UNIVERSIDAD DE SEVILLA

FACULTAD DE MATEMÁTICAS

DEPARTAMENTO DE ESTADÍSTICA E INVESTIGACIÓN OPERATIVA

TRABAJO FIN DE GRADO

COMBINATORIA DE PERMUTACIONES

Presentado por:
Rocío Rodríguez Huertas

Dirigido por: Fernando López Blazquez

Sevilla, Junio de 2016

Índice general

Introducción

El nacimiento y desarrollo de la combinatoria ha sido paralelo al desarrollo de otras ramas de las Matemáticas, tales como el álgebra, la teoría de números, y la probabilidad.

Desde tiempos muy remotos ha habido problemas de combinatoria que han llamado la atención de los matemáticos:

- El problema de los **cuadrados mágicos**, que son matrices de números con la propiedad de que la suma de los elementos de cualquier columna, fila o diagonal es el mismo número. Aparece en un viejo libro chino fechado 2200 a.C. Los cuadrados mágicos de orden 3 fueron estudiados con fines místicos.

- Los **coeficientes binominales**, que son los coeficientes enteros del desarrollo de $(a+b)^n$. Fueron conocidos en el siglo XII.

- El **triángulo de Pascal**, que es una disposición triangular de los coeficientes binominales. Fue desarrollado en el siglo XIII.

La combinatoria se desarrolla en occidente en el siglo XVII debido a los intereses de Blaise Pascal $(1623-1662)$ y Pierre Fermat $(1601-1655)$ por los aspectos matemáticos de los juegos de azar. Comenzaron a recoger muestras de experimentos que realizaban en las mesas de juegos y a registrarlas estadísticamente para estudiar las leyes y regularidades bajo las cuales se regían.

Uno de ellos fue el siguiente: el juego consistía en el lanzamiento de una moneda sucesivas veces. El ganador es el jugador que alcanza primero 6 éxitos (6 caras ó 6 números). Pero el juego se detiene si tras el noveno lanzamiento un jugador tiene 5 éxitos y el otro 4. ¿Cómo se puede repartir entonces la apuesta? No era justo hacerlo con la razón $5:4$. Pascal resolvió el problema aplicando algunos métodos combinatorios y además propuso un método de solución para el caso general, cuando a un jugador le quedaran "r" partidas hasta ganar y al otro jugador le quedaran "s" partidas. Una solución similar a este problema fue dada por Fermat.

La combinatoria se desarrolla de forma más completa con los trabajos de Jacob Bernoulli $(1654-1705)$ y Gottfried Wilhelm Leibnitz $(1646-1716)$ que definieron los conceptos básicos de la combinatoria.

El matemático suizo Leonard Euler fue quien desarrolló a principios del siglo XVIII una auténtica escuela de matemática combinatoria. En sus artículos sobre la partición y descomposición de enteros positivos en sumandos, estableció las bases de uno de los métodos fundamentales para el cálculo de configuraciones combinatorias, el método de las funciones generatrices. También se le considera el padre de la teoría de grafos por el planteamiento y solución de los problemas de los Puentes de

Konigsberg usando por primera vez conceptos y métodos de teoría de grafos. Los primeros problemas de teoría de grafos surgieron de la búsqueda de solución a algunos problemas cotidianos y también en el planteamiento de algunos acertijos matemáticos tales como el problema de los Puentes de Konigsberg, la colocación de reinas en un tablero de ajedrez con alguna restricción, problemas de transporte y el problema del viajero, entre otros. Hoy en día la combinatoria constituye una amplia rama de las Matemáticas con numerosas aplicaciones prácticas a otras ciencias tales como la Biología, la Informática, las Comunicaciones, etc.

Se han descrito numerosas estructuras combinatorias. Es este trabajo nos centraremos en una de las más simples pero no por ello menos importante: las permutaciones.

Una permutación puede ser interpretada de muchas maneras. En el **Capítulo 1**, se consideran las permutaciones como órdenes lineales y el interés se centra en los ascensos en dichas ordenaciones. El número de permutaciones de tamaño n con un número fijo de ascensos se conoce como número Euleriano. Se estudian las propiedades básicas de estos números, diversas funciones generatrices y su relación con los números de Stirling de segunda clase.

En el **Capítulo 2** se estudian las inversiones y otros estadísticos con igual distribución como el índice mayor. Se presentan algunas relaciones de estos conceptos con los determinantes y los matching perfectos en grafos bipartitos.

El **Capítulo 3** está dedicado a la descomposición de permutaciones como producto de ciclos. La descomposición en ciclos de longitud dos es básica para la clasificación de permutaciones en par e impar. Si se considera la descomposición en ciclos disjuntos, el número de permutaciones de longitud n con k ciclos es descrito por los números de Stirling de primera clase (sin signo). Para estos números presentamos fórmulas recurrentes y diversas funciones generatrices asociadas.

Finalmente, en el **Capítulo 4** presentamos algunas aplicaciones de los conceptos estudiados en capítulos anteriores. Destacamos la aplicación a los contrastes de aleatoriedad y la conexión entre momentos factoriales y ordinarios.

Abstract

Permutations are perhaps one of the most basic and important combinatorial structures. They appear in Mathematics and other fields of Science and Technology under many different appearances, for instance as linear orders, elements of the symmetric group, or associated to certain matrices and graphs.

There are also many interesting statistics associated to permutations. Among others, in this work, we explore the number of ascents, the number of inversions and the number of cycles. In connection with theses statistics there are many interesting results and concepts like recurrence formulas, generating functions and a collection of important numbers not only in combinatorics but in some other fields as Eulerian numbers, Stirling numbers of first and second kind, etc.

Finally, in the last chapter we present some aplications to run tests based on the length of ascents and descents and also the connection between central and factorial moments.

Agradecimientos

Puesto que no hubiese podido terminar el grado si no hubiese contado con el apoyo, el cariño, la energía y el tiempo de muchas personas, quería incluir este apartado para poder agradecerles todo lo que me han ayudado en estos cuatro años.

Le dedico este trabajo a mi familia, en especial a mis padres, por el esfuerzo que han tenido que realizar para que hoy pudiera estar escribiendo esto, por su apoyo incondicional y desinteresado en cada momento que creía que no lo conseguiría y por celebrar conmigo cada triunfo ganado. Si hoy estoy aquí es por ellos.

Además, agradecer a mis amigos por permanecer a mi lado día tras día, por aquellas mañanas, tardes y casi noches en la biblioteca y en esas salas del CRAI, donde además de agobios, hemos crecido como personas y como matemáticos. Muchas han sido las horas que hemos empleado en llegar hasta aquí y ahora estamos al borde de conseguirlo.

Y para acabar, agradecer a mi tutor Fernando López Blazquez, por su entrega y dedicación, pues siempre ha estado a disposición cuando lo he necesitado. Me ha ayudado a que esta recta final de la carrera haya sido mas llevadera y con el menor número de complicaciones posibles. Sin su ayuda y conocimientos no hubiese sido posible realizar este proyecto.

En general, le dedico este trabajo a todo aquel que haya aportado un granito de arena para que consiguiera mi sueño.

Capítulo 1

Números Eulerianos y de Stirling

Introducción

En el problema clásico de Newcomb se extraen sucesivamente cartas una tras otra de una baraja de m cartas enumeradas. Las cartas se colocan en un montón, siempre que el número x_j escrito en la carta j-ésima sea mayor o igual que el número x_{j-1} de la carta anterior. Sin embargo, se comienza un nuevo montón cada vez que el número x_j sea menor que x_{j-1}, para $j = 1, 2, \dots, m$.

Es importante la enumeración de las disposiciones de las cartas, pues nos llevará a tener diferentes números de montones.

Por tanto, estamos ante un problema de contar las permutaciones de n tipos de elementos con $s_1, \dots, s_n$ elementos respectivamente, las cuáles incluyen secuencias de k elementos consecutivos no decrecientes.

En este capítulo estudiaremos la enumeración de las permutaciones del conjunto $\{1, 2, \dots, n\}$ que tienen k secuencias crecientes de elementos consecutivos.

Otro problema clásico es el de como distribuir n bolas en k urnas diferentes de forma que ninguna quede vacía. Este estudio lo llevó a cabo Abraham De Moivre en 1718 a través de una simple suma de términos elementales con alternancia de signo entre ellos.

Para resolver dicho problema, analizaremos en la segunda parte del capítulo los números de Stirling de segunda clase que constituyen el coeficiente de las expansiones de las potencias en factoriales, así como sus propiedades básicas, funciones generatrices, expresiones explícitas y relaciones de recurrencia. Fueron introducidos por el matemático James Stirling en 1830. James Stirling también es conocido por la fórmula de Stirling usada para la aproximación de factoriales grandes. La aproximación se expresa como: $ln\, n! \approx n\, ln\, n - n$.

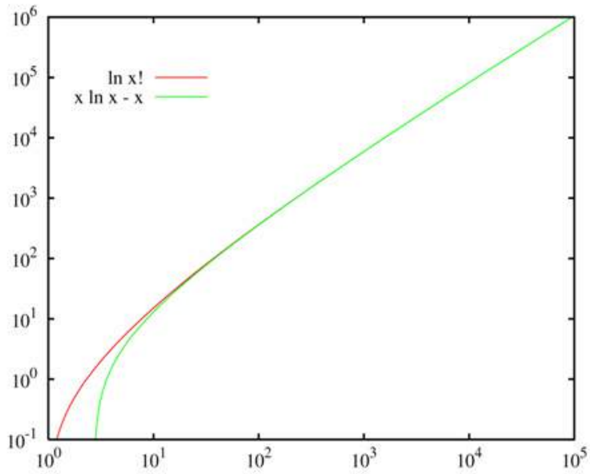


Figura 1.1: Diferencia relativa entre $ln\,n!$ y $n\,ln\,n - n$

Puesto que los factoriales ocupan la misma posición central en el cálculo de diferencias finitas que las potencias en el cálculo infinitesimal, los números de Stirling constituyen una parte del puente que conecta estos dos cálculos. Además, tienen aplicaciones en combinatoria, en problemas de ocupación y en teoría de la probabilidad.

1.1. Números Eulerianos

Definición 1.1.1

Una ordenación lineal de los elementos del conjunto $[n] = \{1, 2, 3, \ldots, n\}$ se llama una **permutación**, o si queremos hacer hincapié en el hecho de que consta de n entradas, una n-permutación.

En otras palabras, una permutación enumera todos los elementos de $[n]$ de modo que cada elemento aparece exactamente una vez.

Ejemplo 1.1.2

Si $n = 3$ entonces las n-permutaciones son: 123, 132, 213, 231, 312, 321.

$\square$

Proposición 1.1.3

El número de n-permutaciones es $n!$.

Demostración

Construimos una n-permutación $p = p_1p_2\cdots p_n$, de forma que podemos elegir n entradas para p_1. Una vez fijado p_1, tenemos $n-1$ entradas para p_2. Este procedimiento lo repetimos para los p_i restantes, disminuyendo una unidad el número de entradas disponibles cada vez que fijamos un p_i.

■

Definición 1.1.4

Sea $p = p_1p_2\cdots p_n$ una permutación. Decimos que i es un **descenso** de p si $p_i > p_{i+1}$. Análogamente, decimos que i es un **ascenso** de p si $p_i < p_{i+1}$.

Definición 1.1.5

Los **números Eulerianos** representan el número de permutaciones de n elementos con $k-1$ descensos. Se denotan por $A(n,k)$, $k = 0, 1, \ldots, n$ $n = 0, 1, \ldots$

Claramente, la definición implica $A(n,k) = 0$ si $k > n$. Son llamados **Eulerianos** para distinguirlos de los **números de Euler** E_{2n}, que aparecen en el desarrollo de la función secante hiperbólica.

Los primeros valores de $A(n,k)$ los recogemos en la siguiente tabla:

n	k								
	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$	$k=9$
$n=1$	1								
$n=2$	1	1							
$n=3$	1	4	1						
$n=4$	1	11	11	1					
$n=5$	1	26	66	26	1				
$n=6$	1	57	302	302	57	1			
$n=7$	1	120	1191	2416	1191	120	1		
$n=8$	1	247	4293	15619	15619	4293	247	1	
$n=9$	1	502	14608	88234	156190	88234	14608	502	502

Tabla 1.1: Números Eulerianos $A(n,k)$

Definición 1.1.6

Sea $p = p_1p_2\cdots p_n$ una permutación con $k-1$ descensos, es decir, p es la unión de k subsecuencias ascendentes. Estas subsecuencias se denominan **rachas ascendentes** de p.

Ejemplo 1.1.7

La permutación $p = 82415367$ tiene 3 descensos en las posiciones 1, 3 y 5 y las rachas ascendentes son (8), (24), (15) y (367).

$\square$

Ejemplo 1.1.8

Consideremos todas las permutaciones de longitud 3: $123, 132, 213, 231, 312, 321$. En negrita están marcados los descensos y entre paréntesis las rachas ascendentes

$$(123),\ (1\mathbf{3})(2),\ (\mathbf{2})(13),\ (2\mathbf{3})(1),\ (\mathbf{3})(12),\ (\mathbf{3})(\mathbf{2})(1).$$

Entonces, recordando que $A(n,k)$ es el número de permutaciones de $[n]$ con k rachas ascendentes:

$$A(3,1) = 1, \quad A(3,2) = 4, \quad A(3,3) = 1.$$

$\square$

A continuación mostramos una fórmula recurrente para la obtención de los números Eulerianos.

Teorema 1.1.9

Para todos los enteros positivos $k \leq n$, se tiene que

$$A(n, k+1) = (k+1)A(n-1, k+1) + (n-k)A(n-1, k). \tag{1.1}$$

Demostración

Intentamos conseguir una n-permutación p con k descensos mediante la inserción de n en una $(n-1)$-permutación p'. Tal inserción tiene como consecuencia que el número de descensos permanezca igual o que aumente en una unidad. Por lo tanto distinguiremos dos casos:

- El número de descensos no varía: esto ocurre cuando n se inserta o bien al final de p' o bien en un descenso de p'. Tenemos $A(n-1, k+1)$ opciones para p' y $(k+1)$ posibles inserciones de n que no cambian el número de descensos, lo cual explica el primer término del lado derecho de (1.1).
- El número de descensos se incrementa en una unidad: esto ocurre cuando n se inserta o bien al principio de p' o bien en un ascenso de p'. Entonces hay $A(n-1, k)$ opciones para p', cada una de estas $(n-1)$-permutaciones tiene $(n-2)-(k-1) = n-k-1$ ascensos que junto con la inserción de n al principio, da lugar a $n-k$ posibles puntos de inserción. Este razonamiento explica el segundo término del lado derecho de (1.1).

■

Nota 1.1.10

Tenemos $A(n, k+1) = A(n, n-k)$, es decir, los números Eulerianos son simétricos. En efecto, si $p = p_1 p_2 \cdots p_n$ tiene k descensos, entonces su reverso $p^r = p_n p_{n-1} \cdots p_1$ tiene $n-k-1$ descensos.

Por convenio $A(0,0) = 1$ y $A(n,0) = 0$ para $n > 0$.

Teorema 1.1.11

Para todo entero no negativo n y para todo número real x, se tiene

$$x^n = \sum_{k=0}^{n} A(n,k) \binom{x+n-k}{n}. \tag{1.2}$$

Demostración

Distinguiremos dos casos:

- Suponemos que x es un entero positivo.

El lado izquierdo cuenta las secuencias de n elementos en las que cada dígito proviene del conjunto $[x]$. Vamos a demostrar que el lado derecho cuenta esas mismas secuencias.

