Matemàtica Discreta

Xavier Povill Clarós

10 de juny de 2020

Índex

1 Enumeració bàsica

1.1 Cardinals

Comentari. En aquest curs considerarem que el naturals no inclouen el 0, a no ser que s'indiqui el contrari.

Notació. Utilitzarem el símbol $[n]$ per representar el conjunt $\{1, \ldots, n\}$.

Definició 1.1.1. Dos conjunts A, B tenen el mateix cardinal si existeix una bijecció entre ells $f : A \longrightarrow B$. En particular, si un conjunt té el mateix cardinal que els naturals, direm que és numerable, i si un conjunt A té el mateix cardinal que $[n]$, aleshores direm que $|A| = n$.

Comentari. Per convenció, el conjunt buit té cardinal zero: $|\emptyset| = 0$.

Proposició 1.1.1.

- *Si* $A \cap B = \emptyset$, *aleshores* $|A \cup B| = |A| + |B|$
- $|A \times B| = |A| \cdot |B|$

1.2 Aplicacions i paraules

Siguin A i B conjunts finits, ens interessa comptar el nombre d'aplicacions que van de A a B. Siguin $n = |A|$ i $m = |B|$. Per cada element de A, hi ha m elements de B als quals pot anar, de manera que el nombre total d'aplicacions és m^n.

El nombre d'aplicacions injectives el podem calcular de manera similar. Pel primer element de A, hi ha m imatges possibles, pel següent, $m - 1$ i així successivament. Per tant, el nombre d'aplicacions injectives de A a B és $m \cdot (m-1) \ldots (m-(n-1))$, que denotarem per $(m)_n$.

Observació. Observem que $(m)_n = \frac{m!}{(m-n)!}$, i que $(n)_n = n!$.

Observació. Siguin A i B conjunts finits, si $|A| \neq |B|$, aleshores no hi haurà cap aplicació bijectiva entre els dos, mentre que si $|A| = |B|$, aleshores una aplicació serà bijectiva si i només si és injectiva.

Proposició 1.2.1. *El nombre de permutacions d'un conjunt de n elements és de $n!$.*

Demostració. Les permutacions són bijeccions d'un conjunt a ell mateix. Per tant, el nombre de permutacions és el nombre de bijeccions entre dos conjunts d'igual cardinal, és a dir, $n!$. □

Definició 1.2.1. Una paraula de llargada k sobre un alfabet A de n símbols és una seqüència $x_1x_2\dots x_k$, amb $x_i \in A$.

Proposició 1.2.2. *El nombre de paraules de llargada k sobre un alfabet A de mida n és n^k.*

Demostració. Una paraula pot ser vista com una aplicació $[k] \longrightarrow A$. Per tant, el nombre de paraules és el nombre d'aplicacions d'aquest tipus, que és n^k. □

Similarment, observem que una paraula sense símbols repetits es correspon a una aplicació injectiva, de manera que el nombre de paraules de llargada k sense símbols repetits és $(n)_k$.

1.3 Subconjunts i coeficients binomials

Proposició 1.3.1. *El nombre de subconjunts de mida k d'un conjunt de mida n és el nombre binomial*

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

Demostració. Per cada subconjunt de mida k tenim $k!$ aplicacions injectives de $[k]$ a $[n]$ (no ens importa l'ordre de les imatges). Per tant, el nombre de subconjunts de mida k és $(n)_k/k!$, que equival a l'expressió de l'enunciat de la proposició. □

Algunes propietats bàsiques dels nombres binomials són

Proposició 1.3.2.

- $\binom{n}{n} = 1$
- $\binom{n}{k} = \binom{n}{n-k}$
- *Per $n \geq k \geq 1$, tenim que* $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

Demostració. Els dos primers resultats es demostren fàcilment operant. El tercer és més fàcil provar-lo de forma combinatòria. Els subconjunts de mida k de n elements es poden dividir en els que contenen el 1 i els que no el contenen. Eliminant el 1, veiem que el primer grup correspon als subconjunts de mida $k-1$ d'un conjunt de mida $n-1$, mentre que el segon correspon als subconjunts de mida k d'un conjunt de mida $n-1$. □

Proposició 1.3.3. *En un anell commutatiu, per a cada dos elements a i b i un natural n, es compleix que*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{k} a^i b^{n-i}$$

Demostració. El coeficient de $a^i b^{n-i}$ és el nombre de maneres de triar i a's en el producte $\underbrace{(a+b)\cdot(a+b)\ldots(a+b)}_{\#n}$, és a dir, $\binom{n}{k}$. □

A partir de la fórmula del binomi de Newton podem demostrar els resultats següents:

Proposició 1.3.4.

$$\sum_{k=0}^{n} = \binom{n}{k} = 2^k$$

Demostració.

$$(1+1)^n = \sum_{k=0}^{n} \binom{n}{k} \implies \sum_{k=0}^{n} \binom{n}{k} = 2^n$$

□

Proposició 1.3.5.

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

Demostració.

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

□

Proposició 1.3.6.

$$\binom{n}{n} + \binom{n+1}{n} + \cdots + \binom{n+m}{n} = \binom{n+m+1}{n+1}$$

Demostració. Ho demostrarem per inducció. Si $m = 0$, la identitat equival a $1 = 1$. Sigui $m > 0$, i suposem que ho hem demostrat per $m - 1$, aleshores,

$$\binom{n}{n} + \cdots + \binom{n+m-1}{n} + \binom{n+m}{n} = \binom{n+m}{n+1} + \binom{n+m}{n} = \binom{n+m+1}{n+1}$$

□

Proposició 1.3.7 (Identitat de Vandermonde)**.**

$$\binom{n+m}{n} = \sum_{k=0}^{n} \binom{n}{k}\binom{m}{n-k}$$

Demostració. Suposem que tenim un conjunt de mida n i un conjunt de mida m. El nombre de maneres de triar n elements de la unió d'aquests dos és el nombre de maneres de triar k del primer i $n - k$ del segon, per qualsevol k des de 0 a n. □

Comentari. En la proposició anterior i a partir d'ara suposarem que $\binom{n}{k} := 0$ si $k > n$. Aquesta definició és coherent amb la caracterització que hem donat de nombre binomial, ja que un subconjunt no pot tenir cardinal superior al conjunt original.

1.4 Multiconjunts i coeficients multinomials

Definició 1.4.1 (Multiconjunt)**.** Un multiconjunt de $[n]$ és una aplicació $\mu : [n] \longrightarrow \mathbb{N}$ que assigna a cada element de $[n]$ la seva multiplicitat en el multiconjunt (i.e., el nombre de vegades que apareix).

Exemple 1.4.1. Per exemple, el multiconjunt $\{1, 1, 1, 2, 4, 4, 4\}$ de $[4]$ està caracteritzat per la funció μ amb valors $\mu(1) = 3$, $\mu(2) = 1$, $\mu(3) = 0$ i $\mu(4) = 3$. Observem que μ no depèn de l'ordre dels elements, de manera que l'ordre dels elements d'un multiconjunt és arbitrari.

Comentari. També s'utilitza la notació $\{1^3, 2, 4^3\}$ per referir-se al multiconjunt de l'exemple anterior, tot i que s'ha d'anar amb compte de que no es confongui aquesta notació amb la notació de l'exponenciació.

Proposició 1.4.1. *El nombre de multiconjunts de* $[n]$ *amb* k *elements és* $\binom{n+k-1}{k}$

Demostració. Establirem una bijecció entre el conjunt de μ's possibles i les paraules binàries de longitud $n + k - 1$ amb $n - 1$ 1's. A cada μ li associem la paraula binària

$$\underbrace{0\ldots0}_{\mu(1)}1\underbrace{0\ldots0}_{\mu(2)}1\ldots1\underbrace{0\ldots0}_{\mu(n)}$$

que observem que té $n-1$ 1's i $n-1+\sum \mu(i) = n-1+k$ caràcters. Similarment, a partir d'una paraula binària de $n + k - 1$ caràcters i $n - 1$ 1's, li associem la funció μ corresponent. Aquesta aplicació és una bijecció, ja que es comprova fàcilment que és exhaustiva i injectiva. Per tant, el

nombre de multiconjunts de $[n]$ de mida k és el nombre de paraules binàries de llargada $n+k-1$ i $n-1$ 1's, que es correspon amb el nombre de maneres de triar $n-1$ posicions d'entre $n+k-1$, és a dir,

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

□

Observem que els multiconjunts els hem definit de manera que no ens importa l'ordre dels seus elements. Aleshores, és interessant preguntar-se de quantes maneres es pot ordenar un multiconjunt donat, és a dir, quantes permutacions diferents dels seus elements podem fer. El nombre de permutacions totals és $k!$, i fixada μ, podem permutar els i's del multiconjunt de $\mu(i)!$ maneres sense alterar la permutació. Per tant, el nombre total d'ordenacions és

$$\frac{k!}{\mu(1)!\mu(2)!\dots\mu(n)!} =: \binom{k}{\mu(1),\mu(2),\dots,\mu(n)}$$

A aquests nombres se'ls coneix com coeficients multinomials, ja que apareixen en el teorema multinomial:

Teorema 1.4.1 (Teorema multinomial)**.**

$$(a_1+\dots+a_n)^m = \sum_{\substack{0\le k_i\le m\\ k_1+\dots+k_n=m}} \binom{m}{k_1,\dots,k_n} a_1^{k_1}\cdot\dots\cdot a_n^{k_n}$$

Exemple 1.4.2. Els multiconjunts es poden aplicar per comptar el nombre d'aplicacions monòtones creixents de $[n]$ a $[k]$. Si només considerem aplicacions estrictament creixents, la resposta és simplement $\binom{k}{n}$. En canvi, si permetem les repeticions d'imatges, tindrem una aplicació per cada multiconjunt de $[k]$ de mida n (ja que l'ordre vindrà fixat per la monotonia), de manera que tindrem $\binom{n+k-1}{n}$ aplicacions.

1.5 Seleccions i distribucions

Definició 1.5.1 (Selecció)**.** Una selecció és un problema que es pot modelar com l'extracció de k boles numerades d'una caixa que conté n boles. Aquesta selecció pot ser amb o sense reposició (depenent de si es tornen les boles a la caixa després de cada extracció) i ordenada o no ordenada (depenent de si ens importa l'ordre en que traiem les boles de la caixa).

Segons les definicions anteriors, el nombre de seleccions en cada cas és el que s'indica a la taula 1.1.

Definició 1.5.2 (Distribució)**.** Una distribució és un problema que es pot modelar com el repartiment de k boles entre n caixes, que considerarem que són distingibles entre sí.

El nombre de distribucions en cada cas es pot veure en la taula 1.3.

Comentari. La taula 1.3 no és la que va posar el professor a classe, sinó la que hi ha als seus apunts.

	Ordenada	No ordenada
Amb reposició	n^k	$\binom{n+k-1}{k}$
Sense reposició	$\frac{n!}{(n-k)!}$	$\binom{n}{k}$

Taula 1.1: Nombre de seleccions de k boles d'entre n boles diferents

	Boles indistingibles	Boles distingibles
Com a molt una bola per caixa	$\binom{n}{k}$	$\frac{n!}{(n-k)!}$
Sense limitacions	$\binom{n+k-1}{k}$	n^k
La caixa i té k_i boles	1	$\binom{k}{k_1,\ldots,k_n}$

Taula 1.2: Nombre de distribucions de k boles en n caixes

1.6 Doble compteig

Siguin A i B dos conjunts finits i sigui $C \subset A \times B$. Definim la matriu $C = (c_{ij})_{i\in A, j\in B}$ on

$$c_{ij} = \begin{cases} 1, & (i,j) \in C \\ 0, & (i,j) \notin C \end{cases}$$

Aleshores, el principi de doble compteig ens diu que

$$\sum_{i\in A}\sum_{j\in B} c_{ij} = \sum_{j\in B}\sum_{i\in A} c_{ij}$$

Aquest principi pot semblar trivial, però es pot aplicar per resoldre problemes que no ho són.

Lema 1.6.1. *En una reunió de n persones, el nombre d'individus que fan un nombre imparell d'encaixades és parell.*

Demostració. Sigui $[n]$ el conjunt de persones i $E \subset [n]^2$ el conjunt de parells de persones que es donen la mà. Sigui $C = \{(x,e) \in [n] \times E : x \in e\} \subset [n] \times E$. Aleshores, segons el principi de doble compteig:

$$\sum_{i\in[n]}\sum_{e\in E} c_{ie} = \sum_{e\in E}\sum_{i\in[n]} c_{ie} = 2|E|$$

Definim el nombre d'encaixades que dona cada persona com

$$d(i) := \sum_{e\in E} c_{ie}$$

Per tant,

$$\sum_{i\in[n]} d(i) = \sum_{d(i) \text{ parell}} d(i) + \sum_{d(i) \text{ imparell}} d(i) = 2|E| \implies \sum_{d(i) \text{ imparell}} d(i) \text{ és parell}$$

I això implica que el nombre de persones amb nombre d'encaixades imparell és parell. □

Teorema 1.6.1 (de Bruijn-Erdös)**.** *Sigui $\mathcal{B}$ una família de subconjunts de $[n]$ tal que cada parella d'elements de $[n]$ estan en un únic conjunt de $\mathcal{B}$. Aleshores, si $|\mathcal{B}| > 1$, tenim que $|\mathcal{B}| > n$.*

Demostració. Definim $b := |\mathcal{B}|$. Suposem que $b \leq n$. Observem que si $i \in [n]$, $B \in \mathcal{B}$ i $i \notin B$, aleshores

$$d(i) = |\{B' \in \mathcal{B} : i \in B'\}| \geq |B|$$

Definim $C = \{(i, B) \in [n] \times \mathcal{B} : i \notin B\}$. Aleshores, per a cada $(i, B) \in C$,

$$n(b - d(i)) \leq n(b - |B|) = nb - n|B| \leq nb - b|B| = b(n - |B|)$$

Ara apliquem el doble compteig:

$$1 = n\frac{1}{n} = \sum_{i\in[n]} \sum_{\substack{B\in\mathcal{B} \\ i\notin B}} \frac{1}{n(b - d(i))} = \sum_{B\in\mathcal{B}} \sum_{\substack{i\in[n] \\ i\notin B}} \frac{1}{n(b - d(i))} \geq \sum_{B\in\mathcal{B}} \sum_{\substack{i\in[n] \\ i\notin B}} \frac{1}{b(n - |B|)} = 1$$

Aleshores, la desigualtat ha de ser estricta, i tirant enrere en la cadena de desigualtats, veiem que $b = n$. Aleshores, o bé $b > n$ o bé $b = n$, de manera que $b \geq n$. □

Definició 1.6.1 (Sistema de triples de Steiner)**.** Un sistema de triples de Steiner és una família de subconjunts de $[n]$ de mida 3 tal que per cada parella d'elements de $[n]$, hi ha una única tripla que els conté.

Proposició 1.6.1. *Si ST_n és un sistema de triples de Steiner, aleshores $n \equiv 1, 3 \mod 6$.*

Demostració. Suposem que S és un sistema de triples de Steiner a $[n]$ Sigui $C = \{(e, B) \in \binom{[n]}{2} \times S : e \in B\}$. Fent doble compteig,

$$3|S| = |C| = \binom{n}{2} \implies |S| = \frac{n(n-1)}{6}$$

A més, veiem que $n - 1$ ha de ser parell, ja que si escollim un element i dividim tots els altres en parelles que formin triples amb l'element separat, aleshores no en pot quedar cap penjat (en cas que en quedés un penjat, ha de tenir una tripla juntament amb l'element separat, i el tercer element d'aquesta tripla tindrà dues triples diferents amb l'element separat, arribant a contradicció). Comprovant tots els casos, veiem que la condició que $n - 1$ és parell juntament amb la condició que $n(n - 1)$ és multiple de 6 impliquen que $n \equiv 1, 3 \mod 6$. □

1.7 Principi de Dirichlet

Proposició 1.7.1 (Principi de Dirichlet)**.** *Sigui $f : [n] \longrightarrow [k]$, aleshores existeix $i \in [k]$ tal que*

$$|f^{-1}(i)| \geq \left\lceil \frac{n}{k} \right\rceil$$

Demostració. Si $|f^{-1}(i)| < \lceil \frac{n}{k} \rceil \ \forall i \in [k]$, aleshores per doble compteig

$$n = \sum_{i=1}^{k} |f^{-1}(i)| \leq k \left(\frac{n+k-1}{k} - 1 \right) = n - 1$$

□

Aquest principi s'aplica per exemple per demostrar el següent teorema, del mateix Dirichlet:

Teorema 1.7.1 (Dirichlet)**.** *Sigui $\alpha \in (0,1)$ un nombre irracional i N enter, aleshores existeixen enters p, q, amb $1 \leq q \leq N$ tals que*

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{q^2}$$

Demostració. Dividim l'interval $[0,1]$ en N subintervals d'igual longitud. Considerem els $n+1$ nombres reals $\{\alpha\}, \{2\alpha\}, \ldots \{(n+1)\alpha\}$, on $\{x\}$ denota la part fraccional de x. Aleshores, pel principi de Dirichlet, existeixen i, j tals que

$$\frac{l}{N} < \{i\alpha\}, \{j\alpha\} < \frac{l+1}{N}$$

per a un cert $l < N$.

