Notas de Matemática Discreta

por

Pablo Fernández Gallardo y José Luis Fernández Pérez
Universidad Autónoma de Madrid

Lo que sigue es una versión preliminar (en formato pdf) de uno de los capítulos del libro “Notas de Matemática Discreta”, que se puede descargar en `www.uam.es/pablo.fernandez`. Agradeceríamos a los posibles lectores que nos enviaran cualquier sugerencia o corrección que consideren oportuna, a las direcciones de correo electrónico `pablo.fernandez@uam.es` ó `joseluis.fernandez@uam.es`.

3.2. Permutaciones

Aunque ya las hemos definido en la subsección 2.2.1 (como un tipo particular de listas), las permutaciones son un objeto combinatorio lo suficientemente rico como para merecer atención especial.

Una **permutación** del conjunto $\{1,\dots,n\}$ es una lista de longitud n sin repetición formada por sus elementos; el conjunto de todas ellas lo llamaremos

$$Perm(\{1,\dots,n\}) = \{\ n\text{-listas sin repetición formadas con los símbolos } \{1,\dots,n\}\}\,.$$

Sabemos, por supuesto, que hay $n!$ de ellas. En los términos en que las estamos definiendo, cada permutación es una (re)ordenación de los elementos de $\{1,\dots,n\}$.

Ya vimos, en el ejemplo 2.2.5, que podemos entender también una permutación de un conjunto finito $\mathcal{X}$ como una aplicación biyectiva de $\mathcal{X}$ en $\mathcal{X}$. Como siempre, para simplificar la notación, supondremos que $\mathcal{X} = \{1,\dots,n\}$.

Para exhibir una permutación podemos escribir la lista correspondiente,

$$(2,7,5,1,\dots,6) \qquad \text{(permutación como lista)}$$

o bien utilizar la siguiente notación:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 7 & 5 & 1 & \dots & 6 \end{pmatrix} \qquad \text{(permutación como aplicación biyectiva)}$$

que nos permite reconocer rápidamente la imagen de cada elemento de $\{1,\dots,n\}$ por la permutación. Es decir, **identificamos** la lista $(2,7,5,1,\dots,6)$ con la aplicación biyectiva que lleva el 1 en el 2, el 2 en el 7, el 3 en el 5, etc.

Unas permutaciones especiales son los **desbarajustes**, las aplicaciones biyectivas que no fijan elemento alguno (el símbolo j nunca va al j, para cada $j = 1,\dots,n$). En términos de listas, son las n-listas tales que, para cada $j = 1,\dots,n$, el símbolo j no ocupa la posición j de la lista. Pronto calcularemos cuántos de estos desbarajustes hay. Otras permutaciones que aparecerán más adelante son las **trasposiciones**, cuyo efecto es el de intercambiar las posiciones de dos elementos (y fijar los $n-2$ restantes).

Para lo que sigue, es conveniente tener presente la definición de permutación como aplicación biyectiva del conjunto en sí mismo. Sean, por ejemplo, las dos siguientes permutaciones del conjunto $\mathcal{X} = \{1,2,3,4,5\}$:

$$f:\ (1,3,2,5,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix} \qquad g:\ (2,1,3,5,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}.$$

La permutación g es una aplicación del conjunto $\{1,2,3,4,5\}$ en sí mismo que lleva, por ejemplo, el elemento 1 en el 2: $g(1) = 2$. Pero también f lo es, y observemos que lleva el 2 en el 3, $f(2) = 3$. Así que si primero hacemos actuar g y luego f, entonces, por ejemplo, el elemento 1 acaba yendo al 3.

A. Composición de permutaciones

Perfilemos adecuadamente esta idea de acción sucesiva de dos permutaciones. Sean f y g dos permutaciones del conjunto $\{1, \dots, n\}$. La **composición** de f con g, que escribiremos como $f \circ g$ (obsérvese el orden en que se escriben) se define como

$$(f \circ g)(x) = f(g(x)), \quad \text{para cada } x \in \{1, \dots, n\},$$

es decir, la acción sucesiva de g *primero* y f después.