Sea $a = a_1 a_2 \cdots a_n$ una secuencia. Reordenamos a en orden no decreciente, es decir, de la forma $a' = a_{i_1} \leq a_{i_2} \leq \cdots \leq a_{i_n}$ con la condición extra de que los dígitos idénticos aparecen en a' en orden creciente de sus índices. Entonces $i = i_1 i_2 \cdots i_n$ es una n-permutación que está únicamente determinada por a. Oberservamos que i_1 nos dice la posición en a de la primera entrada de i, i_2 nos dice la posición en a de la segunda entrada de i y así sucesivamente.

Por ejemplo, si $a = 421132$, primero tenemos que reordenar en orden no decreciente, dando lugar a $a' = 112234$, por lo que $i = 342651$.

Por último, vamos a demostrar que cada permutación i tiene $k-1$ descensos, obteniendo exactamente $x+n-k$ secuencias de a.

Debemos tener en cuenta que si $a_{i_j} = a_{i_{j+1}}$, entonces $i_j < i_{j+1}$. Tomando la implicación contraria, si j es un descenso de $p(a) = i_1 i_2 \cdots i_n$, entonces $a_{i_j} < a_{i_{j+1}}$. Esto quiere decir, que la secuencia a' tiene que ser estrictamente creciente cada vez que j sea un descenso de $p(a)$.

En nuestro ejemplo, $i = 342651$ tiene descenso en 2 y 4 y $a' = 112234$ es estrictamente creciente en dichas posiciones.
¿Cuántas secuencias de a pueden llevar a la permutación $i = 342651$?. Se tiene por el argumento anterior que en secuencias con esa propiedad, nosotros deberíamos tener

$$1 \leq a_3 \leq a_4 < a_2 \leq a_6 < a_5 \leq a_1 \leq x$$

con desigualdad estricta en la tercera y quinta posición. La cadena de desigualdades anterior es obviamente equivalente a

$$1 \leq a_3 < a_4 + 1 < a_2 + 1 < a_6 + 2 < a_5 + 2 < a_1 + 3 \leq x + 3$$

y por consiguiente, el número de secuencias es claramente

$$\binom{x+3}{6}.$$

Por eso, este es el número de secuencias en a para cada $i = 342651$. Generalizando este argumento para todo n y para permutaciones i con $k-1$ descensos, podemos conseguir que cada n-permutación con $k-1$ descensos provenga de

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

secuencias.

- Supongamos que x no es un entero positivo.

Tenemos en cuenta que los dos lados de la ecuación pueden ser vistos como polinomios en la variable x. Ya que coinciden para un número infinito de valores (enteros positivos), éstos deben ser idénticos.

■

Ejemplo 1.1.12

Fijamos $n=3$, usando los números Eulerianos calculados en el **Ejemplo 1.1.8** tenemos:

$$\begin{aligned} x^3 &= \sum_{k=0}^{3} A(3,k)\binom{x+n-k}{3} \\ &= A(3,0)\binom{x+3-0}{3} + A(3,1)\binom{x+3-1}{3} + A(3,2)\binom{x+3-2}{3} \\ &+ A(3,3)\binom{x+3-3}{3} = \binom{x+2}{3} + 4\binom{x+1}{3} + \binom{x}{3}. \end{aligned}$$

□

Corolario 1.1.13

Para todos los enteros positivos n, se tiene que

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

<u>**Demostración**</u>

Cambiamos x por $-x$ en la expresión (1.2) y conseguimos

$$x^n(-1)^n = \sum_{k=0}^{n} A(n,k)\binom{-x+n-k}{n}. \tag{1.3}$$

Ahora calculamos $\binom{-x+n-k}{n}$.

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

Sustituyendo este valor en (1.3)

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

De esta forma obtenemos el resultado

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

$\blacksquare$

Lema 1.1.14: Fórmula de Convolución de Cauchy

Sean x e y números reales y sea z un entero positivo. Entonces

$$\binom{x+y}{z} = \sum_{d=0}^{z}\binom{x}{d}\binom{y}{z-d}.$$

Teorema 1.1.15

Para todos los enteros no negativos n y k, con $k \leq n$, se tiene que

$$A(n,k) = \sum_{r=0}^{k}(-1)^r\binom{n+1}{r}(k-r)^n. \tag{1.4}$$

<u>**Demostración**</u>

Tomamos la expresión

$$x^n = \sum_{k=0}^{n} A(n,k)\binom{x+n-k}{n}, \quad n = 0, 1, \ldots$$

reemplazamos la variable k por j y tomamos $x = k-r$ con $r = 0, 1, \ldots, k$, deduciendo la expresión

$$(k-r)^n = \sum_{j=0}^{k-r} A(n,j)\binom{k-r+n-j}{n}, \quad r = 0, 1, \ldots, k$$

que usando la relación

$$\binom{n+k-r-j}{n} = \binom{n+k-r-j}{k-r-j} = (-1)^{k-r-j}\binom{-n-1}{k-r-j}$$

puede escribirse como

$$(k-r)^n = \sum_{j=0}^{k-r} A(n,j)(-1)^{k-r-j}\binom{-n-1}{k-r-j}, \quad r = 0, 1, \ldots, k$$

Multiplicando a ambos lados de la expresión por $(-1)^r\binom{n+1}{r}$ y sumando para $r = 0, 1, \ldots, k$, conseguimos que

$$\sum_{r=0}^{k}(-1)^r\binom{n+1}{r}(k-r)^n = \sum_{r=0}^{k}\sum_{j=0}^{k-r}(-1)^r\binom{n+1}{r}A(n,j)\binom{-n-1}{k-r-j}(-1)^{k-r-j} =$$

$$= \sum_{j=0}^{k} A(n,j)(-1)^{k-j}\sum_{r=0}^{k-j}\binom{n+1}{r}\binom{-n-1}{k-r-j}$$

y por la fórmula de Cauchy

$$\sum_{r=0}^{k-j}\binom{n+1}{r}\binom{-n-1}{k-r-j} = \binom{0}{k-j} = \delta_{k,j}$$

y así obtenemos la expresión que queríamos.

■

Definición 1.1.16

Los **polinomios eulerianos** se definen como

$$A_n(t) = \sum_{k=0}^{n} A(n,k)t^k, \quad n = 0, 1, \ldots \tag{1.5}$$

Lema 1.1.17

Una alternativa para expresar los polinomios eulerianos $A_n(t)$ es

$$A_n(x) = (1-x)^{n+1}\sum_{j=0}^{\infty} j^n x^j, \quad n = 0, 1, \ldots \tag{1.6}$$

Demostración

Sustituyendo en la expresión (1.5) el valor de $A(n,k)$, obtenido en la expresión (1.4), deducimos que

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

Nos fijamos en la suma interior y observamos que $A(n,k) = 0$, $k > n$ se anula para $k = n+1, n+2, \ldots$, lo que hace posible extender la suma de fuera hasta el infinito.

Por tanto,

$$\begin{aligned} A_n(x) &= \sum_{k=0}^{n} \sum_{r=0}^{k} (-1)^r \binom{n+1}{r} (k-r)^n x^k \\ &= \sum_{r=0}^{\infty} (-1)^r \binom{n+1}{r} x^r \sum_{k=r}^{\infty} (k-r)^n x^{k-r}. \end{aligned}$$

Teniendo en cuenta que

$$\sum_{r=0}^{\infty} (-1)^r \binom{n+1}{r} x^r = (1-x)^{n+1}$$

y tomando $j = k - r$, llegamos a

$$A_n(x) = (1-x)^{n+1} \sum_{j=0}^{\infty} j^n x^j.$$

$\blacksquare$

Ejemplo 1.1.18

Vamos a usar la serie geométrica real de término inicial $a \in \mathbb{R}$ y de razón $r \in \mathbb{R}$

$$\sum_{n=0}^{\infty} ar^n = \frac{a}{1-r}$$

Para $n = 1$ tenemos

$$A_1(x) = (1-x)^2 \sum_{j=0}^{\infty} jx^j = (1-x)^2 \frac{x}{(1-x)^2} = x,$$

y para $n = 2$

$$A_2(x) = (1-x)^2 \sum_{j=0}^{\infty} j^2 x^j = (1-x)^3 \left(\frac{2x^3}{(1-x)^3} + \frac{x}{(1-x)^2} \right) = x + x^2.$$

$\square$

Teorema 1.1.19

La **función generatriz bivariante** de los números Eulerianos $A(n,k)$, $k = 0, 1, \ldots, n, n = 0, 1, \ldots$ viene dada por

$$g(x,u) = \sum_{n=0}^{\infty} \sum_{k=0}^{n} A(n,k) x^k \frac{u^n}{n!} = \frac{1-x}{1-xe^{u(1-x)}}.$$

<u>**Demostración**</u>

Usando la expresión (1.5) obtenemos

$$g(x,u) = \sum_{n=0}^{\infty} A_n(x) \frac{u^n}{n!}$$

y sustituyéndo la expresión (1.6) en la anterior llegamos a

$$g(x,u) = \sum_{n=0}^{\infty} (1-x)^{n+1} \sum_{j=0}^{\infty} j^n x^j \frac{u^n}{n!} = (1-x) \sum_{j=0}^{\infty} x^j \sum_{n=0}^{\infty} \frac{[ju(1-x)]^n}{n!}.$$

Por otro lado, teniendo en cuenta el desarrollo de la función exponencial $\sum_{n=0}^{\infty} \frac{x^n}{n!} = e^x$, se tiene que $\frac{[ju(1-x)]^n}{n!} = e^{ju(1-x)}$ por lo que

$$(1-x) \sum_{j=0}^{\infty} x^j \sum_{n=0}^{\infty} \frac{[ju(1-x)]^n}{n!} = (1-x) \sum_{j=0}^{\infty} x^j e^{ju(1-x)} = (1-x) \sum_{j=0}^{\infty} [xe^{u(1-x)}]^j$$

y el desarrollo de la serie geométrica

$$\sum_{n=0}^{\infty} ax^n = \frac{a}{1-x}$$

obteniendo

$$\sum_{j=0}^{\infty} [xe^{u(1-x)}]^j = \frac{1}{1-xe^{u(1-t)}}.$$

Por tanto,

$$g(x,u) = \frac{1}{1-xe^{u(1-x)}}.$$

■

1.2. Números de Stirling de segunda clase

Una partición de un conjunto $[n]$ en k bloques es una distribución de los elementos de $[n]$ en k subconjuntos no vacíos $B_1, B_2, \ldots, B_k$ de modo que cada elemento se coloca exactamente en un bloque, es decir, $B_1 \cup \cdots \cup B_k = [n]$ y $B_i \cap B_j = \emptyset$, $i \neq j$.

Definición 1.2.20

El número de particiones de $[n]$ en k bloques se denota por $S(n, k)$ y se llama **número de Stirling de segunda clase**. Viene dado por

$$S(n,k) = \frac{1}{k!} \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n,$$

con n y k enteros positivos.

Por convenio, definimos $S(n, 0) = 0$ si $n > 0$ y $S(0, 0) = 1$.

Los primeros valores de los números de Stirling de segunda clase $S(n, k)$ los recogemos en la siguiente tabla:

n	k								
	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$	$k=9$
$n=1$	1								
$n=2$	1	1							
$n=3$	1	3	1						
$n=4$	1	7	6	1					
$n=5$	1	15	25	10	1				
$n=6$	1	31	90	65	15	1			
$n=7$	1	63	301	350	140	21	1		
$n=8$	1	127	966	1701	1050	266	28	1	
$n=9$	1	255	3025	7770	6951	2646	462	36	1

Tabla 1.2: Números de Stirling de segunda clase $S(n, k)$

Ejemplo 1.2.21

El conjunto $[4]$ tiene seis particiones en tres partes, consistiendo cada una de un bloque y dos simples. Las seis particiones son:

$$\begin{array}{ccc} \{1\} & \{2\} & \{3,4\} \\ \{1\} & \{3\} & \{2,4\} \\ \{1\} & \{4\} & \{2,3\} \\ \{2\} & \{3\} & \{1,4\} \\ \{2\} & \{4\} & \{1,3\} \\ \{3\} & \{4\} & \{1,2\} \end{array}$$

Por lo tanto, $S(4,3) = 6$.

□

Notación 1.2.22

Definimos el factorial descendente de x de grado n como

$$(x)_n = x(x-1)\cdots(x-n+1), \quad n = 1, 2, \dots$$

Expresando la n-ésima potencia de x en función de los factoriales de los polinomios de x de grado n, conseguimos

$$x^n = \sum_{k=0}^{n} S(n,k)(x)_k, \quad n = 0, 1, \dots \tag{1.7}$$

Proposición 1.2.23

Definimos la **función generatriz doble** para los números de Stirling de segunda clase como

$$f(x,u) = \sum_{n=0}^{\infty}\sum_{k=0}^{n} S(n,k)(x)_k \frac{u^n}{n!} = e^{xu}.$$

Lema 1.2.24

Para todo k fijo, la **función generatriz exponencial** de los números de Stirling de segunda clase viene dada por

$$f_k(u) = \sum_{n=k}^{\infty} S(n,k)\frac{u^n}{n!} = \frac{(e^u-1)^k}{k!}, \quad k = 0, 1, \dots$$

<u>**Demostración**</u>

Cambiando el orden de sumación en $f(x,u)$, conseguimos

$$f(x,u)=\sum_{k=0}^{n}\sum_{n=k}^{\infty} S(n,k)\frac{u^n}{n!}(x)_k=\sum_{k=0}^{\infty} f_k(u)(x)_k.$$

Por otro lado, tenemos

$$f(x,u)=e^{xu}=[1+(e^u-1)]^x.$$

Usando el desarrollo del Binomio de Newton $(x+y)^r=\sum_{k=0}^{\infty}\binom{r}{k}x^{r-k}y^k$, deducimos lo siguiente

$$[1+(e^u-1)]^x=\sum_{k=0}^{\infty}\binom{x}{k}(e^u-1)^k=\sum_{k=0}^{\infty}\frac{(e^u-1)^k}{k!}(x)_k.$$

Por tanto, comparando ambos coeficientes de x^k, obtenemos el resultado

$$f_k(u)=\frac{(e^u-1)^k}{k!}.$$

■

Los números de Stirling de segunda clase y los números Eulerianos están muy relacionados, como muestran los siguientes teoremas.

Teorema 1.2.25

Para todos los enteros positivos n y r, se tiene

$$S(n,r)=\frac{1}{r!}\sum_{k=0}^{r} A(n,k)\binom{n-k}{r-k}. \tag{1.8}$$

<u>**Demostración**</u>

Si multiplicamos a ambos lados por $r!$, llegamos a que

$$r!S(n,r)=\sum_{k=0}^{r} A(n,k)\binom{n-k}{r-k}.$$

El lado izquierdo representa el número ordenado de particiones, es decir, las particiones cuyo conjunto de bloques está totalmente ordenado, de $[n]$ en r bloques.

Demostraremos ahora que el lado derecho cuenta el mismo número de objetos. Para ello tomamos una partición p contada por $A(n,k)$. Las k rachas ascendentes de p definen una partición ordenada de $[n]$ en k partes.

- Si $k = r$, entonces no hay nada que probar.
- Si $k < r$, entonces separaremos algunas de las rachas ascendentes en varios bloques de elementos consecutivos, en orden, para conseguir una partición ordenada de r bloques. Ya que actualmente tiene k bloques, aumentamos el número de bloques en $r-k$. Esto se puede conseguir eligiendo $r-k$ de $n-k$ "posiciones huecas"(huecos entre dos entradas consecutivas dentro del mismo bloque).

  Esto demuestra que podemos obtener $\sum_{k=0}^{r} A(n,k)\binom{n-k}{r-k}$ particiones ordenadas de $[n]$ en r bloques por el procedimiento anterior. Además cada partición puede ser obtenida exactamente una vez. De hecho, si escribimos los elementos dentro de cada bloque de la partición creciente, sólo podemos leer las entradas de la partición ordenada de izquierda a derecha y conseguir una única permutación teniendo al menos r rachas ascendentes. Esto hace que podamos recuperar los huecos de las posiciones usadas.