Aleshores,

$$|\{i\alpha\} - \{j\alpha\}| < \frac{1}{N}$$

Suposem sense pèrdua de generalitat que $i > j$. Aleshores, per algun enter p,

$$|p - (i-j)\alpha| < \frac{1}{N}$$

Sigui $q := i - j$,

$$\left| \frac{p}{q} - \alpha \right| < \frac{1}{Nq} \leq \frac{1}{q^2}$$

□

Amb arguments més avançats, es pot provar que aquesta fita és asimptòticament òptima.

Un altre exemple d'aplicació és el següent teorema d'Erdös:

Teorema 1.7.2 (Erdös-Szeckeres). *Qualsevol successió de nombres reals de llargada n^2+1 conté una subsuccessió monòtona de llargada $n+1$.*

Demostració. Sigui $x_1, \ldots, x_{n^2+1}$ una successió de nombres reals. Suposem que no conté cap successió monòtona creixent de llargada $n+1$. Aleshores, definim la funció $f : [n^2+1] \longrightarrow [n]$ que a cada i li associa la llargada de la subsucessió monòtona creixent més llarga que es pot fer començant a la posició i de la successió original.

Per definició, tenim que $\forall i,\ 1 \leq f(i) \leq n$, de manera que aplicant el principi de Dirichlet, existeixen $i_1, \ldots, i_{n+1}$ tals que $f(i_1) = \cdots = f(i_{i+1})$. Observem que per $i < j$, $x_i < x_j \implies f(i) \geq f(j) + 1$. Per tant,

$$x_{i_1} > x_{i_2} > \cdots > x_{i_{n+1}}$$

que és una subsuccessió monòtona decreixent. □

Observació. La fita anterior és òptima, ja que existeixen successions de n^2 elements sense cap subsuccessió monòtona de llargada $n+1$. Per exemple:

$$3, 2, 1, 6, 5, 4, 9, 8, 7$$

1.8 Principi d'inclusió i exclusió

El principi d'inclusió-exclusió es pot interpretar com una generalització de la fórmula

$$|A \cup B| = |A| + |B| - |A \cap B|$$

per unions de més de dos conjunts.

Proposició 1.8.1 (Principi d'inclusió-exclusió). *Siguin $A_1, \ldots, A_n$ una col·lecció de conjunts. Aleshores el cardinal de la seva unió és*

$$\left| \bigcup_{i \in [n]} A_i \right| = \sum_{\substack{I \subset [n] \\ I \neq \emptyset}} (-1)^{|I|+1} \left| \bigcap_{i \in I} A_i \right|$$

Demostració. Es pot provar fàcilment per inducció, però a continuació veurem una prova alternativa. Siguin $A = \bigcup_{i \in [n]} A_i$ i $A_I = \bigcup_{i \in I} A_i$. Per a cada $X \subset A$, definim 1_X com la funció característica de X. Sigui $x \in A$, definim $K = K(x)$ com el conjunt de tots els subconjunts de $[n]$ tals que $1_{A_K}(x) = 1$ (i.e. els subconjunts que contenen a x). Aleshores,

$$\sum_{\substack{I \subset [n] \\ I \neq \emptyset}} (-1)^{|I|+1} 1_{A_I}(x) = \sum_{\substack{I \subset K \\ I \neq \emptyset}} (-1)^{|I|+1} 1_{A_I}(x) = \sum_{\substack{I \subset K \\ I \neq \emptyset}} (-1)^{|I|+1} = \sum_{i=1}^{k} (-1)^{i+1} \binom{k}{i} = 1$$

□

Un exemple típic d'aplicació del principi d'inclusió-exclusió és comptar el nombre de desarranjaments.

Definició 1.8.1 (Desarranjament)**.** Un desarranjament és una permutació que no conté cap punt fix.

$$D_n = \{\sigma \in S_n : \sigma(i) \neq i,\ i = 1, \dots, n\}$$

Per trobar el cardinal de D_n, ens definim la següent família de conjunts:

$$A_i = \{\sigma \in S_n : \sigma(i) \neq i\}$$

Aleshores, $D_n = \bar{A}_1 \cap \cdots \cap \bar{A}_n$. Per les lleis de Morgan, $D_n = S_n \setminus \bigcup A_i$, i per tant,

$$|D_n| = |S_n| - \left|\bigcup A_i\right| = |X| - \sum_{\substack{I \subset [n] \\ I \neq \emptyset}} (-1)^{|I|+1} \left|\bigcap_{i \in I} A_i\right| = \sum_{I \subset [n]} (-1)^{|I|} \left|\bigcap_{i \in I} A_i\right|$$

Veiem que el cardinal de la intersecció dels conjunts A_i, $i \in I$ només depèn del cardinal de I, de manera que

$$|D_n| = \sum_{I \subset [n]} (-1)^{|I|}(n - |I|)! = \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)! = n! \sum_{i=0}^{n} \frac{(-1)^n}{i!}$$

Aleshores, per n grans, $|D_n| \to \dfrac{n!}{e}$

Proposició 1.8.2. *Tal i com hem vist a l'exemple anterior, el principi d'inclusió-exclusió també es pot escriure com*

$$\left|\bigcap_{i=1}^{n} \bar{A}_i\right| = \sum_{I \subset [n]} (-1)^{|I|} \left|\bigcap_{i \in I} A_i\right|$$

Demostració. Per les Lleis de Morgan,

$$\left|\bigcap_{i=1}^{n} \bar{A}_i\right| = |X| - \left|\bigcup_{i=1}^{n} A_i\right| = |X| - \sum_{\substack{I \subset [n] \\ I \neq \emptyset}} (-1)^{|I|+1} \left|\bigcap_{i \in I} A_i\right|$$

Canviem el signe de tots els termes del sumatori i incloem el total a dins, ja que $X = \bigcap_{i \in \emptyset} A_i$. Aleshores,

$$\left|\bigcap_{i=1}^{n} \bar{A}_i\right| = \sum_{I \subset [n]} (-1)^{|I|} \left|\bigcap_{i \in I} A_i\right|$$

□

Un altre exemple típic és el de comptar, per un cert n, quants nombres hi ha entre 1 i n que siguin coprimers amb n.

Definició 1.8.2 (Funció phi d'Euler)**.** Definim la funció phi de Euler com

$$\phi(n) = |\{x \in [n] : \gcd(x, n) = 1\}|$$

Suposem que $n = p_1^{\alpha_1} \cdot \cdots \cdot p_k^{\alpha_k}$. Definim A_i com el conjunt d'enters positius menors o iguals que n que són divisibles per p_i. Aleshores el nombre que busquem és

$$\phi(n) = \left|\bigcap_{i=1} \bar{A}_i\right| = \sum_{I \subset [k]} (-1)^{|I|} \left|\bigcap_{i \in I} A_i\right|$$

Observem que

$$\left|\bigcap_{i \in I} A_i\right| = \frac{n}{\prod_{i \in I} p_i}$$

Aleshores,

$$\phi(n) = n \sum_{I \subset [k]} (-1)^{|I|} \frac{1}{\prod_{i \in I} p_i} = n \left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_k}\right)$$

on l'última igualtat es demostra operant algebraicament.

1.9 Particions de conjunts. Nombres de Stirling de segon tipus

Definició 1.9.1 (Partició d'un conjunt)**.** Una partició de $[n]$ en k parts és una col·lecció $A_1, \ldots, A_k$ de subconjunts de $[n]$ tals que $[n] = \bigcup A_i$ i $A_i \cap A_j = \emptyset$ per tots i, j tals que $i \neq j$.

Definició 1.9.2 (Nombre de Stirling de segon tipus)**.** El nombre de particions de $[n]$ en k parts es coneix com el nombre de Striling de segon tipus, que es representa amb

$$\left\{ n \atop k \right\}$$

Observem que $\left\{ n \atop k \right\}$ es pot calcular a partir del nombre d'aplicacions exhaustives entre $[n]$ i $[k]$, ja que podem considerar un subconjunt d'una partició com el conjunt de valors de $[n]$ que comparteixen imatge. Aleshores,

$$\left\{ n \atop k \right\} = \frac{1}{k!} |\{f : [n] \longrightarrow [k],\ f \text{ exhaustiva}\}| = \frac{1}{k!} \sum_{i=1}^{k} (-1)^{k-i} \binom{k}{i} i^n$$

Podem calcular alguns valors dels nombres de Stirling de segon tipus fàcilment. En primer lloc, $\left\{ {n \atop 1} \right\} = 1$, ja que si només podem posar tots els elements en l'únic conjunt que tenim. Per altra banda, si podem fer dos subconjunts,

$$\left\{ {n \atop 2} \right\} = \frac{1}{2}(2^n - 2) = 2^{n-1} - 1,$$

ja que podem agafar qualsevol subconjunt excepte el buit i el total i dividim per dos per no comptar complementaris.

Una propietat interessant dels nombres de Stirling de segon tipus és que compleixen una equació de recurrència similar a la dels nombres combinatoris:

Proposició 1.9.1. *Es satisfà que*

$$\left\{ {n \atop k} \right\} = k \left\{ {n-1 \atop k} \right\} + \left\{ {n-1 \atop k-1} \right\}$$

Demostració. El primer sumand són les particions de les quals $\{n\}$ no és una part, mentre que el segon sumand són les particions que contenen $\{n\}$. □

Definició 1.9.3 (Nombre de Bell)**.** El nombre de totes les particions de $[n]$ (amb un nombre qualsevol de subconjunts) es coneix com nombre de Bell.

$$B_n = \sum_{k=1}^{n} \left\{ {n \atop k} \right\}$$

1.10 Composicions i particions d'enters

Definició 1.10.1 (Composicions)**.** Les composicions d'un enter n en k parts són les solucions de $n = x_1 + \cdots + x_k$ amb $x_k \in \mathbb{N}$ (recordem que en aquesta assignatura $0 \notin \mathbb{N}$).

El conjunt de composicions de n en k parts es denota com

$$c_k(n) = \left\{ (x_1, \ldots, x_k) : x_i \in \mathbb{N},\ \sum_{i=1}^{k} x_i = n \right\}$$

Per exemple, $2+2$, $3+1$ i $1+3$ són composicions diferents de 4 en 2 parts.

Tal i com hem vist a classe de problemes, donat que $x_i \geq 1$, tenim que $|c_k(n)|$ és igual al nombre de maneres de repartir $n-k$ boles entre k caixes numerades, que es correspon al seu torn amb el nombre de paraules binàries de llargada $(n-k)+k-1$ amb $k-1$ zeros. Per tant,

$$|c_k(n)| = \binom{n-k+k-1}{k-1} = \binom{n-1}{k-1}$$

Si considerem composicions de mida arbitrària,

$$|c(n)| = \sum_{k=1}^{n} |c_k(n)| = \sum_{k=1}^{n} \binom{n-1}{k-1} = 2^{n-1}$$

Definició 1.10.2 (Particions)**.** Les particions d'un enter n en k parts són les solucions de $n = x_1 + \cdots + x_k$ tals que $x_i \in \mathbb{N}$ i $x_1 \geq \cdots \geq x_k$.

Similarment al cas de les composicions, definim el conjunt de particions de n en k parts com

$$P_k(n) = \left\{ (x_1, \ldots, x_k) : x_i \in \mathbb{N},\ x_1 \geq \cdots \geq x_k,\ \sum_{i=1}^{k} x_i = n \right\}$$

i denotem $p_k(n) = |P_k(n)|$.

Les particions es poden interpretar com el quocient de les composicions per la relació d'equivalència que ens diu que dues composicions són iguals si tenen els mateixos sumands.

Per valors baixos de k tenim que el nombre de particions de n és

$$p_1(n) = p_n(n) = 1$$
$$p_2(n) = \lfloor \frac{n}{2} \rfloor$$
$$p_3(n) = \left\{ \frac{n^2}{12} \right\}$$

La intuició de l'últim valor és que si considerem un polígon de n costats, el nombre de particions en 3 parts es correspon amb seleccionar 3 vèrtexs del polígon, i dos eleccions de vèrtexs corresponen a la mateixa partició si els triangles que formen són similars. La majoria de triangles tenen simetria per rotació i inversió, de manera que hi ha aproximadament $2n$ còpies de cada triangle. Per tant,

$$p_3(n) \cong \frac{1}{2n}\binom{n}{3} \cong \frac{n^2}{12}$$

Un altre fet interessant és que les particions es poden interpretar com diagrames de Ferrers:

Definició 1.10.3 (Diagrama de Ferrers)**.** Un diagrama de Ferrers, o Tableaux de Young, és una figura geomètrica formada per k files ordenades de més a menys llargada, tal que la suma del nombre de columnes de cada fila és n.

Aquests diagrames van bé per raonar amb particions. Per exemple, les particions de n en k parts es poden classificar en aquelles en les quals $x_k = 1$ i aquelles en que no. La primera es correspon amb $p_{k-1}(n-1)$, mentre que la segona es correspon amb restar una columna de totes les files, és a dir, $p_k(n-k)$. Per tant,

$$p_k(n) = p_{k-1}(n-1) + p_k(n-k)$$

Una altra igualtat interessant és

$$p_k(n) = \ \#\text{ particions de } n \text{ en les quals } x_1 = k$$

Aquesta igualtat es demostra veient que un diagrama de Ferrers amb k files es pot girar al voltant de la diagonal per trobar una partició amb $x_1 = k$, i que aquesta relació és bijectiva.

Les particions són difícils de comptar exactament, però es poden acotar amb el nombre de composicions. Sabem que cada partició dóna lloc com a molt a $k!$ composicions (ja que n'hi poden haver d'iguals si $x_i = x_j$). Per altra banda, per a una partició qualsevol, podem crear una partició amb tots els nombres diferents si definim $y_i = x_i + k - i$ (es veu trivialment que aleshores dos elements no poden ser iguals). Aleshores, tenim una partició de $n + \binom{k}{2}$ en k parts, que es correspon exactament a $k!$ composicions (ja que té tots els termes diferents). Aleshores,

$$\frac{1}{k!}\binom{n-1}{k-1} \leq p_k(n) \leq \frac{1}{k!}\binom{n+\binom{k}{2}-1}{k-1}$$

Observem que quan $n >> k$, aquestes fites són bastant acurades.

1.11 Twelvefold way

Suposem que tenim n boles i k capses. Tant les boles com les caixes poden estar numerades o no (és a dir, poden ser distingibles entre elles o no). El nombre de maneres de distribuir les boles és:

Boles	Capses	Totes	Injectives	Exhaustives
num.	num.	k^n	$(k)_n$	$k!\left\{{n \atop k}\right\}$
no num.	num.	$\binom{n+k-1}{k-1}$	$\binom{k}{n}$	$\binom{n-1}{k-1}$
num.	no num.	$\sum_{i=1}^{k} \left\{{n \atop k}\right\}$	$1_{\{n\leq k\}}$	$\left\{{n \atop k}\right\}$
no num.	no num.	$\sum_{i=1}^{k} p_i(n)$	$1_{\{n\leq k\}}$	$p_k(n)$

Taula 1.3: Nombre de distribucions de n boles entre k capses

Aquesta taula ens permet resumir molts dels resultats als quals hem arribat en aquest capítol.

