreover, this equation simply reads

$$R=\frac{m}{2}\left(\frac{n+1}{1-z}-\frac{n-1}{1+z}\right)$$

with the substitutions $G\to z$ and $\xi\to R+z^{-1}$.

PROOF. We have two assertions to be proved, the first one being standard, and the second one being something quite magic, the idea being as follows:

(1) Consider the equation of F, found in Theorem 11.26, namely:

$$(F-1)(1-z^2F^2)=mzF(1+nzF)$$

With $z\to\xi^{-1}$ and $F\to\xi G$, so that $zF\to G$, we obtain, as desired:

$$(\xi G-1)(1-G^2)=mG(1+nG)$$

(2) Thus, we have our equation for the Cauchy transform, and with this in hand, we can try to go ahead, and use somehow the Stieltjes inversion formula, in order to reach to a formula for the density. This is certainly possible, but our claim is that we can do better, by performing first some clever manipulations on the Cauchy transform.

(3) To be more precise, let us look at the equation of the Cauchy transform that we have. With the substitutions $\xi\to K$ and $G\to z$, this equation becomes:

$$(zK-1)(1-z^2)=mz(1+nz)$$

The point now is that with $K\to R+z^{-1}$ this latter equation becomes:

$$zR(1-z^2)=mz(1+nz)$$

But the solution of this latter equation is trivial to compute, given by:

$$R = m\frac{1+nz}{1-z^2} = \frac{m}{2}\left(\frac{n+1}{1-z} - \frac{n-1}{1+z}\right)$$

Thus, we are led to the conclusion in the statement. □

All the above might look a bit mysterious, but we are into difficult mathematics now, that will take us some time to be understood. In any case, the manipulations made in Theorem 11.27 are quite interesting, and suggest the following definition:

Definition 11.28. *Given a real probability measure μ, define its R-transform by:*

$$G_\mu(\xi) = \int_{\mathbb{R}} \frac{d\mu(t)}{\xi - t} \implies G_\mu\left(R_\mu(\xi) + \frac{1}{\xi}\right) = \xi$$

That is, the R-transform is the inverse of the Cauchy transform, up to a ξ^{-1} factor.

This definition is actually something very deep, due to Voiculescu [88], and we will have the whole remainder of this book for exploring its subtleties. For the moment, let us just take it as such, as something natural emerging from Theorem 11.27.

Getting back now to our questions, we would like to find the probability measure having as R-transform the function in Theorem 11.27. But here, we can only expect to find some kind of modification of the Marchenko-Pastur law, so as a first piece of work, let us just compute the R-transform of the Marchenko-Pastur law. We have here:

Proposition 11.29. *The R-transform of the Marchenko-Pastur law π_t is*

$$R_{\pi_t}(\xi) = \frac{t}{1-\xi}$$

for any $t > 0$.

Proof. This can be done in two steps, as follows:

(1) At $t = 1$, we know that the moments of π_1 are the Catalan numbers, $M_k = C_k$, and we obtain that the Cauchy transform is given by the following formula:

$$G(\xi) = \frac{1}{2} - \frac{1}{2}\sqrt{1 - 4\xi^{-1}}$$

Now with $R(\xi)=\frac{1}{1-\xi}$ being the function in the statement, at $t=1$, we have:

$$\begin{aligned} G\left(R(\xi)+\frac{1}{\xi}\right) &= G\left(\frac{1}{1-\xi}+\frac{1}{\xi}\right) \\ &= G\left(\frac{1}{\xi-\xi^2}\right) \\ &= \frac{1}{2}-\frac{1}{2}\sqrt{1-4\xi+4\xi^2} \\ &= \frac{1}{2}-\frac{1}{2}(1-2\xi) \\ &= \xi \end{aligned}$$

Thus, the function $R(\xi)=\frac{1}{1-\xi}$ is indeed the R-transform of π_1, in the above sense.

(2) In the general case, $t>0$, the proof is similar, by using the moment formula for π_t, that we know from the above. We will be back to this with full details when really needed, and more specifically in Part IV, when doing free probability. □

All this is very nice, and we can now further build on Theorem 11.27, as follows:

THEOREM 11.30. *The R-transform of $m\widetilde{W}$ is given by*

$$R=R_{\pi_s}-R_{\pi_t}$$

in the $d\to\infty$ limit, where $s=m(n+1)/2$ and $t=m(n-1)/2$.

PROOF. We know from Theorem 11.27 that the R-transform of $m\widetilde{W}$ is given by:

$$R=\frac{m}{2}\left(\frac{n+1}{1-z}-\frac{n-1}{1+z}\right)$$

By using now the formula in Proposition 11.29, this gives the result. □

We can now recover the original result of Aubrun [5], as follows:

THEOREM 11.31. *For a block-transposed Wishart matrix $\widetilde{W}=(id\otimes t)W$ we have, in the $n=\beta m\to\infty$ limit, with $\beta>0$ fixed, the formula*

$$\frac{\widetilde{W}}{d}\sim\gamma_\beta^1$$

with γ_β^1 being the shifted version of the semicircle law γ_β, with support centered at 1.

PROOF. This follows from Theorem 11.30. Indeed, in the $n=\beta m\to\infty$ limit, with $\beta>0$ fixed, we are led to the following formula for the Stieltjes transform:

$$f(x)=\frac{\sqrt{4\beta-(1-x)^2}}{2\beta\pi}$$

But this is the density of the shifted semicircle law having support as follows:

$$S=[1-2\sqrt{\beta},1+2\sqrt{\beta}]$$

Thus, we are led to the conclusion in the statement. See [5], [11]. □

Here we have used some standard free probability results at the end, which can be proved by direct computations, and we will be back to this in Part IV.

11e. Exercises

Exercises:

EXERCISE 11.32.

EXERCISE 11.33.

EXERCISE 11.34.

EXERCISE 11.35.

EXERCISE 11.36.

EXERCISE 11.37.

EXERCISE 11.38.

EXERCISE 11.39.

Bonus exercise.

CHAPTER 12

Block modifications

12a. Block modifications

We discuss in this chapter some extensions and unifications of our results from chapter 11. As before with the usual or block-transposed Wishart matrices, there will be some non-trivial combinatorics here, that we will fully understand only later, in Part IV, when doing free probability. Thus, the material below will be an introduction to this.

Let us begin with some general block modification considerations, following [**5**] and the more recent papers [**11**], [**12**]. We have the following construction:

Definition 12.1. *Given a complex Wishart $dn\times dn$ matrix, appearing as*

$$W=YY^*\in M_{dn}(L^\infty(X))$$

with Y being a complex Gaussian $dn\times dm$ matrix, and a linear map

$$\varphi:M_n(\mathbb C)\to M_n(\mathbb C)$$

we consider the following matrix, obtained by applying φ to the $n\times n$ blocks of W,

$$\widetilde{W}=(id\otimes\varphi)W\in M_{dn}(L^\infty(X))$$

and call it block-modified Wishart matrix.

Here we are using some standard tensor product identifications, the details being as follows. Let Y be a complex Gaussian $dn\times dm$ matrix, as above:

$$Y\in M_{dn\times dm}(L^\infty(X))$$

We can then form the corresponding complex Wishart matrix, as follows:

$$W=YY^*\in M_{dn}(L^\infty(X))$$

The size of this matrix being a composite number, $N=dn$, we can regard this matrix as being a $n\times n$ matrix, with random $d\times d$ matrices as entries. Equivalently, by using standard tensor product notations, this amounts in regarding W as follows:

$$W\in M_d(L^\infty(X))\otimes M_n(\mathbb C)$$

With this done, we can come up with our linear map, namely:

$$\varphi:M_n(\mathbb C)\to M_n(\mathbb C)$$

We can apply φ to the tensors on the right, and we obtain a matrix as follows:

$$\widetilde{W}=(id\otimes\varphi)W\in M_d(L^\infty(X))\otimes M_n(\mathbb{C})$$

Finally, we can forget now about tensors, and as a conclusion to all this, we have constructed a matrix as follows, that we can call block-modified Wishart matrix:

$$\widetilde{W}\in M_{dn}(L^\infty(X))$$

In practice now, what we mostly need for fully understanding Definition 12.1 are examples. Following Aubrun [5], and the series of papers by Collins and Nechita [23], [24], [25], we have the following basic examples, for our general construction:

Definition 12.2. *We have the following examples of block-modified Wishart matrices $\widetilde{W}=(id\otimes\varphi)W$, coming from various linear maps $\varphi:M_n(\mathbb{C})\to M_n(\mathbb{C})$:*

(1) *Wishart matrices: $\widetilde{W}=W$, obtained via $\varphi=id$.*
(2) *Aubrun matrices: $\widetilde{W}=(id\otimes t)W$, with t being the transposition.*
(3) *Collins-Nechita one: $\widetilde{W}=(id\otimes\varphi)W$, with $\varphi=tr(.)1$.*
(4) *Collins-Nechita two: $\widetilde{W}=(id\otimes\varphi)W$, with φ erasing the off-diagonal part.*

These examples, whose construction is something very elementary, appear in a wide context of interesting situations, for the most in connection with various questions in quantum physics [5], [23], [24], [25], [67]. They will actually serve as a main motivation for what we will be doing, in what follows. More on this later.

Getting back now to the general case, that of Definition 12.1 as stated, the linear map $\varphi:M_n(\mathbb{C})\to M_n(\mathbb{C})$ there is certainly useful for understanding the construction of the block-modified Wishart matrix $\widetilde{W}=(id\otimes\varphi)W$, as illustrated by the above examples. In practice, however, we would like to have as block-modification "data" something more concrete, such as a usual matrix. To be more precise, we would like to use:

Proposition 12.3. *We have a correspondence between linear maps*

$$\varphi:M_n(\mathbb{C})\to M_n(\mathbb{C})$$

and square matrices $\Lambda\in M_n(\mathbb{C})\otimes M_n(\mathbb{C})$, given by the formula

$$\Lambda_{ab,cd}=\varphi(e_{ac})_{bd}$$

where $e_{ab}\in M_n(\mathbb{C})$ are the standard generators of the matrix algebra $M_n(\mathbb{C})$, given by the formula $e_{ab}:e_b\to e_a$, with $\{e_1,\ldots,e_n\}$ being the standard basis of $\mathbb{C}^n$.

Proof. This is standard linear algebra. Given a linear map $\varphi:M_n(\mathbb{C})\to M_n(\mathbb{C})$, we can associated to it numbers $\Lambda_{ab,cd}\in\mathbb{C}$ by the formula in the statement, namely:

$$\Lambda_{ab,cd}=\varphi(e_{ac})_{bd}$$

Now by using these n^4 numbers, we can construct a $n^2 \times n^2$ matrix, as follows:

$$\Lambda = \sum_{abcd} \Lambda_{ab,cd} e_{ac} \otimes e_{bd} \in M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$$

Thus, we have constructed a correspondence $\varphi \to \Lambda$, and since this correspondence is injective, and the dimensions match, this correspondence is bijective, as claimed. □

Now by getting back to the block-modified Wishart matrices, we have:

PROPOSITION 12.4. *Given a Wishart $dn \times dn$ matrix $W = YY^*$, and a linear map*

$$\varphi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$$

the entries of the corresponding block-modified matrix $\widetilde{W} = (id \otimes \varphi)W$ are given by

$$\widetilde{W}_{ia,jb} = \sum_{cd} \Lambda_{ca,db} W_{ic,jd}$$

where $\Lambda \in M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ is the square matrix associated to φ, as above.