La aplicación g sabe actuar sobre los elementos $\{1, \dots, n\}$, y devuelve los mismos elementos, quizás reordenados. Así que la acción posterior de f está igualmente bien definida. Pero además, y esto es lo importante, estas dos acciones sucesivas producen, en total, una nueva aplicación biyectiva del conjunto en sí mismo (esto es, una permutación). Basta comprobar que $(f \circ g)$ es una aplicación inyectiva: si a y b son tales que

$$(f \circ g)(a) = (f \circ g)(b)\,, \quad \text{es decir, si} \quad f(g(a)) = f(g(b))\,,$$

como f es una aplicación biyectiva esto supondría que $g(a) = g(b)$. Y el que g sea también una aplicación biyectiva nos lleva a que a y b deben ser iguales.

Hemos comprobado que, dadas dos permutaciones cualesquiera f y g, la acción sucesiva de g y f, lo que llamamos su composición $f \circ g$ (insistimos en el orden en que se escriben) es también una permutación. Y es que

> *el conjunto de las permutaciones, dotado de la operación de composición, tiene una estructura de **grupo**.*

El conjunto de la permutaciones de $\{1, \dots, n\}$, entendido como grupo, se suele denotar por S_n, y se le llama el **grupo simétrico**. Esto lo veremos con más detalle en el capítulo 14, pero adelantemos que tener una estructura de grupo supone que se satisfacen una serie de propiedades:

- Si $f, g \in S_n$, entonces $f \circ g \in S_n$ (el conjunto S_n es **cerrado** para la operación de composición).
- Se tiene la propiedad asociativa: si $f, g, h \in S_n$, entonces $(f \circ g) \circ h = f \circ (g \circ h)$.
- La identidad id, es decir, la permutación que deja fijos todos los elementos, es el **elemento neutro** de S_n:

$$id \circ f = f \circ id = f \quad \text{para cualquier } f \in S_n.$$

- Para cada permutación $f \in S_n$ existe su **elemento inverso**, que denominaremos f^{-1}, que verifica que
$$f \circ f^{-1} = f^{-1} \circ f = id\,.$$

La primera propiedad ya la hemos comprobado, la segunda es sencilla de verificar y la tercera es obvia. Sólo la cuarta requiere un momento de reflexión y se deduce de la biyectividad de f (por cierto, el inverso de una permutación es único).

Obsérvese que nada hemos dicho sobre la propiedad conmutativa, porque, en general, la composición de permutaciones *no es conmutativa*. Es decir, es relevante el orden en que escribamos la composición: normalmente, no será lo mismo $(f \circ g)$ que $(g \circ f)$. Veamos un ejemplo:

Ejemplo 3.2.1 *Sea $\mathcal{X} = \{1,2,3,4,5\}$ y consideremos las permutaciones*

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix} \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$$

Calculemos f^2, g^2, $f \circ g$, $g \circ f$, f^{-1}.

Por f^2 entenderemos la composición de f consigo misma, $f \circ f$. Calcularla es sencillo: por ejemplo, $f^2(1) = f(f(1)) = f(1) = 1$, $f^2(2) = f(f(2)) = f(3) = 5$, etc. Así podemos escribir que

$$f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}.$$

Análogamente,

$$g^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

Así que g^2 coincide con la identidad. Si calculamos $f \circ g$ y $g \circ f$ (obsérvese que el orden de acción es diferente), obtenemos

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}, \qquad g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix},$$

lo que comprueba que la composición de permutaciones no es conmutativa. Para calcular la composición $f \circ g$ de dos permutaciones se pueden evaluar las imágenes sucesivas (primero g y luego f) de cada elemento; pero quizás conviene utilizar el siguiente truco: se escribe un primer piso con los elementos en el orden natural, un segundo con la acción de g, y un tercero con la acción de f (sobre los de la segunda fila). Al final, nos olvidamos de la fila intermedia:

$$f \circ g = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} \\ 2 & 1 & 3 & 5 & 4 \\ \mathbf{3} & \mathbf{1} & \mathbf{5} & \mathbf{2} & \mathbf{4} \end{pmatrix}$$

Por último, hallar la inversa de f es lo mismo que calcular la permutación f^{-1} para la que

$$f \circ f^{-1} = id = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

Es decir, aquélla que satisface que

$$\begin{array}{lcl} f\left(f^{-1}(1)\right) = 1 & \Longrightarrow & f^{-1}(1) = 1 \\ f\left(f^{-1}(2)\right) = 2 & \Longrightarrow & f^{-1}(2) = 5 \\ & \vdots & \end{array}$$