1.12 Estimacions i estimacions asimptòtiques

Definició 1.12.1. Donades les funcions $f, g : \mathbb{N} \longrightarrow \mathbb{R}$, direm que $f(n) = \mathcal{O}(g(n))$ si $\exists c \in \mathbb{R}$ tal que $\forall n \geq n_0$,

$$|f(n)| \leq c|g(n)|$$

Per altra banda, direm que $f(n) = o(g(n))$ si

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0,$$

és a dir, si $f(n)$ és asimptòticament menor que $g(n)$. La notació inversa és $f(n) = \Omega g(n)$, que és equivalent a dir que $g(n) = o(f(n))$.

Si dues funcions f, g tenen el mateix creixement asimptòtic, aleshores es diu que $f(n) = \Theta g(n)$, que equival a dir que $f(n) = \mathcal{O}(g(n))$ i $g(n) = \mathcal{O}(f(n))$.

Per últim, si es vol remarcar que les constants també són equivalents, es diu que $f(n) \sim g(n)$, que equival a dir que

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$$

Proposició 1.12.1 (Propietats de la $\mathcal{O}$ de Landau)**.** *Siguin $f(n) = \mathcal{O}(g(n))$ i $h(n) = \mathcal{O}(k(n))$. Aleshores,*

- $f(n) + h(n) = \mathcal{O}(|g(n)| + |k(n)|)$
- $f(n) \cdot h(n) = \mathcal{O}(|g(n)| \cdot |k(n)|)$

Proposició 1.12.2. *Per a qualssevol $a, b \in \mathbb{R}^+$,*

1. $(\ln n)^a = o(n^b)$.
2. $n^a = o(n^b)$ *si* $a < b$.
3. $n^a = o(b^n)$ *per* $b > 1$.
4. $a^n = o(b^n)$ *si* $b > a > 1$.
5. $a^n = o(n^n)$.

Demostració. 1. Aplicant la regla de l'Hôpital, $\lim_{n\to\infty} \frac{\ln n}{n^b} = \frac{1}{b} \lim_{n\to\infty} \frac{1}{n^b} = 0$.

Els altres es fan de manera similar. □

A continuació veurem com podem aplicar tota aquesta notació asimptòtica per estudiar el creixement dels nombres harmònics.

Definició 1.12.2 (Nombre harmònic)**.** Definim la successió de nombres harmònics com

$$H_n = \sum_{i=1}^{n} \frac{1}{i}$$

Proposició 1.12.3. *Els nombres harmònics estan acotats per*

$$\ln n \leq H_n \leq \ln n + 1$$

Demostració. La manera més intuitiva és comparant la suma dels harmònics amb la integral de $1/x$. Considerant les sumes superiors i inferiors, veiem que

$$H_n - 1 \leq \int_1^n \frac{1}{x}\, dx \leq H_n \implies H_n - 1 \leq \ln n \leq H_n \implies$$

$$\implies \begin{cases} H_n \leq 1 + \ln n \\ H_n \geq \ln n \end{cases}$$

□

Per tant, tenim que $H_n \sim \ln n$, i aleshores la sèrie harmònica divergeix.
De fet, es pot demostrar que

$$H_n = \ln n + \gamma + \mathcal{O}\left(\frac{1}{n}\right),$$

on γ és la constant d'Euler-Mascheroni.
Una altra funció de la qual és interessant estudiar-ne el creixement és la funció factorial.

Proposició 1.12.4. *La funció factorial està acotada per*

$$e\left(\frac{n}{e}\right)^n \leq n! \leq en\left(\frac{n}{e}\right)^n$$

Demostració. La desigualtat de la dreta la farem per inducció. Si $n = 1$, es té que $1 \leq 1$. Per $n > 1$, suposant cert per $n-1$, tenim que

$$\begin{aligned} n! = n(n-1)! &\leq ne(n-1)\left(\frac{n-1}{e}\right)^{n-1} = ne\left(\frac{n-1}{e}\right)^n e = ne\left(\frac{n}{e}\right)^n \left(\frac{n-1}{n}\right)^n e \\ &= en\left(\frac{n}{e}\right)^n \left(1-\frac{1}{n}\right)^n e \leq en\left(\frac{n}{e}\right)^n \end{aligned}$$

On hem utilitzat que $(1 - 1/n) \leq e^{-1/n}$.
Per la desigualtat de l'esquerra, ho comparem novament amb una integral:

$$\ln n! = \sum_{i=1}^{n} \ln i \geq \int_1^n \ln x\, dx = x\ln x - x|_1^n = n\ln n - n + 1$$

I per tant $n! \geq e^{n\ln n - n + 1} = n^n e^{-n} e$ □

Si no ens interessa una desigualtat vàlida $\forall n$, sinó només una aproximació asimptòtica, tenim el següent teorema de de Moivre:

Teorema 1.12.1 (de Moivre)**.** *Existeix una constant $c \in \mathbb{R}$ tal que*

$$n! \sim c\frac{n^{n+1/2}}{e^n}$$

Demostració. Considerem la successió $u_n = \dfrac{n^{n+1/2}e^{-n}}{n!}$. Tenim que

$$\ln\frac{u_{n+1}}{u_n} = \left(n+\frac{1}{2}\right)\ln\left(1+\frac{1}{n}\right) - 1$$

Aproximant el logaritme pel seu desenvolupament de Taylor de 3r grau, tenim que per $x \to 0$,

$$\ln 1 + x = x - \frac{x^2}{2} + \frac{x^3}{3} + o(x^3)$$

Aleshores,

$$\ln \frac{u_{n+1}}{u_n} = \left(n + \frac{1}{2}\right)\left(\frac{1}{n} - \frac{1}{2n^2} + \frac{1}{3n^3} + o\left(\frac{1}{n^3}\right)\right) - 1 = \\ = \left(\frac{1}{3n^2} - \frac{1}{4n^2}\right) + o\left(\frac{1}{n^2}\right) = \frac{1}{12n^2} + o\left(\frac{1}{n^2}\right)$$

Donat que aquest valor és menor que 1 $\forall n$, la suma dels $v_n = \ln u_{n+1} - \ln u_n$ convergeix. Però aquesta sèrie és telescòpica, de manera que tenim que

$$\sum_{i\geq 1} \ln u_{n+1} - \ln u_n = c' \implies \lim_{n\to\infty} \ln u_{n+1} = c' \implies \lim_{n\to\infty} u_{n+1} = e^{c'} = c$$

□

Més tard, Stirling va determinar l'expressió exacta d'aquesta constant:

Teorema 1.12.2 (Stirling)**.** *La constant del teorema de de Moivre és $c = \sqrt{2\pi}$, és a dir,*

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

Aquesta aproximació es coneix com fórmula de Stirling.

1.12.1 Nombres binomials

Es poden fer moltes aproximacions dels nombres binomials, i depenent dels valors de n i k, algunes seran més precises que d'altres. Una aproximació poc fina però vàlida $\forall n, k$ és la següent:

Proposició 1.12.5. *Per n, k tals que $0 \leq k \leq n$,*

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq e^k \left(\frac{n}{k}\right)^k$$

Demostració. Per la desigualtat de l'esquerra, sabem que $n/k \leq (n-i)/(k-i)$ per $n \geq k$ i $i \geq 0$, de manera que

$$\left(\frac{n}{k}\right)^k \leq \frac{n}{k} \cdots \frac{n-k+1}{1} = \binom{n}{k}$$

Per la desigualtat de la dreta, utilitzarem que segons 1.12.4, $k! \geq \left(\frac{k}{e}\right)^k$:

$$k! \geq \left(\frac{k}{e}\right)^k \implies \left(\frac{ne}{k}\right)^k \geq \frac{n^k}{k!} \geq \frac{n(n-1)\ldots(n-k+1)}{k!} = \binom{n}{k}$$

□

A continuació veurem estimacions que són més fines per casos particulars. En primer lloc, definim una funció que ens serà útil.

Definició 1.12.3 (Funció d'entropia)**.** Per $x \in [0,1]$, definim la funció d'entropia $H(x)$ com

$$H(x) = -x \ln x - (1-x)\ln(1-x)$$

Els signes negatius són per tal que $H(x) \geq 0$. En el cas $x = 0$, considerarem que $0 \cdot \ln 0 := 0$.

Proposició 1.12.6.

$$\frac{1}{n+1} e^{nH(k/n)} \leq \binom{n}{k} \leq e^{nH(k/n)}$$

Demostració. Definim $p = n/k$. Aleshores,

$$\binom{n}{k} p^k (1-p)^{n-k} \leq \sum_{j=0}^{n} \binom{n}{j} p^j (1-p)^{n-j} = 1$$

Per tant,

$$\binom{n}{k} \leq p^{-k}(1-p)^{n-k} = e^{-k\ln p - (n-k)\ln(1-p)} = e^{-np\ln p - n(1-p)\ln(1-p)} = e^{nH(p)}$$

Per la cota inferior, farem servir que la successió (a_j) definida com

$$a_j = \binom{n}{j} p^j (1-p)^{n-j}$$

satisfà que $a_1 \leq \cdots \leq a_{np} \geq \cdots \geq a_n$. (Per demostrar-ho calcularíem el quocient entre termes consecutius de la successió). Aleshores, $\forall p$,

$$1 = \sum_{j=0}^{n} \binom{n}{j} p^j (1-p)^{n-j} \leq (n+1)\binom{n}{k} p^k (1-p)^{n-k} \implies$$
$$\implies \binom{n}{k} \geq \frac{1}{n+1} e^{-k\ln p - (n-k)\ln(1-p)} = \frac{1}{n+1} e^{nH(p)}$$

□

En particular, gràcies a aquesta proposició tenim que

$$\ln \binom{n}{k} = nH\left(\frac{k}{n}\right) + \mathcal{O}(\ln n),$$

de manera que si $H(k/n)$ no és massa petit, les fites anteriors donen una bona aproximació del nombre binomial (ja que és un terme lineal en n amb error logarítmic en n).

A vegades no ens interessarà conèixer el valor d'un coeficient binomial qualsevol, sinó el valor del coeficient binomial més gran de cada fila del triangle de Pascal (i.e. nombres binomials amb

n fix). Suposant que el nombre de fila és parell, podem escriure $n = 2m$. Aleshores busquem una aproximació de

$$\binom{2m}{m} = \frac{(2m)!}{(m!)^2}$$

Per valors de m grans, podem aproximar el factorial per la fórmula de Stirling a dalt i a baix:

$$\binom{2m}{m} \sim \frac{\left(\frac{2m}{e}\right)^{2m}\sqrt{4\pi m}}{\left(\frac{m}{e}\right)^{2m}2\pi m} = \frac{2^{2m}}{\sqrt{\pi m}}$$

Donat que la suma de tots els nombres binomials de la fila $2m$ és 2^{2m}, podem dir que el nombre binomial central és aproximadament $1/\sqrt{\pi m}$ del total per a valors de $2m$ grans.

Per altra banda, si fixem k, aleshores tenim que

$$\binom{n}{k} \sim \frac{n^k}{k!}$$

Veiem que

$$\binom{n}{k} = \frac{n^k}{k!}\left(\frac{n-1}{n}\right)\dots\left(\frac{n-k+1}{n}\right) = \frac{n^k}{k!}\left(1-\frac{1}{n}\right)\dots\left(1-\frac{k-1}{n}\right)$$

Quan k és fix i $n \to \infty$, tots els factors de la dreta tendeixen a 1, de manera que el nombre binomial tendeix a $n^k/k!$.

Quan tant n com k són grans, podem aplicar Stirling a tots els factorials:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \sim \frac{(n/e)^n\sqrt{2\pi n}}{(k/e)^k\sqrt{2\pi k}((n-k)/e)^{n-k}\sqrt{2\pi(n-k)}}$$

Fent que $p := n/k$, l'expressió anterior es redueix a

$$\frac{1}{\sqrt{2\pi}}\frac{1}{\sqrt{np(1-p)}}\frac{1}{p^k(1-p)^{n-k}} = \frac{e^{nH(p)}}{\sqrt{2\pi np(1-p)}}$$

1.12.2 Nombre de Striling de segon tipus

Recordem que els nombres de Stirling de segon tipus els havíem definit a partir d'una suma:

$$\left\{{n \atop k}\right\} := \frac{1}{k!}\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}j^n$$

Aquesta expressió és complicada de tractar, així que per valors de n gran, utilitzarem l'aproximació següent:

Proposició 1.12.7. *Per un cert k fix i $n \to \infty$, tenim que*

$$\left\{{n \atop k}\right\} \sim \frac{k^n}{k!}$$

Demostració. Ens és suficient veure que el límit del quocient quan $n \to \infty$ és 1.

$$\lim_n \frac{\frac{1}{k!}\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}j^n}{k^n/k!} = \lim_n \underbrace{\sum_{j=0}^{k-1}(-1)^{k-j}\binom{k}{j}\left(\frac{j}{k}\right)^n}_{\to 0} + 1 = 1$$

□

1.12.3 Particions de n en k parts

Tal i com ja vam comentar, el nombre de particions es pot acotar a partir del nombre de composicions:

Proposició 1.12.8. *Sigui $p_k(n)$ el nombre de particions de n en k parts. Aleshores,*

$$\binom{n-1}{k-1} \leq k!\, p_k(n) \leq \binom{n+\binom{k}{2}-1}{k-1}$$

Demostració. Tota partició es pot permutar per donar lloc a $k!$ composicions. El problema és que algunes d'aquestes poden ser iguals, de manera que el nombre de particions és més gran que el nombre de composicions dividit per $k!$ (desigualtat de l'esquerra).

Per veure la desigualtat de la dreta, donada una partició, podem fer tots els seus elements diferents sumant 0 a l'element més petit, 1 al següent, i així successivament, fins a sumar $k-1$ a l'element més gran. Aleshores, aquesta partició es correspondrà exactament a $k!$ composicions diferents de $n+\binom{k}{2}$ en k parts. El problema és que poden haver-hi composicions que no derivin de cap partició, de manera que en lloc d'una igualtat hi tenim una desigualtat. □

Observem que per a k fix i $n \to \infty$,

$$\binom{n+\binom{k}{2}-1}{k-1} \sim \binom{n-1}{k-1}$$

de manera que

$$p_k(n) \sim \frac{1}{k!}\binom{n-1}{k-1} \sim \frac{n^{k-1}}{k!(k-1)!}$$

2

Equacions de recurrència i funcions generadores

2.1 Equacions de recurrència

Definició 2.1.1 (Equació de recurrència)**.** Donada una successió (a_n), es diu que aquesta satisfà una equació de recurrència d'ordre k si existeix una funció g i un $n_0 \in \mathbb{N}$ tals que per $\forall n \geq n_0$,

$$a_n = g(a_{n-1}, \ldots, a_{n-k}, n)$$

Exemple 2.1.1. Un exemple d'equació de recurrència d'ordre 1 és $a_n = a_{n-1} + n$, $\forall n \geq 1$; $a_0 = 0$. Moltes vegades ens interessa passar d'una successió expresada en forma recurrent a una fórmula general que ens doni a_n en funció únicament de n. Per exemple, la recurrència anterior correspon a la successió

$$a_n = \binom{n+1}{2}$$

2.2 Funcions generadores

Definició 2.2.1 (Funció generadora)**.** Donada una successió de nombres (a_n), la funció generadora de (a_n) és una funció

$$A(z) = a_0 + a_1 z + a_2 z^2 + \cdots = \sum_{n \geq 0} a_n z^n$$

és a dir, una sèrie de potències on els coeficients són els termes de la successió.

Exemple 2.2.1. Sigui $a_n = 1\ \forall n$ una successió, la funció generadora de (a_n) és

$$A(z) = \sum_{n\geq 0} z^n$$

I per $|z| < 1$, $A(z) = \dfrac{1}{1-z}$.