PROOF. Again, this is trivial linear algebra, coming from the following computation:

$$\widetilde{W}_{ia,jb} = \sum_{cd} W_{ic,jd} \varphi(e_{cd})_{ab} = \sum_{cd} \Lambda_{ca,db} W_{ic,jd}$$

Thus, we are led to the conclusion in the statement. □

At the level of the main examples, from Definition 12.2, the very basic linear maps $\varphi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ used there can only correspond to some basic examples of matrices $\Lambda \in M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$, via the correspondence in Proposition 12.3. This is indeed the case, and in order to clarify this, and at a rather conceptual level, let us formulate:

DEFINITION 12.5. *Let $P(k,l)$ be the set of partitions between an upper row of k points, and a lower row of l points. Associated to any $\pi \in P(k,l)$ is the linear map*

$$T_\pi(e_{i_1} \otimes \ldots \otimes e_{i_k}) = \sum_{j_1 \ldots j_l} \delta_\pi \begin{pmatrix} i_1 & \ldots & i_k \\ j_1 & \ldots & j_l \end{pmatrix} e_{j_1} \otimes \ldots \otimes e_{j_l}$$

between tensor powers of $\mathbb{C}^N$, called "easy", with the Kronecker type symbol on the right being given by $\delta_\pi = 1$ when the indices fit, and $\delta_\pi = 0$ otherwise.

Observe the obvious connection with notion of easy group, the point being that a closed subgroup $G \subset U_N$ is easy precisely when its Tannakian category $C_G = (C_G(k,l))$ with $C_G(k,l) \subset \mathcal{L}((\mathbb{C}^N)^k, (\mathbb{C}^N)^l)$ is spanned by easy maps.

For our purposes, we will need a slight modification of Definition 12.5, as follows:

Definition 12.6. *Associated to any partition $\pi\in P(2s,2s)$ is the linear map*

$$\varphi_\pi(e_{a_1\ldots a_s,c_1\ldots c_s})=\sum_{b_1\ldots b_s}\sum_{d_1\ldots d_s}\delta_\pi\begin{pmatrix}a_1&\ldots&a_s&c_1&\ldots&c_s\\ b_1&\ldots&b_s&d_1&\ldots&d_s\end{pmatrix}e_{b_1\ldots b_s,d_1\ldots d_s}$$

obtained from T_π by contracting all the tensors, via the operation

$$e_{i_1}\otimes\ldots\otimes e_{i_{2s}}\to e_{i_1\ldots i_s,i_{s+1}\ldots i_{2s}}$$

with $\{e_1,\ldots,e_N\}$ standing as usual for the standard basis of $\mathbb C^N$.

In relation with our Wishart matrix considerations, the point is that the above linear map φ_π can be viewed as a "block-modification" map, as follows:

$$\varphi_\pi:M_{N^s}(\mathbb C)\to M_{N^s}(\mathbb C)$$

As an illustration, let us discuss the case $s=1$. There are 15 partitions $\pi\in P(2,2)$, and among them, the most "basic" are the 4 partitions $\pi\in P_{even}(2,2)$. We have:

Theorem 12.7. *The partitions $\pi\in P_{even}(2,2)$ are as follows,*

$$\pi_1=\begin{bmatrix}\circ&\bullet\\ \circ&\bullet\end{bmatrix}\quad,\quad\pi_2=\begin{bmatrix}\circ&\bullet\\ \bullet&\circ\end{bmatrix}\quad,\quad\pi_3=\begin{bmatrix}\circ&\circ\\ \bullet&\bullet\end{bmatrix}\quad,\quad\pi_4=\begin{bmatrix}\circ&\circ\\ \circ&\circ\end{bmatrix}$$

with the associated linear maps $\varphi_\pi:M_n(\mathbb C)\to M_n(\mathbb C)$ being as follows,

$$\varphi_1(A)=A\quad,\quad\varphi_2(A)=A^t\quad,\quad\varphi_3(A)=Tr(A)1\quad,\quad\varphi_4(A)=A^\delta$$

and the associated square matrices $\Lambda_\pi\in M_n(\mathbb C)\otimes M_n(\mathbb C)$ being as follows,

$$\Lambda^1_{ab,cd}=\delta_{ab}\delta_{cd}\quad,\quad\Lambda^2_{ab,cd}=\delta_{ad}\delta_{bc}\quad,\quad\Lambda^3_{ab,cd}=\delta_{ac}\delta_{bd}\quad,\quad\Lambda^4_{ab,cd}=\delta_{abcd}$$

producing the main examples of block-modified Wishart matrices, from Definition 12.2.

Proof. This is something elementary, coming from the formula in Definition 12.6. Indeed, in the case $s=1$, that we are interested in here, this formula becomes:

$$\varphi_\pi(e_{ac})=\sum_{bd}\delta_\pi\begin{pmatrix}a&c\\ b&d\end{pmatrix}e_{bd}$$

Now in the case of the 4 partitions in the statement, such maps are given by:

$$\varphi_1(e_{ac})=e_{ac}\quad,\quad\varphi_2(e_{ac})=e_{ca}\quad,\quad\varphi_3(e_{ac})=\delta_{ac}\sum_b e_{bb}\quad,\quad\varphi_4(e_{ac})=\delta_{ac}e_{aa}$$

Thus, we obtain the formulae in the statement. Regarding now the associated square matrices, appearing via $\Lambda_{ab,cd}=\varphi(e_{ac})_{bd}$, these are given by:

$$\Lambda^1_{ab,cd}=\delta_{ab}\delta_{cd}\quad,\quad\Lambda^2_{ab,cd}=\delta_{ad}\delta_{bc}\quad,\quad\Lambda^3_{ab,cd}=\delta_{ac}\delta_{bd}\quad,\quad\Lambda^4_{ab,cd}=\delta_{abcd}$$

Thus, we are led to the conclusions in the statement. □

As a conclusion so far to what we did in this chapter, we have a nice definition for the block-modified Wishart matrices, and then a fine-tuning of this definition, using easy maps, which in the simplest case, that of the 4 partitions $\pi \in P_{even}(2,2)$, produces the main 4 examples of block-modified Wishart matrices. The idea in what follows will be that of doing the combinatorics, a bit as in chapter 11, as to extend the results there.

12b. Asymptotic moments

Moving ahead now, we would first like to study the distribution of the arbitrary block-modified Wishart matrices $\widetilde{W} = (id \otimes \varphi)W$. We will use as before the moment method. However, things will be more tricky in the present setting, and we will need:

Definition 12.8. *The generalized colored moments of a random matrix*

$$W \in M_N(L^\infty(X))$$

with respect to a colored integer $e = e_1 \ldots e_p$, and a permutation $\sigma \in S_p$, are the numbers

$$M_e^\sigma(W) = \frac{1}{N^{|\sigma|}} E\left(\sum_{i_1,\ldots,i_p} W_{i_1 i_{\sigma(1)}}^{e_1} \ldots W_{i_p i_{\sigma(p)}}^{e_p}\right)$$

where $|\sigma|$ is the number of cycles of σ.

This is something quite technical, in the spirit of the free probability and free cumulant work in [72], that we will need in what follows. In order to understand how these generalized moments work, consider the standard cycle in S_p, namely:

$$\gamma = (1 \to 2 \to \ldots \to p \to 1)$$

If we use this cycle $\gamma \in S_p$ as our permutation $\sigma \in S_p$ in the above definition, the corresponding generalized moment of a random matrix W is then the usual moment:

$$\begin{aligned} M_e^\gamma(W) &= \frac{1}{N} E\left(\sum_{i_1,\ldots,i_p} W_{i_1 i_2}^{e_1} \ldots W_{i_p i_1}^{e_p}\right) \\ &= (E \circ tr)(W^{e_1} \ldots W^{e_p}) \end{aligned}$$

In general, we can decompose the computation of $M_e^\sigma(W)$ over the cycles of σ, and we obtain in this way a certain product of moments of W. See [72].

As a second illustration now, in relation with the usual square matrices, and more specifically with the square matrices $\Lambda \in M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ as in Proposition 12.3, we have the following formula, that we will use many times in what follows:

Proposition 12.9. *Given a usual square matrix, of composed size,*

$$\Lambda\in M_n(\mathbb C)\otimes M_n(\mathbb C)$$

we have the following generalized moment formula,

$$(M_e^\sigma\otimes M_e^\tau)(\Lambda)=\frac{1}{n^{|\sigma|+|\tau|}}\sum_{i_1,\ldots,i_p}\sum_{j_1,\ldots,j_p}\Lambda^{e_1}_{i_1j_1,i_{\sigma(1)}j_{\tau(1)}}\ldots\ldots\Lambda^{e_p}_{i_pj_p,i_{\sigma(p)}j_{\tau(p)}}$$

valid for any two permutations $\sigma,\tau\in S_p$, and any colored integer $e=e_1\ldots e_p$.

Proof. This is something obvious, applying the construction in Definition 12.8 with $N=n^2$, $X=\{.\}$, $W=\Lambda$, and then making a tensor product of the corresponding moments M_e^σ, M_e^τ, regarded as linear functionals on $M_n(\mathbb C)\otimes M_n(\mathbb C)$. $\square$

Consider now the embedding $NC(p)\subset S_p$ obtained by "cycling inside each block". That is, each block $b=\{b_1,\ldots,b_k\}$ with $b_1<\ldots<b_k$ of a given noncrossing partition $\sigma\in NC(p)$ produces by definition the cycle $(b_1\ldots b_k)$ of the corresponding permutation $\sigma\in S_p$. Observe that the one-block partition $\gamma\in NC(p)$ corresponds in this way to the standard cycle $\gamma\in S_p$. Also, the number of blocks $|\sigma|$ of a partition $\sigma\in NC(p)$ corresponds to the number of cycles $|\sigma|$ of the corresponding permutation $\sigma\in S_p$.

With these conventions, we have the following result, from [11], [12], generalizing our various Wishart matrix moment computations, that we did so far in this book:

Theorem 12.10. *The asymptotic moments of a block-modified Wishart matrix*

$$\widetilde{W}=(id\otimes\varphi)W$$

with parameters $d,m,n\in\mathbb N$ as before, are given by the formula

$$\lim_{d\to\infty}M_e\left(\frac{\widetilde{W}}{d}\right)=\sum_{\sigma\in NC(p)}(mn)^{|\sigma|}(M_e^\sigma\otimes M_e^\gamma)(\Lambda)$$

where $\Lambda\in M_n(\mathbb C)\otimes M_n(\mathbb C)$ is the square matrix associated to $\varphi:M_n(\mathbb C)\to M_n(\mathbb C)$.