■

Corolario 1.2.26

Para todos los enteros positivos n y k, se tiene

$$A(n,k) = \sum_{r=1}^{k} S(n,r)r!\binom{n-r}{k-r}(-1)^{k-r}. \tag{1.9}$$

Demostración

Consideramos la fórmula (1.8) para cada $r \leq k$ y multiplicamos por $r!$, entonces

$$r!S(n,r) = \sum_{k=0}^{r} A(n,k)\binom{n-k}{r-k}$$

- Si $r = 1$ $\quad 1! \cdot S(n,1) = \sum_{k=0}^{1} A(n,k)\binom{n-k}{1-k} = A(n,1)\binom{n-1}{0}$

- Si $r = 2$

$$\begin{aligned} 2!\cdot S(n,2) &= \sum_{k=0}^{2} A(n,k)\binom{n-k}{2-k} \\ &= A(n,1)\binom{n-1}{1} + A(n,2)\binom{n-2}{0} \end{aligned}$$

La ecuación para r general es

$$r!\cdot S(n,r) = \sum_{i=1}^{k} A(n,i)\binom{n-i}{r-i} \tag{1.10}$$

y la última ecuación

$$k!\cdot S(n,k) = \sum_{i=1}^{k} A(n,i)\binom{n-i}{r-i}. \tag{1.11}$$

Nuestro objetivo es eliminar cada término del lado derecho de (1.11), excepto el término $A(n,k)\binom{n-k}{k-k} = A(n,k)$. Esto se puede conseguir multiplicando (1.10) por $(-1)^{k-r}\binom{n-r}{k-r}$ y haciendo esto para todo r $\in [k-1]$.

De esta forma obtenemos lo siguiente:

$$\sum_{r=1}^{k} S(n,k)r!(-1)^{k-r}\binom{n-r}{k-r} = \sum_{r=1}^{k} r!(-1)^{k-r}\binom{n-r}{k-r}\sum_{i=1}^{r}\frac{1}{r!}A(n,i)\binom{n-i}{r-i}$$

o cambiando el orden de sumación

$$\sum_{r=1}^{k} S(n,k)r!(-1)^{k-r}\binom{n-r}{k-r} = \sum_{i=1}^{r} A(n,i)\binom{n-i}{r-i}\sum_{r=1}^{k}(-1)^{k-r}\binom{n-r}{k-r} \tag{1.12}$$

cuyo lado izquierdo es idéntico al lado derecho de (1.9).

Es obvio que el coeficiente de $A(n,k)$ del lado derecho es $\binom{n-k}{k-k} = 1$. Por lo tanto, nuestra demostración acabará si podemos probar que el coeficiente $t(n,i)$ de $A(n,i)$ en la última espresión es igual a 0 si $i < k$.

Tenemos en cuenta que $\binom{n-i}{r-i} = 0$ si $r < i$. Por tanto, para cualquier $i < k$ fijo, se obtiene lo siguiente:

$$t(n,i)=\sum_{r=i}^{k}\binom{n-i}{r-i}\binom{n-r}{k-r}(-1)^{k-r}=\sum_{i=1}^{r}\binom{n-i}{r-i}\binom{k-n-1}{k-r}=\binom{k-i-1}{k-i}=0$$

por la fórmula de Convolución de Cauchy.

Esto prueba que si $i<k$, entonces $A(n,i)$ desaparece en el lado derecho de (1.12)

Hemos observado que $A(n,k)$ tiene coeficiente 1 ahí, y éste puede ser visto tomando $k=i$ en la última expresión, con $t(n,i)=\binom{-1}{0}=1$. De esta forma tendríamos probado el corolario.

■

Capítulo 2

Inversiones

2.1. La función generatriz del número de inversiones para permutaciones

Definición 2.1.1

Sea $p = p_1 p_2 \cdots p_n$ una permutación. Decimos que (p_i, p_j) es una **inversión** de p si $i < j$, pero $p_i > p_j$.

El **número de inversiones** de p se denotará por $i(p)$ o $inv(p)$ con $0 \leq i(p) \leq \binom{n}{2}$ para todas las n-permutaciones y los dos valores extremos se alcanzan mediante permutaciones $12 \cdots n$ y $n(n-1) \cdots 1$, respectivamente.

Ejemplo 2.1.2

La permutación 42153 tiene cinco inversiones: $(4,2)$, $(4,1)$, $(4,3)$, $(2,1)$ y $(5,3)$.

$\square$

Definición 2.1.3

Sea p una permutación de $[n]$. Para $i = 1, \ldots, n-1$ definimos

$$a_{ij} = a_i(p) = \textbf{número de inversiones} \text{ de } p \text{ de la forma } (i+1, j),$$

es decir, la entrada $(i+1)$ precede exactamente a a_i entradas menores, entonces se verifica

$$inv(p) = \sum_{i=1}^{n-1} a_i.$$

Ejemplo 2.1.4

Sea $p = 246153$ con 7 inversiones las cuales recogemos en la siguiente tabla:

$(2, 1)$	$a_1 = 1$
$(4, 1), (4, 3)$	$a_3 = 2$
$(6, 1), (6, 5), (6, 3)$	$a_5 = 3$
$(5, 3)$	$a_4 = 1$

Tabla 2.1: Tabla de inversiones

□

A continuación definimos la función generatriz de la enumeración de todas las permutaciones de longitud n con respecto a su número de inversiones.

Teorema 2.1.5

Para todos los enteros positivos $n \geq 2$, tenemos

$$\sum_{p \in S_n} x^{i(p)} = I_n(x) = (1 + x)(1 + x + x^2) \cdots (1 + x + x^2 + \cdots + x^{n-1}). \qquad (2.1)$$

<u>**Demostración**</u>

Observamos que los valores $(a_1, a_2, \ldots, a_{n-1})$ con $a_i \in \{0, \ldots, i - 1\}$ definen unívocamente a cada permutación de $[n]$, por lo que cada término de la forma $x^{a_1} \cdots x^{a_{n-1}}$ en el desarrollo de I_n se corresponde con una única permutación.
La demostración del resultado se hará por inducción en n.

- Si $n = 2$, entonces hay dos permutaciones, $p = 12$ que no tiene inversiones y $p' = 21$ que tiene una inversión. Por eso $\sum_{p \in S_2} x^{i(p)} = 1 + x$ como pretendíamos.
  Además, $p = 12$ está representado por el término 1 de la expansión y $p' = 21$ está representado por el término x de la expansión.
- Ahora asumimos que es cierto para $n - 1$ y probamos que es cierto para n.
  Sea p una permutación de longitud $n - 1$. Insertamos la entrada n en p para conseguir la nueva permutación q. Si insertamos n en la última posición no creamos nuevas inversiones; sin embargo si insertamos n en la penúltima

posición de p, creamos una nueva inversión. En general, si insertamos n en p, de manera que le precedan exactamente i entradas de p, creamos i nuevas inversiones. Por lo tanto, dependiendo de donde insertemos n, la nueva permutación q tiene 0 ó 1 ó 2, etc., ó $n-1$ inversiones más que p.

Si p estaba representada por el término de la expansión $x^{a_1}x^{a_2}\cdots x^{a_{n-2}}$ y n se inserta de manera que precede i entradas, entonces q se representa por el nuevo término de la expansión $x^{a_1}x^{a_2}\cdots x^{a_{n-2}}x^i$. Este argumento es válido para todo p, probando (2.1).

■

Definición 2.1.6

Sea

$$I_n(x) = \prod_{j=1}^{n-1}(1+x+\cdots+x^j) = \sum_{k=0}^{\binom{n}{2}} b(n,k)x^k,$$

entonces $b(n,k)$ es el número de n-permutaciones con k inversiones, es decir, el coeficiente de x^k en $I_n(x)$.

Los primeros valores de $b(n,k)$ los recogemos en la siguiente tabla:

$b(n,k)$	k									
	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$	$k=9$	$k=10$
$n=1$	1									
$n=2$	1	1								
$n=3$	1	2	2	1						
$n=4$	1	3	5	6	5	3	1			
$n=5$	1	4	9	15	20	22	20	15	9	4

Tabla 2.2: Números $b(n,k)$

Nos preguntamos a continuación, si es posible encontrar un procedimiento recursivo, o incluso mejor, una fórmula explícita para esos números tal y como lo hicimos para los números $A(n,k)$ en el capítulo anterior.

Lema 2.1.7

Sea $n \geq k$. Entonces

$$b(n+1,k) = b(n+1,k-1) + b(n,k). \tag{2.2}$$

Demostración

Sea $p = p_1p_2 \cdots p_{n+1}$ una $(n+1)$-permutación con k inversiones donde $k \leq n$.

- Si $p_{n+1} = n+1$, entonces podemos omitir $n+1$ desde el final de p y conseguir una n-permutación con k inversiones, lo que explica el segundo sumando del lado derecho de (2.2).
- Si $p_i = n+1$ para $i \leq n$, entonces intercambiamos $n+1$ y la entrada inmediatamente siguiente.
  Este resultado es una $(n+1)$-permutación con $k-1$ inversiones en las cuales la entrada $n+1$ no es la primera posición. Sin embargo, toda $(n+1)$-permutación con $k-1$ inversiones tiene esta propiedad (que $n+1$ no es la primera posición). Esto explica el primer sumando del lado derecho de (2.2).

  Por tanto, queda completa la demostración y también el porqué la condición $n \geq k$ es necesaria.

■

Además (2.2) no se verifica en general si $k > n-1$, pues si $k > \frac{\binom{n}{2}}{2}$ entonces $b(n+1,k) < b(n+1,k-1)$ lo que hace imposible $b(n+1,k) = b(n+1,k-1) + b(n,k)$.

La búsqueda de una fórmula explícita para los números $b(n,k)$ es más difícil incluso si asumimos $n \geq k$.

Examinando el polinomio $I_n(x) = \sum_{k=0}^{\binom{n}{2}} b(n,k)x^k$ podemos deducir que:

$$\begin{aligned}
b(n,0) &= 1 = \binom{n}{0} \\
b(n,1) &= n-1 = \binom{n}{1} - \binom{n}{0} && n \geq 1 \\
b(n,2) &= \binom{n}{2} - \binom{n}{0} && n \geq 2 \\
b(n,3) &= \binom{n+1}{3} - \binom{n}{1} && n \geq 3 \\
b(n,4) &= \binom{n+2}{4} - \binom{n+1}{2} && n \geq 4
\end{aligned}$$

Definición 2.1.8

Una **composición** de n en k partes es una solución de la ecuación

$$a_1 + a_2 + \cdots + a_k = n \text{ con } a_i \in \mathbb{N}^+.$$

Definición 2.1.9

Sea n un entero positivo. Si $a_1 + a_2 + \cdots + a_k = n$ y los a_i son todos enteros positivos, entonces decimos que la k-tupla $(a_1, a_2, \ldots, a_k)$ es una **composición débil** de n en k partes.

Observación 2.1.10

El número de composiciones de n en k partes es $\binom{n-1}{k-1}$, mientras que el número de composiciones débiles de n en k partes es $\binom{n+k-1}{k-1}$.

Definición 2.1.11

Sea $a_1 \geq a_2 \geq \cdots a_m \geq 1$, enteros tales que $a_1 + a_2 + \cdots + a_m = n$. Entonces el vector $a = (a_1, a_2, \ldots, a_m)$ se llama **partición** del entero n y los números a_i son las partes de la partición a. El número total de particiones se denota por $p(n)$.

Ejemplo 2.1.12

Consideramos el entero 6. Las particiones de 6 son

$$(6), (5,1), (4,2), (3,3), (4,1,1), (3,2,1), (2,2,2),$$

$$(3,1,1,1), (2,2,1,1), (2,1,1,1,1), (1,1,1,1,1,1).$$

Por tanto, $p(6) = 11$.

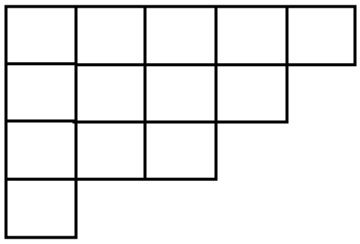
$\square$

Definición 2.1.13

Se define el **diagrama de Ferrers** o **diagrama de Young** de una partición $a = (a_1, \ldots, a_k)$ de n como un arreglo de cajas cuadradas ordenadas en k filas horizontales (justificadas a la izquierda) de tamaños $a_1, \ldots, a_k$ respectivamente ordenadas verticalmente.

Ejemplo 2.1.14

El diagrama de Ferrers de $(5,4,3,1)$ es



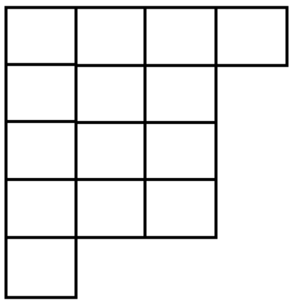
□

Definición 2.1.15

La **partición conjugada** de a es la partición a^* cuyo diagrama de Ferrers es el traspuesto del diagrama de a.

Ejemplo 2.1.16

Considerando la partición del **Ejemplo 2.1.14**, vemos que $a^* = (4, 3, 3, 3, 1)$ y su diagrama de Ferrers es el siguiente



□

2.2. Índice mayor

Definición 2.2.17

Sea $p = p_1 p_2 \cdots p_n$ una permutación. Definimos $D(p)$ como el **conjunto de descensos** de p.

Ejemplo 2.2.18

Sea $p = 4276135$, entonces 1, 3 y 4 son los descensos de p, por lo que $D(p) =$

$\{1, 3, 4\}$.

$\square$

Definición 2.2.19

Sea $p = p_1 p_2 \cdots p_n$ una permutación y definimos el **índice mayor** $maj(p)$ de p como la suma de los descensos de p. Esto es, $maj(p) = \sum_{i \in D(p)} i$.

Ejemplo 2.2.20

Si $p = 415623$, entonces el conjunto de descensos $D(p) = \{1, 4\}$ y $maj(p) = 5$.

$\square$

Teorema 2.2.21

Para todos los enteros positivos n y todos los enteros no negativos k, hay tantas n-permutaciones con k inversiones como n-permutaciones con índice mayor k.

En otras palabras, el número de inversiones y el índice mayor están equidistribuidos en S_n.
Un estadístico s definido en el conjunto de permutaciones S_n que tiene la misma distribución que i se denomina **Mahoniano**.

Demostración

Para cualquier permutación $p = p_1 p_2 \cdots p_n$, decimos que p_i es una entrada grande si $p_i > p_n$ y llamamos a p_i entrada pequeña si $p_i < p_n$.

Vamos a ir probando el resultado recursivamente, definiendo una biyección

$$\phi : S_n \longrightarrow S_n \;\; \forall p \in S_n,$$

donde la igualdad $maj(p) = i(\phi(p))$ se mantiene. Nuestra aplicación ϕ tendrá la característica adicional de mantener el último elemento de p fijo.

Lo probamos por inducción en n. Definimos $\phi(1) = 1$ para el caso inicial de $n = 1$ y $\phi(12) = 12$ y $\phi(21) = 21$ para el caso $n = 2$.
Asumimos que hemos definido ϕ para toda $(n-1)$-permutación, con el fin de definir ϕ para todas las n-permutaciones. Sea $p = p_1 p_2 \cdots p_n$ cualquier n-permutación.

Distinguimos dos casos:

1. Primero consideramos el caso cuando p_{n-1} es una entrada pequeña. En este caso, tomamos $w_p = \phi(p_1p_2\cdots p_{n-1}) = q_1q_2\cdots q_{n-1}$. Sea $q_{i_1}, q_{i_2}, \ldots, q_{i_j}$ las entradas pequeñas de p en w_p. Fijamos $i_o = 0$.
   Sea $Q_j = q_{i_{j-1}+1}\cdots q_{i_j}$ que proporciona la única descomposición de w en subpalabras que contienen exactamente una entrada pequeña y la contiene en el último lugar.