Así se obtiene que

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}$$

Un pequeño truco nos puede ayudar a la hora de calcular f^{-1}: basta "darle la vuelta" a f (intercambiar las dos filas) y luego reordenar (la de arriba):

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix} \Longrightarrow f^{-1} = \begin{pmatrix} 1 & 3 & 5 & 4 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \xrightarrow{\text{reordenar}} f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}$$

para obtener la permutación f^{-1}. ♣

Pronto veremos otra manera efectiva de calcular la inversa de una permutación. Pero insistimos en que, pese a que la composición de permutaciones no es en general conmutativa, en el caso del inverso no hay que tener cuidado de definirlo por la izquierda o por la derecha: es único.

B. Orden de una permutación

Para acabar esta descripción (que retomaremos en el capítulo 14), señalemos un último concepto. Antes de explicarlo, necesitamos saber cuál el el inverso de la composición de dos permutaciones: supongamos que f y g son dos elementos de S_n. Entonces,

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1} .$$

Nótese que se invierte el orden de acción de los inversos. Para comprobarlo, basta utilizar la propiedad asociativa (que nos permite olvidarnos de los paréntesis):

$$(f \circ g) \circ \big(g^{-1} \circ f^{-1}\big) = f \circ \underbrace{g \circ g^{-1}}_{id} \circ f^{-1} = f \circ f^{-1} = id .$$

Hemos acordado que, para $k \geq 1$, f^k significa la acción sucesiva (k veces) de la permutación f. ¿Cuál es el inverso de, por ejemplo, f^2? Con la observación anterior,

$$\big(f^2\big)^{-1} = (f \circ f)^{-1} = f^{-1} \circ f^{-1} = \big(f^{-1}\big)^2 .$$

A esa composición de la permutación f^{-1} consigo misma la llamaremos, claro, f^{-2}. Si la componemos k veces, hablaremos de f^{-k}. Y si, para completar la notación, decidimos que $f^0 = id$, tenemos un álgebra de estas composiciones que resulta ser útil: dados unos enteros s y t,

$$f^s \circ f^t = f^{s+t} .$$

Esto no es más que notación, pero simplifica las cosas. Comprobarlo es sencillo: basta escribir todas las f y f^{-1} que nos indiquen los valores de s y t (según sean positivos o negativos) e ir "cancelando" por parejas.

Ahora podemos introducir el concepto de **orden** de una permutación. Démonos $f \in S_n$ y listemos las sucesivas composiciones f^k, para cada $k \geq 1$:

$$f, f^2, f^3, \ldots, f^{n!}, f^{n!+1}$$

La lista, que seguiría más allá, la hemos cortado tras escribir un total de $n!+1$ permutaciones. En S_n no hay más que $n!$ permutaciones distintas, así que, por el principio del palomar, necesariamente dos permutaciones de las que aparecen en la lista han de ser la misma. Es decir, con seguridad existirán dos enteros $s, t \geq 1$ (supongamos que $s > t$) tales que

$$f^s = f^t \,.$$

Componiendo con f^{-t} a los dos lados, obtenemos que $f^{s-t} = f^0 = id$, donde $s - t > 0$. Lo que quiere decir esto es que, dada una permutación, existen enteros no negativos k tales que $f^k = id$. Pues bien, el orden de la permutación f es el **menor** entero positivo para el que se cumple esta propiedad[13] (véase también el ejercicio 3.2.1). Veremos en un momento una manera eficaz de calcular el orden de una permutación.

3.2.1. Permutaciones y ciclos

Existe un tipo especial de permutaciones particularmente importantes, porque podemos utilizarlas como piezas básicas para construir cualquier otra: son los llamados **ciclos**.

Un ciclo en S_n es una permutación que fija un cierto número de elementos de $\{1,\dots,n\}$ (quizás ninguno, en cuyo caso hablaríamos de una **permutación cíclica**), mientras que a los restantes los mueve "cíclicamente". Se entiende fácilmente en un ejemplo: la permutación de S_5 dada por

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

fija los elementos 1 y 5, mientras que, para los restantes,

$$2 \xrightarrow{f} 4 \xrightarrow{f} 3 \xrightarrow{f} 2 \,.$$

Para describir esta permutación, utilizaremos el siguiente símbolo:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix} = \circlearrowleft_5(2\,4\,3)\,,$$

que pretende resumir toda la información relevante sobre la permutación: es de S_5, mueve cíclicamente los elementos 2, 4 y 3 (en el orden indicado) y fija los restantes (1 y 5).