Proof. We use the formula for the matrix entries of $\widetilde{W}$, directly in terms of the matrix Λ associated to the map φ, from Proposition 12.4, namely:

$$\widetilde{W}_{ia,jb}=\sum_{cd}\Lambda_{ca,db}W_{ic,jd}$$

By conjugating this formula, we obtain the following formula for the entries of the adjoint matrix $\widetilde{W}^*$, that we will need as well, in what follows:

$$\widetilde{W}^*_{ia,jb}=\sum_{cd}\bar{\Lambda}_{db,ca}\bar{W}_{jd,ic}=\sum_{cd}\Lambda^*_{ca,db}W_{ic,jd}$$

Thus, we have the following global formula, valid for any exponent $e \in \{1, *\}$:

$$\widetilde{W}^e_{ia,jb} = \sum_{cd} \Lambda^e_{ca,db} W_{ic,jd}$$

In order to compute the moments of $\widetilde{W}$, observe first that we have:

$$\begin{aligned} tr(\widetilde{W}^{e_1} \ldots \widetilde{W}^{e_p}) &= \frac{1}{dn} \sum_{i_r a_r} \prod_s \widetilde{W}^{e_s}_{i_s a_s, i_{s+1} a_{s+1}} \\ &= \frac{1}{dn} \sum_{i_r a_r c_r d_r} \prod_s \Lambda^{e_s}_{c_s a_s, d_s a_{s+1}} W_{i_s c_s, i_{s+1} d_s} \\ &= \frac{1}{dn} \sum_{i_r a_r c_r d_r j_r b_r} \prod_s \Lambda^{e_s}_{c_s a_s, d_s a_{s+1}} Y_{i_s c_s, j_s b_s} \bar{Y}_{i_{s+1} d_s, j_s b_s} \end{aligned}$$

The average of the general term can be computed by the Wick rule, which gives:

$$E\left(\prod_s Y_{i_s c_s, j_s b_s} \bar{Y}_{i_{s+1} d_s, j_s b_s}\right) = \#\left\{\sigma \in S_p \middle| i_{\sigma(s)} = i_{s+1}, c_{\sigma(s)} = d_s, j_{\sigma(s)} = j_s, b_{\sigma(s)} = b_s\right\}$$

Let us look now at the above sum. The i, j, b indices range over sets having respectively d, d, m elements, and they have to be constant under the action of $\sigma\gamma^{-1}, \sigma, \sigma$. Thus when summing over these i, j, b indices we simply obtain a factor as follows:

$$f = d^{|\sigma\gamma^{-1}|} d^{|\sigma|} m^{|\sigma|}$$

Thus, we obtain the following moment formula:

$$(E \circ tr)(\widetilde{W}^{e_1} \ldots \widetilde{W}^{e_p}) = \frac{1}{dn} \sum_{\sigma \in S_p} d^{|\sigma\gamma^{-1}|} (dm)^{|\sigma|} \sum_{a_r c_r} \prod_s \Lambda^{e_s}_{c_s a_s, c_{\sigma(s)} a_{s+1}}$$

On the other hand, we know from Proposition 12.9 that the generalized moments of the matrix $\Lambda \in M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ are given by the following formula:

$$(M^\sigma_e \otimes M^\tau_e)(\Lambda) = \frac{1}{n^{|\sigma|+|\tau|}} \sum_{i_1 \ldots i_p} \sum_{j_1 \ldots j_p} \Lambda^{e_1}_{i_1 j_1, i_{\sigma(1)} j_{\tau(1)}} \ldots\ldots \Lambda^{e_p}_{i_p j_p, i_{\sigma(p)} j_{\tau(p)}}$$

By combining the above two formulae, we obtain the following moment formula:

$$(E \circ tr)(\widetilde{W}^{e_1} \ldots \widetilde{W}^{e_p}) = \sum_{\sigma \in S_p} d^{|\sigma|+|\sigma\gamma^{-1}|-1} (mn)^{|\sigma|} (M^\sigma_e \otimes M^\gamma_e)(\Lambda)$$

We use now the standard fact, that we know well from before, that for $\sigma \in S_p$ we have an inequality as follows, with equality precisely when $\sigma \in NC(p)$:

$$|\sigma| + |\sigma\gamma^{-1}| \leq p + 1$$

Thus with $d\to\infty$ the sum restricts over the partitions $\sigma\in NC(p)$, and we get:

$$\lim_{d\to\infty}M_e\big(\widetilde{W}\big)=d^p\sum_{\sigma\in NC(p)}(mn)^{|\sigma|}(M_e^\sigma\otimes M_e^\gamma)(\Lambda)$$

Thus, we are led to the conclusion in the statement. □

With the above result in hand, we are left with the question of recovering the asymptotic law of $\widetilde{W}=(id\otimes\varphi)W$, out of the asymptotic moments found there. The question here only involves the matrix $\Lambda\in M_n(\mathbb{C})\otimes M_n(\mathbb{C})$, and to be more precise, given such a matrix, we would like to find the real or complex probability measure, or abstract distribution, having as colored moments the following numbers:

$$M_e=\sum_{\sigma\in NC_p}(mn)^{|\sigma|}(M_e^\sigma\otimes M_e^\gamma)(\Lambda)$$

Although this is basically a linear algebra problem, the underlying linear algebra is of quite difficult type, and this question cannot really be solved, in general. We will see however that this question can be solved for our basic examples, coming from Theorem 12.7, and more generally, for a certain joint generalization of all these examples.

12c. Basic computations

Once again by following [11], [12], let us introduce, as a solution to the questions mentioned above, the following technical notion:

Definition 12.11. *We call a square matrix $\Lambda\in M_n(\mathbb{C})\otimes M_n(\mathbb{C})$ multiplicative when*

$$(M_e^\sigma\otimes M_e^\gamma)(\Lambda)=(M_e^\sigma\otimes M_e^\sigma)(\Lambda)$$

holds for any $p\in\mathbb{N}$, any exponents $e_1,\ldots,e_p\in\{1,*\}$, and any $\sigma\in NC(p)$.

This notion is something quite technical, but we will see many examples in what follows. For instance, the square matrices Λ coming from the basic linear maps φ appearing in Definition 12.2 are all multiplicative. More on this later.

Regarding now the output measure, that we want to compute, this can only appear as some kind of modification of the Marchenko-Pastur law π_t. In order to discuss such modifications, recall from chapter 11 the following key formula:

$$R_{\pi_t}(\xi)=\frac{t}{1-\xi}$$

To be more precise, this is something that we used in chapter 11, when dealing with the block-transposed Wishart matrices. But this suggests formulating:

Definition 12.12. *A measure μ having as R-transform a function of type*

$$R_\mu(\xi) = \sum_{i=1}^s \frac{c_i z_i}{1 - \xi z_i}$$

with $c_i > 0$ and $z_i \in \mathbb{R}$, will be called modified Marchenko-Pastur law.

All this might seem a bit mysterious, but we are into difficult mathematics here, so we will use the above notion as stated, and we will understand later what is behind our computations. By anticipating a bit, however, the situation is as follows:

(1) As a first comment on the above notion, there is an obvious similarity here with the theory of the compound Poisson laws from chapter 3.

(2) The truth is that π_t is the free Poisson law of parameter t, and the modified Marchenko-Pastur laws introduced above are the general compound free Poisson laws.

(3) Also, the mysterious R-transform used above is the Voiculescu R-transform [88], which is the analogue of the log of the Fourier transform in free probability.

More on all this later, in Part IV, when systematically doing free probability. Based on this analogy, however, we can label our modified Marchenko-Pastur laws, in the same way as we labeled in chapter 3 the compound Poisson laws, as follows:

Definition 12.13. *We denote by π_ρ the modified Marchenko-Pastur law satisfying*

$$R_\mu(\xi) = \sum_{i=1}^s \frac{c_i z_i}{1 - \xi z_i}$$

with $c_i > 0$ and $z_i \in \mathbb{R}$, with ρ being the following measure,

$$\rho = \sum_{i=1}^s c_i \delta_{z_i}$$

which is a discrete positive measure in the complex plane, not necessarily of mass 1.

Getting back now to the block-modified Wishart matrices, and to the formula in Theorem 12.10, the above abstract notions, from Definition 12.11 and from Definition 12.12, are exactly what we need for further improving all this. Again by following [11], [12], we have the following result, substantially building on Theorem 12.10:

Theorem 12.14. *Consider a block-modified Wishart matrix*

$$\widetilde{W} = (id \otimes \varphi) W$$

and assume that the matrix $\Lambda \in M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ associated to φ is multiplicative. Then

$$\frac{\widetilde{W}}{d} \sim \pi_{mn\rho}$$

holds, in moments, in the $d \to \infty$ limit, where $\rho = law(\Lambda)$.

PROOF. This is something quite tricky, using all the above:

(1) Our starting point is the asymptotic moment formula found in Theorem 12.10, for an arbitrary block-modified Wishart matrix, namely:

$$\lim_{d\to\infty} M_e\left(\frac{\widetilde{W}}{d}\right) = \sum_{\sigma\in NC_p}(mn)^{|\sigma|}(M_e^\sigma\otimes M_e^\gamma)(\Lambda)$$

(2) Since our modification matrix $\Lambda\in M_n(\mathbb{C})\otimes M_n(\mathbb{C})$ was assumed to be multiplicative, in the sense of Definition 12.11, this formula reads:

$$\lim_{d\to\infty} M_e\left(\frac{\widetilde{W}}{d}\right) = \sum_{\sigma\in NC_p}(mn)^{|\sigma|}(M_e^\sigma\otimes M_e^\sigma)(\Lambda)$$

(3) On the other hand, a bit of calculus and combinatorics show that, in the context of Definition 12.12, given a square matrix $\Lambda\in M_n(\mathbb{C})\otimes M_n(\mathbb{C})$, having distribution $\rho = law(\Lambda)$, the moments of the modified Marchenko-Pastur law $\pi_{mn\rho}$ are given by the following formula, for any choice of the extra parameter $m\in\mathbb{N}$:

$$M_e(\pi_{mn\rho}) = \sum_{\sigma\in NC_p}(mn)^{|\sigma|}(M_\sigma^e\otimes M_\sigma^e)(\Lambda)$$

(4) The point now is that with this latter formula in hand, our previous asymptotic moment formula for the block-modified Wishart matrix $\widetilde{W}$ simply reads:

$$\lim_{d\to\infty} M_e\left(\frac{\widetilde{W}}{d}\right) = M_e(\pi_{mn\rho})$$

Thus we have indeed $\widetilde{W}/d\sim\pi_{mn\rho}$, in the $d\to\infty$ limit, as stated. □

All the above was of course a bit technical, but we will come back later to this, with some further details, once we will have a better understanding of the R-transform, of the free Poisson limit theorem, and of the other things which are hidden in all the above. In any case, welcome to free probability. Or perhaps to theoretical physics. The above theorem was our first free probability one, in this book, and many other to follow.

Let us we work out now some explicit consequences of Theorem 12.14, by using the modified easy linear maps from Definition 12.6. We recall from there that any modified easy linear map φ_π can be viewed as a "block-modification" map, as follows:

$$\varphi_\pi : M_{N^s}(\mathbb{C})\to M_{N^s}(\mathbb{C})$$

In order to verify that the corresponding matrices Λ_π are multiplicative, we will need to check that all the functions $\varphi(\sigma,\tau) = (M_\sigma^e\otimes M_\tau^e)(\Lambda_\pi)$ have the following property:

$$\varphi(\sigma,\gamma) = \varphi(\sigma,\sigma)$$

For this purpose, we can use the following result, coming from [12]:

PROPOSITION 12.15. *The following functions $\varphi : NC(p) \times NC(p) \to \mathbb{R}$ are multiplicative, in the sense that they satisfy the condition $\varphi(\sigma,\gamma) = \varphi(\sigma,\sigma)$:*

(1) $\varphi(\sigma,\tau) = |\sigma\tau^{-1}| - |\tau|$.
(2) $\varphi(\sigma,\tau) = |\sigma\tau| - |\tau|$.
(3) $\varphi(\sigma,\tau) = |\sigma \wedge \tau| - |\tau|$.

PROOF. All this is elementary, and can be proved as follows:

(1) This follows indeed from the following computation:

$$\varphi_1(\sigma,\gamma) = |\sigma\gamma^{-1}| - 1 = p - |\sigma| = \varphi_1(\sigma,\sigma)$$

(2) This follows indeed from the following computation:

$$\varphi_2(\sigma,\gamma) = |\sigma\gamma| - 1 = |\sigma^2| - |\sigma| = \varphi_2(\sigma,\sigma)$$

(3) This follows indeed from the following computation:

$$\varphi_3(\sigma,\gamma) = |\gamma| - |\gamma| = 0 = |\sigma| - |\sigma| = \varphi_3(\sigma,\sigma)$$

Thus, we are led to the conclusions in the statement. □

We can get back now to the easy modification maps, and we have:

PROPOSITION 12.16. *The partitions $\pi \in P_{even}(2,2)$ are as follows,*

$$\pi_1 = \begin{bmatrix} \circ & \bullet \\ \circ & \bullet \end{bmatrix} \quad , \quad \pi_2 = \begin{bmatrix} \circ & \bullet \\ \bullet & \circ \end{bmatrix} \quad , \quad \pi_3 = \begin{bmatrix} \circ & \circ \\ \bullet & \bullet \end{bmatrix} \quad , \quad \pi_4 = \begin{bmatrix} \circ & \circ \\ \circ & \circ \end{bmatrix}$$

with the associated linear maps $\varphi_\pi : M_n(\mathbb{C}) \to M_N(\mathbb{C})$ being as follows:

$$\varphi_1(A) = A \quad , \quad \varphi_2(A) = A^t \quad , \quad \varphi_3(A) = Tr(A)1 \quad , \quad \varphi_4(A) = A^\delta$$

The corresponding matrices Λ_π are all multiplicative, in the sense of Definition 12.11.