   Por ejemplo, si $q_1\cdots q_6 = 537914$, entonces hay dos entradas pequeñas, 1 y 2 y por tanto $Q_1 = 53$ y $Q_2 = 791$. Ahora definimos

   $$f(Q_j) = \begin{cases} Q_j & \text{si } Q_j \text{ es a lo sumo de longitud 1} \\ x_mx_1x_2\cdots x_{m-1} & \text{si } Q_j = x_1x_2\cdots x_m, \text{ con } m \geq 2 \end{cases}$$

   Finalmente, definimos

   $$f(w_p) = f(Q_1)f(Q_2)\cdots f(Q_k)$$

   y

   $$\phi(p) = f(w_p)p_n.$$

   Por ejemplo, sea $n = 5$ y $p = 54213$. Entonces tenemos $w_p = \phi(5421) = 5421$ y $Q_1 = 542$, $Q_2 = 1$. Por lo tanto, $f(w_p) = 2541$, de manera que $\phi(p) = 25413$.

2. Cuando p_{n-1} es una entrada grande, el procedimiento es muy similar. La única diferencia es en la definición de las subpalabras Q_j. En este caso, Q_j proporciona la única descomposición de w en subpalabras que contienen exactamente una entrada grande y la contiene en la útima posición.

   Por ejemplo, sea $n = 5$ y $p = 13452$. Entonces tenemos $w_p = \phi(1345) = 1345$ y $Q_1 = 13$, $Q_2 = 4$, $Q_3 = 5$. Por lo tanto, $f(w_p) = 3145$ y $\phi(p) = 31452$.

Es fácil ver que $\phi : S_n \longrightarrow S_n$ es una biyección. De hecho, verificando ambos casos, vemos que la primera regla fue usada para crear $\phi(p)$ si y sólo si el último elemento de $\phi(p)$ es mayor que el primer elemento de $\phi(p)$.

Una vez que conocemos la regla que fue usada para crear $\phi(p)$ podemos recuperar w_p desde $f(w_p)$. De hecho, si la primera (respectivamente segunda) regla fue usada, entonces $f(Q_i)$ son las subpalabras que contienen sólo una entrada pequeña (respectivamente grande) y contiene la entrada pequeña (respectivamente grande) en la primera (respectivamente última) posición. Como f es una biyección,

es posible recuperar Q_i desde $f(Q_i)$ y por tanto es posible recuperar w_p.
Finalmente, $\phi : S_{n-1} \longrightarrow S_{n-1}$ es una biyección por inducción, por eso, recuperamos $p_1p_2\cdots p_{n-1}$ desde $f(p_1p_2\cdots p_{n-1}) = w_p$.

Todavía, necesitamos probar que $\phi : S_n \longrightarrow S_n$ tiene la propiedad deseada, es decir, transforma una permutación con índice mayor k en una permutación con k inversiones. Probamos esto, considerando, los dos casos de arriba por separado.

1. Cuando p_{n-1} es una entrada pequeña, entonces

$$maj(p) = maj(p_1p_2\cdots p_{n-1}) = i(\phi(p_1p_2\cdots p_{n-1})) = i(w_p) \tag{2.3}$$

¿Cómo cambia la aplicación f el número de inversiones de w_p? No cambia el orden entre las entradas pequeñas ni entre las entradas grandes. Si una entrada pequeña pertenece a la subpalabra Q_j de longitud $t > 1$, entonces salta hacia delante y pasa a preceder a $t-1$ entradas grandes de Q_j, decreciendo el número de inversiones por $t-1$.

Como cada entrada grande sería precedida por una entrada pequeña, la disminución total en el número de inversiones es igual al número de entradas grandes, es decir, $n - p_n$.
Sin embargo, fijando p_n al final de $f(w_p)$ crearemos precisamente $n-p_n$ nuevas inversiones. Por lo tanto

$$i(\phi(p)) = i(f(w_p)p_n) = i(w_p)$$

la cual comparada con (2.3) demuestra que $maj(p) = i(\phi(p))$ como queríamos.

2. Cuando p_{n-1} es una entrada grande, entonces

$$maj(p) = maj(p_1p_2\cdots p_{n-1}) + (n-1) \tag{2.4}$$

$$= i(\phi(p_1p_2\cdots p_{n-1})) + n - 1 = i(w_p) + n - 1 \tag{2.5}$$

Cuando f se aplica a w_p, cada entrada grande salta perteneciendo a una subpalabra de longitud $t > 1$, salta hacia delante, pasa todas las $t-1$ entradas pequeñas de la subpalabra e incrementa el número de inversiones por $t-1$. Cada entrada pequeña es pasada por una entrada grande, por eso, el incremento en total en el número de inversiones es igual al número de entradas pequeñas, es decir, p_{n-1}. Por otro lado, fijando p_n al final de $f(w_p)$ creará precisamente $n-p_n$ nuevas inversiones. Por lo tanto

$$i(\phi(p)) = i(f(w_p))p_n = i(w_p) + (p_n - 1) + (n - p_n) = i(w_p) + n - 1$$

la cual comparada con (2.4) demuestra que otra vez $maj(p) = i(\phi(p))$ como queríamos.

■

2.3. Una aplicación. Determinantes y grafos

2.3.1. La definición explícita de los determinantes

Algunos autores definen el determinante de una matriz cuadrada de dimensión n de forma recursiva:

- Si $n = 1$, $\det(a) = a$.
- Si $n = 2$, $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$.
- Si $n > 2$,
$$\det A = \sum_{j=1}^{n} (-1)^{j-1} a_{1j} A_{1j}$$
donde A_{ij} es la matriz de dimensiones $(n-1) \times (n-1)$ y j-ésima columna de A.
Veremos que esta definición recursiva implica el siguiente resultado.

Teorema 2.3.22

Sea $A = (a_{ij})$ una matriz $n \times n$. Entonces tenemos

$$\det A = \sum_{p \in S_n} (-1)^{i(p)} a_{1_{p_1}} a_{2_{p_2}} \cdots a_{n_{p_n}}. \tag{2.6}$$

Esto es, el determinante de A se obtiene tomando todas las $n!$ posibles n-tuplas de entradas en cada fila y cada columna y multiplicando los elementos de cada n-tupla juntoS. Finalmente tomamos una suma de estos $n!$ productos, donde el signo es determinado por la paridad de $i(p)$ y p es una permutación determinada por cada n-tupla elegida.

En otras palabras, las n-tuplas corresponden a todas las posibles colocaciones de n torres en un tablero de ajedrez de $n \times n$ de manera que no hay dos de ellos pegado con otro.

<u>**Demostración**</u>

Probamos el teorema por inducción en n.

- Los casos iniciales $n = 1$ y $n = 2$ son obvios.
- Asumimos que es cierto para matrices de dimensión $(n-1) \times (n-1)$, lo que significa que

$$\det A_{1j} = \sum_{q} (-1)^{i(q)} a_{2_{q_2}} a_{3_{q_3}} \cdots a_{n_{q_n}} \tag{2.7}$$

donde $q = q_1 q_2 \cdots q_n$ es una permutación parcial, eso es, una lista ordenada de enteros $1, 2, \ldots, j-1, j+1, \ldots, n$.

Por lo tanto, $a_{1j} \cdot \det A_{1j}$ contribuirá a los productos de todas las n-tuplas empezando con a_{1j} para $\det A$. En otras palabras, $a_{1j} \cdot \det A_{1j}$ corresponderá a todas las colocaciones de torres en posición de no ataque en cuales, hay una torre en posición j de la primera fila. Este argumento se puede aplicar para cada j. Por eso, el teorema se probará si podemos demostrar que los signos de esos productos son los adecuados.

Sustituyendo la expresión probada por A_{1j} por la fórmula (2.7) vemos que el signo de la n-tupla que pertenece a q es $(-1)^{j+i(q)}$. Y de hecho, la permutación $p = jq_2q_3 \cdots q_n$ tiene precisamente $j-1$ inversiones más que la permutación parcial $q = q_2q_3 \cdots q_n$ puesto que j es más grande que los otros $j-1$ elementos. Esto demuestra que la n-tupla tiene signo $(-1)^{j-1}$.

■

Ejemplo 2.3.23

Sea $n = 3$. Hay tres 3-permutaciones con un número par de inversiones, 123, 312, 231 y hay tres 3-permutaciones con un número impar de inversiones, 132, 213 y 321. Entonces tenemos que:

$$\det A = a_{11}a_{22}a_{33} + a_{13}a_{21}a_{32} + a_{12}a_{23}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}.$$

□

2.3.2. Matchings perfectos en grafos bipartitos

Definición 2.3.24

Un **grafo** es un par $G = (V, E)$, donde V es un conjunto de vértices o nodos (normalmente finito) y E un conjunto de aristas o arcos que relacionan estos nodos, representando relaciones binarias entre los elementos de un conjunto.

Definición 2.3.25

Se llama **orden** del grafo $G = (V, E)$ al número de vértices de G. Se representa por $|V|$.

Definición 2.3.26

Un **par no ordenado** es un conjunto de la forma $\{a, b\}$, de manera que $\{a, b\} = \{b, a\}$. Para los grafos, estos conjuntos pertenecen al conjunto de las partes de V, denotado por $\mathcal{P}(V)$. Si el conjunto V tiene n elementos, entonces su cardinal viene dado por

$$|\mathcal{P}(V)| = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} + \cdots + \binom{n}{n} = 2^n = 2^{|V|}.$$

Ejemplo 2.3.27

Sea el conjunto $A = \{1, 2, 3\}$. El conjunto de partes de A es:

$$\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}\}$$

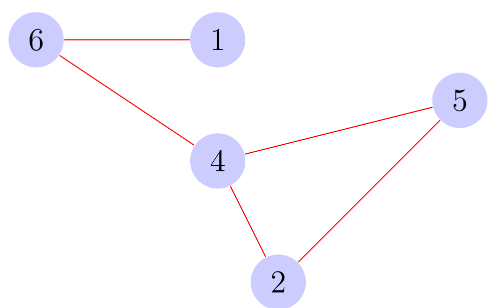
y su cardinal $|\mathcal{P}(A)| = 2^3 = 8$.

$\square$

Definición 2.3.28

Decimos que $G = (V, E)$ es un **grafo no dirigido** o simplemente un grafo si $V \neq \emptyset$ y $E \subseteq \{x \in \mathcal{P}(V) : |x| = 2\}$ es un conjunto de pares no ordenados de elementos de V.

Un ejemplo de grafo no dirigido es el siguiente:



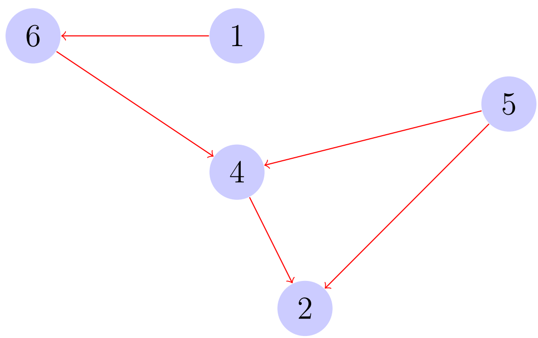
Definición 2.3.29

Un **par ordenado** es una pareja de objetos en la que se distingue un elemento de otro. El par ordenado cuyo primer elemento es a y segundo elemento b se denota por (a, b), que es diferente del par (b, a), en cuyo caso, el primer elemento es b y el segundo a.

Definición 2.3.30

Decimos que $G = (V, E)$ es un **grafo dirigido** si $V \neq \emptyset$ y $E \subseteq \{(a, b) \in V \times V : a \neq b\}$ es un conjunto de pares ordenados de elementos de V. Es decir, una arista (a, b) tiene como nodo inicial a a y como nodo final a b.

Un ejemplo de grafo dirigido es el siguiente:



Definición 2.3.31

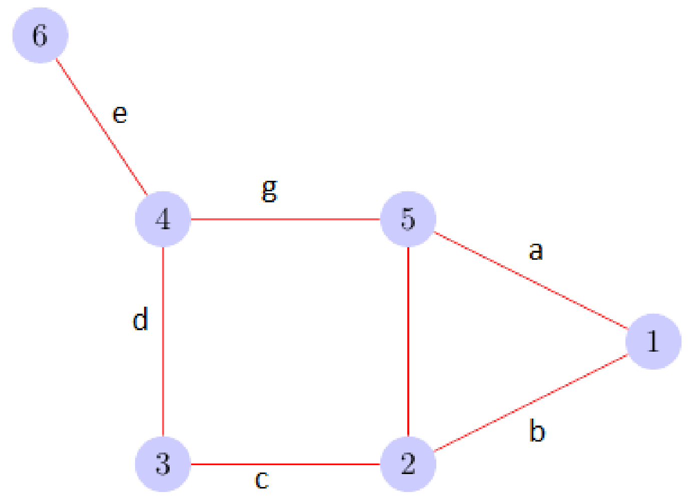
La **matriz de incidencia** de un grafo G es la matriz $C(G) = (c_{ij})$ en la cual

$$c_{ij} = \begin{cases} 1 & \text{si la arista } i \text{ incide en el vértice } j \\ 0 & \text{en otro caso} \end{cases}$$

Luego, la suma de los 1's en cada fila indica la cantidad de aristas que inciden sobre ese nodo.

Ejemplo 2.3.32

Consideremos el grafo siguiente:



cuya matriz de incidencia es:

$$\begin{array}{cc} \begin{matrix} a & b & c & d & e & f & g \end{matrix} & \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} & \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{matrix} \end{array}$$

$\square$

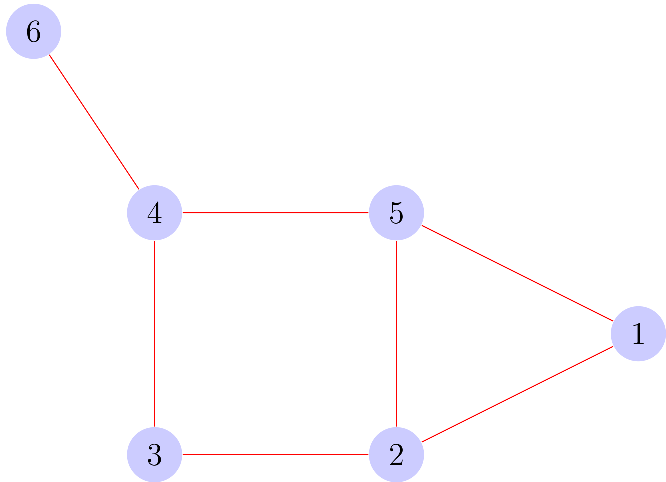
Definición 2.3.33

La **matriz de adyacencia** de un grafo G es la matriz $D(G) = (d_{ij})$ en la cual

$$d_{ij} = \begin{cases} 1 & \text{si el vértice } i \text{ está conectado con el vértice } j \\ 0 & \text{en otro caso} \end{cases}$$

Ejemplo 2.3.34

Consideremos el grafo siguiente:



cuya matriz de adyacencia es:

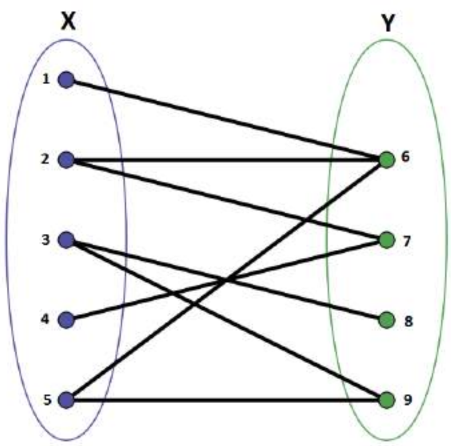
$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$\square$

Definición 2.3.35

Un grafo $G = (V, E)$ es **bipartito** si V puede descomponerse en dos subconjuntos X e Y de forma que todas las aristas de G tienen un vértice en X y otro en Y.