La identidad, que fija todos los elementos de $\{1,\dots,5\}$, podría venir descrita con el símbolo $\circlearrowleft_5(1)$, o quizás con $\circlearrowleft_5(2)$, $\circlearrowleft_5(3)$, etc. Por razones que se entenderán pronto, escribimos el ciclo f como la composición de las siguientes tres permutaciones:

$$f = \circlearrowleft_5(1) \circ \circlearrowleft_5(2\,4\,3) \circ \circlearrowleft_5(5)$$

(hemos compuesto dos veces con la identidad, y eso no cambia nada).

[13] Siguiendo con el argumento del principio del palomar, podemos comprobar que el orden de f es siempre menor o igual que $n!$. Sabemos que existen enteros s y t, con $1 \leq t < s \leq n!+1$, tales que $f^s = f^t$. Pero claro, $s - t \leq n!$, así que el orden de f ha de ser también $\leq n!$. De hecho, el orden de f es siempre un divisor de $n!$ (véase el ejercicio 3.2.3).

Si el contexto estuviera claro (es decir, si sabemos en qué S_n estamos trabajando), nos podríamos olvidar del subíndice e incluso del símbolo $\circlearrowleft$. En este caso, escribiríamos

$$f = (1)\,(2\,4\,3)\,(5)\,,$$

que es la notación que aparece habitualmente en otros textos. Observemos que el orden en que se componen estos ciclos es irrelevante, y que, mientras sigan el mismo orden, cuál es el primer elemento del ciclo tampoco importa: podríamos haber escrito, por ejemplo, $(4\,3\,2)$. Pero salvo por estas cuestiones de escritura, la descripción es única. La **longitud** de un ciclo es el número de elementos que mueve realmente su acción.

Como un ciclo es un caso especial de permutación, tendrá un orden. En este caso, es muy sencillo de calcular: veámoslo en el ejemplo. Como los elementos 1 y 5 quedan fijos, no nos preocupamos de ellos. Y para los otros tres,

$$\begin{array}{ccccccc} & f & & f & & f & \\ 2 & \longrightarrow & 4 & \longrightarrow & 3 & \longrightarrow & 2 \\ 3 & \longrightarrow & 2 & \longrightarrow & 4 & \longrightarrow & 3 \\ 4 & \longrightarrow & 3 & \longrightarrow & 2 & \longrightarrow & 4 \end{array}$$

¡Ajá!, la tercera aplicación de f nos devuelve la configuración original. Así que $f^3 = id$ y el orden del ciclo es 3; justo el número de elementos que se mueven cíclicamente (su longitud).

Para comprobar que esto es un resultado general, analicemos un poco más detenidamente cuál es la estructura de un ciclo: sea f un ciclo de longitud k en S_n. Fijará $n-k$ elementos y moverá cíclicamente los restantes:

$$f = \circlearrowleft_n(a_1\,a_2\,\ldots\,a_{k-1}\,a_k)\,.$$

Es decir, bajo la acción de f,

$$a_1 \xrightarrow{f} a_2 \xrightarrow{f} \cdots \xrightarrow{f} a_{k-1} \xrightarrow{f} a_k \xrightarrow{f} a_1\,.$$

En otras palabras, $a_2 = f(a_1)$, $a_3 = f(a_2) = f^2(a_1)$ y así hasta $a_k = f^{k-1}(a_1)$, mientras que $f^k(a_1) = a_1$. De manera que el ciclo se podría reescribir como

$$f = \circlearrowleft_n(a_1\,f(a_1)\,\ldots\,f^{k-2}(a_1)\,f^{k-1}(a_1))\,.$$

Nos interesa entender la permutación f^k. Desde luego, $f^k(a_1) = a_1$. Pero para a_2 tenemos algo análogo:

$$f^k(a_2) = f^k f(a_1) = f f^k(a_1) = f(a_1) = a_2\,.$$

Lo mismo ocurre para cualquier elemento del ciclo, como podrá comprobar el lector (quizás argumentando que, en realidad, el ciclo es el mismo sea cual sea el primer elemento de él que escribamos, mientras que preservemos el orden). Por supuesto, como f fija los elementos que no estén en el ciclo, también lo hará f^k. De manera que f^k es la permutación identidad, y como además k es el primer entero no negativo para el que sucede esto, el orden del ciclo f es justamente k, su longitud como ciclo.