PROOF. The first part of the statement is something that we already know, from Theorem 12.7. In order to prove the last assertion, recall from Theorem 12.7 that the associated square matrices, appearing via $\Lambda_{ab,cd} = \varphi(e_{ac})_{bd}$, are given by:

$$\Lambda^1_{ab,cd} = \delta_{ab}\delta_{cd} \quad , \quad \Lambda^2_{ab,cd} = \delta_{ad}\delta_{bc} \quad , \quad \Lambda^3_{ab,cd} = \delta_{ac}\delta_{bd} \quad , \quad \Lambda^4_{ab,cd} = \delta_{abcd}$$

Since these matrices are all self-adjoint, we can assume that all the exponents are 1 in Definition 12.11, and the multiplicativity condition there becomes:

$$(M_\sigma \otimes M_\gamma)(\Lambda) = (M_\sigma \otimes M_\sigma)(\Lambda)$$

In order to check this condition, observe that for the above 4 matrices, we have:

$$(M^\sigma\otimes M^\tau)(\Lambda_1) = \frac{1}{n^{|\sigma|+|\tau|}}\sum_{i_1\ldots i_p}\delta_{i_{\sigma(1)}i_{\tau(1)}}\ldots\delta_{i_{\sigma(p)}i_{\tau(p)}}=n^{|\sigma\tau^{-1}|-|\sigma|-|\tau|}$$

$$(M^\sigma\otimes M^\tau)(\Lambda_2) = \frac{1}{n^{|\sigma|+|\tau|}}\sum_{i_1\ldots i_p}\delta_{i_1 i_{\sigma\tau(1)}}\ldots\delta_{i_p i_{\sigma\tau(p)}}=n^{|\sigma\tau|-|\sigma|-|\tau|}$$

$$(M^\sigma\otimes M^\tau)(\Lambda_3) = \frac{1}{n^{|\sigma|+|\tau|}}\sum_{i_1\ldots i_p}\sum_{j_1\ldots j_p}\delta_{i_1 i_{\sigma(1)}}\delta_{j_1 j_{\tau(1)}}\ldots\delta_{i_p i_{\sigma(p)}}\delta_{j_p j_{\tau(p)}}=1$$

$$(M^\sigma\otimes M^\tau)(\Lambda_4) = \frac{1}{n^{|\sigma|+|\tau|}}\sum_{i_1\ldots i_p}\delta_{i_1 i_{\sigma(1)} i_{\tau(1)}}\ldots\delta_{i_p i_{\sigma(p)} i_{\tau(p)}}=n^{|\sigma\wedge\tau|-|\sigma|-|\tau|}$$

By using now the results in Proposition 12.15, this gives the result. □

Summarizing, the partitions $\pi\in P_{even}(2,2)$ provide us with some concrete input for Theorem 12.14. The point now is that, when using this input, we obtain the main known computations for the block-modified Wishart matrices, from [5], [23], [24], [67]:

Theorem 12.17. *The asymptotic distribution results for the block-modified Wishart matrices coming from the partitions $\pi_1,\pi_2,\pi_3,\pi_4\in P_{even}(2,2)$ are as follows:*

1. *Marchenko-Pastur: $\frac{1}{d}W\sim\pi_t$, where $t=m/n$.*
2. *Aubrun type: $\frac{1}{d}(id\otimes t)W\sim\pi_\nu$, with $\nu=\frac{m(n-1)}{2}\delta_{-1}+\frac{m(n+1)}{2}\delta_1$.*
3. *Collins-Nechita one: $n(id\otimes tr(.)1)W\sim\pi_t$, where $t=mn$.*
4. *Collins-Nechita two: $\frac{1}{d}(id\otimes(.)^\delta)W\sim\pi_m$.*

Proof. All these results follow from Theorem 12.14, with the maps $\varphi_1,\varphi_2,\varphi_3,\varphi_4$ in Proposition 12.16 producing the 4 matrices in the statement, modulo some rescalings, and with the computation of the corresponding distributions being as follows:

(1) Here $\Lambda=\sum_{ac}e_{ac}\otimes e_{ac}$, and so $\Lambda=nP$, where P is the rank one projection on $\sum_a e_a\otimes e_a\in\mathbb{C}^n\otimes\mathbb{C}^n$. Thus we have the following formula, which gives the result:

$$\rho=\frac{n^2-1}{n^2}\delta_0+\frac{1}{n^2}\delta_n$$

(2) Here $\Lambda=\sum_{ac}e_{ac}\otimes e_{ca}$ is the flip operator, $\Lambda(e_c\otimes e_a)=e_a\otimes e_c$. Thus $\rho=\frac{n-1}{2n}\delta_{-1}+\frac{n+1}{2n}\delta_1$, and so we have the following formula, which gives the result:

$$mn\rho=\frac{m(n-1)}{2}\delta_{-1}+\frac{m(n+1)}{2}\delta_1$$

(3) Here $\Lambda=\sum_{ab}e_{aa}\otimes e_{bb}$ is the identity matrix, $\Lambda=1$. Thus in this case we have the following formula, which gives $\pi_{mn\rho}=\pi_{mn}$, and so $n\widetilde{W}\sim\pi_{mn}$, as claimed:

$$\rho=\delta_1$$

(4) Here $\Lambda=\sum_a e_{aa}\otimes e_{aa}$ is the orthogonal projection on $span(e_a\otimes e_a)\subset\mathbb C^n\otimes\mathbb C^n$. Thus we have the following formula, which gives the result:

$$\rho=\frac{n-1}{n}\delta_0+\frac{1}{n}\delta_1$$

Summarizing, we have proved all the assertions in the statement. □

12d. Further results

We develop now some general theory, for the partitions $\pi\in P_{even}(2s,2s)$, with $s\in\mathbb N$. Let us begin with a reformulation of Definition 12.6, in terms of square matrices:

PROPOSITION 12.18. *Given $\pi\in P(2s,2s)$, the square matrix $\Lambda_\pi\in M_n(\mathbb C)\otimes M_n(\mathbb C)$ associated to the linear map $\varphi_\pi:M_n(\mathbb C)\to M_n(\mathbb C)$, with $n=N^s$, is given by:*

$$(\Lambda_\pi)_{a_1\ldots a_s,b_1\ldots b_s,c_1\ldots c_s,d_1\ldots d_s}=\delta_\pi\begin{pmatrix}a_1&\ldots&a_s&c_1&\ldots&c_s\\ b_1&\ldots&b_s&d_1&\ldots&d_s\end{pmatrix}$$

In addition, we have $\Lambda_\pi^*=\Lambda_{\pi^\circ}$, where $\pi\to\pi^\circ$ is the blockwise middle symmetry.

PROOF. The formula for Λ_π follows from the formula of φ_π from Definition 12.6, by using our standard convention $\Lambda_{ab,cd}=\varphi(e_{ac})_{bd}$. Regarding now the second assertion, observe that with $\pi\to\pi^\circ$ being as above, for any multi-indices a,b,c,d we have:

$$\delta_\pi\begin{pmatrix}c_1&\ldots&c_s&a_1&\ldots&a_s\\ d_1&\ldots&d_s&b_1&\ldots&b_s\end{pmatrix}=\delta_{\pi^\circ}\begin{pmatrix}a_1&\ldots&a_s&c_1&\ldots&c_s\\ b_1&\ldots&b_s&d_1&\ldots&d_s\end{pmatrix}$$

Since Λ_π is real, we conclude we have the following formula:

$$(\Lambda_\pi^*)_{ab,cd}=(\Lambda_\pi)_{cd,ab}=(\Lambda_{\pi^\circ})_{ab,cd}$$

This being true for any a,b,c,d, we obtain $\Lambda_\pi^*=\Lambda_{\pi^\circ}$, as claimed. □

In order to compute now the generalized $*$-moments of Λ_π, we first have:

PROPOSITION 12.19. *With $\pi\in P(2s,2s)$ and Λ_π being as above, we have*

$$\begin{aligned}(M_\sigma^e\otimes M_\tau^e)(\Lambda_\pi)\ &=\ \frac{1}{n^{|\sigma|+|\tau|}}\sum_{i_1^1\ldots i_p^s}\sum_{j_1^1\ldots j_p^s}\delta_{\pi^{e_1}}\begin{pmatrix}i_1^1&\ldots&i_1^s&i_{\sigma(1)}^1&\ldots&i_{\sigma(1)}^s\\ j_1^1&\ldots&j_1^s&j_{\tau(1)}^1&\ldots&j_{\tau(1)}^s\end{pmatrix}\\ &\qquad\qquad\vdots\\ &\qquad\qquad\delta_{\pi^{e_p}}\begin{pmatrix}i_p^1&\ldots&i_p^s&i_{\sigma(p)}^1&\ldots&i_{\sigma(p)}^s\\ j_p^1&\ldots&j_p^s&j_{\tau(p)}^1&\ldots&j_{\tau(p)}^s\end{pmatrix}\end{aligned}$$

with the exponents $e_1,\ldots,e_p\in\{1,*\}$ at left corresponding to $e_1,\ldots,e_p\in\{1,\circ\}$ at right.

Proof. In multi-index notation, the general formula for the generalized $*$-moments for a tensor product square matrix $\Lambda \in M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$, with $n = N^s$, is:

$$\begin{aligned}(M_\sigma^e \otimes M_\tau^e)(\Lambda) &= \frac{1}{n^{|\sigma|+|\tau|}} \sum_{i_1^1 \ldots i_p^s} \sum_{j_1^1 \ldots j_p^s} \Lambda^{e_1}_{i_1^1 \ldots i_1^s j_1^1 \ldots j_1^s, i_{\sigma(1)}^1 \ldots i_{\sigma(1)}^s j_{\tau(1)}^1 \ldots j_{\tau(1)}^s} \\ & \qquad\qquad \vdots \\ & \qquad\qquad \Lambda^{e_p}_{i_p^1 \ldots i_p^s j_p^1 \ldots j_p^s, i_{\sigma(p)}^1 \ldots i_{\sigma(p)}^s j_{\tau(p)}^1 \ldots j_{\tau(p)}^s}\end{aligned}$$

By using now the formulae in Proposition 12.3 for the matrix entries of Λ_π, and of its adjoint matrix $\Lambda_\pi^* = \Lambda_{\pi^\circ}$, this gives the formula in the statement. □

As a conclusion, the quantities $(M_\sigma^e \otimes M_\tau^e)(\Lambda_\pi)$ that we are interested in can be theoretically computed in terms of π, but the combinatorics is quite non-trivial. As explained in [**12**], some simplifications appear in the symmetric case, $\pi = \pi^\circ$. Indeed, for such partitions we can use the following decomposition result:

Proposition 12.20. *Each symmetric $\pi \in P_{even}(2s, 2s)$ has a finest symmetric decomposition $\pi = [\pi_1, \ldots, \pi_R]$, with the components π_t being of two types, as follows:*

1. *Symmetric blocks of π. Such a block must have $r + r$ matching upper legs and $v + v$ matching lower legs, with $r + v > 0$.*
2. *Unions $\beta \sqcup \beta^\circ$ of asymmetric blocks of π. Here β must have $r + u$ unmatching upper legs and $v + w$ unmatching lower legs, with $r + u + v + w > 0$.*

Proof. Consider indeed the block decomposition of our partition, $\pi = [\beta_1, \ldots, \beta_T]$. Then $[\beta_1, \ldots, \beta_T] = [\beta_1^\circ, \ldots, \beta_T^\circ]$, so each block $\beta \in \pi$ is either symmetric, $\beta = \beta^\circ$, or is asymmetric, and disjoint from β°, which must be a block of π too. The result follows. □

The idea will be that of decomposing over the components of π. First, we have:

Proposition 12.21. *For the pairing $\eta \in P_{even}(2s, 2s)$ having horizontal strings,*

$$\eta = \begin{bmatrix} a & b & c & \ldots & a & b & c & \ldots \\ \alpha & \beta & \gamma & \ldots & \alpha & \beta & \gamma & \ldots \end{bmatrix}$$

we have $(M_\sigma \otimes M_\tau)(\Lambda_\eta) = 1$, for any $p \in \mathbb{N}$, and any $\sigma, \tau \in NC(p)$.