Notació. Definim la funció $[z^n]$ com una funció que pren com a argument una sèrie de potències i torna el seu coeficient n-èssim. Per exemple, sigui $A(z)$ la sèrie de potències donada per $A(z) = \sum_{n\geq 0} a_n z^n$, aleshores

$$[z^n]A(z) = a_n$$

2.2.1 Nombres de Fibonacci

Sigui (F_n) la successió de nombres de Fibonacci, definida per $F_0 = 0$, $F_1 = 1$, i per $n \geq 2$, l'equació de recurrència

$$F_n = F_{n-1} + F_{n-2}$$

Per estudiar el creixement asimptòtic dels nombres de Fibonacci, tractarem amb la seva funció generadora. Sigui $F(z)$ la funció generadora de (F_n), aleshores

$$\begin{aligned} F(z) &= \sum_{n\geq 0} F_n z^n = F_0 + F_1 z + \sum_{n\geq 2}(F_{n-1} + F_{n-2})z^n \\ &= F_0 + F_1 z + \sum_{n\geq 2} F_{n-1} z^n + \sum_{n\geq 2} F_{n-2} z^2 \end{aligned}$$

Aquest últim pas en el qual hem separat les sèries no està del tot justificat, però d'ara endavant considerarem que les sèries "es comporten bé" i que podem operar amb elles algebraicament.

A continuació expressem cada una de les sèries anteriors en funció de $F(z)$:

$$\begin{gathered} F(z) = F_0 + F_1 z + z(F(z) - F_0) + z^2 F(z) = z + zF(z) + z^2 F(z) \implies \\ \implies F(z) = \frac{z}{1 - z - z^2} \end{gathered}$$

Un cop tenim una expressió tancada de la funció generadora, per trobar els termes de la successió, hem d'expressar-la en forma de sèrie de potències.

Pel cas de $F(z)$ racionals, el procediment estàndard és descomposar $F(z)$ en fraccions simples de la forma

$$\frac{A}{1 - Bz}$$

En el cas de la successió de Fibonacci,

$$F(z) = \frac{z}{1 - z - z^2} = \frac{z}{(1 - \alpha z)(1 - \beta z)}$$

on $\alpha = \dfrac{1+\sqrt{5}}{2}$ i $\beta = \dfrac{1-\sqrt{5}}{2}$. Descomposem en fraccions simples:

$$F(z) = \frac{z}{1-z-z^2} = \frac{A}{1-\alpha z} + \frac{B}{1-\beta z} \implies A = -B = \frac{1}{\sqrt{5}}$$

A més, a partir de la fórmula de la suma de la sèrie geomètrica, tenim que

$$\frac{1}{1-\alpha z} = \sum_{n\geq 0} \alpha^n z^n, \qquad \frac{1}{1-\beta z} = \sum_{n\geq 0} \beta^n z^n$$

Així doncs, la funció generadora dels nombres de Fibonacci és

$$F(z) = \frac{1}{\sqrt{5}} \left(\sum_{n\geq 0} (\alpha^n - \beta^n) z^n \right)$$

I per tant, el terme n-èssim de la successió de Fibonacci serà el coeficient n-èssim de la sèrie de potències:

$$a_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$$

Donat que $|\beta| < 1$, $\beta^n \to 0$ quan $n \to \infty$, de manera que asimptòticament la successió de Fibonacci es comporta com una sèrie geomètrica de raó α.

$$F_n \sim \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n$$

2.3 Sèries formals

Definició 2.3.1 (Sèrie formal)**.** Una sèrie formal és una seqüència $a = (a_0, a_1, \dots)$ amb $a_i \in \mathbb{C}$ on es defineixen les dues operacions següents:

- $a + b = (a_n + b_n,\ n \geq 0)$ (Suma)
- $a \cdot b = \left(\sum_{k=0}^{n} a_k b_{n-k},\ n \geq 0 \right)$ (Producte de convolució)

Observem que la suma és associativa, commutativa, té element neutre i invers, de manera que les sèries formals són un grup Abelià respecte la suma. Per altra banda, el producte és associatiu, commutatiu, té element neutre i és distributiu respecte la suma. Per tant, les sèries formals amb la suma i el producte de convolució són un anell.

Definició 2.3.2 (Anell de sèries formals)**.** L'anell de sèries formals $\mathbb{C}[z]$ és el conjunt de sèries formals amb la suma i el producte definits anteriorment.

Proposició 2.3.1. *$a = (a_0, a_1, \dots)$ és invertible respecte del producte sii $a_0 \neq 0$.*

Demostració. Si existeix b tal que $a \cdot b = 1$, aleshores $a_0 b_0 = 1 \implies a_0 \neq 0$.

Recíprocament, si $a_0 \neq 0$, podem definir una seqüència b tal que $a \cdot b = 1$. Ho definirem recursivament:

$$a_0 b_0 = 1 \implies b_0 = \frac{1}{a_0}$$
$$a_1 b_0 + a_0 b_1 = 0 \implies b_1 = -\frac{1}{a_0} b_0 a_1$$

i en general, per $n \geq 1$,

$$a_n b_0 + \cdots + a_0 b_n = 0 \implies b_n = -\frac{1}{a_0} \left(a_1 b_0 + \cdots + a_1 b_{n-1}\right)$$

□

Exemple 2.3.1. La sèrie $1 - z = (1, -1, 0, \ldots)$ és invertible, ja que $a_0 \neq 0$. El seu invers és la sèrie geomètrica

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

Observem que si fem el seu producte de convolució,

$$(1 - z) \cdot \frac{1}{1-z} = (1, 1-1, 1-1, \ldots) = (1, 0, 0, \ldots)$$

Aquest exemple és important perquè observem que si interpretem les sèries com a funcions de z, aleshores per $z = 2$,

$$\frac{1}{1-2} = -1 \text{ mentre que } 1 + 2 + 2^2 + \cdots = \infty$$

Per tant, quan manipulem algebraicament les sèries de potències, hem de tenir en ment que estem treballant amb representacions formals de les sèries, i que hi ha igualtats que poden no ser vàlides per certs valors de z.

Una altra operació que podem fer amb les sèries formals és la derivada, que es defineix de la següent manera:

Definició 2.3.3 (Derivada formal)**.** Si $A(z) = \sum_{n \geq 0} a_n z^n$, definim l'operador derivada com

$$\frac{d}{dz} A(z) = A'(z) = \sum_{n \geq 1} n a_n z^{n-1}$$

Podem definir les sèries exponencial i logaritme de la següent manera:

$$-\ln(1 - z) = \sum_{n \geq 1} \frac{z^n}{n}$$
$$\exp(z) = e^z = \sum_{n \geq 0} \frac{z^n}{n!}$$

i amb aquestes definicions, observem que les sèries satisfan totes les propietats de les funcions, com per exemple:

$$\exp(z)\exp(w) = \exp(z+w)$$
$$\log((A(z))^m) = m\log(A(z))$$

Exemple 2.3.2. Les operacions amb sèries de potències tindran molt a veure amb alguns dels conceptes de combinatòria que vam estudiar en el primer capítol. Per exemple, suposem que volem calcular la potència m-èssima de la sèrie geomètrica. Veiem que

$$\frac{1}{(1-z)^m} = \left(\sum_{n\geq 0} z^n\right)^m = \sum_{n\geq 0} c_n z^n,$$

on c_n és el nombre de maneres de triar m índexos tals que sumin n, és a dir,

$$c_n = \binom{n+m-1}{n}$$

Aquest exemple és un cas concret d'un teorema més general:

Teorema 2.3.1 (Fórmula del binomi de Newton)**.** *Per a qualsevol $\alpha \in \mathbb{C}$,*

$$(1+z)^\alpha = \sum_{n\geq 0} \binom{\alpha}{n} z^n$$

on definim l'extensió dels nombres binomials als complexos com

$$\binom{\alpha}{n} = \frac{\alpha(\alpha-1)\ldots(\alpha-n+1)}{n!}$$

Demostració. Sigui $A(z) = (1+z)^\alpha$. Veiem que $A(z)$ es pot escriure com una sèrie, ja que la composició de sèries dona una sèrie, i

$$A(z) = \exp(\log(A(z))) = \exp(\alpha\log(1+z))$$

Per tant, $\exists a_n$ tals que $A(z) = \sum_{n\geq 0} a_n z^n$. Considerem la derivada de la sèrie logaritme:

$$\frac{d}{dz}(\log A(z)) = \frac{A'(z)}{A(z)} = \frac{\alpha(1+z)^{\alpha-1}}{(1+z)^\alpha} = \frac{\alpha}{1+z}$$

d'on treiem que $(1+z)A'(z) = \alpha A(z)$. Desenvolupant-ho, tenim que

$$(1+z)\left(a_1 + 2a_2 z + 3a_3 z^2 + \ldots\right) = \alpha\left(a_0 + a_1 z + a_2 z^2 + \ldots\right)$$

Es pot demostrar que $a_0 = 1$ (no ho demostrarem, però intuitivament correspon al cas $z = 0$). Aleshores, recursivament podem anar trobant els coeficients de la sèrie:

$$a_1 = \alpha a_0 \implies a_1 = \alpha$$
$$2a_2 + a_1 = \alpha a_1 \implies a_2 = \frac{\alpha(\alpha-1)}{2}$$

i es pot comprovar que en general s'obté

$$a_n = \binom{\alpha}{n}$$

□

2.4 Equacions de recurrència lineals a coeficients constants i homogènies

Definició 2.4.1 (Equació lineal homogènia a coeficients constants)**.** Diem que una successió $a = (a_0, a_1, \dots)$ satisfà una equació lineal homogènia d'ordre k a coeficients constants, si existeixent $c_1, c_2, \dots, c_k \in \mathbb{C}$ tals que $\forall\, n \geq k$,

$$a_n = c_1 a_{n-1} + \cdots + c_k a_{n-k}$$

La gràcia d'aquest tipus de successions és que tenim un teorema que ens permet trobar la seva funció generadora i per tant trobar una fórmula tancada del seu terme general.

Teorema 2.4.1. *Si $a = (a_0, a_1, \dots)$ satisfà una equació de recurrència lineal homogènia d'ordre k a coeficients constants, aleshores*

$$A(z) = \frac{P(z)}{1 - c_1 z - c_2 z^2 - \cdots - c_k z^k}$$

on $P(z)$ és un polinomi de grau menor que k. I en particular,

$$a_n = \sum_{i=1}^{r} p_i(n) \alpha_i^n,$$

on $\alpha_1, \dots, \alpha_r$ són les arrels de $Q(z) = z^k - c_1 z^{k-1} - \cdots - c_k$, i els $p_i(n)$ són polinomis en n de grau menor que la multiplicitat de l'arrel α_i.

Demostració.

$$\begin{aligned} A(z) = \sum_{n\geq 0} a_n z^n &= \underbrace{\sum_{n=0}^{k-1} a_n z^n}_{A_{k-1}(z)} + \sum_{n\geq k} \left(c_1 a_{n-1} + \cdots + c_k a_{n-k}\right) z^n \\ &= A_{k-1}(z) + c_1 \sum_{n\geq k} a_{n-1} z^n + \cdots + c_k \sum_{n\geq k} a_{n-k} z^n \\ &= A_{k-1}(z) + c_1 z \left(A(z) - A_{k-2}(z)\right) + \cdots + c_k z^k \left(A(z)\right) \end{aligned}$$

Aïllant els termes amb $A(z)$ veiem que

$$A(z)\left(1 - c_1 z - \cdots - c_k z^k\right) = A_{k-1}(z) + c_1 z A_{k-2}(z) + \cdots + c_{k-1} z^{k-1} A_0(z)$$

i s'observa que cada terme del polinomi de la dreta té grau menor que k.

Un cop trobada la funció generadora, l'hem d'expressar com a sèrie de potències per demostrar la segona part del teorema. Per fer-ho, utilitzarem la fórmula següent:

$$\frac{1}{(1-\alpha z)^m} = \sum_{n\geq 0} \binom{n+m-1}{n} \alpha^n z^n$$

Aquesta fórmula prové de l'observació que cada terme amb $\alpha^n z^n$ apareixerà tantes vegades a l'esquerra com solucions tingui l'equació $n_1 + \cdots + n_m = n$, on n_i són enters no negatius.

El polinomi característic l'havíem definit com

$$Q(z) = z^k - c_1 z^{k-1} - \cdots - c_k$$

Suposem que aquest polinomi es pot descomposar en

$$Q(z) = (z-\alpha_1)^{m_1} \dots (z-\alpha_r)^{m_r}$$

on $m_1 + \cdots + m_r = k$. Aleshores, fent el canvi $z \leftarrow 1/z$, tenim que

$$1 - c_1 z - \cdots - c_k z^k = (1-\alpha_1 z)^{m_1} \dots (1-\alpha_r z)^{m_r}$$

Substituint a l'expressió que hem trobat abans de la funció generadora, veiem que

$$A(z) = \frac{P(z)}{(1-\alpha_1 z)^{m_1} \dots (1-\alpha_r z)^{m_r}}$$

Ho descomposem en fraccions simples:

$$A(z) = \sum_{i=1}^{r} \sum_{j=1}^{m_i} \frac{A_{ij}}{(1-\alpha_i z)^j} = \sum_{i=1}^{r} \sum_{j=1}^{m_i} A_{ij} \sum_{n\geq 0} \binom{n+j-1}{n} \alpha_i^n z^n$$

Observem que els coeficients n-èssims d'aquesta sèrie de potències són de la forma

$$a_n = \sum_{i=1}^{r} p_i(n) \alpha_i^n,$$

on α_i són les arrels del polinomi característic de l'equació de recurrència i p_i són polinomis en n de grau menor que m_i (la multiplicitat de l'arrel α_i en el polinomi característic). □

2.5 Equacions de recurrència lineals a coeficients constants no homogènies

Definició 2.5.1 (Equació de recurrència no homogènia)**.** Una equació de recurrència no homogènia lineal i a coeficients constants és una equació de la forma

$$a_n = c_1 + a_{n-1} + \cdots + c_k a_{n-k} + f(n)$$

on f és una funció de n qualsevol.

Volem trobar una expressió de la funció generadora governades per aquest tipus d'equacions de recurrència.

Proposició 2.5.1. *L'equació generadora és*

$$A(z) = \frac{P(z) + F(z)}{1 - c_1 z - \cdots - c_k z^k}$$

on $P(z)$ és un polinomi de grau menor que k i $F(z) = \sum_{n\geq 0} f(n) z^n$.

Demostració. Agafem l'equació de recurrència, multipliquem per z^n als dos costats i sumem $\forall\, n \geq k$, obtenint

$$\sum_{n\geq k} a_n z^n = n \geq k \left(c_1 a_{n-1} + \cdots + c_k a_{n-k} + f(n)\right) z*$$

$$A(z) - \underbrace{\sum_{n=0}^{k} a_n z^n}_{:=A_{k-1}(z)} = c_1 \sum_{n\geq k} a_{n-1} z^n + \cdots + c_k \sum_{n\geq k} a_{n-k} z^n + \sum_{n\geq k} f(n) z^n$$

$$A(z) - A_{k-1}(z) = c_1 z \left(A(z) - A_{k-2}(z)\right) + \cdots + c_k z^k A(z) + F(z) - F_{k-1}(z)$$

$$A(z)\left(1 - c_1 z - \cdots - c_k z^k\right) = P(z) + F(z)$$

□

Per una certa classe de funcions, podem trobar una expressió més explícita de la funció generadora:

Proposició 2.5.2. *Si $f(n) = p(n)\alpha^n$, on $p(n)$ és un polinomi de grau $k-1$ i $\alpha \in \mathbb{C}$, aleshores*

$$F(z) = \frac{P(z)}{(1 - \alpha z)^k}$$

on $P(z)$ és un polinomi de grau menor que k.

Demostració. En primer lloc ho provarem per funcions del tipus $f(n) = n^{k-1}\alpha^n$. Ho provarem per inducció sobre k. Per $k = 1$, $f(n) = \alpha^n \implies F(z) = \dfrac{1}{1 - \alpha z}$.