A. Descomposición en ciclos

Los ciclos son permutaciones especialmente interesantes porque toda permutación se puede escribir como composición de ellos (y de manera única). Esta composición (o más bien, descomposición) es muy útil: nos informa de los subconjuntos de $\{1,\dots,n\}$ en los que la acción de la permutación es independiente.

Consideremos la siguiente permutación f de un conjunto con 7 elementos:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 2 & 6 & 4 & 7 \end{pmatrix}.$$

Observamos que los elementos $\{1,3\}$ se mueven cíclicamente con f:

$$1 \xrightarrow{f} 3 \xrightarrow{f} 1$$

De la misma forma, $2 \xrightarrow{f} 5 \xrightarrow{f} 6 \xrightarrow{f} 4 \xrightarrow{f} 2$ y $7 \xrightarrow{f} 7$. Pues bien, la permutación f se puede escribir como la composición de los siguientes ciclos:

$$f = \circlearrowleft_7(1\,3) \circ \circlearrowleft_7(2\,5\,6\,4) \circ \circlearrowleft_7(7)\,.$$

La comprobación es sencilla, sólo hay que observar que los subconjuntos de elementos que mueve cada ciclo son disjuntos dos a dos. La permutación de la derecha es, simplemente, la identidad. Para las dos de la izquierda,

$$\begin{array}{rccccccc}
 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
\circlearrowleft_7(2\,5\,6\,4) & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
 & 1 & \mathbf{5} & 3 & \mathbf{2} & \mathbf{6} & \mathbf{4} & 7 \\
\circlearrowleft_7(1\,3) & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
 & \mathbf{3} & 5 & \mathbf{1} & 2 & 6 & 4 & 7
\end{array}$$

(en negrita, los elementos que se mueven realmente en cada permutación). Y el resultado es la permutación f de partida. Observemos que el orden de presentación de los ciclos no es relevante (estas permutaciones sí conmutan, pues mueven conjuntos de elementos disjuntos dos a dos); y en qué elemento empieza el ciclo, tampoco: f se podría escribir también como

$$f = \circlearrowleft_5(7) \circ \circlearrowleft_5(1\,3) \circ \circlearrowleft_5(2\,5\,6\,4) \quad \text{o como} \quad f = \circlearrowleft_5(7) \circ \circlearrowleft_5(3\,1) \circ \circlearrowleft_5(4\,2\,5\,6)\,.$$

Hagamos el argumento en general, diseñando de paso un algoritmo para obtener la descomposición en ciclos de una permutación $f \in S_n$. Empezamos con un cierto elemento de $\{1,\dots,n\}$, por ejemplo el 1, y escribimos la lista

$$1, f(1), f^2(1), f^3(1), f^4(1), \dots$$

Esta lista es tan larga como queramos, pero sólo hay n elementos en $\{1,\dots,n\}$ así que, de nuevo por el principio del palomar, contendrá dos números repetidos. Esto es, existirán dos enteros positivos $s > t$ para los que

$$f^s(1) = f^t(1)\,.$$

Pero más aún, como estamos tratando con permutaciones, $f^{s-t}(1)$ coincide con $id(1) = 1$. Así que en esa lista no sólo hay repeticiones sino que, además, aparece algún 1 (además del primero). El primer paso del algoritmo consistiría, entonces, en ir construyendo la lista anterior hasta encontrar el primer (nuevo) 1; al terminar, habremos detectado el ciclo en el que está encuadrado el elemento 1:

$$\circlearrowleft_n(1, f^1(1), f^2(1) \dots)\,.$$

Si este ciclo tuviera longitud n, ya habríamos terminado: f sería una permutación cíclica. En caso contrario, si la longitud fuera $< n$ (podría ser incluso 1, si es que $f(1) = 1$), quedaría trabajo por hacer. Por ser ordenados, buscaríamos el primer elemento de $\{1, \dots, n\}$ que no hubiera sido ya incluido en el ciclo anterior y repetiríamos con él el procedimiento. Nótese que ningún elemento de este nuevo ciclo puede pertenecer al ciclo anterior. El proceso continuaría hasta alcanzar a todos los elementos de $\{1, \dots, n\}$.