Proof. As a first observation, the result holds at $s = 1$, due to the computations in the proof of Proposition 12.16. In general, by using Proposition 12.19, we obtain:

$$\begin{aligned}(M_\sigma \otimes M_\tau)(\Lambda_\eta) &= \frac{1}{n^{|\sigma|+|\tau|}} \sum_{i_1^1 \ldots i_p^s} \sum_{j_1^1 \ldots j_p^s} \delta_{i_1^1 i_{\sigma(1)}^1} \ldots \delta_{i_1^s i_{\sigma(1)}^s} \cdot \delta_{j_1^1 j_{\tau(1)}^1} \ldots \delta_{j_1^s j_{\tau(1)}^s} \\ & \qquad\qquad \vdots \\ & \qquad\qquad \delta_{i_p^1 i_{\sigma(p)}^1} \ldots \delta_{i_p^s i_{\sigma(p)}^s} \cdot \delta_{j_p^1 j_{\tau(p)}^1} \ldots \delta_{j_p^s j_{\tau(p)}^s}\end{aligned}$$

By transposing the two $p \times s$ matrices of Kronecker symbols, we obtain:

$$(M_\sigma \otimes M_\tau)(\Lambda_\eta) = \frac{1}{n^{|\sigma|+|\tau|}} \sum_{i_1^1\ldots i_p^1} \sum_{j_1^1\ldots j_p^1} \delta_{i_1^1 i_{\sigma(1)}^1} \ldots \delta_{i_p^1 i_{\sigma(p)}^1} \cdot \delta_{j_1^1 j_{\tau(1)}^1} \ldots \delta_{j_p^1 j_{\tau(p)}^1}$$

$$\vdots$$

$$\sum_{i_1^s\ldots i_p^s} \sum_{j_1^s\ldots j_p^s} \delta_{i_1^s i_{\sigma(1)}^s} \ldots \delta_{i_p^s i_{\sigma(p)}^s} \cdot \delta_{j_1^s j_{\tau(1)}^s} \ldots \delta_{j_p^s j_{\tau(p)}^s}$$

We can now perform all the sums, and we obtain in this way:

$$(M_\sigma \otimes M_\tau)(\Lambda_\eta) = \frac{1}{n^{|\sigma|+|\tau|}} (N^{|\sigma|} N^{|\tau|})^s = 1$$

Thus, the formula in the statement holds indeed. □

We can now perform the decomposition over the components, as follows:

THEOREM 12.22. *Assuming that $\pi \in P_{even}(2s, 2s)$ is symmetric, $\pi = \pi^\circ$, we have*

$$(M_\sigma \otimes M_\tau)(\Lambda_\pi) = \prod_{t=1}^{R} (M_\sigma \otimes M_\tau)(\Lambda_{\pi_t})$$

whenever $\pi = [\pi_1, \ldots, \pi_R]$ is a decomposition into symmetric subpartitions, which each π_t being completed with horizontal strings, coming from the standard pairing η.

PROOF. We use the general formula in Proposition 12.19. In the symmetric case the various e_x exponents dissapear, and we can write the formula there as follows:

$$(M_\sigma \otimes M_\tau)(\Lambda_\pi) = \frac{1}{n^{|\sigma|+|\tau|}} \# \left\{ i, j \middle| \ker \begin{pmatrix} i_x^1 & \ldots & i_x^s & i_{\sigma(x)}^1 & \ldots & i_{\sigma(x)}^s \\ j_x^1 & \ldots & j_x^s & j_{\tau(x)}^1 & \ldots & j_{\tau(x)}^s \end{pmatrix} \leq \pi, \forall x \right\}$$

The point now is that in this formula, the number of double arrays $[ij]$ that we are counting naturally decomposes over the subpartitions π_t. Thus, we have a formula of the following type, with K being a certain normalization constant:

$$(M_\sigma \otimes M_\tau)(\Lambda_\pi) = K \prod_{t=1}^{R} (M_\sigma \otimes M_\tau)(\Lambda_{\pi_t})$$

Regarding now the precise value of K, our claim is that this is given by:

$$K = \frac{n^{(|\sigma|+|\tau|)R}}{n^{|\sigma|+|\tau|}} \cdot \frac{1}{n^{(|\sigma|+|\tau|)(R-1)}} = 1$$

Indeed, the fraction on the left comes from the standard $\frac{1}{n^{|\sigma|+|\tau|}}$ normalizations of all the $(M_\sigma \otimes M_\tau)(\Lambda)$ quantities involved. As for the term on the right, this comes from the contribution of the horizontal strings, which altogether contribute as the strings of the standard pairing $\eta \in P_{even}(2s, 2s)$, counted $R - 1$ times. But, according to Proposition 12.21, the strings of η contribute with a $n^{|\sigma|+|\tau|}$ factor, and this gives the result. □

Summarizing, in the easy case we are led to the study of the partitions $\pi \in P_{even}(2s,2s)$ which are symmetric, and we have so far a decomposition formula for them.

Let us keep building on the material developed above. Our purpose will be that of converting Theorem 12.22 into an explicit formula, that we can use later on. For this, we have to compute the contributions of the components. First, we have:

PROPOSITION 12.23. *For a symmetric partition $\pi \in P_{even}(2s,2s)$, consisting of one symmetric block, completed with horizontal strings, we have*

$$(M_\sigma \otimes M_\tau)(\Lambda_\pi) = N^{|\lambda|-r|\sigma|-v|\tau|}$$

where $\lambda \in P(p)$ is a partition constructed as follows,

$$\lambda = \begin{cases} \sigma \wedge \tau & \text{if } r, v \geq 1 \\ \sigma & \text{if } r \geq 1, v = 0 \\ \tau & \text{if } r = 0, v \geq 1 \end{cases}$$

and where r/v is half of the number of upper/lower legs of the symmetric block.

PROOF. Let us denote by $a_1,\ldots,a_r$ and $b_1,\ldots,b_v$ the upper and lower legs of the symmetric block, appearing at left, and by $A_1,\ldots,A_{s-r}$ and $B_1,\ldots,B_{s-v}$ the remaining legs, appearing at left as well. With this convention, Proposition 12.19 gives:

$$\begin{aligned}(M_\sigma \otimes M_\tau)(\Lambda_\pi) &= \frac{1}{n^{|\sigma|+|\tau|}} \sum_{i_1^1\ldots i_p^s} \sum_{j_1^1\ldots j_p^s} \prod_x \delta_{i_x^{a_1}\ldots i_x^{a_r} i_{\sigma(x)}^{a_1}\ldots i_{\sigma(x)}^{a_r} j_x^{b_1}\ldots j_x^{b_v} j_{\tau(x)}^{b_1}\ldots j_{\tau(x)}^{b_v}} \\ &\qquad \delta_{i_x^{A_1} i_{\sigma(x)}^{A_1}} \cdots\cdots \delta_{i_x^{A_{s-r}} i_{\sigma(x)}^{A_{s-r}}} \\ &\qquad \delta_{j_x^{B_1} j_{\tau(x)}^{B_1}} \cdots\cdots \delta_{j_x^{B_{s-v}} j_{\tau(x)}^{B_{s-v}}}\end{aligned}$$

If we denote by $k_1,\ldots,k_p$ the common values of the indices affected by the long Kronecker symbols, coming from the symmetric block, we have then:

$$\begin{aligned}(M_\sigma \otimes M_\tau)(\Lambda_\pi) &= \frac{1}{n^{|\sigma|+|\tau|}} \sum_{k_1\ldots k_p} \\ &\qquad \sum_{i_1^1\ldots i_p^s} \prod_x \delta_{i_x^{a_1}\ldots i_x^{a_r} i_{\sigma(x)}^{a_1}\ldots i_{\sigma(x)}^{a_r} k_x} \cdot \delta_{i_x^{A_1} i_{\sigma(x)}^{A_1}} \cdots \delta_{i_x^{A_{s-r}} i_{\sigma(x)}^{A_{s-r}}} \\ &\qquad \sum_{j_1^1\ldots j_p^s} \prod_x \delta_{j_x^{b_1}\ldots j_x^{b_v} j_{\tau(x)}^{b_1}\ldots j_{\tau(x)}^{b_v} k_x} \cdot \delta_{j_x^{B_1} j_{\tau(x)}^{B_1}} \cdots \delta_{j_x^{B_{s-v}} j_{\tau(x)}^{B_{s-v}}}\end{aligned}$$

Let us compute now the contributions of the various i,j indices involved. If we regard both i,j as being $p \times s$ arrays of indices, the situation is as follows:

– On the $a_1,\ldots,a_r$ columns of i, the equations are $i_x^{a_e} = i_{\sigma(x)}^{a_e} = k_x$ for any e,x. Thus when $r \neq 0$ we must have $\ker k \leq \sigma$, in order to have solutions, and if this condition is satisfied, the solution is unique. As for the case $r = 0$, here there is no special condition to be satisfied by k, and we have once again a unique solution.

– On the $A_1, \ldots, A_{s-r}$ columns of i, the conditions on the indices are the "trivial" ones, examined in the proof of Proposition 12.21. According to the computation there, the total contribution coming from these indices is $(N^{|\sigma|})^{s-r} = N^{(s-r)|\sigma|}$.

– Regarding now j, the situation is similar, with a unique solution coming from the $b_1, \ldots, b_v$ columns, provided that the condition $\ker k \leq \tau$ is satisfied at $v \neq 0$, and with a total $N^{(s-v)|\tau|}$ contribution coming from the $B_1, \ldots, B_{s-v}$ columns.

As a conclusion, in order to have solutions i, j, we are led to the condition $\ker k \leq \lambda$, where $\lambda \in \{\sigma \wedge \tau, \sigma, \tau\}$ is the partition constructed in the statement. Now by putting everything together, we deduce that we have the following formula:

$$\begin{aligned}(M_\sigma \otimes M_\tau)(\Lambda_\pi) &= \frac{1}{n^{|\sigma|+|\tau|}} \sum_{\ker k \leq \lambda} N^{(s-r)|\sigma|+(s-v)|\tau|} \\ &= N^{-s|\sigma|-s|\tau|} N^{|\lambda|} N^{(s-r)|\sigma|+(s-v)|\tau|} \\ &= N^{|\lambda|-r|\sigma|-v|\tau|}\end{aligned}$$

Thus, we have obtained the formula in the statement, and we are done. □

In the two-block case now, we have a similar result, as follows:

PROPOSITION 12.24. *For a symmetric partition $\pi \in P_{even}(2s, 2s)$, consisting of a symmetric union $\beta \sqcup \beta^\circ$ of two asymmetric blocks, completed with horizontal strings, we have*

$$(M_\sigma \otimes M_\tau)(\Lambda_\pi) = N^{|\lambda|-(r+u)|\sigma|-(v+w)|\tau|}$$

where $r + u$ and $v + w$ represent the number of upper and lower legs of β, and where $\lambda \in P(p)$ is a partition constructed according to the following table,

$ru\backslash vw$	11	10	01	00
11	$\sigma^2 \wedge \sigma\tau \wedge \sigma\tau^{-1}$	$\sigma^2 \wedge \sigma\tau^{-1}$	$\sigma^2 \wedge \sigma\tau$	σ^2
10	$\sigma\tau \wedge \sigma\tau^{-1}$	$\sigma\tau^{-1}$	$\sigma\tau$	$\emptyset$
01	$\tau\sigma \wedge \tau^2$	$\tau\sigma$	$\tau^{-1}\sigma$	$\emptyset$
00	τ^2	$\emptyset$	$\emptyset$	$-$

with the 1/0 indexing symbols standing for the positivity/nullness of the corresponding variables r, u, v, w, and where $\emptyset$ denotes a formal partition, having 0 blocks.