Per $k > 1$, per hipòtesi d'inducció, tenim que

$$F_{k-1}(z) = \frac{P_{k-1}(z)}{(1 - \alpha z)^{k-1}} = \sum_{n\geq 0} n^{k-2} \alpha^n z^n$$

Derivant aquesta sèrie, veiem que

$$F'_{k-1}(z) = \sum_{n\geq 1} n^{k-1} \alpha^n z^{n-1} = \frac{F_k(z)}{z}$$

Per tant, només hem de veure que $zF'_{k-1}(z)$ té la forma que volem que tingui $F_k(z)$:

$$zF'_{k-1}(z) = z\left(\frac{P_{k-1}(z)}{(1-\alpha z)^{k-1}}\right)' = \frac{P'_{k-1}(z)\,(1-\alpha z)^{k-1} + \alpha(k-1)\,(1-\alpha z)^{k-2}\,P_{k-1}(z)}{(1-\alpha z)^{2k-2}}$$

Simplificant els termes del numerador i denominador, ens queda una expressió de la forma

$$\frac{P_k(z)}{(1-\alpha)^k}$$

tal i com volíem veure. Per extendre-ho a polinomis formats per diversos termes, simplement fa falta aplicar la linealitat. □

Corol·lari 2.5.1. *Si $f(n) = p_1(n)\alpha_1^n + \cdots + p_r(n)\alpha_r^n$, on p_i són polinomis en n de grau menor que k i $\alpha_i \in \mathbb{C}$, aleshores $F(z)$ i $A(z)$ són fraccions racionals.*

Exemple 2.5.1. Suposem que tenim l'equació de recurrència

$$a_n = 10a_{n-1} + n$$

que ens defineix una successió (a_n) a partir de $a_0 = 0$. Aplicant la 1a proposició,

$$F(z) = \sum_{n\geq 0} nz^n = \frac{1}{(1-z)^2} - \frac{1}{1-z} = \frac{z}{(1-z)^2}$$

Per tant,

$$A(z) = \frac{c + \frac{z}{(1-z)^2}}{1-10z} = \frac{c(1-z)^2 + z}{(1-10z)(1-z)^2}$$

Habitualment no substituïm valors de z en $A(z)$, ja que no sabem quan la sèrie és convergent, però sí que sabem que per $z = 0$, $A(z) = a_0$ i convergeix. Per tant, imposant $A(0) = a_0 = 0$, obtenim $c = 0$. El següent pas és transformar-ho en suma de fraccions simples:

$$\frac{z}{(1-10z)(1-z)^2} = z\left(\frac{A}{10-z} + \frac{B}{1-z} + \frac{C}{(1-z)^2}\right) = \sum_{n\geq 0}\left(A10^n + B + (n+1)C\right)z^{n+1}$$

Els nombres $\sqrt{a_{2n+1}}$ són coneguts com nombres esquizofrènics, i presenten moltes propietats interessants. Per exemple, quan són irracionals, presenten expressions decimals molt periòdiques.

2.6 Exemples

2.6.1 Nombres de Stirling de segon ordre

Recordem que definíem els nombres de Stirling de segon ordre

$$\left\{ n \atop k \right\}$$

com el nombre de particions de $[n]$ en k parts.
Sigui $S_k(z) = \sum_{n\geq 0} \left\{ {n \atop k} \right\} z^n$, amb $\left\{ {0 \atop 0} \right\} = 1$. Per trobar la funció generadora, utilitzarem la següent recurrència:

$$\left\{ {n \atop k} \right\} + \left\{ {n-1 \atop k-1} \right\} + k \left\{ {n-1 \atop k} \right\}$$

que es compleix per $n \geq k \geq 1$. Aleshores,

$$\sum_{n\geq k} \left\{ {n \atop k} \right\} z^n = \sum_{n\geq k} \left\{ {n-1 \atop k-1} \right\} z^n + k \sum_{n\geq k} \left\{ {n-1 \atop k} \right\} z^n = zS_{k-1}(z) + kzS_k(z)$$

Aïllant, tenim que

$$S_k(z) = \frac{z}{1-kz} S_{k-1}(z) = \frac{z^k}{(1-kz)(1-(k-1)z)\dots(1-z)}$$

Descomposant-ho en fraccions simples, tenim que

$$S_k(z) = z^k \left(\sum_{j=1}^{k} \frac{A_j}{1-jz} \right)$$

Per a trobar els A_j, tenim en compte que

$$\frac{1}{(1-z)\dots(1-kz)} = \frac{A_1}{1-z} + \dots + \frac{A_k}{1-kz}$$

Per tant, per a un cert i fix,

$$\frac{1-iz}{(1-z)\dots(1-kz)} = \frac{1}{(1-z)\dots(1-(i-1)z)(1-(i+1)z)\dots(1-kz)} = A_i + \sum_{\substack{j=1 \\ j\neq i}}^{k} \frac{A_j(1-iz)}{(1-jz)}$$

Evaluant a $z = 1/i$, tenim que

$$A_i = \frac{1}{(1-z)\dots(1-(i-1)z)(1-(i+1)z)\dots(1-kz)} = \frac{i^{k-1}(-1)^{k-i}}{(i-1)!(k-i)!}$$

Aleshores, la funció generadora és

$$S_k(z) = z^k \left(\sum_{j=1}^{k} \frac{A_j}{1-jz} \right) = z^k \left(\sum_{j=1}^{k} A_j \sum_{n\geq 0} j^n z^n \right) = \sum_{n\geq 0} \left(\sum_{j=1}^{k} \frac{j^{k-1}(-1)^{k-j}}{(j-1)!(k-j)!} j^n z^{n+k} \right)$$

Els nombres de Stirling de segon ordre seran els coeficients d'aquesta sèrie:

$$\left\{ {n \atop k} \right\} = \sum_{j=1}^{k} \frac{j^{n-1}(-1)^{k-j}}{(j-1)!(k-j)!} = \frac{1}{k!} \sum_{j=1}^{k} \binom{k}{j} j^n (-1)^{k-j}$$

fórmula a la qual ja havíem arribat en el capítol anterior.

2.6.2 Nombres de Catalan

Sigui S_n el conjunt de seqüències de -1's i 1's que sumen 0. Veiem que

$$s_n = |S_n| = \begin{cases} \binom{2m}{m} & n = 2m \text{ parell} \\ 0 & n \text{ senar} \end{cases}$$

Una pregunta natural que ens podem fer a continuació és quantes d'aquestes seqüències no tenen cap suma parcial negativa?

Definició 2.6.1 (Nombres de Catalan)**.** Sigui $C_n = \{(x_1, \ldots, x_{2n}) \in S_{2n} : \sum_{i=1}^{k} x_i \geq 0,\ \forall\, k \in [2n]\}$. Aleshores diem que $c_n = |C_n|$ és l'n-èssim *nombre de Catalan.*

Per visualitzar millor aquestes seqüències, s'acostumen a utilitzar els camins de Dyck:

Definició 2.6.2 (Camí de Dyck)**.** Camins de $(0,0)$ a $(0,2n)$ a $\mathbb{Z}^2$ amb passes $(1,1)$ i $(1,-1)$ i que mai creuen l'eix d'abscisses.

Es pot veure fàcilment que hi ha una bijecció entre els camins de Dyck de longitud $2n$ i les seqüències de Catalan de longitud $2n$, de manera que a partir d'ara ens hi referirem indistintament.

Per comptar el nombre de camins, definim $C_{n,k}$ com el conjunt de camins de Dyck de llargada $2n$ i que toca per primer cop l'eix d'abscisses al punt $(2k, 0)$. Observem que el nombre de camins d'aquest tipus és el nombre de camins de llargada $2k-2$ (pel primer tram) multiplicat pel nombre de camins de llargada $2n-2k$. Per tant,

$$c_{n,k} = c_{k-1} \cdot c_{n-k}$$

Aleshores,

$$c_n = \sum_{k=1}^{n} c_{n,k} = \sum_{k=1}^{n} c_{k-1} \cdot c_{n-k} = \sum_{k=0}^{n-1} c_k \cdot c_{n-k-1}$$

on definim $c_0 = 1$.

Aquesta equació de recurrència no és lineal, de manera que no podem aplicar els mètodes vists anteriorment. Observem però que l'equació de recurrència pren la forma d'un producte de convolució, cosa que ens indica que ho podrem expressar com el producte de dues sèries.

Sigui $C(z)$ la seva funció generadora, veiem que

$$C(z) = \sum_{n\geq 0} c_n z^n = 1 + \sum_{n\geq 1} \left(\sum_{k=0}^{n-1} c_k c_{(n-1)-k} \right) z^{n-1} = 1 + z\,(C(z))^2$$

Resolent-ho tal com resoldríem una equació de segon grau, tenim que

$$zC(z)^2 - C(z) + 1 = 0 \implies C(z) = \frac{1 \pm \sqrt{1-4z}}{2z},$$

on considerem que $C(0) = 1 = c_0$.

D'aquestes dues expressions, ens convé agafar la de signe menys, ja que si no per $z \to 0$ tindríem $C(z) = 2/0 = \infty$. Per tant, pendrem la funció generadora

$$C(z) = \frac{1 - \sqrt{1-4z}}{2z}$$

Observem que la z dividint no ens provoca cap indeterminació en $z = 0$, ja que

$$\begin{aligned} C(z) &= \frac{1}{2z}\left(1 - (1-4z)^{1/2}\right) = \frac{1}{2z}\left(1 - \sum_{n\geq 0}\binom{1/2}{n}4^n z^n (-1)^n\right) \\ &= \frac{1}{2}\sum n \geq 1 \binom{1/2}{n} 4^n z^{n-1}(-1)^{n-1} \end{aligned}$$

Els nombres de Catalan seran els coeficients d'aquesta sèrie de potències:

$$c_n = \frac{1}{2}\binom{1/2}{n+1}(-1)^n 4^{n+1}$$

Per expressar-ho de manera més senzilla, observem que

$$\binom{1/2}{n} = \frac{1}{n!}\frac{(2n-3)!!}{2^n}(-1)^{n-1}$$

Substituint-ho en l'expressió anterior, tenim que

$$c_n = \frac{1}{2}\frac{1}{(n+1)!}\frac{(2n-1)!!}{2^{n+1}}4^{n+1} = \frac{2^n}{(n+1)!}(2n-1)!!$$

Completant el doble factorial amb els nombres parells, veiem que

$$c_n = \frac{2^n}{n+1}\frac{(2n)!}{2^n n! n!} \implies c_n = \frac{1}{n+1}\binom{2n}{n}$$

2.6.3 Particions d'enters

Recordem que havíem definit les particions de n com el nombre de solucions de $x_1 + \cdots + x_n = n$, amb $x_1 \geq \cdots \geq x_n \geq 0$ enters no negatius. La seva funció generadora associada és

$$P(z) = \sum_{n\geq 0} p(n) z^n$$

En primer lloc, estudiarem el nombre de particions de n tals $\forall i \in [n]$, $1 \leq x_i \leq k$. Euler va trobar que la seva funció generadora és

$$P_{\{1,\ldots,k\}}(z) = \prod_{i=1}^{k} \frac{1}{1-z^i}$$

Demostració.

$$\prod_{i=1}^{k} \frac{1}{1-z^i} = \left(\sum_{n\geq 0} z^n\right) \cdots \left(\sum_{n\geq 0} z^{kn}\right)$$
$$= \sum_{n\geq 0} (\#\text{ nombre de solucions de } n = n_1 + 2n_2 + \cdots + kn_k)\, z^n$$

Observem que aquest coeficient es correspon amb $p_{\{1,\ldots,k\}}(n)$, ja que

$$n = n_1 + 2n_2 + \cdots + kn_k \iff n = \underbrace{1+\cdots+1}_{n_1} + \underbrace{2+\cdots+2}_{n_2} + \cdots + \underbrace{k+\cdots+k}_{n_k}$$

□

És interessant observar que aquest nombre és igual al nombre de particions de com a molt k parts:

$$p_{\{1,\ldots,k\}}(n) = p_{\leq k}(n)$$

Això es deu a que podem expressar les particions com a diagrames de Ferrers. Depenent de si els llegim per files o per columnes, obtenim un tipus de particions o l'altre. Per exemple, suposem que interpretem la longitud de la i-èssima fila del diagrama de Ferrers com x_i. Aleshores, $p_{\{1,\ldots,k\}}(n)$ és el nombre de diagrames amb files de longitud menor que k. Invertint el diagrama, obtenim un diagrama amb k files o menys, cosa que es correspon a una partició amb com a molt k parts, que pertany a $p_{\leq k}(n)$.

A partir de la funció generadora anterior, Euler va suposar que la funció generadora de les particions (on hi poden haver tants grups com es vulguin) seria

$$P(z) = \prod_{k=1}^{\infty} \frac{1}{1-z^k}$$

A variable complexa es veurà amb més detall el comportament d'aquesta funció.

Aquests resultats es poden generalitzar, i per exemple el nombre de particions que només utilitzen els nombres 2, 7 i 9 té la funció generadora

$$P_{\{2,7,9\}}(z) = \frac{1}{1-z^2}\frac{1}{1-z^7}\frac{1}{1-z^9} = \frac{1}{1-z^2-z^7+z^{11}+z^{16}-z^{18}}$$

Quan expressem aquesta sèrie com a fraccions simples, tenim que

$$P_{\{2,7,9\}}(z) = \frac{A}{(1-z)^3} + \frac{B}{(1-z)^2} + \frac{C}{(1-z)} + \sum \frac{C_i}{1-\alpha_i z}$$

i el terme dominant del coeficient n-èssim serà el corresponent a la primera fracció, que serà

$$\binom{n+2}{n} = \mathcal{O}(n^2)$$

Aquest problema, el problema de trobar el nombre de particions amb un conjunt finit de summands possibles es coneix com el problema del canvi de Polya.

Teorema 2.6.1 (Euler)**.** *Sigui $p_1(n)$ el nombre de particions de n en parts senars, i sigui $p_d(n)$ el nombre de particions de n en parts diferents. Aleshores,*

$$p_d(n) = p_1(n)$$

Demostració. La funció generadora és

$$\begin{aligned} P_d(z) &= \sum_{n\geq 0} p_d z^n = (1+z)(1+z^2)\cdots = \prod_{k\geq 1}(1+z^k) \\ &= \prod_{k\geq 1}(1+z^k)\left(\frac{1-z^k}{1-z^k}\right) = \prod_{k\geq 1}\frac{1-z^{2k}}{1-z^k} \\ &= \prod_{k\geq 1}\frac{1}{1-z^{2k-1}} = P_1(z) \end{aligned}$$

Donat que les funcions generadores són iguals, el nombre de particions de n de cada tipus també serà igual per qualsevol n. □

3

Probabilitat Discreta

3.1 Espais de probabilitat

Per definir matemàticament el concepte de probabilitat, definirem els esdeveniments aleatoris com subconjunts d'un conjunt de referència, que anomenarem espai mostral.

Definició 3.1.1 (Espai mostral)**.** Un espai mostral és un parell $(\Omega, \mathcal{A})$ on Ω és un conjunt i $\mathcal{A} \subset 2^\Omega$ és una família de subconjunts de Ω que satisfà les següents propietats:

1. $\Omega \in \mathcal{A}$.
2. Si $A \in \mathcal{A}$, aleshores $\Omega \setminus A = \bar{A} \in \mathcal{A}$.
3. Si $(A_n)_{n\geq 1}$ és una successió de conjunts de $\mathcal{A}$, aleshores $\bigcup_{n\geq 1} A_n \in \mathcal{A}$.

Les famílies de subconjunts que compleixen les propietats anteriors s'anomenen σ-àlgebres:

Definició 3.1.2 (σ-àlgebra)**.** Una σ-àlgebra de conjunts de Ω és una família de subconjunts de Ω que conté a Ω i que és tancada per unions numerables i complements.

Proposició 3.1.1. *Sigui $\mathcal{A}$ una σ-àlgebra de conjunts de Ω. Aleshores,*

1. *$\emptyset \in \mathcal{A}$.*
2. *Si $(A_n)_{n\geq 1}$ és una successió de conjunts de $\mathcal{A}$, aleshores $\bigcap_{n\geq 1} A_i \in \mathcal{A}$.*

Demostració. Per la primera, només cal veure que $\emptyset = \bar{\Omega}$. Per la segona, donat que $\bar{A}_n \in \mathcal{A}$ per tot n,

$$\bigcup_{n\geq 1} \bar{A}_n \in \mathcal{A} \implies \overline{\bigcup_{n\geq 1} \bar{A}_n} = \bigcap_{n\geq 1} A_i \in \mathcal{A}$$

on hem aplicat una de les lleis de Morgan. □

Exemple 3.1.1. Considerem que tirem un dau. El conjunt d'esdeveniments possibles formen el conjunt $\Omega = \{1, 2, 3, 4, 5, 6\}$. A partir dels esdeveniments elementals, podem definir altres esdeveniments, com "sortir parell" o "sortir més gran que 2", que es corresponen als subconjunts $\{2, 4, 6\}$ i $\{3, 4, 5, 6\}$. La combinació d'esdeveniments amb els connectors lògics $\vee$, $\wedge$ o $\neg$ es pot traslladar a combinació de conjunts mitjançant $\cup$, $\cap$ i complements.