El resultado de este algoritmo es único, salvo que el orden de composición de los ciclos resultantes es irrelevante y que podemos elegir, como primer elemento de cada ciclo, el elemento del mismo que deseemos. Los ciclos que obtenemos, recordemos, son disjuntos dos a dos.

Normalmente, los ciclos de orden 1 no se escriben, aunque esto puede dar lugar a ciertas confusiones, a menos que el contexto esté muy claro. Por ejemplo, $f = (1\,2)$ podría ser interpretado como una lista, o quizás como un ciclo. Visto como una lista, sería la permutación de la izquierda; visto como ciclo, la de la derecha:

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}; \qquad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Esto, cuando se trate realmente de una permutación de S_2, porque podría también representar una de, digamos, S_4:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}.$$

Por eso conviene escribir los ciclos de longitud 1, o bien utilizar la notación que sugerimos, $\circlearrowleft_4(1\,2)$.

El lenguaje de los ciclos simplifica bastantes cálculos con permutaciones. Por ejemplo, para calcular el inverso de una permutación dada, basta leer los ciclos de la permutación original "al revés":

$$\begin{aligned} f &= \circlearrowleft_9(1\,2\,4) \circ \circlearrowleft_9(3\,8\,7) \circ \circlearrowleft_9(5) \circ \circlearrowleft_9(6\,9) \\ f^{-1} &= \circlearrowleft_9(4\,2\,1) \circ \circlearrowleft_9(7\,8\,3) \circ \circlearrowleft_9(5) \circ \circlearrowleft_9(9\,6) \end{aligned}$$

Al fin y al cabo, si el elemento 3 va al 8 a través de f, el 8 ha de ir al 3 a través de f^{-1}. No es ya tan útil, en general, para describir la composición de dos permutaciones, porque se pueden mezclar los ciclos de cada una.

B. Orden de una permutación y ciclos

Otra tarea que se simplifica notablemente es la del cálculo del orden de una permutación. Ya vimos que si la permutación es un ciclo de longitud k, entonces el orden de la permutación es también k. ¿Y en el caso general? Veamos un ejemplo: sea la permutación de S_5 dada por la composición de ciclos

$$f = \circlearrowright_5(2\,1) \circ \circlearrowright_5(3\,5\,4)\,.$$

Si partimos del orden natural, $(1, \dots, 5)$, cuando apliquemos f^2, los elementos $\{1, 2\}$ habrán vuelto a sus posiciones originales; no así los restantes. Con f^3 son $\{3, 4, 5\}$ los que vuelven al orden original; pero los dos primeros se han descolocado. Si pensamos un momento, nos convenceremos de que tenemos que aplicar 6 veces f para recuperar la configuración original. Si f tuviera dos ciclos de longitudes 2 y 4, un argumento análogo nos diría que $f^4 = id$ y que, por tanto, su orden sería 4.

En general, si una permutación f se escribe como composición de ciclos, cuyas longitudes son $l_1, \dots, l_m$ (podría haber varios ciclos de cada una de las longitudes), su orden será

$$orden(f) = \text{mín}\{k \geq 1 \,:\, f^k = id\} = \text{mcm}(l_1, \dots, l_m)\,,$$

donde $\text{mcm}(l_1, \dots, l_m)$ representa al mínimo común múltiplo de los números $l_1, \dots, l_m$.

C. El número de permutaciones con una determinada estructura de ciclos

Una cuestión combinatoria muy interesante es la de contar el número de permutaciones cuya descomposición en ciclos reúne una serie de propiedades dada. La estructura a la que se refiere el título de este epígrafe puede ser muy diversa: que el número total de ciclos esté fijo, que no haya determinado tipo de ciclos, que el número de ciclos de cada tipo posible esté determinado…

En la subsección 3.3.2 veremos, por ejemplo, cómo contar cuántas permutaciones de $\{1, \dots, n\}$ tienen un cierto número, digamos k, de ciclos. Antes, en la subsección 3.2.4, calcularemos cuántos desbarajustes (permutaciones que no fijan elemento alguno, es decir, sin ciclos de orden 1) hay.