PROOF. Let us denote by $a_1, \ldots, a_r$ and $c_1, \ldots, c_u$ the upper legs of β, by $b_1, \ldots, b_v$ and $d_1, \ldots, d_w$ the lower legs of β, and by $A_1, \ldots, A_{s-r-u}$ and $B_1, \ldots, B_{s-v-w}$ the remaining legs of π, not belonging to $\beta\sqcup\beta^\circ$. The formula in Proposition 12.19 gives:

$$\begin{aligned}(M_\sigma\otimes M_\tau)(\Lambda_\pi) &= \frac{1}{n^{|\sigma|+|\tau|}}\sum_{i_1^1\ldots i_p^s}\sum_{j_1^1\ldots j_p^s}\prod_x\delta_{i_x^{a_1}\ldots i_x^{a_r}i_{\sigma(x)}^{c_1}\ldots i_{\sigma(x)}^{c_u}j_x^{b_1}\ldots j_x^{b_v}j_{\tau(x)}^{d_1}\ldots j_{\tau(x)}^{d_w}}\\
&\qquad\delta_{i_x^{c_1}\ldots i_x^{c_u}i_{\sigma(x)}^{a_1}\ldots i_{\sigma(x)}^{a_r}j_x^{d_1}\ldots j_x^{d_w}j_{\tau(x)}^{b_1}\ldots j_{\tau(x)}^{b_v}}\\
&\qquad\delta_{i_x^{A_1}i_{\sigma(x)}^{A_1}}\ldots\ldots\delta_{i_x^{A_{s-r}}i_{\sigma(x)}^{A_{s-r-u}}}\\
&\qquad\delta_{j_x^{B_1}j_{\tau(x)}^{B_1}}\ldots\ldots\delta_{j_x^{B_{s-v}}j_{\tau(x)}^{B_{s-v-w}}}\end{aligned}$$

We have now two long Kronecker symbols, coming from $\beta\sqcup\beta^\circ$, and if we denote by $k_1,\ldots,k_p$ and $l_1,\ldots,l_p$ the values of the indices affected by them, we obtain:

$$\begin{aligned}(M_\sigma\otimes M_\tau)(\Lambda_\pi) &= \frac{1}{n^{|\sigma|+|\tau|}}\sum_{k_1\ldots k_p}\sum_{l_1\ldots l_p}\\
&\sum_{i_1^1\ldots i_p^s}\prod_x\delta_{i_x^{a_1}\ldots i_x^{a_r}i_{\sigma(x)}^{c_1}\ldots i_{\sigma(x)}^{c_u}k_x}\cdot\delta_{i_x^{c_1}\ldots i_x^{c_u}i_{\sigma(x)}^{a_1}\ldots i_{\sigma(x)}^{a_r}l_x}\cdot\delta_{i_x^{A_1}i_{\sigma(x)}^{A_1}}\ldots\delta_{i_x^{A_{s-r-u}}i_{\sigma(x)}^{A_{s-r-u}}}\\
&\sum_{j_1^1\ldots j_p^s}\prod_x\delta_{j_x^{b_1}\ldots j_x^{b_v}j_{\tau(x)}^{d_1}\ldots j_{\tau(x)}^{d_w}k_x}\cdot\delta_{j_x^{d_1}\ldots j_x^{d_w}j_{\tau(x)}^{b_1}\ldots j_{\tau(x)}^{b_v}l_x}\cdot\delta_{j_x^{B_1}j_{\tau(x)}^{B_1}}\ldots\delta_{j_x^{B_{s-v-w}}j_{\tau(x)}^{B_{s-v-w}}}\end{aligned}$$

Let us compute now the contributions of the various i,j indices. On the $a_1,\ldots,a_r$ and $c_1,\ldots,c_u$ columns of i, regarded as an $p\times s$ array, the equations are as follows:

$$i_x^{a_e}=i_{\sigma(x)}^{c_f}=k_x\quad,\quad i_x^{c_f}=i_{\sigma(x)}^{a_e}=l_x$$

If we denote by i_x the common value of the $i_x^{a_e}$ indices, when e varies, and by I_x the common value of the $i_x^{c_f}$ indices, when f varies, these equations simply become:

$$i_x=I_{\sigma(x)}=k_x\quad,\quad I_x=i_{\sigma(x)}=l_x$$

Thus we have 0 or 1 solutions. To be more precise, depending now on the positivity/nullness of the parameters r,u, we are led to 4 cases, as follows:

Case 11. Here $r,u\geq 1$, and we must have $k_x=l_{\sigma(x)},k_{\sigma(x)}=l_x$.

Case 10. Here $r\geq 1,u=0$, and we must have $k_{\sigma(x)}=l_x$.

Case 01. Here $r=0,u\geq 1$, and we must have $k_x=l_{\sigma(x)}$.

Case 00. Here $r=u=0$, and there is no condition on k,l.

In what regards now the $A_1,\ldots,A_{s-r}$ columns of i, the conditions on the indices are the "trivial" ones, examined in the proof of Proposition 12.21. According to the computation there, the total contribution coming from these indices is:

$$C_i=(N^{|\sigma|})^{s-r}=N^{(s-r)|\sigma|}$$

The study for the j indices is similar, and we will only record here the final conclusions. First, in what regards the $b_1,\ldots,b_v$ and $d_1,\ldots,d_w$ columns of j, the same discussion as above applies, and we have once again 0 or 1 solutions, as follows:

Case 11'. Here $v,w\geq 1$, and we must have $k_x=l_{\tau(x)},k_{\tau(x)}=l_x$.

Case 10'. Here $v\geq 1,w=0$, and we must have $k_{\tau(x)}=l_x$.

Case 01'. Here $v=0,w\geq 1$, and we must have $k_x=l_{\tau(x)}$.

Case 00'. Here $v=w=0$, and there is no condition on k,l.

As for the $B_1,\ldots,B_{s-v-w}$ columns of j, the conditions on the indices here are "trivial", as in Proposition 8.21, and the total contribution coming from these indices is:

$$C_j=(N^{|\tau|})^{s-v-w}=N^{(s-v-w)|\tau|}$$

Let us put now everything together. First, we must merge the conditions on k,l found in the cases 00-11 above with those found in the cases 00'-11'. There are $4\times 4=16$ computations to be performed here, and the "generic" computation, corresponding to the merger of case 11 with the case 11', is as follows:

$$\begin{aligned}
&k_x=l_{\sigma(x)},k_{\sigma(x)}=l_x,k_x=l_{\tau(x)},k_{\tau(x)}=l_x\\
\iff\quad &l_x=k_{\sigma(x)},k_x=l_{\sigma(x)},k_x=l_{\tau(x)},k_x=l_{\tau^{-1}(x)}\\
\iff\quad &l_x=k_{\sigma(x)},k_x=k_{\sigma^2(x)}=k_{\sigma\tau(x)}=k_{\sigma\tau^{-1}(x)}
\end{aligned}$$

Thus in this case l is uniquely determined by k, and k itself must satisfy:

$$\ker k\leq\sigma^2\wedge\sigma\tau\wedge\sigma\tau^{-1}$$

We conclude that the total contribution of the k,l indices in this case is:

$$C_{kl}^{11,11}=N^{|\sigma^2\wedge\sigma\tau\wedge\sigma\tau^{-1}|}$$

In the remaining 15 cases the computations are similar, with some of the above 4 conditions, that we started with, dissapearing. The conclusion is that the total contribution of the k,l indices is as follows, with λ being the partition in the statement:

$$C_{kl}=N^{|\lambda|}$$

With this result in hand, we can now finish our computation, as follows:

$$\begin{aligned}
(M_\sigma\otimes M_\tau)(\Lambda_\pi)&=\frac{1}{n^{|\sigma|+|\tau|}}C_{kl}C_iC_j\\
&=N^{|\lambda|-(r+u)|\sigma|-(v+w)|\tau|}
\end{aligned}$$

Thus, we have obtained the formula in the statement, and we are done. □

As a conclusion now to all this, we have the following result:

THEOREM 12.25. *For a symmetric partition $\pi \in P_{even}(2s,2s)$, having only one component, in the sense of Proposition 12.20, completed with horizontal strings, we have*

$$(M_\sigma \otimes M_\tau)(\Lambda_\pi) = N^{|\lambda|-r|\sigma|-v|\tau|}$$

where $\lambda \in P(p)$ is the partition constructed as in Proposition 12.23 and Proposition 12.24, and where r/v is half of the total number of upper/lower legs of the component.

PROOF. This follows indeed from Proposition 12.23 and Proposition 12.24. □

Generally speaking, the formula that we found in Theorem 12.25 does not lead to the multiplicativity condition from Definition 12.11, and this due to the fact that the various partitions $\lambda \in P_p$ constructed in Proposition 12.24 have in general a quite complicated combinatorics. To be more precise, we first have the following result:

PROPOSITION 12.26. *For a symmetric partition $\pi \in P_{even}(2s,2s)$ we have*

$$(M_\sigma \otimes M_\tau)(\Lambda_\pi) = N^{f_1+f_2}$$

where f_1, f_2 are respectively linear combinations of the following quantities:

(1) $1, |\sigma|, |\tau|, |\sigma\wedge\tau|, |\sigma\tau|, |\sigma\tau^{-1}|, |\tau\sigma|, |\tau^{-1}\sigma|$.
(2) $|\sigma^2|, |\tau^2|, |\sigma^2\wedge\sigma\tau|, |\sigma^2\wedge\sigma\tau^{-1}|, |\tau\sigma\wedge\tau^2|, |\sigma\tau\wedge\sigma\tau^{-1}|, |\sigma^2\wedge\sigma\tau\wedge\sigma\tau^{-1}|$.

PROOF. This follows indeed by combining Theorem 12.22 and Theorem 12.25, with concrete input from Proposition 12.23 and Proposition 12.24. □

In the above result, the partitions in (1) lead to the multiplicativity condition in Definition 12.11, and so to compound free Poisson laws, via Theorem 12.14. However, the partitions in (2) have a more complicated combinatorics, which does not fit with Definition 12.11, nor with the finer multiplicativity notions introduced in [12].

Summarizing, in order to extend the 4 basic computations that we have, we must fine-tune our formalism. A natural answer here comes from the following result:

PROPOSITION 12.27. *For a partition $\pi \in P(2s,2s)$, the following are equivalent:*

(1) *φ_π is unital modulo scalars, i.e. $\varphi_\pi(1) = c1$, with $c \in \mathbb{C}$.*
(2) *$\left[\begin{smallmatrix}\mu\\ \pi\end{smallmatrix}\right] = \mu$, where $\mu \in P(0,2s)$ is the pairing connecting $\{i\} - \{i+s\}$, and where $\left[\begin{smallmatrix}\mu\\ \pi\end{smallmatrix}\right] \in P(0,2s)$ is the partition obtained by putting μ on top of π.*

In addition, these conditions are satisfied for the 4 partitions in $P_{even}(2,2)$.