Així doncs, l'esdeveniment "sortir parell i més gran que 2" es correspon a $A \cap B = \{4, 6\}$, mentre que "sortir imparell o més gran que 2" és $\bar{A} \cup B = \{1, 3, 4, 5, 6\}$.

Els exemples més senzills de σ-àlgebres són $\mathcal{A} = \{\emptyset, \Omega\}$, la σ-àlgebra trivial, i $\mathcal{A} = 2^\Omega$, la de tots els subconjunts de Ω.

Proposició 3.1.2. *Siguin $\mathcal{A}$ i $\mathcal{B}$ dues σ-àlgebres. Aleshores, la seva intersecció $\mathcal{C} = \mathcal{A} \cap \mathcal{B}$ és una σ-àlgebra.*

Demostració.

1. $\Omega \in \mathcal{A}, \mathcal{B} \implies \Omega \in \mathcal{A} \cap \mathcal{B} = \mathcal{C}$.
2. $A \in \mathcal{C} \implies A \in \mathcal{A}, \mathcal{B} \implies \bar{A} \in \mathcal{A}, \mathcal{B} \implies \bar{A} \in \mathcal{C}$.
3. $(A_n)_n \in \mathcal{C} \implies (A_n)_n \in \mathcal{A}, \mathcal{B} \implies \bigcup (A_n)_n \in \mathcal{A}, \mathcal{B} \implies \bigcup (A_n)_n \in \mathcal{C}$.

□

Donat que no tota família de subconjunts és una σ-àlgebra, a vegades ens interessa saber quina és la σ-àlgebra més petita que conté una certa família de subconjunts:

Definició 3.1.3. Sigui $\mathcal{A}_0 \subset 2^\Omega$ una família de subconjunts de Ω. Definim la σ-àlgebra $\langle \mathcal{A}_0 \rangle$ generada per $\mathcal{A}_0$ com la menor σ-àlgebra que conté $\mathcal{A}_0$. Equivalentment,

$$\langle \mathcal{A}_0 \rangle = \bigcap_{\mathcal{A} \supset \mathcal{A}_0} \mathcal{A}$$

Per exemple, donat un conjunt $A \subset \Omega$, la σ-àlgebra que genera és $\langle A \rangle = \{\emptyset, A, \bar{A}, \Omega\}$.

Definició 3.1.4 (Probabilitat)**.** Una probabilitat sobre un espai mostral $(\Omega, \mathcal{A})$ és una aplicació $\Pr : \mathcal{A} \longrightarrow [0, 1]$, que satisfà que

1. $\Pr(\Omega) = 1$.
2. Si $(A_n)_{n \geq 1}$ és una successió de conjunts de $\mathcal{A}$ disjunts dos a dos, $\Pr(\bigcup A_n) = \sum \Pr(A_n)$.

Definició 3.1.5 (Espai de probabilitat)**.** Un espai de probabilitat és una terna $(\Omega, A, \Pr)$ on $\mathcal{A}$ és una σ-àlgebra de conjunts de Ω i Pr és una probabilitat sobre $(\Omega, \mathcal{A})$. Direm que aquest espai és *discret* si Ω és numerable.

Algunes propietats immediates de la definició són:

Proposició 3.1.3.

1. *$Pr(\bar{A}) = 1 - Pr(A)$.*
2. *Si $A \subset B$, aleshores $Pr(A) \leq Pr(B)$.*
3. *$Pr(A \cup B) = Pr(A) + Pr(B) - Pr(A \cap B)$.*
4. *Si $(A_n)_{n\geq 0}$ és una successió de subconjunts de $\mathcal{A}$, $Pr(\cup_{n\geq 0} A_n) \leq \sum_{n\geq 0} Pr(A_n)$.*
5. *Si l'espai és discret i $\mathcal{A}$ conté els elements de Ω, $Pr(A) = \sum_{\omega\in A} Pr(\{\omega\})$.*

Demostració. A classe es va deixar com a exercici.

1. Sigui $A \in \mathcal{A}$. A i $\bar{A}$ són disjunts, de manera que $\Pr(A\cup\bar{A}) = \Pr(A)+\Pr(\bar{A}) \implies \Pr(\bar{A}) = \Pr(\Omega) - \Pr(A) = 1 - \Pr(A)$.
2. Si $A \subset B$, $A \cap \bar{B} = \emptyset$. A més, $A \cup \bar{B} \in \mathcal{A}$. Aleshores,
$$\Pr(A) + \Pr(\bar{B}) = \Pr(A \cup \bar{B}) \leq 1 \implies \Pr(A) \leq 1 - (1 - \Pr(B)) = \Pr(B)$$
3. Observem que $A \setminus (A \cap B)$, $B \setminus (A \cap B)$ i $A \cap B$ són disjunts. Per tant,
$$\begin{aligned}\Pr(A \cup B) &= \Pr(A \setminus (A \cap B)) + \Pr(B \setminus (A \cap B)) + \Pr(A \cap B) = \\ &= \Pr(A) + \Pr(B) - \Pr(A \cap B)\end{aligned}$$
4. Donada una successió $(A_n)_{n\geq 0} \subset \mathcal{A}$, tenim que
$$\bigcup_{n\geq 0} A_n = \bigsqcup_{n\geq 0} \left(A_n \setminus \bigcup_{i=0}^{n-1} A_i \right)$$
Aleshores, aplicant primer 3.1.3 i després 2:
$$\Pr(\cup_{n\geq 0} A_n) = \sum_{n\geq 0} \Pr(A_n \setminus \cup_{i=0}^{n-1} A_i) \leq \sum_{n\geq 0} \Pr(A_n)$$
5. Sigui $A \in \Omega$. Donat que l'espai és discret, $A = \bigsqcup_{n\geq 1}\{\omega_n\}$. Per hipòtesi, tots els $\{\omega_i\}$ pertanyen a $\mathcal{A}$, de manera que
$$\Pr(A) = \sum_{n\geq 1} \Pr(\{\omega_n\})$$

□

Observem que si $\Omega = \{\omega_1, \omega_2, \dots\}$ és un conjunt numerable i $\mathcal{A} = 2^\Omega$, aleshores qualsevol assignació de $\Pr(\omega_i) = p_i$, amb $0 \leq p_i \leq 1$ i $\sum_i p_i = 1$ és una probabilitat sobre $(\Omega, \mathcal{A})$.

En particular, si Ω és un conjunt finit i $\Pr(\omega) = 1/|\Omega|$ per a tot $\omega \in \Omega$, aleshores, per a qualsevol subconjunt $A \subset \Omega$,

$$\Pr(A) = \frac{|A|}{|\Omega|}$$

En aquest cas es diu que Pr és una distribució *uniforme* sobre Ω i el càlcul de probabilitats és equivalent a l'enumeració de conjunts.

La fórmula d'inclusió-exclusió té una formulació anàloga en probabilitats, que presentarem a continuació. En el cas de la distribució uniforme, és equivalent al principi d'inclusió-exclusió en enumeració, de manera que és una extensió a qualsevol distribució de proabbilitat d'aquest principi enumeratiu.

Proposició 3.1.4 (Fórmula d'inclusió-exclusió)**.** *Siguin $A_1, \dots, A_n$ successos en un espai de probabilitat $(\Omega, \mathcal{A}, Pr)$. Aleshores,*

$$Pr(\cap_{i=1}^n \bar{A}_i) = \sum_{I \subset [n]} (-1)^{|I|+1} Pr(\cap_{i \in I} A_i)$$

Demostració. La demostració la veurem més endavant, com a cas particular d'un resultat més general. □

3.2 Independència i probabilitat condicionada

Definició 3.2.1 (Independència)**.** Sigui $(\Omega, \mathcal{A}, \Pr)$ un espai de probabilitat. Es diu que $A, B \in \mathcal{A}$ són independents si

$$\Pr(A \cap B) = \Pr(A) \cdot \Pr(B)$$

En general, direm que una família de conjunts $A_1, \dots, A_n$ és independent si, per a qualsevol subconjunt $I \subset [n]$,

$$\Pr(\cap_{i \in I} A_i) = \prod_{i \in I} \Pr(A_i)$$

És important tenir en compte que la independència d'una família de conjunts és una propietat global de la família i que, per tant, no és suficient ni que els conjunts siguin independents dos a dos ni que

$$\Pr(\cap_{i=1}^n A_i) = \prod_{i=1}^n \Pr(A_i)$$

Exemple 3.2.1. Sigui $\Omega = \{\omega_1, \omega_2, \omega_3, \omega_4, \omega_5\}$, amb

$$\Pr(\omega_1) = 1/8, \quad \Pr(\omega_2) = \Pr(\omega_3) = \Pr(\omega_4) = 3/16, \quad \Pr(\omega_5) = 5/16$$

Siguin $A = \{\omega_1, \omega_2, \omega_3\}$, $B = \{\omega_1, \omega_2, \omega_4\}$ i $C = \{\omega_1, \omega_3, \omega_4\}$. Aleshores, veiem que

$$\Pr(A) = \Pr(B) = \Pr(C) = \frac{1}{2}$$
$$\Pr(A \cap B \cap C) = \frac{1}{8} = \Pr(A)\Pr(B)\Pr(C)$$

però en canvi

$$\Pr(A \cap B) = \frac{5}{16} \neq \frac{1}{4} = \Pr(A)\Pr(B)$$

de manera que A, B i C no són independents.

Un exemple de que la independència dos a dos tampoc garantitza la independència global és el següent:

Exemple 3.2.2. Sigui

$$\Omega = \{0,1\}^n = \{(x_1, \ldots, x_n) : x_i \in \{0,1\}\}$$

el conjunt de seqüències binàries de llargada n. Sigui A_{ij} l'esdeveniment $x_i = x_j$. Aleshores, és fàcil comprovar que A_{12}, A_{13} i A_{23} són independents dos a dos, però no ho són en conjunt, ja que

$$\Pr(A_{12} \cap A_{23} \cap A_{12}) = \frac{1}{4} \neq \frac{1}{8} = \Pr(A_{12})\Pr(A_{23})\Pr(A_{13})$$

Quan dos esdeveniments A, B no són independents, la probabilitat de la seva intersecció pot ser més gran o més petita que $\Pr(A)\Pr(B)$ en funció de la dependència que hi ha entre els dos esdeveniments. Aquesta dependència es mesura mitjançant el concepte de probabilitat condicionada:

Definició 3.2.2 (Probabilitat condicionada)**.** Sigui $(\Omega, \mathcal{A}, \Pr)$ un espai de probabilitat i sigui $B \in \mathcal{A}$ amb $\Pr(B) > 0$. Definim la probabilitat condicionada a B com la probabilitat sobre $(\Omega, \mathcal{A})$ donada per l'aplicació

$$\begin{aligned} \Pr(\cdot|B) : &\mathcal{A} \longrightarrow [0,1] \\ &A \mapsto \frac{\Pr(A \cap B)}{\Pr(B)} \end{aligned}$$

Demostració. Per tal que la definició tingui sentit, hem de veure que $\Pr(\cdot|B)$ és efectivament una probabilitat. En primer lloc,

$$\Pr(\Omega|B) = \frac{\Pr(\Omega \cap B)}{\Pr(B)} = \frac{\Pr(B)}{\Pr(B)} = 1$$

Donada una família numerable de conjunts $(A_n)_n$ disjunts dos a dos,

$$\begin{aligned} \Pr(\cup_n A_n|B) &= \frac{\Pr((\cup_n A_n) \cap B)}{\Pr(B)} = \frac{\Pr(\cup_n (A_n \cap B))}{\Pr(B)} = \frac{\sum_n \Pr(A_n \cap B)}{\Pr(B)} \\ &= \sum_n \frac{\Pr(A_n \cap B)}{\Pr(B)} = \sum_n \Pr(A_n|B) \end{aligned}$$

on s'ha utilitzat que si A_i i A_j són disjunts, aleshores $A_i \cap B$ i $A_j \cap B$ també. □

La probabilitat condicionada és una renormalitació de la probabilitat dins el nou espai mostral definit pel subconjunt B. S'interpreta com la probabilitat d'un esdeveniment "sabent que B s'ha realitzat" (ja que $\Pr(B|B) = 1$ i per tant B és un esdeveniment segur).

Observem que A i B (successos amb probabilitat no nul·la) són independents si i només si

$$\Pr(A|B) = \Pr(A) \quad \text{i} \quad \Pr(B|A) = \Pr(B)$$

Per tant, intuitivament, A i B són independents si el fet que ocorri B no altera la probabilitat de que ocorri A, i viceversa.

La probabilitat condicionada ens permet escriure una fórmula general per la probabilitat de la intersecció:

Proposició 3.2.1. *Siguin $A_1, \dots, A_n$ successos en un espai de probabilitat amb $Pr(A_i) > 0$ per a tot i. Aleshores,*

$$Pr(\cap_{i=1}^n A_i) = Pr(A_1)Pr(A_2|A_1)Pr(A_3|A_1 \cap A_2) \dots Pr(A_n|A_1 \cap A_2 \cap \dots \cap A_{n-1})$$

Demostració. Es comprova substituint a la dreta per la definició de probabilitat condicionada i simplificant els factors repetits. □

En moltes situacions, tenim informació sobre les probabilitats condicionades i volem trobar la probabilitat sense condicionar. En aquests casos utilitzarem la fórmula de probabilitat total:

Proposició 3.2.2 (Fórmula de probabilitat total)**.** *Sigui $B_1, \dots, B_n$ una partició de Ω en un espai de probabilitat $(\Omega, \mathcal{A}, Pr)$. Si $Pr(B_i) > 0$ per a tot i, aleshores, per a qualsevol $A \in \mathcal{A}$,*

$$Pr(A) = Pr(A|B_1)Pr(B_1) + \dots + Pr(A|B_n)Pr(B_n)$$

Demostració. Observem que $A = (A \cap B_1) \sqcup \dots \sqcup (A \cap B_n)$. Per tant,

$$\Pr(A) = \Pr(A \cap B_1) + \dots + \Pr(A \cap B_n) = \Pr(A|B_1)\Pr(B) + \dots + \Pr(A|B_n)\Pr(B_n)$$

□

En particular, si $0 < \Pr(B) < 1$,

$$\Pr(A) = \Pr(A|B)\Pr(B) + \Pr(A|\bar{B})\Pr(\bar{B})$$

Sovint, de les dues probabilitats condicionades $\Pr(A|B)$ i $\Pr(B|A)$ n'hi ha una que és més fàcil de calcular. La fórmula de Bayes ens permet relacionar-les:

Proposició 3.2.3 (Fórmula de Bayes)**.** *Siguin A, B esdeveniments en un espai de probabilitat amb $Pr(A), Pr(B) > 0$. Aleshores,*

$$Pr(A|B) = \frac{Pr(B|A)Pr(A)}{Pr(B|A)Pr(A) + Pr(B|\bar{A})Pr(\bar{A})}$$

Demostració. De la definició de probabilitat condicionada,

$$\Pr(A|B)\Pr(B) = \Pr(A \cap B) = \Pr(B|A)\Pr(A)$$

Aplicant la fórmula de la probabilitat total,

$$\Pr(A|B) = \frac{\Pr(B|A)\Pr(A)}{\Pr(B)} = \frac{\Pr(B|A)\Pr(A)}{\Pr(B|A)\Pr(A) + \Pr(B|\bar{A})\Pr(\bar{A})}$$

□

3.3 Variables aleatòries

Habitualment s'identifiquen els esdeveniments d'un espai de probabilitat amb nombres reals. Així aconseguim estandaritzar la teoria de probabilitat i no hem de treballar amb esdeveniments arbitraris, sinó amb esdeveniments representats per nombres reals. Per exemple, el resultat de tirar una moneda s'identifica amb $\Omega = \{0, 1\}$ i el de tirar un dau amb $\Omega = \{1, \ldots, 6\}$. La definició formal és la següent:

Definició 3.3.1 (Variable aleatòria)**.** Una variable aleatòria sobre un espai de probabilitat $(\Omega, \mathcal{A}, \Pr)$ és una aplicació $X : \Omega \longrightarrow \mathbb{R}$ tal que, $\forall x \in \mathbb{R}$, el conjunt $\{\omega \in \Omega : X(\omega) \leq x\}$ pertany a $\mathcal{A}$.