Un caso especial de desbarajustes son las permutaciones cíclicas. Para contar cuántas permutaciones cíclicas hay en S_n observamos que, para construir el ciclo que incluye a todos los elementos, primero los ordenamos ($n!$ maneras posibles) y luego tenemos en cuenta que, dado un orden relativo entre los elementos, la elección de cuál va el primero no es relevante. Como hay n posibles maneras de elegir ese primer elemento, la respuesta final es que

$$\#\{\text{permutaciones cíclicas en } S_n\} = \frac{n!}{n} = (n-1)!$$

Visto desde otro punto de vista, como tenemos la libertad de elegir cuál es el primer elemento de la lista, sólo hay que ordenar los $n-1$ elementos restantes. Un argumento análogo nos permite contar cuántas permutaciones son ciclos de orden k: elegimos primero los k elementos del ciclo, para luego determinar el orden dentro del ciclo. Esto se puede hacer de $\binom{n}{k}(k-1)!$ maneras. En particular, hay $\binom{n}{2}$ trasposiciones distintas.

Un planteamiento más general consistiría en prescribir cuántos ciclos de cada posible longitud deben tener las permutaciones que nos interesan. Esto es, dar una lista de enteros no negativos $(b_1, \dots, b_n)$ donde, para cada $j = 1, \dots, n$, el número b_j es el número de ciclos de longitud j. Obsérvese que se tendrá que

$$\sum_{j=1}^{n} b_j = \#\text{total de ciclos} \qquad \text{y que} \qquad \sum_{j=1}^{n} j\, b_j = n\,,$$

porque cada uno de los elementos de $\{1, \dots, n\}$ está en algún ciclo. Por ejemplo, las permutaciones cíclicas son las que tienen $b_n = 1$ y $b_j = 0$ para el resto. Ser un desbarajuste sólo requiere que $b_1 = 0$.

La pregunta que nos interesa responder es la siguiente: dados unos números $b_j \geq 0$ tales que $\sum_{j=1}^{n} j\, b_j = n$, ¿cuántas permutaciones de S_n tienen b_1 ciclos de longitud 1, b_2 de longitud 2, etc.?

Para dar lugar a descomposiciones en ciclos con las especificaciones requeridas, comenzamos con una lista arbitraria de n elementos. Ahora marcamos los ciclos, partiendo la lista en trozos sucesivos: los b_1 primeros elementos están en los ciclos de orden 1, los $2b_2$ siguientes, en los de orden 2, y así sucesivamente:

$$\underbrace{(\bullet)\cdots(\bullet)}_{b_1}\ \underbrace{(\bullet\,\bullet)\cdots(\bullet\,\bullet)}_{b_2}\ \underbrace{(\bullet\,\bullet\,\bullet)\cdots(\bullet\,\bullet\,\bullet)}_{b_3}\ \cdots$$

Pero, ¿cuántas de esas listas dan lugar a la misma descomposición en ciclos? Observemos que, dentro de cada uno de los ciclos que hemos marcado, podemos rotar circularmente los elementos (elegir el que va primero) sin cambiar de qué ciclo se trata. Cada trozo de tamaño j tiene j posibles rotaciones. Así que el número total de rotaciones de los trozos que dan lugar a la misma descomposición en ciclos es

$$1 \overset{b_1 \text{ veces}}{\cdots} 1 \cdot 2 \overset{b_2 \text{ veces}}{\cdots} 2\ \cdots = 1^{b_1}\, 2^{b_2}\ \cdots n^{b_n}\,.$$

Pero además, y ya por último, podemos permutar, por ejemplo, los trozos de longitud 1 entre sí (¡pero no con los demás!). Y, en general, los trozos de longitud j entre ellos mismos: esto se puede hacer de $j!$ maneras. Reuniendo todas estas observaciones, llegamos a la respuesta buscada:

$$\boxed{\#\left\{\begin{array}{c}\text{permutaciones de } S_n\\ \text{con } b_j \text{ ciclos de longitud } j\end{array}\right\} = \frac{n!}{1^{b_1}2^{b_2}\cdots n^{b_n}\ b_1!b_2!\cdots b_n!}}$$

El lector podrá comprobar que con esta fórmula recuperamos los resultados para los casos vistos anteriormente: permutaciones cíclicas ($b_n = 1$ y $b_1 = b_2 = \cdots = b_{n-1} = 0$), ciclos de orden k ($b_k = 1$, $b_1 = n - k$ y el resto de los b_j cero) o trasposiciones ($b_2 = 1$, $b_1 = n - 2$ y el resto de los b_j cero).