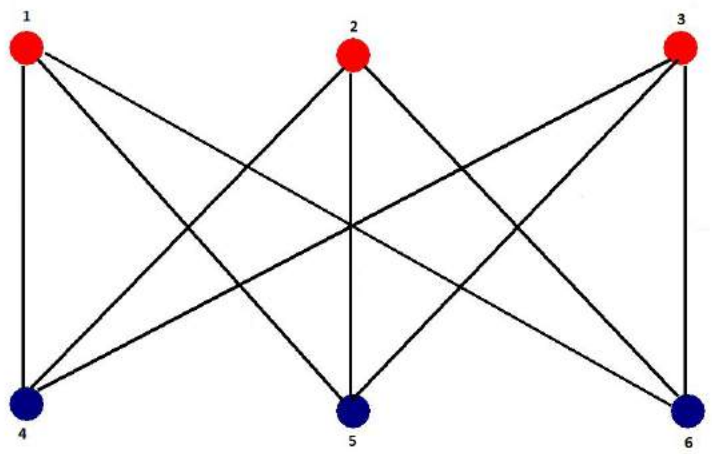
Un ejemplo de grafo bipartito es el siguiente:



Definición 2.3.36

Un grafo $G = (V, E)$ es **bipartito completo** si V puede descomponerse en dos subconjuntos X e Y de forma que todos los vértices de X están conectados con todos los vértices de Y.

Un ejemplo de grafo bipartito completo es el siguiente:



Definición 2.3.37

La **matriz de adyacencia** truncada de un grafo simple bipartito G es la matriz $B(G) = (b_{ij})$ en la cual

$$b_{ij} = \begin{cases} 1 & \text{si hay una arista entre } i \in X \text{ y } j \in Y \\ 0 & \text{en otro caso} \end{cases}$$

En otras palabras, las filas de B representan los vértices de X y las columnas de B representan los vértices de Y.

Ejemplo 2.3.38

Consideramos el grafo bipartito de la **Definición 2.3.35**, entonces su matriz de adyacencia es la siguiente:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

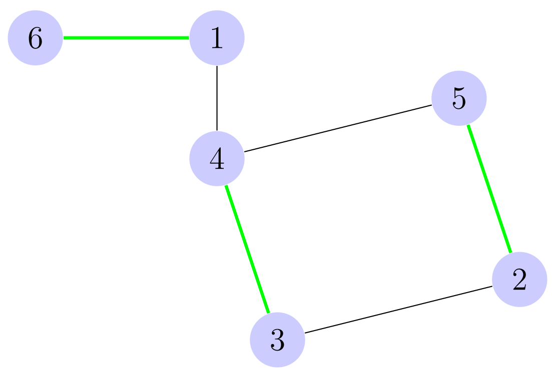
□

Definición 2.3.39

Dado un grafo $G = (V, E)$, un **matching** es un conjunto de ejes no adyacentes dos a dos, es decir que no tienen ningún vértice común. Un matching es **perfecto** si contiene a todos los vértices del grafo.

Ejemplo 2.3.40

Un ejemplo de un grafo matching perfecto lo podemos visualizar a continuación representado de color verde:



□

Teorema 2.3.41

Sea G un grafo bipartito con $[X] = [Y] = n$ que no contenga a un matching perfecto. Entonces $\det B(G) = 0$.

Demostración

Probamos que $\det B(G) = 0$, demostrando que todos los $n!$ sumandos de la definición explicíta (2.6) de $B(G)$ son igual a 0. Esto se debe a la existencia de un término distinto de cero $b_{1_{p1}} b_{2_{p2}} \cdots b_{n_{pn}}$, es decir, a la existencia de un matching perfecto, en el cual $i \in X$ es emparejado con $p_i \in Y$.

■

Definición 2.3.42

El número de todos los matching perfectos de G pueden obtenerse mediante el cálculo de la **permanente** de $B(G)$ definida por

$$perB(G) = \sum_{p \in S_n} b_{1_{p1}} b_{2_{p2}} \cdots b_{n_{pn}}.$$

es decir, $perB(G)$ se define como $\det B(G)$, excepto que cada término se añade con un signo positivo.

Capítulo 3

Permutaciones como producto de ciclos

Introducción

Las permutaciones de un conjunto finito de n elementos se pueden distinguir y enumerar de acuerdo a ciertas características que poseen.

Este capítulo está dedicado a la enumeración de las permutaciones de un conjunto de n elementos. Estas permutaciones se descomponen en un número determinado o no de ciclos de cualquier longitud, cuyo número de ciclos correponde a un subconjunto de números enteros no negativos.

Además, veremos como las permutaciones se clasifican en pares e impares, en función del número de trasposiciones en las que pueden ser descompuestas. La enumeración de las permutaciones pares e impares de ciclos se reduce al problema anterior de la enumeración de las permutaciones por ciclos.

Por último, estudiaremos los números de Stirling de primera clase que constituyen el coeficiente de las expansiones de los factoriales en potencias, así como sus propiedades básicas, funciones generatrices y expresiones explícitas.

3.1. Descomposición de una permutación en ciclos

Definición 3.1.1

Sea $f : [n] \to [n]$ una biyección. Entonces decimos que f es una **permutación**

del conjunto $[n]$.

Ejemplo 3.1.2

Sea 43251 una permutación de longitud cinco. Entonces decimos que la función $f : [5] \to [5]$ definida por $f(1) = 4$, $f(2) = 3$, $f(3) = 2$, $f(4) = 5$ y $f(5) = 1$ es una permutación de [5].

$\square$

Definición 3.1.3

Sean f y g dos permutaciones de $[n]$. Podemos definir su **producto** $f \cdot g$ como $(f \cdot g)(i) = g(f(i))$ para $i \in [n]$, es decir, el producto de dos permutaciones se define como la composición de éstas.

Ejemplo 3.1.4

Consideramos las permutaciones

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 6 & 4 & 1 \end{pmatrix}$$

y

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 3 & 6 & 2 \end{pmatrix}$$

Luego;

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 1 & 2 \end{pmatrix}$$

$\square$

El conjunto de todas las permutaciones de $[n]$ forman un grupo cuando lo dotamos con esta operación.

Por tanto, el conjunto de todas las permutaciones de $[n]$ se denota por S_n y se llama **grupo simétrico** de grado n, es decir, S_n representa el grupo de las biyecciones del conjunto $\{1, \ldots, n\}$ sobre sí mismo. Además cada grupo finito de n elementos es un subgrupo de S_n.

Proposición 3.1.5

El conjunto de las permutaciones S_n verifica las siguientes propiedades:

1. S_n es un grupo finito con $|S_n| = n!$.

2. Si $n > 2$, entonces S_n no es abeliano, por eso, en general $fg \neq gf$.

Una forma de escribir las permutaciones es mediante la **notación cíclica**, por ejemplo, $f = (13)(245)$. Cuando leemos una permutación en esta notación, hacemos una aplicación con cada elemento y el que se une a su derecha, excepto para los elementos finales de cada ciclo, que se asignan al primer elemento de dicho ciclo.

Definición 3.1.6

Un elemento $\sigma \in S_n$ es un **ciclo** de longitud m ($m \leq n$) cuando existe

$$I = \{a_1, a_2, \ldots, a_m\} \subset \{1, 2, \ldots, n\}$$

tal que:

1. $\sigma(a_i) = a_{i+1} \quad \forall i = 1, 2, \ldots, m-1, \quad \sigma(a_m) = a_1$
2. $\sigma(j) = j \ \ \forall j \notin I$

Es decir, el ciclo σ lo notaremos simplemente por $(a_1 a_2 \cdots a_m)$ y al número m lo llamaremos **longitud** del ciclo σ. Con este notación se tiene

$$(a_1 a_2 \cdots a_m) = (a_2 \cdots a_m a_1) = \cdots = (a_m a_1 \cdots a_{m-1}).$$

Definición 3.1.7

Diremos que dos ciclos $(a_1 \cdots a_m)$ y $(b_1 \cdots b_r)$ son **disjuntos** si

$$\forall i, j \quad 1 \leq i \leq m, \ \ 1 \leq j \leq r, \ \ a_i \neq b_j.$$

Luego, si $\sigma, \tau \in S_n$, son dos ciclos disjuntos, se tiene que $\sigma\tau = \tau\sigma$.

Definición 3.1.8

Sea $\sigma \in S_n$ con $\sigma = \sigma_1 \cdots \sigma_k$ la descomposición de σ en producto de ciclos disjuntos. Entonces, el **orden** de σ se define como

$$o(\sigma) = mcm(o(\sigma_1), \ldots, o(\sigma_k)).$$

Ejemplo 3.1.9

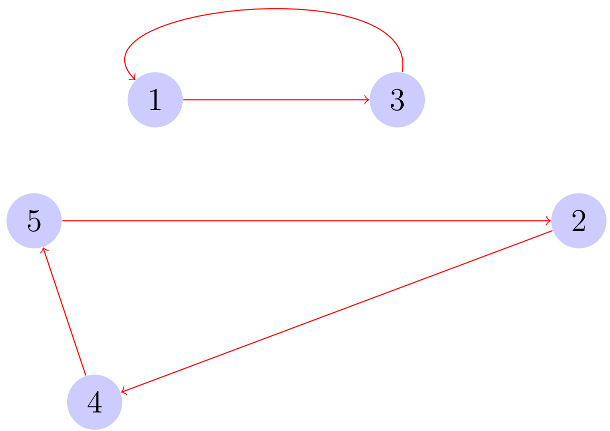
En S_7, la siguiente permutación se descompone en ciclos disjuntos de la siguiente forma

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 7 & 1 & 2 & 4 \end{pmatrix} = (135)(26)(47)$$

$\square$

Ejemplo 3.1.10

La permutación $f = 34152$ indica que f permuta cíclicamente los elementos 3 y 1 entre ellos y los elementos 2, 4, 5 entre ellos. Este fenómeno está ilustrado a continuación:



$\square$

Ejemplo 3.1.11

Sea $g = (12)(356)(4)$ una permutación, para la cual podemos hacer las siguientes precisiones:

- Primero, si los ciclos son disjuntos, el orden entre los ciclos no importa, es decir, $(12)(356)(4) = (356)(4)(12) = (4)(12)(356)$
  De hecho, la imagen de cada $i \in [n]$ sólo depende de la posición dentro del ciclo y algunos otros elementos en el ciclo.
- Segundo, si un ciclo tiene al menos tres elementos, entonces el orden de los elementos dentro de cada ciclo importa hasta un cierto punto. De hecho, los ciclos (356), (563) y (635) describen la misma acción de g en los elementos 3, 5 y 6.

$\square$

Nos gustaría tener un único modo de escribir nuestras permutaciones usando la notación de ciclos. Por tanto, escribiremos el elemento más grande de cada ciclo primero y organizaremos los ciclos en orden creciente de sus primeros elementos. Este modo de escribir las permutaciones se llama **notación cíclica canónica**.

Ejemplo 3.1.12

La permutación $(312)(45)(8)(976)$ está en notación cíclica canónica.

□

Definición 3.1.13

Una trasposición es un ciclo de orden dos.

Teorema 3.1.14

Toda permutación de S_n, distinta de 1, se puede descomponer como producto de trasposiciones.

<u>Demostración</u>

Basta probar que todo ciclo de S_n puede ser compuesta en producto de trasposciones. Sea, pues $\sigma = (a_1 a_2 \cdots a_m)$, entonces

$$(a_1 a_2 \cdots a_m) = (a_1 a_m) \cdots (a_1 a_3)(a_1 a_2).$$

■

Ejemplo 3.1.15

Haciendo uso del **Ejemplo 3.1.9**, tenemos que la descomposción en trasposiciones es la siguiente:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 7 & 1 & 2 & 4 \end{pmatrix} = (135)(26)(47) = (15)(13)(26)(47).$$

□

Nota 3.1.16

La descomposición de una permutación como producto de trasposiciones no es única. Por ejemplo (23) = (13)(23)(12).

3.1.1. Una aplicación. Signo y determinantes

La descomposición en ciclos de una permutación f aporta mucha información sobre f.

Un modo común de ajustar las permutaciones en los marcos algebráicos es definiendo **matrices de permutación** es decir, matrices cuadradas cuyas entradas son todas igual a 0 ó 1 y contienen exactamente un 1 en cada fila y cada columna. Hay dos formas igualmente útiles para hacer esto.

Sea $p = p_1p_2\cdots p_n$ una n-permutación y sea A_p una matriz de dimensión $n \times n$

$$A_p(j,i) = \begin{cases} 1 & \text{si } p_i = j \\ 0 & \text{en otro caso} \end{cases}$$

Además la aplicación $f : S_n \to \mathbb{R}^{n\times n}$ definida por $f(p) = A_p$ es un homomorfismo, es decir, $A_{pq} = A_pA_q$.

Por ejemplo, si $p = 3421 = (4132)$, entonces tenemos

$$A_p = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Ahora sea, B_p, una matriz de dimensión $n \times n$ definida por

$$B_p(i,j) = \begin{cases} 1 & \text{si } p_i = j \\ 0 & \text{en otro caso} \end{cases}$$

Entonces

$$B_p = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Para cualquier p, la matriz B_p es la traspuesta de A_p. Además, $A_pB_p = B_pA_p = I$ así que A_p y B_p son inversas una de la otra. Por tanto, la inversa de una matriz de permutación es su traspuesta.

Comparando las definiciones de A_p y B_p, podemos preguntarnos cuando la primera es más fácil de usar y cuando lo es la segunda. La ventaja de la primera definición es que la aplicación $f : S_n \to \mathbb{R}^{n\times n}$ definida por $f(p) = A_p$ es un homomorfismo. Esto no es verdad para la aplicación $g : S_n \to \mathbb{R}^{n\times n}$ definida por $g(p) = B_p$. Esta aplicación es un anti-homomorfismo, es decir, $B_{pq} = B_q B_p$. Esto puede ser útil cuando usamos nuestras matrices para permutar vectores de tamaño n.

Por ejemplo, sea

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

Si la permutación $p = 3421 = (4132)$ actúa en las coordenadas de estos vectores, lleva el vector $\mathbf{x}$ en $p(\mathbf{x}) = \begin{pmatrix} x_3 \\ x_4 \\ x_2 \\ x_1 \end{pmatrix}$ obtendríamos este vector simplemente tomando el producto $B_p\mathbf{x}$. Si ahora otra permutación q actúa en el vector $p(\mathbf{x})$, entonces obtenemos la imagen calculando $B_q(B_p\mathbf{x}) = B_{pq}(\mathbf{x})$. Si en lugar del vector columna $\mathbf{x}$, hemos trabajado con el vector fila $\mathbf{y} = (y_1, y_2, y_3, y_4)$, entonces usaremos las matrices A_p y A_q para calcular las imágenes y yA_p y $yA_{pq} = yA_pA_q$.

3.2. Permutaciones pares e impares

Una permutación de un conjunto finito W_n ya sea un ciclo o una descomposición en ciclos disjuntos, la descomposición es única salvo reordenamiento de ciclos. Además, cada ciclo se puede generar por trasposiciones. De hecho, un ciclo (w_i) de longitud 1 se puede generar como $(w_i) = (w_i w_j)(w_j w_i), i \neq j$, mientras que un ciclo $(w_{i_1} w_{i_2} \cdots w_{i_{k-1}} w_{i_k})$ de longitud $k \geq 2$ se puede generar por $k-1$ trasposiciones como

$$(w_{i_1} w_{i_2} \cdots w_{i_{k-1}} w_{i_k}) = (w_{i_1} w_{i_k})(w_{i_1} w_{i_{k-1}}) \cdots (w_{i_1} w_{i_2})$$

Como consecuencia, una permutación de un conjunto finito W_n se puede descomponer en trasposiciones. Pero mientras que la descomposición de una permutación en ciclos disjuntos es única salvo reordenamiento de ciclos, la descomposición en trasposiciones entre los que tienen dos o más elementos en común se puede realizar de diferentes formas. Sin embargo, en estas descomposiciones diferentes de una permutación, el número de trasposiciones es en cualquiera de los casos par o impar.