Direm que la variable aleatòria X és discreta si $\mathrm{Im}(X)$ és numerable.

En la definició es vol assegurar que, per a cada $x \in \mathbb{R}$, el conjunt $X^{-1}((-\infty, x]) = \{\omega \in \Omega : X(\omega) \leq x\}$ pertany a la σ-àlgebra $\mathcal{A}$, i que per tant se'n pot calcular la probabilitat. En particular, podrem calcular la probabilitat dels esdeveniments $X^{-1}(A) = \{\omega \in \Omega : X(\omega) \in A\}$ per a tots els conjunts $A \subset \mathbb{R}$ que pertanyen a la σ-àlgebra generada pels intervals de la forma $(-\infty, x]$. Aquesta família de subconjunts de $\mathbb{R}$, que conté tots els intervals oberts, s'anomena la σ-àlgebra de Borel de $\mathbb{R}$, i es denota per $\mathcal{B}(\mathbb{R})$.

Observació. Per a $a, b \in \mathbb{R}$, $a < b$, els intervals $(-\infty, a)$, (a, ∞), (a, b), $(a, b]$ i $[a, b]$ formen part de la σ-àlgebra de Borel.

Demostració. En els apunts oficials es deixa com a exercici.

- $(-\infty, a) = \bigcup_{n \geq 1} (-\infty, a - 1/n]$
- $(a, \infty) = (-\infty, a]^c$
- $(a, b) = (-\infty, b) \cap (a, \infty)$
- $(a, b] = (-\infty, b] \cap (a, \infty)$
- $[a, b] = \bigcap_{n \geq 1} (a - 1/n, b]$

□

Observem aleshores que amb la σ-àlgebra de Borel tindrem definida la probabilitat de què X es trobi en un d'aquests intervals.

La distribució de probabilitat d'una variable discreta s'identifica amb la seva *funció de distribució de probabilitat* i la seva *funció de probabilitat*.

Definició 3.3.2 (Funció de probabilitat)**.** La funció de probabilitat d'una variable aleatòria discreta és una aplicació de $\mathrm{Im}(X)$ a $\mathbb{R}$ definida com $\Pr(X = x) := \Pr(\{\omega \in \Omega : X(\omega) = x\})$.

Definició 3.3.3 (Funció de distribució de probabilitat)**.** La funció de distribució de probabilitat d'una variable aleatòria X és l'aplicació

$$\begin{aligned} F_X : \mathbb{R} &\longrightarrow [0,1] \\ x &\mapsto \Pr(X \leq x) \end{aligned}$$

on definim $\{X \leq x\} := \{\omega \in \Omega : X(\omega) \leq x\}$.

Observem que la funció de distribució d'una variable aleatòria discreta és una funció esglaonada, amb discontinuïtats de salt en els x tals que $\Pr(X = x) > 0$, com es pot veure a la figura 3.1.

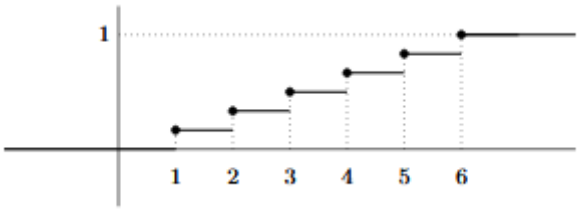

Figura 3.1: Funció distribució de probabilitat pel llançament d'un dau

Per tal de dir que dues variables aleatòries són independents, demanarem que tots els esdeveniments associats a cadascuna de les variables aleatòries siguin independents:

Definició 3.3.4 (Independència de variables aleatòries)**.** Dues variables aleatòries són independents si els esdeveniments $\{X \leq x\}$ i $\{Y \leq y\}$ són independents per a cada $x, y \in \mathbb{R}$.

Si X i Y són variables aleatòries discretes, una definició equivalent és que els esdeveniments $\{X = x\}$ i $\{Y = y\}$ són independents per a cada $x, y \in \mathbb{R}$.

Amb un lleuger abús de notació, escriurem $\{X = x, Y = y\}$ per referir-nos a la intersecció $\{X = x\} \cap \{Y = y\}$. Així doncs, dues variables aleatòries discretes són independents si

$$\Pr(X = x, Y = y) = \Pr(X = x) \Pr(Y = y), \quad \forall x, y \in \mathbb{R}$$

3.4 Models discrets de probabilitat

En aquesta secció estudiarem alguns models aleatoris bàsics a partir dels quals es poden estudiar fenòmens aleatoris més complexos.

3.4.1 Uniforme

Suposem que tenim una variable aleatòria X que pren valors en un conjunt finit $\{a_1, \ldots, a_n\}$.

Definició 3.4.1 (Distribució uniforme)**.** Direm que X segueix una distribució uniforme si $\forall i \in [n]$,

$$\Pr(X = a_i) = \frac{1}{n}$$

Per denotar-ho, escriurem $X \sim U(n)$. Sense pèrdua de generalitat, considerarem aleshores que X pren valors en $[n]$.

En un model uniforme, el càlcul de probabilitats està relacionat directament amb la enumeració, ja que per qualsevol subconjunt $A \subset [n]$, tenim la fórmula clàssica de "casos favorables entre casos possibles":

$$\Pr(X \in A) = \frac{|A|}{n}$$

3.4.2 Bernouilli

Considerem un espai de probabilitat $(\Omega, \mathcal{A}, \Pr)$ i un esdeveniment $A \in \mathcal{A}$. En el model de Bernouilli, només es considera si A ha succeït o no. És a dir, el model de Bernouilli pren un cert $A \in \mathcal{A}$ i associa els $\omega \in A$ amb un resultat positiu ($X(\omega) = 1$) i els $\omega \notin A$ amb un resultat negatiu ($X(\omega) = 0$). A aquesta variable aleatòria la denominarem 1_A:

$$1_A(\omega) := \begin{cases} 1, & \omega \in A \\ 0, & \omega \notin A \end{cases}$$

La seva funció de probabilitat ve donada per

$$\begin{cases} \Pr(1_A = 1) = p \\ \Pr(1_A = 0) = 1 - p \end{cases}$$

Quan X segueix una distribució de Bernouilli on $\Pr(A) = \Pr(1_A = 1) = p$, ho denotarem com $X \sim B(p)$.

3.4.3 Binomial

En el model binomial considerem una experiència de Bernouilli (i.e, en la qual només ens fixem en si un esdeveniment A es produeix o no) i la repetim un nombre n fix de vegades. La variable aleatòria binomial compta el nombre d'"èxits" en les n repeticions (i.e, el nombre de vegades que ha succeït A).

Els paràmetres de la distribució binomial són el nombre de repeticions n i la probabilitat d'èxit p. Escriurem per tant $X \sim \text{Bin}(n, p)$. Cada resultat es pot identificar amb una seqüència binària $(x_1, \ldots x_n)$, amb $x_i \in \{0, 1\}$, on X compta el nombre de 1's. Com que les repeticions

són independents, la probabilitat d'una seqüència amb k 1's és $p^k(1-p)^{n-k}$, de manera que la funció probabilitat és

$$\Pr(X=k)=\binom{n}{k}p^k(1-p)^{n-k},\ \text{amb } k=0,1,\dots,n$$

Observem que, en general, si $X_1,\dots,X_n$ són variables aleatòries de Bernouilli, $X_i\sim B(p)$, i independents entre elles, aleshores $X=X_1+\cdots+X_n$ segueix la distribució binomial $X\sim \text{Bin}(n,p)$.

3.4.4 Poisson

En una funció de probabilitat amb n gran i p petita, el coeficient binomial pot ser molt gran i les potències de p molt petites, de manera que resulta poc eficient calcular numèricament la funció de probabilitat. En aquesta situació, molt freqüent en la pràctica, podem aproximar la distribució binomial asimptòticament:

Proposició 3.4.1. *Sigui $X_n\sim Bin(n,\lambda/n)$ per a un cert $\lambda\in\mathbb{R}^+$. Aleshores, $\forall\, k\in\{0,1,\dots,n\}$,*

$$\lim_{n\to\infty}\Pr(X_n=k)=\frac{\lambda^k}{k!}e^{-\lambda}$$

Demostració. Sigui $p_n=\lambda/n$. Per a k fix i $n\to\infty$, tenim

$$\Pr(X_n=k)=\binom{n}{k}p_n^k(1-p_n)^{n-k}\sim\frac{n^k}{k!}p_n^k(1-p_n)^{n-k}=\frac{(np_n)^k}{k!}\underbrace{\left(1-\frac{\lambda}{n}\right)^n}_{\sim e^{-\lambda}}\underbrace{(1-p_n)^{-k}}_{\sim 1}\sim\frac{\lambda^k}{k!}e^{-\lambda}$$

□

La variable aleatòria X que prèn valors de naturals amb la funció de probabilitat

$$\Pr(X=k)=\frac{\lambda^k}{k!}e^{-\lambda},\ \text{per } k=0,1,2,\dots,$$

es coneix amb el nom de *variable aleatòria de Poisson*, i escriurem que $X\sim\text{Pois}(\lambda)$. Com hem vist abans, un model de Bernouilli amb un gran nombre n de repeticions i probabilitat d'èxit p petita s'aproxima per una distribució de Poisson amb paràmetre $\lambda=np$.

3.4.5 Geomètrica

Sigui X una variable aleatòria que compta el nombre de repeticions independents d'una variable aleatòria de Bernouilli $Y\sim B(p)$ fins que apareix el primer èxit. Aleshores, diem que X té una *distribució geomètrica*, i ho representem com $X\sim\text{Geom}(p)$.

La funció de probabilitat d'una variable geomètrica és

$$\Pr(X=k)=(1-p)^{k-1}p,\ \text{amb } k=1,2,3,\dots$$

i la seva funció de distribució de probabilitat és

$$\Pr(X > k) = \sum_{i>k} \Pr(X = i) = \sum_{i>k} (1-p)^{i-1} p = p(1-p)^k \underbrace{\sum_{j\geq 0} (1-p)^j}_{1/p} = (1-p)^k$$

Habitualment es diu que les variables aleatòries geomètriques "no tenen memòria", ja que $\forall\, k, m > 0$,

$$\Pr(X > k+m | X > m) = \frac{\Pr(X > k+m)}{\Pr(X > m)} = \frac{(1-p)^{k+m}}{(1-p)^m} = (1-p)^k = \Pr(X > k)$$

La següent proposició ens diu que el recíproc també és cert:

Proposició 3.4.2. *Sigui X una variable aleatòria que prèn valors naturals $1, 2, \ldots$ amb $\Pr(X = 1) = p > 0$. Si X no té memòria, aleshores $X \sim$ Geom(p).*

Demostració. Si X no té memòria, aleshores per a cada parell d'enters k, m,

$$\Pr(X > k+m | X > m) = \Pr(X > k) \implies \Pr(X > k+m) = \Pr(X > k) \Pr(X > m)$$

En particular, per $m = 1$,

$$\Pr(X > k+1) = \Pr(X > k) \Pr(X > 1) = \Pr(X > 1)^{k+1} = (1-p)^{k+1}$$

Això determina la funció de probabilitat, ja que

$$\Pr(X = k) = \Pr(X > k) - \Pr(X > k+1) = (1-p)^k - (1-p)^{k+1} = (1-p)^{k-1} p$$

i per tant $X \sim \text{Geom}(p)$. □

3.4.6 Hipergeomètrica

Suposem que tenim una urna amb b boles blanques i n boles negres. Sigui $N = b+n$. Extraiem k boles de la urna sense reposició. Aleshores, diem que la variable X que compta el nombre de boles blanques en la mostra segueix una llei hipergeomètrica $X \sim \text{HGeom}(n, b, k)$. Els paràmetres d'aquest model són N, el nombre total de boles, b, el nombre de boles blanques, i k, el nombre de boles que s'extreuen. La funció de probabilitat és

$$\Pr(X = i) = \frac{\binom{b}{i}\binom{n}{k-i}}{\binom{N}{k}}$$

Al denominador hi trobem el nombre de mostres de mida k d'una població de mida N, que tenen totes la mateixa probabilitat. Al numerador, es compta quantes d'aquestes mostres tenen i boles blanques i $k-i$ boles negres.

Perquè el model tingui sentit, s'ha de satisfer que $0 \leq i \leq b$, $0 \leq k - i \leq n$ i $0 \leq k \leq N$. Aquestes condicions queden implícitament recollides a la fórmula anterior, ja que recordem que havíem definit els nombres binomials de manera que

$$\binom{m}{l} = 0, \text{ si } l \in \mathbb{Z} \setminus \{0, 1, \ldots, m\}$$

Observem que el model binomial dona la probabilitat d'extreure b boles blanques en k extraccions amb reposició, mentre que el model hipergeomètric correspon al cas sense reposició. Els dos models són semblants (i.e. la distribució de probabilitat és asimptòticament la mateixa) si N és molt gran en relació a k, ja que llavors les boles extretes i no reposades són negligibles en comparació amb el gran nombre de boles que encara hi ha a la urna.

3.5 Esperança i variància

Els moments d'una variable aleatòria són nombres que recullen informació sobre la distribució de probabilitat de la variable aleatòria. El moment més senzill és l'esperança, o valor mitjà.

3.5.1 Esperança

Definició 3.5.1 (Esperança)**.** Sigui X una variable aleatòria discreta que prèn valors al conjunt numerable $X \subset \mathbb{R}$. L'esperança de X és

$$\mathbb{E}(X) = \sum_{x \in X} x \Pr(X = x)$$

que està ben definida si la sèrie és absolutament convergent (ja que hem de poder reordenar els seus termes com vulguem sense canviar el seu valor).

Si X prèn valors a un conjunt finit $\{a_1, \ldots, a_n\}$ amb la distribució uniforme $\Pr(X = a_i) = 1/n$, aleshores

$$\mathbb{E}(X) = \sum_{i=1}^{n} a_i \Pr(X = a_i) = \frac{1}{n} \sum_{i=1}^{n} a_i$$

és a dir, l'esperança d'una variable uniforme és el valor mitjà (la mitjana aritmètica) dels esdeveniments possibles. Per a aquest motiu a l'esperança també se la coneix com a *valor mitjà* de X.

Si X prèn valors a un conjunt infinit numerable, aleshores $\mathbb{E}(x)$ és una sèrie numèrica que en general pot no ser convergent. Si la sèrie divergeix, diem simplement que la variable no té esperança. També direm que la variable no té esperança si la sèrie convergeix però no convergeix absolutament, ja que en aquest cas es podrien reordenar els termes de la suma per tal que la sèrie tingués un altre valor, i l'esperança no estaria ben definida.

Exemple 3.5.1. Sigui X la variable aleatòria que prèn valors als enters positius amb funció de probabilitat

$$\Pr(X = n) = \frac{6}{\pi^2}\frac{1}{n^2}$$

Aleshores, l'esperança de X és

$$\sum_{n\geq 1} n \Pr(X = n) = \frac{6}{\pi^2}\sum_{n\geq 1}\frac{1}{n} = \infty$$

que és una sèrie divergent. Per tant, direm que la variable X no té esperança.

La propietat bàsica de l'esperança és la seva linealitat:

Proposició 3.5.1. *Siguin X, Y dues variables aleatòries discretes, i sigui $\lambda \in \mathbb{R}$. Aleshores,*

$$\mathbb{E}(X + Y) = \mathbb{E}(X) + \mathbb{E}(Y)$$
$$\mathbb{E}(\lambda X) = \lambda \mathbb{E}(X)$$

Demostració. Per a la primera,

$$\begin{aligned}
\mathbb{E}(X + Y) &= \sum_{x\in\mathcal{X}, y\in\mathcal{Y}} (x + y) \Pr(X = x, Y = y) \\
&= \sum_{x\in\mathcal{X}} x \sum_{y\in\mathcal{Y}} \Pr(X = x, Y = y) + \sum_{y\in\mathcal{Y}} y \sum_{x\in\mathcal{X}} \Pr(X = x, Y = y) \\
&= \sum_{x\in\mathcal{X}} x \Pr(X = x) + \sum_{y\in\mathcal{Y}} y \Pr(Y = y) \\
&= \mathbb{E}(X) + \mathbb{E}(Y)
\end{aligned}$$

Per a la segona, si $\lambda = 0$ és directe, mentre que si $\lambda \neq 0$, utilitzem que $\Pr(\lambda X = \lambda x) = \Pr(X = x)$:

$$\mathbb{E}(\lambda X) = \sum_{x\in\mathcal{X}} \lambda x \Pr(\lambda X = \lambda x) = \lambda \sum_{x\in\mathcal{X}} x \Pr(X = x) = \lambda \mathbb{E}(X)$$

□

A continuació calcularem l'esperança en cadascun dels models bàsics de probabilitat de la secció anterior.