PROOF. We use the formula of φ_π from Definition 12.6, namely:

$$\varphi_\pi(e_{a_1\ldots a_s,c_1\ldots c_s}) = \sum_{b_1\ldots b_s}\sum_{d_1\ldots d_s}\delta_\pi\begin{pmatrix}a_1 & \ldots & a_s & c_1 & \ldots & c_s\\ b_1 & \ldots & b_s & d_1 & \ldots & d_s\end{pmatrix} e_{b_1\ldots b_s,d_1\ldots d_s}$$

By summing over indices $a_i = c_i$, we obtain the following formula:

$$\varphi_\pi(1) = \sum_{a_1\ldots a_s}\sum_{b_1\ldots b_s}\sum_{d_1\ldots d_s}\delta_\pi\begin{pmatrix}a_1 & \ldots & a_s & a_1 & \ldots & a_s\\ b_1 & \ldots & b_s & d_1 & \ldots & d_s\end{pmatrix} e_{b_1\ldots b_s,d_1\ldots d_s}$$

Let us first find out when $\varphi_\pi(1)$ is diagonal. In order for this condition to hold, the off-diagonal terms of $\varphi_\pi(1)$ must all vanish, and so we must have:

$$b\neq d \implies \delta_\pi\begin{pmatrix}a_1 & \ldots & a_s & a_1 & \ldots & a_s\\ b_1 & \ldots & b_s & d_1 & \ldots & d_s\end{pmatrix} = 0, \forall a$$

Our claim is that for any $\pi\in P(2s,2s)$ we have the following formula:

$$\sup_{a_1\ldots a_s}\delta_\pi\begin{pmatrix}a_1 & \ldots & a_s & a_1 & \ldots & a_s\\ b_1 & \ldots & b_s & d_1 & \ldots & d_s\end{pmatrix} = \delta_{[{}^{\mu}_{\pi}]}\begin{pmatrix}b_1 & \ldots & b_s & d_1 & \ldots & d_s\end{pmatrix}$$

Indeed, each of the terms of the sup on the left are smaller than the quantity on the right, so $\leq$ holds. Also, assuming $\delta_{[{}^{\mu}_{\pi}]}(bd) = 1$, we can take $a_1,\ldots,a_s$ to be the indices appearing on the strings of μ, and we obtain the following formula:

$$\delta_\pi\begin{pmatrix}a & a\\ b & d\end{pmatrix} = 1$$

Thus, we have equality. Now with this equality in hand, we conclude that we have:

$$\begin{aligned}
&\varphi_\pi(1) = \varphi_\pi(1)^\delta\\
\iff\ &\delta_{[{}^{\mu}_{\pi}]}\begin{pmatrix}b_1 & \ldots & b_s & d_1 & \ldots & d_s\end{pmatrix} = 0, \forall b\neq d\\
\iff\ &\delta_{[{}^{\mu}_{\pi}]}\begin{pmatrix}b_1 & \ldots & b_s & d_1 & \ldots & d_s\end{pmatrix} \leq \delta_\mu\begin{pmatrix}b_1 & \ldots & b_s & d_1 & \ldots & d_s\end{pmatrix}, \forall b,d\\
\iff\ &\begin{bmatrix}\mu\\ \pi\end{bmatrix}\leq\mu
\end{aligned}$$

Let us investigate now when (1) holds. We already know that π must satisfy $[{}^{\mu}_{\pi}]\leq\mu$, and the remaining conditions, concerning the diagonal terms, are as follows:

$$\sum_{a_1\ldots a_s}\delta_\pi\begin{pmatrix}a_1 & \ldots & a_s & a_1 & \ldots & a_s\\ b_1 & \ldots & b_s & b_1 & \ldots & b_s\end{pmatrix} = c, \forall b$$

As a first observation, the quantity on the left is a decreasing function of $\lambda = \ker b$. Now in order for this decreasing function to be constant, we must have:

$$\sum_{a_1\ldots a_s}\delta_\pi\begin{pmatrix}a_1 & \ldots & a_s & a_1 & \ldots & a_s\\ 1 & \ldots & s & 1 & \ldots & s\end{pmatrix} = \sum_{a_1\ldots a_s}\delta_\pi\begin{pmatrix}a_1 & \ldots & a_s & a_1 & \ldots & a_s\\ 1 & \ldots & 1 & 1 & \ldots & 1\end{pmatrix}$$

We conclude that the condition $[{}^{\mu}_{\pi}]\leq\mu$ must be strengthened into $[{}^{\mu}_{\pi}]=\mu$, as claimed. Finally, the last assertion is clear, by using either (1) or (2). □

In the symmetric case, $\pi=\pi^\circ$, we have the following result:

Proposition 12.28. *Given a partition $\pi\in P(2s,2s)$ which is symmetric, φ_π is unital modulo scalars precisely when its symmetric components are as follows,*

1. *Symmetric blocks with $v\leq 1$,*
2. *Unions of asymmetric blocks with $r+u=0,v+w=1$,*
3. *Unions of asymmetric blocks with $r+u\geq 1,v+w\leq 1$,*

with the conventions from Proposition 12.20 for the values of r,u,v,w.

Proof. This follows from what we have, the idea being as follows:

– We know from Proposition 12.27 that the condition in the statement is equivalent to $\left[\begin{smallmatrix}\mu\\ \pi\end{smallmatrix}\right]=\mu$, and we can see from this that π satisfies the condition if and only if all the symmetric components of π satisfy the condition. Thus, we must simply check the validity of $\left[\begin{smallmatrix}\mu\\ \pi\end{smallmatrix}\right]=\mu$ for the partitions in Proposition 12.20, and this gives the result.

– To be more precise, for the 1-block components the study is trivial, and we are led to (1). Regarding the 2-block components, in the case $r+u=0$ we must have $v+w=1$, as stated in (2). Finally, assuming $r+u\geq 1$, when constructing $\left[\begin{smallmatrix}\mu\\ \pi\end{smallmatrix}\right]$ all the legs on the bottom will become connected, and so we must have $v+w\leq 1$, as stated in (3). □

Summarizing, the condition that φ_π is unital modulo scalars is a natural generalization of what happens for the 4 basic partitions in $P_{even}(2,2)$, and in the symmetric case, we have a good understanding of such partitions. However, the associated matrices Λ_π still fail to be multiplicative, and we must come up with a second condition, coming from:

Theorem 12.29. *If $\pi\in P(2s,2s)$ is symmetric, the following are equivalent:*

1. *The linear maps $\varphi_\pi,\varphi_{\pi^*}$ are both unital modulo scalars.*
2. *The symmetric components have ≤ 2 upper legs, and ≤ 2 lower legs.*
3. *The symmetric components appear as copies of the 4 elements of $P_{even}(2,2)$.*

Proof. By applying the results in Proposition 12.28 to the partitions π,π^*, and by merging these results, we conclude that the equivalence (1) $\iff$ (2) holds indeed. As for the equivalence (2) $\iff$ (3), this is clear from definitions. □

Let us put now everything together. The idea will be that of using the partitions found in Theorem 12.29 as an input for Proposition 12.26, and then for the general block-modification machinery developed in the beginning of this chapter. We will need:

Proposition 12.30. *The following functions $\varphi:NC(p)\times NC(p)\to\mathbb R$ are multiplicative, in the sense that they satisfy the condition $\varphi(\sigma,\gamma)=\varphi(\sigma,\sigma)$:*

1. $\varphi(\sigma,\tau)=|\tau\sigma|-|\tau|$.
2. $\varphi(\sigma,\tau)=|\tau^{-1}\sigma|-|\tau|$.

Proof. This follows from some standard combinatorics, the idea being as follows:

(1) We can use here the well-known fact, explained in chapter 11, that the numbers $|\gamma\sigma|-1$ and $|\sigma^2|-|\sigma|$ are equal, both counting the number of blocks of σ having even size. Thus we have the following computation, which gives the result:

$$\varphi_1(\sigma,\gamma)=|\gamma\sigma|-1=|\sigma^2|-|\sigma|=\varphi_1(\sigma,\sigma)$$

(2) Here we can use the well-known formula $|\sigma\gamma^{-1}|-1=p-|\sigma|$, and the fact that $\sigma\gamma^{-1},\gamma^{-1}\sigma$ have the same cycle structure as the left and right Kreweras complements of σ, and so have the same number of blocks. Thus we have the following computation:

$$\varphi_2(\sigma,\gamma)=|\gamma^{-1}\sigma|-1=p-|\sigma|=\varphi_2(\sigma,\sigma)$$

But this gives the second formula in the statement, and we are done. □

We can now formulate our main multiplicativity result, as follows:

PROPOSITION 12.31. *Assuming that $\pi\in P_{even}(2s,2s)$ is symmetric, $\pi=\pi^\circ$, and is such that $\varphi_\pi,\varphi_{\pi^*}$ are unital modulo scalars, we have a formula of the following type:*

$$(M_\sigma\otimes M_\tau)(\Lambda_\pi)=N^{a+b|\sigma|+c|\tau|+d|\sigma\wedge\tau|+e|\sigma\tau|+f|\sigma\tau^{-1}|+g|\tau\sigma|+h|\tau^{-1}\sigma|}$$

Moreover, the square matrix Λ_π is multiplicative, in the sense of Definition 12.11.

PROOF. The first assertion follows from Proposition 12.26. Indeed, according to the various results in Theorem 12.29, the list of partitions appearing in Proposition 12.26 (2) dissapears in the case where both $\varphi_\pi,\varphi_{\pi^*}$ are unital modulo scalars, and this gives the result. As for the second assertion, this follows from the formula in the statement, and from the various results in Proposition 12.15 and Proposition 12.30. □

As a main consequence, Theorem 12.14 applies, and gives:

THEOREM 12.32. *Given a partition $\pi\in P_{even}(2s,2s)$ which is symmetric, $\pi=\pi^\circ$, and which is such that $\varphi_\pi,\varphi_{\pi^*}$ are unital modulo scalars, for the corresponding block-modified Wishart matrix $\widetilde{W}=(id\otimes\varphi_\pi)W$ we have the asymptotic convergence formula*

$$m\widetilde{W}\sim\pi_{mn\rho}$$

in $*$-moments, in the $d\to\infty$ limit, where $\rho=law(\Lambda_\pi)$.

PROOF. This follows by putting together the results that we have. Indeed, due to Proposition 12.31, Theorem 12.14 applies, and gives the convergence result. □

Summarizing, we have now an explicit block-modification machinery, valid for certain suitable partitions $\pi\in P_{even}(2s,2s)$, which improves the previous theory from [**12**].

As a conclusion to all this, the block modification of the complex Wishart matrices leads, somehow out of nothing, to a whole new world, populated by beasts such as the R-transform, the modified Marchenko-Pastur laws, and many more. Looks like we have opened the Pandora box. We will see however later, in Part IV, that this whole new world, called free probability, is in fact not that much different from ours.

12e. Exercises

Exercises:

Exercise 12.33.

Exercise 12.34.

Exercise 12.35.

Exercise 12.36.

Exercise 12.37.

Exercise 12.38.

Exercise 12.39.

Exercise 12.40.

Bonus exercise.

Part IV

Operator laws

CHAPTER 13

Operator laws

13a.

13b.

13c.

13d.

13e. Exercises

Exercises:

EXERCISE 13.1.

EXERCISE 13.2.

EXERCISE 13.3.

EXERCISE 13.4.

EXERCISE 13.5.

EXERCISE 13.6.

EXERCISE 13.7.

EXERCISE 13.8.

Bonus exercise.

CHAPTER 14

Free probability

14a.

14b.

14c.

14d.

14e. Exercises

Exercises:

Exercise 14.1.

Exercise 14.2.

Exercise 14.3.

Exercise 14.4.

Exercise 14.5.

Exercise 14.6.

Exercise 14.7.

Exercise 14.8.

Bonus exercise.

CHAPTER 15

Geometric aspects

15a.