Definición 3.2.17

Una permutación se llama **impar** si tiene un número impar de trasposiciones. Análogamente, una permutación se llama **par** si tiene un número par de trasposiciones.

Ejemplo 3.2.18

Consideramos el conjunto $\{1, 2, 3\}$ el cual tiene 6 permutaciones:

$$(12), (13), (23), (123), (231), \mathrm{Id}$$

. Entonces (12), (13) y (23) son permutaciones impares, pues son una única trasposición; en cambio, (123) = (13)(12), (231) = (21)(23) e Id son permutaciones pares, pues estan formadas por dos trasposiciones.

□

La siguiente proposición demuestra que tenemos que ser cuidadosos con las palabras impar y par, ya que un ciclo es par, (impar) si está formado por un número impar, (par) de elementos, respectivamente.

Porposición 3.2.19

Una permutación que consta de exactamente un ciclo par, (impar) es impar, (par) respectivamente.

Demostración

Probamos por inducción en n, longitud de un ciclo.

• Para $n = 1$ y $n = 2$, la afirmación es cierta.

• Ahora, sea $n \geq 3$ y consideramos el ciclo $(p_1 p_2 \cdots p_n)$ de tal forma que $(p_1 p_2 \cdots p_n) = (p_1 p_2 \cdots p_{n-1})(p_{n-1} p_n)$. La multiplicación por $(p_{n-1} p_n)$ al final simplemente intercambia las últimas dos entradas de $(p_1 p_2 \cdots p_{n-1})$ y por tanto, se incrementa el número de inversiones en una unidad o decrece en una unidad. En cualquiera de los dos casos, cambia la paridad del número de inversiones. Luego, la prueba se tiene por inducción en la hipótesis.

■

Lema 3.2.20

Sea p una permutación. Entonces las siguientes afirmaciones son equivalentes.

(i) p es par.

(ii) $\det A_p = \det B_p = 1$.

(iii) El número de ciclos par de p es par.

Demostración

- *(i)* $\Leftrightarrow$ *(ii)*. Esto se tiene por la definición de determinantes, pues el determinante de una matriz de permutación B_p sólo tiene un término distinto de cero y este es $(-1)^{i(p)} \prod_{i=1}^{n} b_{i_{p(i)}}$. El resultado se tiene con cada término ya que el signo del producto es igual a 1.

- *(ii)* $\Leftrightarrow$ *(iii)*. Puesto que p es el producto de sus ciclos, por la **Proposición 3.2.19**, los ciclos pares corresponden a permutaciones impares, por eso el determinante de sus matrices de permutación es -1. Por tanto, tiene que haber un número par de ellos para que el determinante de su producto sea 1.

■

En particular, el producto de dos permutaciones pares es par y la inversa de una permutación par es par. Como la permutación identidad es par, el conjunto de todas las permutaciones pares en S_n forman un subgrupo.

Este subgrupo se llama **grupo alternado** de grado n, se denota por A_n y tiene $\frac{n!}{2}$ elementos para $n \geq 2$. Sabemos que A_n es un grupo simple si $n \geq 5$, es decir, sólo tiene como subgrupos normales al grupo trivial y a sí mismo. Además A_n es mayor que cualquier subgrupo propio de S_n. De hecho, otro subgrupo propio de S_n es de tamaño al menos $(n-1)!$.

3.3. Tipos de permutaciones

Es común preguntarse cuántas n-permutaciones tienen una estructura de ciclo dado, por ejemplo, cuántas 12-permutaciones contienen un 4-ciclo, dos 3-ciclos, un 2-ciclo y cero 1-ciclo.

Otra cuestión sería cuántas n-permutaciones tienen exactamente k ciclos. Para facilitar la respuesta de la primera cuestión, creamos la siguiente definición.

3.3.1. El tipo de una permutación

Definición 3.3.21

Sea p una n-permutación que tiene exactamente a_i ciclos de longitud i para todos los enteros positivos $i \in [n]$. Entonces decimos que p es de **tipo** $(a_1, a_2, \ldots, a_n)$.

Ejemplo 3.3.22

La permutación $p = (4)(56)(27398)$ es de tipo $(1, 1, 0, 0, 1, 0, 0, 0, 0)$.

$\square$

Proposición 3.3.23

Sea $(a_1, a_2, \ldots, a_n)$ una n-tupla de enteros no negativos tales que $\displaystyle\sum_{i=1}^{n} a_i i = n$. Entonces el número de n-permutaciones del tipo $(a_1, a_2, \ldots, a_n)$ es

$$\frac{n!}{a_1! a_2! \cdots a_n! 1^{a_1} 2^{a_2} \cdots n^{a_n}}.$$

<u>**Demostración**</u>

Escribimos los elementos de $[n]$ en orden lineal en uno de los $n!$ modos posibles. A continuación colocamos paréntesis entre los números de tal forma que las primeras a_1 entradas son los a_1 ciclos de longitud 1, las siguientes $2a_2$ entradas forman los a_2 ciclos de longitud 2, etc.

Las permutaciones que obtenemos de este modo serán del tipo $(a_1, a_2, \ldots, a_n)$, pero no serán todas diferentes. De hecho, los conjuntos de entradas que forman ciclos de la misma longitud pueden ser permutados entre sí sin cambiar el resultado de la permutación.

Por tanto, obtenemos cada permutación de $a_1!a_2! \cdots a_n!$ órdenes lineales permutando ciclos de la misma longitud. Finalmente, cada i-ciclo se puede obtener de i modos diferentes pues cualquier entrada puede ser la primera posición. Por lo que incluso, si fijamos los conjuntos de entradas en cada ciclo, hay $1^{a_1}2^{a_2} \cdots n^{a_n}$ órdenes lineales diferentes que podrían dar lugar a cualquier permutación del tipo $(a_1, a_2, \ldots, a_n)$.

Esto demuestra, en general, que cada permutación se obtiene de

$$a_1!a_2! \cdots a_n!1^{a_1}2^{a_2} \cdots n^{a_n}$$

órdenes lineales lo que prueba el resultado.

■

Como consecuencia del resultado anterior, sabemos que existen $(n-1)!$ permutaciones de longitud n que constan de un n-ciclo y $\dfrac{(2n)!}{n!2^n}$ permutaciones de longitud $2n$ que constan de n ciclos de longitud 2.

3.3.2. Una aplicación. Permutaciones conjugadas

Definición 3.3.24

En el grupo simétrico S_n dos permutaciones g y h se dicen **conjugadas** la una de la otra si existe un elemento $f \in S_n$ talque fgf^{-1}.

En otras palabras, dos permutaciones son conjugadas en S_n si y sólo si se obtienen como composición del mismo número de ciclos disjuntos de las mismas longitudes.

Observación 3.3.25

La relación "g y h son permutaciones conjugadas" es una relación de equivalencia.

Definición 3.3.26

Las **clases de conjugación** de un $\sigma \in S_n$ están formadas por aquellas permutaciones que tienen la misma estructura cíclica que σ.

Ejemplo 3.3.27

En S_5, las permutaciones $(123)(45)$ y $(143)(25)$ son conjugadas; en cambio, $(123)(45)$ y $(12)(45)$ no lo son.

□

El grupo S_3, está formado por 6 permutaciones de tres elementos. Tiene tres clases de conjugación, que son las siguientes:

- La identidad: $(123 \longrightarrow 123)$.
- Las permutaciones que intercambian dos elementos:
$$(123 \longrightarrow 231, 123 \longrightarrow 213, 123 \longrightarrow 321)$$
.
- Las permutaciones cíclicas de tres elementos:
$$(123 \longrightarrow 231, 123 \longrightarrow 312)$$
.

La descomposición en ciclos de g y h revelan si son permutaciones conjugadas o no. Este es el contenido del siguiente lema.

Lema 3.3.28

Los elementos g y h de S_n son conjugados en S_n si y sólo si son del mismo tipo.

Demostración

Recordamos que si g y h son dos n-permutaciones, entonces la acción gh en $[n]$ se obtiene aplicando primero g a $[n]$ y luego aplicando h al resultado.

Primero suponemos que g y h son conjugadas, es decir, $fgf^{-1} = h$ para algunos $f \in S_n$.

Sea $(b_1, b_2, \ldots, b_k)$ un ciclo de g. Entonces $g^i(b_1) = b_{i+1} \ \forall i \in [k-1]$ y $g^k(b_1) = b_1$. Como $h = fgf^{-1}$, tenemos $h^i = fgf^{-1}fgf^{-1} \cdots fgf^{-1} = fg^if^{-1}$. Por lo tanto, $h^i(x) = (fg^if^{-1})(x)$. Ahora elegimos x tal que $f(x) = b_1$. Entonces

$$(fg^if^{-1})(x) = f^{-1}(g^i(b_1)) = f^{-1}(b_{i+1}) \quad \text{si} \quad i \in [k-1] \quad \text{y} \quad (fg^kf^{-1})(x) = f^{-1}(b_1).$$

Así multiplicando por f a la izquierda y f^{-1} a la derecha, el ciclo $(b_1, b_2, \ldots, b_k)$ se transforma en el ciclo $(f^{-1}(b_1), \ldots, f^{-1}(b_k))$, por lo que los k-ciclos de g y h se corresponden biyectivamente.

Por último suponemos que g y h son del mismo tipo. Construimos una permutación f tal que $fgf^{-1} = h$.

Si $(b_1, b_2, \ldots, b_k)$ es un ciclo de g y $(c_1, c_2, \ldots, c_k)$ es un ciclo de h, entonces el argumento del párrafo anterior demuestra que debemos elegir f tal que $f^{-1}(b_i) = c_i$ para $i \in [k]$. Esto define f^{-1} para k entradas.

Luego, de forma análoga, encontramos f^{-1} para las restantes $n-k$ entradas en cada uno de los restantes ciclos.

■

3.4. Números de Stirling de primera clase

Definición 3.4.29

El número de n-permutaciones con k-ciclos se llama **número de Stirling sin signo de primera clase** y se denota por $c(n,k)$. Viene dado por la expresión

$$x(x+1)\cdots(x+n-1) = \sum_{k=0}^{n} c(n,k)x^k.$$

donde $c(n,k)$ es el coeficiente de x^k en $x(x+1)\cdots(x+n-1)$.

Por convenio $c(n,0) \geq 0$, $n \geq 1$ y $c(0,0) = 1$.

Los primeros valores de los números de Stirling sin signo de primera clase $c(n,k)$ los recogemos en la siguiente tabla:

n	k								
	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$	$k=9$
$n=1$	1								
$n=2$	1	1							
$n=3$	2	3	1						
$n=4$	6	11	6	1					
$n=5$	24	50	35	10	1				
$n=6$	120	274	225	85	15	1			
$n=7$	720	1764	1624	735	175	21	1		
$n=8$	5040	13068	13132	6769	1960	322	28	1	
$n=9$	40320	109584	188124	67284	22449	4536	546	36	1

Tabla 3.1: Números de Stirling sin signo de primera clase $c(n,k)$

Ejemplo 3.4.30

Para todos los enteros positivos $n > 1$, tenemos

$$c(n, n-2) = 2\binom{n}{3} + \frac{1}{2}\binom{n}{2}\binom{n-2}{2}.$$

Hay dos opciones para que una n-permutación pueda tener $n-2$ ciclos. Una de ellas, es tener un 3-ciclo y $n-3$ puntos fijos y la otra tener dos 2-ciclos y $n-4$ puntos fijos.

□

Lema 3.4.31

Los números de Stirling sin signo de primera clase satisfacen

$$c(n,k) = c(n-1, k-1) + (n-1)c(n-1, k).$$

Demostración

Sea p una n-permutación con k ciclos. Puede ocurrir que:

- La entrada n de p forme ella misma un $1-$ciclo, en cuyo caso al quitar la entrada n resulta una $(n-1)$-permutación con $k-1$ ciclos, lo que explica el primer sumando del lado derecho
- La entrada n de p forme parte de un ciclo de longitud superior a 1, entonces p puede asignar n a cualquiera de los $(n-1)$ valores restantes y al suprimir n resulta una $(n-1)$-permutación con k ciclos, lo que explica el segundo sumando del lado derecho.

Con esto queda probado el resultado.

■

Corolario 3.4.32

Para todo k fijo, la **función generatriz exponencial** de los números de Stirling sin signo de primera clase es

$$h_k(u) = \sum_{n=k}^{\infty} c(n,k)\frac{u^n}{n!} = \frac{[-\ln(1-u)]^k}{k!}.$$

Definición 3.4.33

Los **números de Stirling de primera clase** se definen como

$$x(x-1)\cdots(x-n+1) = \sum_{k=0}^{n} s(n,k)x^k,$$

es decir, $s(n,k)$ es el coeficiente de x^k en $x(x-1)\cdots(x-n+1)$.

Una forma alternativa de definirlos usando los números de Stirling sin signo de primera clase es

$$s(n,k) = (-1)^{n-k}c(n,k).$$

Los primeros valores de los números de Stirling de primera clase $s(n,k)$ los recogemos en la siguiente tabla:

n	k								
	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$	$k=9$
$n=1$	1								
$n=2$	-1	1							
$n=3$	2	-3	1						
$n=4$	-6	11	-6	1					
$n=5$	24	-50	35	-10	1				
$n=6$	-120	274	-225	85	-15	1			
$n=7$	720	-1764	1624	-735	175	-21	1		
$n=8$	-5040	13068	-13132	6769	-1960	322	-28	1	
$n=9$	40320	-109584	188124	-67284	22449	-4536	546	-36	1

Tabla 3.2: Números de Stirling de primera clase $s(n,k)$

Definición 3.4.34

Definimos la **función generatriz doble** para los números de Stirling de primera clase como

$$f(x,u) = \sum_{n=0}^{\infty}\sum_{k=0}^{n} s(n,k)x^k \frac{u^n}{n!} = (1+u)^x$$

Notación 3.4.35

El factorial de x de grado n, $(x)_n = x(x-1)\cdots(x-n+1)$, viene dado por

$$(x)_n = \sum_{k=0}^{n} s(n,k)x^k, \quad n = 0,1,\ldots \tag{3.1}$$

Por convenio $(x)_0 = 1$.

Proposición 3.4.36

Una forma alternativa de expresar la función generatriz mediante la expresión

$$f(x,u) = \sum_{n=0}^{\infty} (x)_n \frac{u^n}{n!}.$$

Lema 3.4.37

Para todos los enteros positivos k y n, tenemos

$$ks(n,k) = \sum_{l=k-1}^{n-1} (-1)^{n-l-1} \frac{(n)_{n-l}}{n-l} \cdot s(l,k-1).$$

Demostración

Sabemos que $f(x,u) = (1+u)^x$. Luego,

$$\frac{\partial f(x,u)}{\partial x} = f(x,u)ln(1+x).$$

El coeficiente de $\frac{x^{k-1}u^n}{n!}$ del lado izquierdo es $ks(n,k)$. El lado derecho es igual a

$$f(x,u)\sum_{l=1}^{\infty}(-1)^{l+1}\frac{u^l}{l} = \sum_{i=0}^{\infty}\sum_{j=0}^{i} s(i,j)x^j\frac{u^i}{i!} \cdot \sum_{l=1}^{\infty}(-1)^{l+1}\frac{u^l}{l}.$$

Por lo tanto, el coeficiente de $\dfrac{x^{k-1}u^n}{n!}$ del lado derecho es

$$n!\sum_{l=k-1}^{n-1}(-1)^{n-l-1}\cdot s(l,k-1)\cdot\frac{1}{n-l}\cdot\frac{1}{l!},$$

lo que prueba nuestro resultado.