- **Bernouilli:** Si $X \sim B(p)$, aleshores $\mathbb{E}(X) = 0 \Pr(X = 0) + 1 \Pr(X = 1) = p$.
- **Binomial:** Si $X \sim \mathrm{Bin}(n, p)$, aleshores X es pot expressar com a la suma de n variables de Bernouilli, i, donat que l'esperança és lineal, $\mathbb{E}(X) = np$.
- **Poisson:** Si $X \sim \mathrm{Pois}(\lambda)$, aleshores

$$\mathbb{E}(X) = \sum_{k\geq 0} k \Pr(X = k) = \sum_{k\geq 1} \frac{\lambda^k}{(k-1)!} e^{-\lambda} = \lambda e^{-\lambda} \underbrace{\sum_{k\geq 1} \frac{\lambda^{k-1}}{(k-1)!}}_{e^\lambda} = \lambda$$

- **Geomètrica:** Si $x \sim \text{Geom}(p)$, aleshores

$$\mathbb{E}(X) = \sum_{k\geq 1} k \Pr(X = k) = \sum_{k\geq 1} k(1-p)^{k-1}p = p\sum_{k\geq 1} k(1-p)^{k-1} = \frac{p}{(1-(1-p))^2} = \frac{1}{p}$$

  on hem utilitzat que la sèrie que teníem era la derivada d'una sèrie geomètrica de raó $1-p$.

- **Hipergeomètrica:** Si $X \sim \text{HGeom}(n, b, N)$ (on n és el nombre d'extraccions, b el nombre de boles blanques i $N > b, n$ el nombre total de boles), aleshores X es pot escriure com la suma de n variables de Bernouilli amb probabilitat b/N, i

$$\mathbb{E}(X) = \frac{nb}{N}$$

  Si les extraccions són amb reposició obtenim una binomial amb el mateix valor mitjà.

3.5.2 Variància

De manera anàloga a l'esperança, podem definir els moments d'ordre k:

Definició 3.5.2 (Moment d'ordre k)**.** Sigui X una variable aleatòria amb esperança $\mathbb{E}(X) = m$. El *moment d'ordre k* de X és

$$\mathbb{E}(X^k) = \sum_{x\in\mathcal{X}} x^k \Pr(X = x)$$

i el *moment centrat d'ordre k* és

$$\mathbb{E}((X-m)^k) = \sum_{x\in\mathcal{X}} (x-m)^k \Pr(X = x)$$

Definició 3.5.3 (Variància)**.** La *variància* d'una variable aleatòria X és el seu moment central d'ordre 2:

$$\text{Var}(X) = \mathbb{E}((X-m)^2)$$

i la seva arrel quadrada $\sigma_X = \sqrt{\text{Var}(X)}$ és la *desviació típica* de X.

Habitualment la variància es calcula desenvolupant el quadrat:

$$\text{Var}(X) = \mathbb{E}((X-m)^2) = \mathbb{E}(X^2) - 2m\mathbb{E}(X) + m^2 = \mathbb{E}(X^2) - \mathbb{E}(X)^2$$

De la definició de variància tenim a més que

$$\text{Var}(aX+b) = \mathbb{E}(((aX+b) - \mathbb{E}(aX+b))^2) = \mathbb{E}(a^2(X-\mathbb{E}(X))^2) = a^2\text{Var}(X)$$

és a dir, la variància és invariant per translacions i les constants multiplicatives poden sortir a fora elevades al quadrat (i.e. és un operador quadràtic).

Recordem que havíem definit la independència de dues variables aleatòries com que totes les parelles d'esdeveniments possibles fossin independents:

Definició 3.5.4 (Independència)**.** Les variables aleatòries X i Y són independents si $\forall x, y$,

$$\Pr(X = x, Y = y) = \Pr(X = x)\Pr(Y = y)$$

Així, per exemple, tant una variable aleatòria que segueixi una distribució binomial com una que segueixi una distribució hipergeomètrica estan formades per la suma de variables aleatòries de Bernouilli, però en el primer cas són independents mentre que en el segon no.

La noció d'independència ens és útil per calcular variàncies degut a la proposició següent:

Proposició 3.5.2. *Siguin X i Y dues variables aleatòries independents. Aleshores,*

$$\mathrm{Var}(X + Y) = \mathrm{Var}(X) + \mathrm{Var}(Y)$$

Demostració. De la definició de variància, tenim que

$$\begin{aligned}\mathrm{Var}(X + Y) &= \mathbb{E}((X + Y)^2) - \mathbb{E}(X + Y)^2 \\ &= \mathbb{E}(X^2) + \mathbb{E}(Y^2) + 2\mathbb{E}(XY) - \mathbb{E}(X)^2 - \mathbb{E}(Y)^2 - 2\mathbb{E}(X)\mathbb{E}(Y)\end{aligned}$$

Donat que les variables són independents,

$$\mathbb{E}(XY) = \sum_x \sum_y xy \Pr(X = x, Y = y) = \sum_x x \Pr(X = x) \sum_y y \Pr(Y = y) = \mathbb{E}(X)\mathbb{E}(Y)$$

Aleshores,

$$\mathrm{Var}(X + Y) = \mathbb{E}(X^2) - \mathbb{E}(X)^2 + \mathbb{E}(Y^2) - \mathbb{E}(Y)^2 = \mathrm{Var}(X) + \mathrm{Var}(Y)$$

□

A continuació calcularem la variància en cada un dels models bàsics de probabilitat que hem vist anteriorment.

- **Bernoulli:** Si $x \sim B(p)$, aleshores $\mathbb{E}(X^2) = \mathbb{E}(X) = p$ i $\mathrm{Var}(X) = \mathbb{E}(X^2) - \mathbb{E}(X)^2 = p - p^2 = pq$. Observem que, si ho interpretem com una funció de p, la variància serà màxima per $p = 1/2$, i s'anul·larà quan $p = 0, 1$.
- **Binomial:** Si $x \sim \mathrm{Bin}(n, p)$, aleshores X es pot expressar com la suma de n variables de Bernoulli $B(p)$, i per tant

$$\mathrm{Var}(X) = npq$$

- **Poisson:** Si $X \sim \mathrm{Pois}(\lambda)$, aleshores

$$\begin{aligned}\mathbb{E}(X^2) &= \sum_{k\geq 0} k^2 \Pr(X = k) = \sum_{k\geq 1} k(k-1)\Pr(X = k) + \sum_{k\geq 1} k \Pr(X = k) = \\ &= \lambda^2 e^{-\lambda} \underbrace{\sum_{k\geq 2} \frac{\lambda^{k-2}}{(k-2)!}}_{=e^\lambda} + \lambda = \lambda^2 + \lambda\end{aligned}$$

  Per tant, la variància és

$$\mathrm{Var}(X) = \mathbb{E}(X^2) - \mathbb{E}(X)^2 = \lambda^2 + \lambda - \lambda^2 = \lambda$$

- **Geomètrica:** Si $X \sim \text{Geom(p)}$, aleshores

$$\mathbb{E}(X^2) = \sum_{k\geq 1} k^2 \Pr(X=k) = \sum_{k\geq 2} k(k-1)\Pr(X=k) + \sum_{k\geq 1} k\Pr(X=k) =$$
$$= pq\sum_{k\geq 2} k(k-1)q^{k-2} + \frac{1}{p} = \frac{2q}{p^2} + \frac{1}{p}$$

Per tant, la variància serà

$$\text{Var}(X) = \mathbb{E}(X^2) - \mathbb{E}(X)^2 = \frac{2q+p}{p^2} - \frac{1}{p^2} = \frac{2q+p-1}{p^2} = \frac{q}{p^2}$$

3.6 Desigualtat de Txebixov

3.6.1 Desigualtats de Markov i Txebixov

Hem definit la variància com la mitjana dels quadrats de les desviacions de la variable aleatòria respecte a l'esperança. Per tant, es pot entendre la variància com una mesura de com de dispersos es troben els valors de X. Aquest sentit queda reflectit en la desigualtat de Txebixov, que veurem a continuació. Primer veurem una desigualtat semblant per a l'esperança:

Teorema 3.6.1 (Desigualtat de Markov)**.** *Sigui X una variable aleatòria amb esperança finita. Si X pren valors positius, aleshores per a tot $a \in \mathbb{R}^+$ tenim que*

$$\Pr(X \geq a) \leq \frac{\mathbb{E}(X)}{a}$$

Demostració. Tenim que

$$\mathbb{E}(X) = \sum_x x\Pr(X=x) \geq \sum_{x\geq a} x\Pr(X=x) \geq \sum_{x\geq a} a\Pr(X=x) = a\Pr(X\geq a)$$

on hem utilitzat que X no pren valors negatius. □

Teorema 3.6.2 (Desigualtat de Txebixov)**.** *Sigui X una variable aleatòria amb esperança i variància finita. Aleshores, per a tot $a \in \mathbb{R}^+$, tenim que*

$$\Pr(|X - \mathbb{E}(X)| \geq a) \leq \frac{\text{Var}(X)}{a^2}$$

Demostració. Aplicant la desigualtat de Markov a la variable aleatòria $(X - \mathbb{E}(X))^2$, tenim que

$$\Pr(|X-\mathbb{E}(X)| \geq a) = \Pr((X-\mathbb{E}(X))^2 \geq a^2) \leq \frac{\mathbb{E}((X-\mathbb{E}(X))^2)}{a^2}$$

i per la definició de variància,

$$\mathbb{E}((X-\mathbb{E}(X))^2) = \text{Var}(X)$$

□

Observem que, prenent $a = \sigma k$ (on σ és la desviació estàndard), podem escriure també la desigualtat de Txebixov com

$$\Pr(|X - \mathbb{E}(X)| \geq k\sigma) \leq \frac{1}{k^2}$$

Així podem saber, per exemple, que la probabilitat que una variable aleatòria es desviï més de dues desviacions estàndard de l'esperança és més petita que 1/4.

La desigualtat de Txebixov té l'avantatge que és vàl·lida per qualsevol distribució, però per segons quins casos pot no donar una fita gaire bona.

3.6.2 Llei dels grans nombres

Suposem que tenim un espai de probabilitat $(\Omega, \mathcal{A}, \Pr)$. Aleshores, donat un $A \in \mathcal{A}$ amb $\Pr(A) = p$, podem definir la variable aleatòria $X \sim \text{Bin}(n, p)$ com el nombre d'aparicions de A en n repeticions independents.

A partir d'aquesta variable, podem definir la freqüència relativa de A com la variable aleatòria X/n, que veiem que compleix que $\mathbb{E}(X/n) = p$ i $\text{Var}(X/n) = pq/n$.

Amb aquestes definicions podem enunciar el resultat següent:

Proposició 3.6.1 (Llei dels grans nombres)**.** *La freqüència relativa d'un esdeveniment A tendeix a la seva probabilitat $p = \Pr(A)$ quan el nombre de repeticions tendeix a infinit.*

Demostració. Donat que $\mathbb{E}(X/n) = p$, hem de veure que, per tot $\varepsilon > 0$,

$$\Pr(|X/n - \mathbb{E}(X/n)| \geq \varepsilon) \to 0 \quad \text{quan } n \to \infty$$

Per un $\varepsilon > 0$ fixat, per la desigualtat de Txebixov tenim que

$$\Pr(|X/n - \mathbb{E}(X/n)|) \geq \varepsilon) \leq \frac{\text{Var}(X/n)}{\varepsilon^2} = \frac{pq}{n\varepsilon}$$

Aleshores, aquest valor tendirà a zero per $n \to \infty$. □

3.7 Funcions generadores de probabilitat

Quan treballem amb variables aleatòries discretes que prenen valors als naturals, podem considerar les seves funcions generadores:

Definició 3.7.1 (Funció generadora de probabilitat)**.** Sigui X una variable aleatòria discreta que pren valors als naturals. Aleshores definim la funció generadora de probabilitat de X com

$$G_X(z) = \sum_{n \geq 0} \Pr(X = n) z^n$$

que es correspon a la funció generadora de la successió $(\Pr(X = k))_k$.

Una característica de les funcions generadores de probabilitat és que es poden representar com una esperança:

Proposició 3.7.1. *Sigui X una variable aleatòria discreta que pren valors als naturals. Aleshores,*

$$G_X(z) = \mathbb{E}(z^X)$$

Demostració. Recordem que definíem l'esperança d'una funció de la variable aleatòria com

$$\mathbb{E}(f(X)) = \sum_x f(x) \Pr(X = x)$$

Aleshores, per aquest cas concret,

$$\mathbb{E}(z^X) = \sum_{x \geq 0} z^x \Pr(X = x) = G_X(z)$$

□

Alguns exemples de funcions generadores de probabilitat per a distribucions de probabilitat que haguem vist són:

- **Bernoulli:** Si $X \sim B(p)$, aleshores

$$G_X(z) = \Pr(X = 0) + \Pr(X = 1)z = q + pz$$

- **Binomial:** Si $X \sim \text{Bin}(n, p)$, aleshores

$$G_X(z) = \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} z^k = (pz + q)^n$$

- **Poisson:** Si $X \sim \text{Pois}(\lambda)$, aleshores

$$G_X(z) = \sum_{k \geq 0} \frac{\lambda^k}{k!} e^{-\lambda} z^k = e^{\lambda z} e^{-\lambda} = e^{-\lambda(1-z)}$$

- **Geomètrica:** Si $X \sim \text{Geom}(p)$, aleshores

$$G_X(z) = \sum_{k \geq 1} p q^{k-1} z^k = \frac{pz}{1 - qz}$$

Les funcions generadores de probabilitat són útils per trobar els moments de les variables aleatòries:

Proposició 3.7.2. *Sigui X una variable aleatòria discreta amb funció generadora $G_X(z)$. Aleshores,*

$$\mathbb{E}(X) = G'_X(1)$$
$$\mathrm{Var}(X) = G''_X(1) + G'_X(1) - G'_X(1)^2$$

i en general tenim que

$$\mathbb{E}(X(X-1)\dots(X-k+1)) = G_X^{(k)}(1)$$

Demostració. Tenim que

$$G_X^{(n)}(z) = \sum_{k\geq n} k(k-1)\dots(k-n+1)\Pr(X=k)z^{k-n}$$

I per tant,

$$G_X^{(n)}(1) = \sum_{k\geq n} k(k-1)\cdot(k-n+1)\Pr(X=k) = \mathbb{E}(X(X-1)\dots(X-n+1))$$

L'expressió de l'esperança surt directament, i la variància recordem que es podia escriure com

$$\mathrm{Var}(X) = \mathbb{E}(X^2) - \mathbb{E}(X)^2 = \mathbb{E}(X(X-1)) + \mathbb{E}(X) - \mathbb{E}(X)^2$$

□

A l'expressió $\mathbb{E}(X(X-1)\dots(X-n+1))$ se l'anomena *moment factorial k-èssim de X* i, tal com hem vist, es poden utilitzar per calcular tant els moments ordinaris com els moments centrats.

Una altra propietat útil de les funcions generadores és que permeten obtenir la distribució de la suma de variables independents:

Proposició 3.7.3. *Siguin X i Y variables aleatòries discretes independents amb funcions generadores $G_X(z)$ i $G_Y(z)$. Aleshores,*

$$G_{X+Y}(z) = G_X(z)G_Y(z)$$

Demostració. Utilitzant l'equivalència que hem vist abans,

$$G_{X+Y}(z) = \mathbb{E}(z^{X+Y}) = \mathbb{E}(z^X z^Y) = \mathbb{E}(z^X)\mathbb{E}(z^Y) = G_X(z)G_Y(z)$$

□