15b.

15c.

15d.

15e. Exercises

Exercises:

Exercise 15.1.

Exercise 15.2.

Exercise 15.3.

Exercise 15.4.

Exercise 15.5.

Exercise 15.6.

Exercise 15.7.

Exercise 15.8.

Bonus exercise.

CHAPTER 16

Quantum graphs

16a.

16b.

16c.

16d.

16e. Exercises

Congratulations for having read this book, and no exercises for this final chapter.

Bibliography

[1] G.W. Anderson and B. Farrell, Asymptotically liberating sequences of random unitary matrices, *Adv. Math.* **255** (2014), 381–413.

[2] G.W. Anderson, A. Guionnet and O. Zeitouni, An introduction to random matrices, Cambridge Univ. Press (2010).

[3] M. Anshelevich, Free Meixner states, *Comm. Math. Phys.* **276** (2007), 863–899.

[4] O. Arizmendi, I. Nechita and C. Vargas, On the asymptotic distribution of block-modified random matrices, *J. Math. Phys.* **57** (2016), 1–27.

[5] G. Aubrun, Partial transposition of random states and non-centered semicircular distributions, *Random Matrices Theory Appl.* **1** (2012), 125–145.

[6] V.I. Arnold, Mathematical methods of classical mechanics, Springer (1974).

[7] M.F. Atiyah, The geometry and physics of knots, Cambridge Univ. Press (1990).

[8] T. Banica, Calculus and applications (2026).

[9] T. Banica, Linear algebra and group theory (2026).

[10] T. Banica, Principles of operator algebras (2024).

[11] T. Banica and I. Nechita, Asymptotic eigenvalue distributions of block-transposed Wishart matrices, *J. Theoret. Probab.* **26** (2013), 855–869.

[12] T. Banica and I. Nechita, Block-modified Wishart matrices and free Poisson laws, *Houston J. Math.* **41** (2015), 113–134.

[13] R.J. Baxter, Exactly solved models in statistical mechanics, Academic Press (1982).

[14] S.T. Belinschi and H. Bercovici, Partially defined semigroups relative to multiplicative free convolution, *Int. Math. Res. Not.* **2** (2005), 65–101.

[15] S.T. Belinschi, M. Bożejko, F. Lehner and R. Speicher, The normal distribution is $\boxplus$-infinitely divisible, *Adv. Math.* **226** (2011), 3677–3698.

[16] H. Bercovici and V. Pata, Stable laws and domains of attraction in free probability theory, *Ann. of Math.* **149** (1999), 1023–1060.

[17] H. Bercovici and D.V. Voiculescu, Free convolutions of measures with unbounded support, *Indiana Univ. Math. J.* **42** (1993), 733–773.

[18] I. Bengtsson and K. Życzkowski, Geometry of quantum states, Cambridge Univ. Press (2006).

[19] N. Berline, E. Getzler and M. Vergne, Heat kernels and Dirac operators, Springer (2004).

[20] A. Bose, Random matrices and non-commutative probability, CRC Press (2021).

[21] B. Collins, Moments and cumulants of polynomial random variables on unitary groups, the Itzykson-Zuber integral, and free probability, *Int. Math. Res. Not.* **17** (2003), 953–982.

[22] B. Collins and S. Matsumoto, On some properties of orthogonal Weingarten functions, *J. Math. Phys.* **50** (2009), 1–18.

[23] B. Collins and I. Nechita, Random quantum channels I: graphical calculus and the Bell state phenomenon, *Comm. Math. Phys.* **297** (2010), 345–370.

[24] B. Collins and I. Nechita, Random quantum channels II: entanglement of random subspaces, Rényi entropy estimates and additivity problems, *Adv. Math.* **226** (2011), 1181–1201.

[25] B. Collins and I. Nechita, Gaussianization and eigenvalue statistics for random quantum channels (III), *Ann. Appl. Probab.* **21** (2011), 1136–1179.

[26] B. Collins and P. Śniady, Integration with respect to the Haar measure on unitary, orthogonal and symplectic groups, *Comm. Math. Phys.* **264** (2006), 773–795.

[27] A. Connes, Noncommutative geometry, Academic Press (1994).

[28] S. Curran, Quantum rotatability, *Trans. Amer. Math. Soc.* **362** (2010), 4831–4851.

[29] S. Curran and R. Speicher, Quantum invariant families of matrices in free probability, *J. Funct. Anal.* **261** (2011), 897–933.

[30] P. Di Francesco, Meander determinants, *Comm. Math. Phys.* **191** (1998), 543–583.

[31] P.A.M. Dirac, Principles of quantum mechanics, Oxford Univ. Press (1930).

[32] R. Durrett, Probability: theory and examples, Cambridge Univ. Press (1990).

[33] A. Einstein, Relativity: the special and the general theory, Dover (1916).

[34] L.C. Evans, Partial differential equations, AMS (1998).

[35] W. Feller, An introduction to probability theory and its applications, Wiley (1950).

[36] E. Fermi, Thermodynamics, Dover (1937).

[37] M. Février and A. Nica, Infinitesimal non-crossing cumulants and free probability of type B, *J. Funct. Anal.* **258** (2010), 2983–3023.

[38] R.P. Feynman, R.B. Leighton and M. Sands, The Feynman lectures on physics, Caltech (1963).

[39] P. Flajolet and R. Sedgewick, Analytic combinatorics, Cambridge Univ. Press (2009).

[40] M. Fukuda and P. Śniady, Partial transpose of random quantum states: exact formulas and meanders, *J. Math. Phys.* **54** (2013), 1–31.

[41] C. Godsil and G. Royle, Algebraic graph theory, Springer (2001).

[42] D.J. Griffiths, Introduction to electrodynamics, Cambridge Univ. Press (2017).

[43] D.J. Griffiths and D.F. Schroeter, Introduction to quantum mechanics, Cambridge Univ. Press (2018).

[44] D.J. Griffiths, Introduction to elementary particles, Wiley (2020).

[45] A. Guionnet, M. Krishnapur and O. Zeitouni, The single ring theorem, *Ann. of Math.* **174** (2011), 1189–1217.

[46] J. Harris, Algebraic geometry, Springer (1992).

[47] R. Hartshorne, Algebraic geometry, Springer (1977).

[48] F. Hiai and D. Petz, The semicircle law, free random variables and entropy, AMS (2000).

[49] H. Hofer and E. Zehnder, Symplectic invariants and Hamiltonian dynamics, Birkhäuser (1994).

[50] L. Hörmander, The analysis of linear partial differential operators, Springer (1983).

[51] R.A. Horn and C.R. Johnson, Matrix analysis, Cambridge Univ. Press (1985).

[52] K. Huang, Introduction to statistical physics, CRC Press (2001).

[53] J.E. Humphreys, Introduction to Lie algebras and representation theory, Springer (1972).

[54] V.F.R. Jones, Subfactors and knots, AMS (1991).

[55] L.P. Kadanoff, Statistical physics: statics, dynamics and renormalization, World Scientific (2000).

[56] T. Kibble and F.H. Berkshire, Classical mechanics, Imperial College Press (1966).

[57] C. Köstler, R. Speicher, A noncommutative de Finetti theorem: invariance under quantum permutations is equivalent to freeness with amalgamation, *Comm. Math. Phys.* **291** (2009), 473–490.

[58] M. Kumar, Quantum: Einstein, Bohr, and the great debate about the nature of reality, Norton (2009).

[59] T. Lancaster and K.M. Blundell, Quantum field theory for the gifted amateur, Oxford Univ. Press (2014).

[60] L.D. Landau and E.M. Lifshitz, Mechanics, Pergamon Press (1960).

[61] L.D. Landau and E.M. Lifshitz, The classical theory of fields, Addison-Wesley (1951).

[62] L.D. Landau and E.M. Lifshitz, Quantum mechanics: non-relativistic theory, Pergamon Press (1959).

[63] S. Lang, Algebra, Addison-Wesley (1993).

[64] P. Lax, Linear algebra and its applications, Wiley (2007).

[65] P. Lax, Functional analysis, Wiley (2002).

[66] W. Liu, General de Finetti type theorems in noncommutative probability, *Comm. Math. Phys.* **369** (2019), 837–866.

[67] V.A. Marchenko and L.A. Pastur, Distribution of eigenvalues in certain sets of random matrices, *Mat. Sb.* **72** (1967), 507–536.

[68] M.L. Mehta, Random matrices, Elsevier (2004).

[69] J.A. Mingo and A. Nica, Annular noncrossing permutations and partitions, and second-order asymptotics for random matrices, *Int. Math. Res. Not.* **28** (2004), 1413–1460.

[70] J.A. Mingo and M. Popa, Freeness and the transposes of unitarily invariant random matrices, *J. Funct. Anal.* **271** (2016), 883–921.

[71] J.A. Mingo and R. Speicher, Free probability and random matrices, Springer (2017).

[72] A. Nica and R. Speicher, Lectures on the combinatorics of free probability, Cambridge Univ. Press (2006).

[73] M.A. Nielsen and I.L. Chuang, Quantum computation and quantum information, Cambridge Univ. Press (2000).

[74] R.K. Pathria and and P.D. Beale, Statistical mechanics, Elsevier (1972).

[75] A. Peres, Quantum theory: concepts and methods, Kluwer (1993).

[76] P. Petersen, Linear algebra, Springer (2012).

[77] W. Rudin, Principles of mathematical analysis, McGraw-Hill (1964).

[78] W. Rudin, Real and complex analysis, McGraw-Hill (1966).

[79] W. Rudin, Functional analysis, McGraw-Hill (1973).

[80] W. Rudin, Fourier analysis on groups, Dover (1974).

[81] B. Ryden, Introduction to cosmology, Cambridge Univ. Press (2002).

[82] D.V. Schroeder, An introduction to thermal physics, Oxford Univ. Press (1999).

[83] I.R. Shafarevich, Basic algebraic geometry, Springer (1974).

[84] R. Shankar, Fundamentals of physics, Yale Univ. Press (2014).

[85] R. Speicher, Multiplicative functions on the lattice of noncrossing partitions and free convolution, *Math. Ann.* **298** (1994), 611–628.

[86] R. Speicher, Combinatorial theory of the free product with amalgamation and operator-valued free probability theory, *Mem. Amer. Math. Soc.* **132** (1998).

[87] D.V. Voiculescu, Addition of certain noncommuting random variables, *J. Funct. Anal.* **66** (1986), 323–346.

[88] D.V. Voiculescu, Multiplication of certain noncommuting random variables, *J. Operator Theory* **18** (1987), 223–235.

[89] D.V. Voiculescu, Limit laws for random matrices and free products, *Invent. Math.* **104** (1991), 201–220.

[90] D.V. Voiculescu, K.J. Dykema and A. Nica, Free random variables, AMS (1992).

[91] J. von Neumann, Mathematical foundations of quantum mechanics, Princeton Univ. Press (1955).

[92] J. von Neumann and O. Morgenstern, Theory of games and economic behavior, Princeton Univ. Press (1944).

[93] J. Watrous, The theory of quantum information, Cambridge Univ. Press (2018).

[94] S. Weinberg, Foundations of modern physics, Cambridge Univ. Press (2011).

[95] S. Weinberg, Lectures on quantum mechanics, Cambridge Univ. Press (2012).

[96] D. Weingarten, Asymptotic behavior of group integrals in the limit of infinite rank, *J. Math. Phys.* **19** (1978), 999–1001.

[97] H. Weyl, The theory of groups and quantum mechanics, Princeton Univ. Press (1931).

[98] H. Weyl, The classical groups: their invariants and representations, Princeton Univ. Press (1939).

[99] H. Weyl, Space, time, matter, Princeton Univ. Press (1918).

[100] E. Wigner, Characteristic vectors of bordered matrices with infinite dimensions, *Ann. of Math.* **62** (1955), 548–564.