■

Lema 3.4.38

Para todo k fijo, la **función generatriz exponencial** de los números de Stirling de primera clase viene dada por

$$f_k(u)=\sum_{n=k}^{\infty}s(n,k)\frac{u^n}{n!}=\frac{[ln(1+u)]^k}{k!}.$$

<u>**Demostración**</u>

Cambiando el orden de sumación en $f(x,u)$, conseguimos que

$$f(x,u)=\sum_{k=0}^{n}\sum_{n=k}^{\infty}s(n,k)\frac{u^n}{n!}x^k=\sum_{k=0}^{n}f_k(u)x^k.$$

Por otro lado, tenemos que

$$f(x,u)=(1+u)^x=e^{xln(1+u)}=e^{[ln(1+u)]x}$$

Usando el desarrollo de la función exponencial $\displaystyle\sum_{n=0}^{\infty}\frac{x^n}{n!}=e^x$, deducimos lo siguiente

$$e^{[ln(1+u)]x}=\sum_{k=0}^{\infty}\frac{[ln(1+u)]^k}{k!}x^k$$

Por tanto, comparando ambos coeficientes de x^k, llegamos a

$$f_k(u)=\frac{[ln(1+u)]^k}{k!}.$$

■

Lema 3.4.39

Para todos los enteros positivos k y n tenemos

$$s(n+1,k+1)=\sum_{m=k}^{n}(-1)^{m-k}\binom{m}{k}s(n,m).$$

Demostración

Derivamos nuestra función generatriz $f_k(u)$ y después desplazamos los índices por uno, consiguiendo

$$\begin{aligned}\sum_{n=k}^{\infty} s(n+1,k+1)\frac{u^n}{n!} = \frac{(1+u)^{-1}\left[\ln(1+u)\right]^k}{k!} = \\ &= \exp(-\ln(1+u))\frac{\left[\ln(1+u)\right]^k}{k!} = \\ &= \sum_{m=k}^{\infty} \frac{(-1)^m\left[\ln(1+u)\right]^m}{m!}\cdot\frac{\left[\ln(1+u)\right]^k}{k!} = \\ &= \sum_{m=k}^{\infty} \frac{(-1)^{m-k}\left[\ln(1+u)\right]^m}{(m-k)!k!}\end{aligned}$$

Notamos que $f_k(u)$ es muy similar al último miembro de la última expresión, esto indica que reorganizándolo conseguimos

$$\begin{aligned}\sum_{n=k}^{\infty} s(n+1,k+1)\frac{u^n}{n!} &= \sum_{m=k}^{\infty}(-1)^{m-k}\binom{m}{k}\sum_{n=m}^{\infty} s(n,m)\frac{u^n}{n!} = \\ &= \sum_{n=k}^{\infty}\left[\sum_{m=k}^{n}(-1)^{m-k}\binom{m}{k}s(n,m)\right]\frac{u^n}{n!},\end{aligned}$$

y el resultado se obtiene comparando los coeficientes de $\dfrac{u^n}{n!}$.

■

Capítulo 4

Aplicaciones

4.1. Test de rachas ascendentes y descendentes

4.1.1. Introducción

Deinición 4.1.1

Se definen las **secuencias pseudo-aleatorias** como aquellas secuencias cuyos elementos disponen de propiedades similares a las secuencias aleatorias.

Los generadores de uso más frecuentes para estas secuencias son de la forma:

$$x_{i+1} = kx_i + c\,mod(m), \quad i = 0, 1, 2, \ldots \tag{4.1}$$

donde i, k, c y x_0 son enteros menores que m; la secuencia $\{x^i/m \ \text{ con } \ i = 1, 2, \ldots\}$ se considera una secuencia aleatoria procedente de una distribución uniforme $(0, 1)$.

Un generador de esta forma se llama **congruente multiplicativo** si $c = 0$ y **congruente mixto** si $c \neq 0$.

El objetivo está en asegurarnos una elección adecuada de k, c y m de tal forma que los elementos de una secuencia no se repitan hasta que se haya generado un número suficiente de elementos y pasen por ciertos test estadísticos.

Empíricamente, se ha comprobado que si una secuencia pseudo-aleatoria generada por algunos de los algoritmos anteriores no supera alguno de los test de aleatoriedad clásica, entonces tampoco supera los test de rachas ascendentes y descendentes, lo cual evidencia que estos test son bastante potentes.

4.1.2. Test de rachas ascendentes y descendentes

Consideramos una secuencia

$$\{x_i; \quad i = 1, 2, \ldots, n\}$$

generada por un generador de números pseudo-aleatorio.

Hay varios tipos de rachas ascendentes de longitud r:

- Rachas internas:

$$x_{i-1} > x_i < x_{i+1} < \cdots < x_{i+r} > x_{i+r+1}$$

- Rachas iniciales:

$$x_1 < x_2 < \cdots < x_{r+1} > x_{r+2}, \quad 1 \leq r < n-2$$

- Rachas finales:

$$x_{n-r-1} > x_{n-r} < x_{n-r+1} < \cdots < x_n, \quad 1 \leq r \leq n-2$$

- Rachas completas:

$$x_1 < x_2 < \cdots < x_n$$

De forma análoga se definen las rachas descendentes.

Ejemplo 4.1.2

Consideramos la secuencia

$$S = \{33, 42, 5, 17, 47, 12, 10, 3, 9\};$$

si leemos de izquierda a derecha vemos que existen:

- Una racha ascendente de longitud 1.
- Una racha descendente de longitud 1.
- Una racha ascendente de longitud 2.
- Una racha descendente de longitud 3.
- Una racha ascendente de longitud 1.

□

El test de rachas ascendentes y descendentes se basa es la comparación de los números esperados y reales entre rachas de varias longitudes.

A continuación mostraremos algunos resultados importantes con respecto a las rachas, son las "disposiciones especiales"de las secuencias monótonas.

Consideramos un secuencia

$$\{u_i; \quad i = 1, 2, \ldots, m; \;\; u_i > u_j \Leftrightarrow i > j\} \tag{4.2}$$

es decir, una secuencia de m inecuaciones en orden ascendente de magnitud.

Una secuencia

$$\{x_i; \; i = 1, 2, \ldots, m\},$$

obtenida a partir de permutaciones de la secuencia (4.2) se dice que son "**disposiciones especiales**"de $u_1, u_2, \ldots, u_m$ si

$$x_1 > x_2 < \cdots < x_{m-1} > x_m.$$

Luego, el número de " disposiciones especiales"viene dado por:

- Si ($x_2 = u_1$ y $x_{m-1} = u_m$) $= (m-2)(m-3)$ ya que tenemos $(m-2)$ posibilidades para elegir el valor de x_1 y $(m-3)$ para elegir el valor de x_m.
- Si ($x_1 = u_m$ y $x_2 = u_1$) $= (m-3)$ esto obliga a que $x_m = u_{m-1}$, por tanto tenemos $(m-3)$ posibilidades de colocar el resto de elementos.
- Si ($x_m = u_1$ y $x_{m-1} = u_m$) $= (m-3)$ esto obliga a que $x_1 = u_m$, por tanto tenemos $(m-3)$ posibilidades de colocar el resto de elementos.
- Si ($x_m = u_1$ y $x_{m-1} = u_m$) $= 1$ pues sólo tenemos una posibilidad de colocar el resto de elementos.

Por tanto, el número total de disposiciones especiales es

$$(m-2)(m-3) + (m-3) + (m-3) + 1 = m^2 - 3m + 1.$$

Si cada disposición es igualmente probable, la probabilidad de que ocurra cualquier disposición es $\frac{1}{m!}$, por lo que la probabilidad de las disposiciones especiales es

$$\frac{(m^2 - 3m + 1)}{m!}. \tag{4.3}$$

En una secuencia pseudo-aleatoria de longitud n hay $(n - r - 2)$ subsecuencias $x_{i-1}, x_i, \ldots, x_{n-r}$. Por tanto, si

$$x_{i-1} > x_i < x_{i+1} < \cdots < x_{i+r} > x_{i+r+1} \tag{4.4}$$

la subsecuencia es una "disposición especial"de $(r+3)$ números; pero (4.4) es la condición que define las rachas ascendentes de longitud r.

Luego, la esperanza de las rachas ascendentes de longitud r se deriva de la expresión (4.3) tomando $m = r + 3$

$$\frac{((r+3)^2 - 3(r+3) + 1)(n-r-2)}{(r+3)!} = \frac{(r^2+3r+1)(n-r-2)}{(r+3)!}, \quad r \leq n-2 \quad (4.5)$$

y por simetría, esta expresión representa también la esperanza del número de rachas descendentes.

Si consideramos las disposiciones de la forma

$$x_1 < x_2 < \cdots < x_{m-1} > x_m.$$

La esperanza de las rachas de longitud r es $4\dfrac{(r+1)}{(r+2)!}$ si $r < n-1$. Como hay $n!$ posibles disposiciones de n números, la esperanza de la racha completa es $\dfrac{2}{n!}$.

Agrupando estos resultados, la esperanza del número de rachas descendentes de longitud r viene dada por

$$\mathbb{E}(r) = \begin{cases} 2 \times \dfrac{(r^2+3r+1)(n-r-2)}{(r+3)!} + 4 \times \dfrac{(r+1)}{(r+2)!} & \\ = 2\left\{\dfrac{(r^2+3r+1)n - (r^3+3r^2-r-4)}{(r+3)!}\right\} & si \quad r < n-1 \\ \dfrac{2}{n!} & si \quad r = n-1 \end{cases} \quad (4.6)$$

Entonces el valor esperado del número de rachas descendentes de longitud mayor o igual que r es:

$$\mathbb{E}_1(r) = \sum_{\alpha=r}^{n-1} \mathbb{E}(\alpha).$$

Ahora, para cualquier (a_0, a_1, a_2, a_3) tal que $\displaystyle\sum_{i=0}^{3} a_i = 0$ se define

$$\begin{aligned} S_r(a_0, a_1, a_2, a_3, \ldots, a_m) &= \sum_{\alpha=r}^{n-2} \sum_{i=0}^{m} \frac{a_i}{(\alpha+i-1)!}, r \geq 1 \\ &= \frac{a_0}{(r-1)!} + \frac{a_0+a_1}{r!} + \frac{a_0+a_1+a_2}{(r+1)!} + \frac{a_0+a_1+a_2+a_3}{(r+2)!} \\ &+ \cdots + \frac{a_0+a_1+\cdots+a_m}{(n-m)!} + \cdots + \frac{a_{m-3}+a_{m-2}+a_{m-1}+a_m}{(n-2)!} \\ &+ \frac{a_{m-2}+a_{m-1}+a_m}{(n-1)!} + \frac{a_{m-1}+a_m}{n!} + \frac{a_m}{(n+1)!} \end{aligned} \quad (4.7)$$

Consideramos ahora $\mathbb{E}(\alpha)$, para $\alpha < n-1$. Observamos los dos términos que constituyen el numerador de (4.6), los cuales pueden ser escritos como

$$\alpha^2 + 3\alpha + 1 = (\alpha+3)(\alpha+2) - 2(\alpha+3) + 1 \text{ donde } a_1 = 1, a_2 = -2, a_3 = 1$$

y

$$\begin{aligned}\alpha^3 + 3\alpha^2 - \alpha - 4 = {} & (\alpha+3)(\alpha+2)(\alpha+1) \\ & - 3(\alpha+3)(\alpha+2) + 3(\alpha+3) - 1 \text{ donde } a_0 = 1, a_1 = -3, a_2 = 3, a_3 = -1\end{aligned}$$

Usando las expresiones (4.6), (4.7) y $m = 3$, llegamos a

$$\begin{aligned}
\mathbb{E}_1(r) &= 2 \times \left\{ nS_r(0,1,-2,1) - S_r(1,-3,3,-1) + \frac{1}{n!} \right\} \\
&= 2 \times \left[n \times \left\{ \frac{0}{(r-1)!} + \frac{1}{r!} + \frac{0+1-2}{(r+1)!} + \frac{0+1-2+1}{(r+2)!} + \frac{0+1-2+1}{(n-2)!} \right.\right. \\
&\left. + \frac{1-2+1}{(n-1)!} + \frac{-2+1}{n!} + \frac{1}{(n+1)!} \right\} - \left(\frac{1}{(r-1)!} + \frac{1-3}{r!} + \frac{1-3+3}{(r+1)!} \right. \\
&\left.\left. + \frac{1-3+3-1}{(r+2)!} + \frac{1-3+3-1}{(n-2)!} + \frac{-3+3-1}{(n-1)!} + \frac{3-1}{n!} + \frac{-1}{(n+1)!} \right) + \frac{1}{n!} \right] \\
&= 2 \times \left[n \times \left\{ \frac{1}{r!} - \frac{-1}{(r+1)!} - \frac{-1}{n!} + \frac{1}{(n+1)!} \right\} \right. \\
&\left. - \frac{1}{(r-1)!} + \frac{2}{r!} - \frac{1}{(r+1)!} + \frac{1}{(n-1)!} - \frac{2}{n!} + \frac{1}{(n+1)!} + \frac{1}{n!} \right] \\
&= 2 \times \left\{ \frac{(r+1)n - (r^2 + r - 1)}{(r+2)!} \right\}, \quad 1 \leq r \leq n-1. \qquad (4.8)
\end{aligned}$$

Por otro lado, el número esperado de rachas es $\mathbb{E}_1(1) = \dfrac{2n-1}{3}$. Usando la epxresión (4.6) tenemos

$$\left(\frac{3}{2n-1}\right) \sum_{r=1}^{n-1} r\mathbb{E}(r) = \frac{6}{2n-1} \left[\sum_{r=1}^{n-2} \left\{ \frac{nr(r^2+3r+1) - r(r^3+3r^2+r-4)}{(r+3)!} \right\} + \frac{n-1}{n!} \right] \qquad (4.9)$$

Calculando los términos del numerador por separado, obtenemos

$$r(r^2+3r+1) = (r+3)(r+2)(r+1) + a(r+3)(r+2) + b(r+3) + c$$

- Si $r = -3$; $\quad -3(9-9+1) = c \Rightarrow c = -3$

- Si $r = -2$; $\quad -2(4 - 6 + 1) = b - 3 \Rightarrow b = 5$
- Si $r = -1$; $\quad -1(1 - 3 + 1) = 2a + 10 - 3 \Rightarrow a = -3$

$$r(r^3+3r^2+r-4) = (r+3)(r+2)(r+1)r+a(r+3)(r+2)(r+1)+b(r+3)(r+2)+c(r+3)+d$$

- Si $r = -3$; $\quad -3(-27 + 27 - 3 - 4) = d \Rightarrow d = 21$
- Si $r = -2$; $\quad -2(-8 + 12 - 2 - 4) = c + 21 \Rightarrow c = -17$
- Si $r = -1$; $\quad -1(-1 + 3 - 1 - 4) = 2b - 34 + 21 \Rightarrow b = 8$
- Si $r = 0$; $\quad 0 = 6a + 48 - 51 + 21 \Rightarrow a = -3$

y entonces la longitud media de una racha es:

$$\frac{6}{2n-1}\left\{nS_1\{1,-3,5,-3\} - S_1\{1,-3,8,-17,21\} + \frac{n-1}{n!}\right\}.$$

Por tanto, para obtener el test generamos una secuencia de números $N_1, N_2, \ldots$ donde N_r es el número de rachas de longitud r en la secuencia. Levene y Wolfowitz en 1944 demostraron que para un n grande el estadístico

$$\frac{\sum_{\alpha} (N_\alpha - \mathbb{E}[\alpha])^2}{\mathbb{E}[\alpha]}$$

sigue un distribución χ^2.

Sin embargo, en 1954, Cochran sugirió que tales aproximaciones son buenas sólo cuando el 80 % de los valores esperados es mayor que 5.

Cuando α aumenta, $\mathbb{E}[\alpha]$, se hace rápidamente menor que 5, por eso

$$\frac{\left(\sum_{\alpha=r}^{n-1} N_\alpha - \mathbb{E}_1[\alpha]\right)^2}{\mathbb{E}_1[\alpha]}.$$

Por lo tanto,

$$\sum_{\alpha=1}^{r-1} \frac{(N_\alpha - \mathbb{E}[\alpha])^2}{\mathbb{E}[\alpha]} + \frac{\left(\sum_{\alpha=r}^{n-1} N_\alpha - \mathbb{E}_1[r]\right)^2}{\mathbb{E}_1[r]} \tag{4.10}$$

sigue una distribución χ^2 con $r-1$ grados de libertad.

Ejemplo 4.1.3

Consideramos una secuencia de $n = 500$ números con $N_1 = 180$, $N_2 = 90$, $N_3 = 30$, $N_4 = 8$, $N_5 = 2$, $N_6 = 0$ y $N_7 = 1$.

Usando (4.6) obtenemos:

$$\begin{aligned}
\mathbb{E}(1) &= \frac{2(1+3+1)500-(1+3-1-4)}{4!} = 208,4\\
\mathbb{E}(2) &= \frac{2(4+6+1)500-(8+12-2-4)}{5!} = 91,4\\
\mathbb{E}(3) &= \frac{2(9+9+1)500-(27+27-3-4)}{6!} = 26,3\\
\mathbb{E}(4) &= \frac{2(16+12+1)500-(64+64-4-4)}{7!} = 5,71\\
\mathbb{E}(5) &= \frac{2(25+15+1)500-(125+75-5-4)}{8!} = 1,01
\end{aligned}$$

Por otro lado, por la expresión (4.10) tomando $r = 5$ tenemos:

$$\frac{((N_1-\mathbb{E}(1))^2}{\mathbb{E}(1)} + \frac{((N_2-\mathbb{E}(2))^2}{\mathbb{E}(2)} + \frac{((N_3-\mathbb{E}(3))^2}{\mathbb{E}(3)} + \frac{((N_4-\mathbb{E}(4))^2}{\mathbb{E}(4)} + \frac{((N_5-\mathbb{E}_1(5))^2}{\mathbb{E}_1(5)}$$

Luego, sustituyendo cada valor:

$$\begin{aligned}
\chi_4^2 &= \frac{(180-208,4)^2}{208,4} + \frac{(90-91,4)^2}{91,4} + \frac{(30-26,3)^2}{26,3} + \frac{(8-5,71)^2}{5,71} + \frac{((N_5-\mathbb{E}_1(5))^2}{\mathbb{E}_1(5)}\\
&= 3,87 + 0,02 + 0,52 + 0,92 + \frac{((N_5-\mathbb{E}_1(5))^2}{\mathbb{E}_1(5)}
\end{aligned}$$

Ahora calculamos $\mathbb{E}_1(5)$ usando (4.8):

$$\mathbb{E}'(5) = 2\frac{(5+1)500-(25+5-1)}{7!} = 1,18$$

Por tanto, sustituyendo en la expresión anterior:

$$\chi_4^2 = 3,87 + 0,02 + 0,52 + 0,92 + 2,81 = 8,13.$$

Como conclusión, vemos que no hay evidencias significativas al nivel de significación del 5 % de rechazar la hipótesis de que las rachas de una secuencia podrían ocurrir aleatoriamente.

□

4.2. Aplicaciones de los números de Stirling al cálculo de momentos

4.2.1. Momentos ordinarios en función de los momentos factoriales

Dada una variables aleatoria X con función de distribución $F(x)$ unidimensional definida en $\mathbb{R}$, el **momento ordinario** de orden n es:

$$\alpha_n = \mathbb{E}[X^n] = \int_{\mathbb{R}} x^n dF(x) \tag{4.11}$$

la cual suponemos que es finita.

Por otro lado, el **momento factorial** de orden r, se define como

$$f_r = \mathbb{E}[X(X-1)\cdots(X-r+1)] = \mathbb{E}(X)_r \tag{4.12}$$

Usando (1.7) podemos calcular los momentos ordinarios en función de los momentos factoriales:

$$\alpha_n = \mathbb{E}[X^n] = \mathbb{E}\left[\sum_{k=1}^{n} S(n,r)(X)_r\right] = \sum_{k=1}^{n} S(n,r) f_r \tag{4.13}$$

Ejemplo 4.2.3

Los primeros 4 momentos ordinarios en función de los primeros 4 momentos factoriales son:

$$\begin{aligned}
\alpha_1 &= f_1 \\
\alpha_2 &= f_1 + f_2 \\
\alpha_3 &= f_1 + 3f_2 + f_3 \\
\alpha_4 &= f_1 + 7f_2 + 6f_3 + f_4
\end{aligned}$$

Para obtener los coeficientes de los f_i tenemos que ver la **Tabla 1.4**.

□

4.2.2. Momentos factoriales en función de los momentos ordinarios

A continuación obtendremos una relación de los momentos factoriales de orden n en función de los momentos ordinarios.
Partimos de la descomposición dada en (3.1)

$$x_{(n)} = \sum_{r=1}^{n} s(n,k)x^k$$

y tenemos que

$$f_n = \mathbb{E}[(X)_n] = \sum_{k=1}^{n} s(n,k)\mathbb{E}[X^k] = \sum_{k=1}^{n} s(n,k)\alpha_k$$

donde α_k es el momento ordinario de orden k de acuerdo con (4.11) y f_n representa el momento factorial (4.12).

Ejemplo 4.2.4

Los 4 primeros momentos factoriales en función de los 4 primeros momentos ordinarios son:

$$\begin{aligned}
f_1 &= \alpha_1 \\
f_2 &= -\alpha_1 + \alpha_2 \\
f_3 &= 2\alpha_1 - 3\alpha_2 + \alpha_3 \\
f_4 &= -6\alpha_1 + 11\alpha_2 - \alpha_3 + \alpha_4
\end{aligned}$$

Para obtener los coeficientes de los f_i tenemos que ver la **Tabla 1.3**.

□

4.3. Conexión con los momentos centrales

El **momento central** de orden m, en caso de que exista, se define como $\mu_m = \mathbb{E}[(X-\mu)^m]$ donde $\mu = \mathbb{E}[X]$.

Es posible escribir los momentos centrales en función de los momentos ordinarios:

$$\begin{aligned}\mu_m = \mathbb{E}[(X-\mu)^m] &= \mathbb{E}\left[\sum_{k=0}^{m}\binom{m}{k}x^k(-\mu)^{m-k}\right]\\ &= \sum_{k=0}^{m}\binom{m}{k}\alpha_k(-\mu)^{m-k}.\end{aligned} \tag{4.14}$$

A partir de la expresión anterior es posible encontrar una conexión entre los momentos centrales y los momentos factoriales sustituyendo en (4.14) la expresión (4.13). Así por ejemplo, la varianza:

$$\begin{aligned}\mu_2 &= \binom{2}{0}(-\mu)^2 + \binom{2}{1}\alpha_1(-\mu) + \binom{2}{2}\alpha_2\\ &= \mu^2 - 2\mu f_1 + (f_1 + f_2)\\ &= f_1^2 - 2f_1^2 + f_1 + f_2 = f_2 - f_1^2 + f_1\end{aligned}$$

y el momento central de tercer orden:

$$\begin{aligned}\mu_3 &= \binom{3}{3}(-\mu)^3 + \binom{3}{1}\alpha_1(-\mu)^2 + \binom{3}{2}\alpha_2(-\mu) + \binom{3}{3}\alpha_3\\ &= -f_1^3 + 3f_1^3 - 3f_1(f_1+f_2) + (f_1 + 3f_2 + f_3)\\ &= 2f_1^3 - 3f_1^2 - 3f_1f_2 + f_1 + 3f_2 + f_3\end{aligned}$$

y así sucesivamente.

4.4. Distribuciones

A continuación reflejaremos todos los conceptos que hemos estudiado en las secciones anteriores para diversas distribuciones.

4.4.1. Distribución de Poisson

La distribución de Poisson es útil para modelar la probabilidad de ocurrencia de sucesos con probabilidades muy pequeñas, o sucesos "raros". Depende del parámetro $\lambda > 0$ y su función de probabilidad viene dada por

$$P(X = x) = \frac{\lambda^x}{x!}e^{-\lambda} \quad x = 0, 1, 2, 3, \ldots$$

El momento factorial de orden r es

$$f_r = \mathbb{E}[(X)_r] = \sum_{r=1}^{\infty} \frac{x(x-1)\cdots(x-r+1)}{x!}\lambda^x e^{-\lambda}$$
$$= \lambda^r \sum_{x\geq r} \frac{\lambda^{x-r}}{(x-r)!}e^{-\lambda} = \lambda^r e^{-x} \sum_{y=0}^{\infty} \frac{\lambda^y}{y'!} = \lambda^r$$

donde se ha usado el cambio $y = x - r$ y el hecho de que $\sum_{y=0}^{\infty} \frac{\lambda^y}{y!} = e^{\lambda}$.

Por tanto,

$$f_r = \lambda^r, \quad r \geq 0. \tag{4.15}$$

La expresión del momento ordinario de orden k se obtiene sustituyendo el valor f_r en (4.13), por el obtenido en la expresión (4.15) de forma que

$$\alpha_k = \sum_{r=1}^{n} S(n,r)\lambda^r.$$

Los momentos centrales de segundo orden (varianza) se obtienen de la siguiente forma

$$\mu_2 = f_2 - f_1^2 + f_1 = \lambda^2 - \lambda^2 + \lambda = \lambda.$$

4.4.2. Distribución Binomial

Un experimento de Bernoulli se caracteriza por ser dicotómico, es decir, sólo son posibles dos resultados. A uno de estos se denomina éxito y tiene una probabilidad de ocurrencia p y al otro, fracaso, con una probabilidad $q = 1-p$. En la distribución binomial el anterior experimento se repite n veces, de forma independiente, y se trata de calcular la probabilidad de un determinado número de éxitos.

Su función de probabilidad viene dada por:

$$P(X = x) = \binom{n}{x} p^x q^{n-x} \quad x = 0, 1, 2, \ldots, n$$

El momento factorial de orden r es

$$f_r = \mathbb{E}[(X)_r] = \sum_{x=0}^{n} (x)_r \binom{n}{x} p^x q^{n-x}$$
$$= \sum_{x=r}^{n} \binom{n-r}{x-r} p^{x-r} q^{n-r-x+r} (n)_r p^r$$
$$= \sum_{x=r}^{n} \binom{n-r}{x-r} p^{x-r} q^{n-x} (n)_r p^r = (n)_r p^r, \tag{4.16}$$

donde se ha usado el hecho de que $\sum_{x=r}^{n} \binom{n-r}{x-r} p^{x-r} q^{n-x} = 1$ como consecuencia del binomio de Newton.

La expresión del momento ordinario de orden k se obtiene sustituyendo el valor f_r en (4.13), por el obtenido en la expresión (4.16) de forma que

$$\alpha_k = \sum_{r=1}^{n} S(n,r)(n)_r p^r.$$

4.4.3. Distribución Hipergeométrica

Es una distribución de probabilidad discreta relacionada con muestreos aleatorios y sin reemplazamiento. Si consideramos una urna con N bolas de las cuales a son blancas y el resto b son negras, la probabilidad de que al extraer n bolas ($n \leq N$) sin reemplazamiento sean x blancas ($0 \leq x \leq a$) y $n - x \leq b$ negras es

$$P(X = x) = \frac{\binom{a}{x}\binom{b}{n-x}}{\binom{N}{n}} \quad x \leq a, \; n - x \leq b$$

El momento factorial de orden r es:

$$f_r = E[(X)_r] = \sum_{x=0}^{n} (x)_r \frac{\binom{a}{x}\binom{b}{n-x}}{\binom{N}{n}} = (n)_r \sum_{x=r} \frac{\binom{a-r}{x-r}\binom{b}{n-x}}{\frac{(N)_r}{(n)_r}\binom{N-r}{n-r}} = \frac{(a)_r(n)_r}{(N)_r}$$

pues

$$\sum_{x=r} \binom{a-r}{x-r}\binom{b}{n-x} = \binom{N-r}{n-r}$$

y $a + b - r = N - r$.

Por tanto,

$$\alpha_r = \frac{(a)_r(n)_r}{(N)_r}. \tag{4.17}$$

La expresión del momento ordinario de orden k se obtiene sustituyendo el resultado obtenido en (4.17) en la expresión (4.13), obteniendo así

$$\alpha_k = \sum_{r=1}^{n} S(n,r) \frac{(a)_r(n)_r}{(N)_r}.$$

4.4.4. Distribución Binomial Negativa

Es una distribución de probabilidad discreta, también conocida con el nombre de distribución de Pascal.

Supongamos que se repite un experimento de Bernoulli de manera independiente hasta que se obtiene el n-ésimo éxito. Entonces la variable aleatoria X que cuenta el número de fracasos obtenidos hasta dicho momento es una variable aleatoria binomial negativa de parámetro n y p, donde p es la probabilidad de éxito en cada ensayo Bernoulli.

La función de probabilidad viene dada por:

$$P(X=x)=\frac{\Gamma(n+x)}{x!\Gamma(n)}p^nq^k=\frac{(n+x-1)!}{x!(n-1)!}p^nq^k=\binom{n+x-1}{x}q^xp^n \quad x=0,1,2\dots$$

es decir, han sucedido $n+x$ expermientos. El último debe ser necesariamente favorable y todos con probabilidad constante p.

El momento factorial de orden r es:

$$\begin{aligned}
f_r=E[(X)_r]&=\sum_{x=0}^{\infty}(x)_r\binom{n+x-1}{x}q^xp^n\\
&=\sum_{x=0}^{\infty}(x)_r\frac{(n+x-1)!}{x!(n-1)!}q^xp^n=\sum_{x=r}^{\infty}\frac{(n+x-1)!}{(x-r)!(n-1)!}q^xp^n\\
&=\sum_{y=0}^{\infty}\frac{(n+r+y-1)!}{y!(n-1)!}q^{y+r}p^n=\frac{q^r}{p^r}(n+r-1)_{(r)}\sum_{y=0}^{\infty}\frac{(n+r+y-1)!}{y!(n-1)!}q^yp^{n+r}\\
&=\frac{q^r}{p^r}(n+r-1)_{(r)}
\end{aligned}$$

usando que el cambio $y=x-r$ y el hecho de que $\sum_{y=0}^{\infty}\frac{(n+r+y-1)!}{y!(n-1)!}q^yp^{n+r}=1$ por ser función de probabilidad.

Por tanto

$$f_r=\frac{q^r}{p^r}(n+r-1)_{(r)}. \tag{4.18}$$

La expresión del momento ordinario de orden k se obtiene sustituyendo el resultado obtenido en (4.18) en la expresión (4.13), obteniendo así

$$\alpha_k=\sum_{r=1}^{\infty}S(n,r)(n+r-1)_{(r)}\left(\frac{q}{p}\right)^r.$$

Bibliografía

[1] Bóna, Miklós, *Combinatorics of pemutations*, Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, 2012.

[2] Charalambides, Charalambos A, *Enumerative combinatorics*, CRC Press eries on Discrete Mathematics and its Applications, Chapman & Hall/CRC, Boca Raton, FL, 2002.

[3] Knuth, Donald E, *Art of Computer Programming, Volume 3, Sorting and Searching*, Addison-Wesley Professional, 2013.

[4] Urbelz Ibarrola, Francisco Javier, *Los números de Stirling aplicados a la Estadística*, Estadística Española, 1985, 107, 111–142.

[5] Downham, DY, *The runs up and down test*, The Computer Journal, JSTOR, 1969, 12, 4, 373–376.