3.2.2. Permutaciones pares e impares

Una trasposición de S_n intercambia dos elementos de $\{1, \dots, n\}$ y fija los restantes. Tiene un ciclo de longitud 2 y otros $n-2$ ciclos de longitud 1:

$$\circlearrowleft_n(a\,b) \circ \circlearrowleft_n(c) \circ \circlearrowleft_n(d) \circ \cdots$$

donde a y b son los elementos intercambiados. Estas permutaciones, de estructura por otra parte tan simple, nos van a servir para descomponer permutaciones generales (aunque será un tipo de descomposición diferente a la de los ciclos).

Ejemplo 3.2.2 *Consideremos la permutación $f = \circlearrowleft_5(1\,2\,5)$.*

Esta permutación de S_5 mueve los elementos $1 \to 2 \to 5 \to 1$ (y fija los restantes). Esto es, es de la forma (al menos para los elementos que nos interesan)

$$f = \begin{pmatrix} 1 & 2 & \cdots & 5 \\ 2 & 5 & \cdots & 1 \end{pmatrix}$$

Pero esa acción la podemos realizar también con la aplicación sucesiva de las trasposiciones que intercambian el 1 y el 2 y el 1 y el 5:

$$\begin{array}{rcccc} & 1 & 2 & \cdots & 5 \\ \circlearrowleft_5(1\,2) & \downarrow & \downarrow & & \downarrow \\ & 2 & 1 & \cdots & 5 \\ \circlearrowleft_5(1\,5) & \downarrow & \downarrow & & \downarrow \\ & 2 & 5 & \cdots & 1 \end{array}$$

Así que podríamos escribir que el ciclo es la composición sucesiva de estas dos trasposiciones:

$$\circlearrowleft_5(1\,2\,5) = \circlearrowleft_5(1\,5) \circ \circlearrowleft_5(1\,2)\,.$$

¡Cuidado!, ahora los ciclos de cada trasposición no son disjuntos, así que es importante señalar el orden en que se aplican (prúebese a componer las trasposiciones al revés). El lector podrá comprobar también que esa misma permutación f se puede escribir como

$$\circlearrowleft_5(1\,2\,5) = \circlearrowleft_5(1\,2) \circ \circlearrowleft_5(1\,5) \circ \circlearrowleft_5(2\,5) \circ \circlearrowleft_5(1\,2)\,.$$

Es decir, la escritura en términos de trasposiciones no es única; y además importa el orden en que se aplican (porque no tienen por qué ser disjuntas). ♣

Para el caso de una permutación general, todo lo que necesitamos es comprobar que un ciclo se puede escribir siempre como composición de trasposiciones. Una permutación genérica se escribirá como composición de ciclos, cada uno de los cuales, a su vez, se podrá escribir como composición de trasposiciones.

Nótese que, por ejemplo, los ciclos de orden 1 se pueden escribir como composición (dos veces) de la misma trasposición. Los ciclos de orden dos ya son, ellos mismos, trasposiciones. Analicemos entonces el caso de un ciclo de longitud 3, digamos $f = \circlearrowleft_n(a_1\,a_2\,a_3)$, para el que

$$f(a_1) = a_2\,, \quad f(a_2) = a_3 \quad \text{y } f(a_3) = a_1\,.$$

El mismo efecto se consigue trasponiendo, sucesivamente, el primer elemento con los restantes (en el orden en que aparecen en el ciclo), como se sugería en el ejemplo 3.2.2; esto es,

$$f = \underbrace{\circlearrowleft_n(a_1\, a_3)}_{f_3} \circ \underbrace{\circlearrowleft_n(a_1\, a_2)}_{f_2} .$$

Nótese el orden: primero trasponemos a_1 con a_2 (lo que llamamos f_2) y luego a_1 con a_3, con f_3. El lector podrá comprobar que, efectivamente, $f = f_3 \circ f_2$ y obtener la descomposición análoga en el caso de un ciclo ciclo de longitud 4,

$$f = \circlearrowleft_n(a_1\, a_2\, a_3\, a_4) = \circlearrowleft_n(a_1\, a_4) \circ \circlearrowleft_n(a_1\, a_3) \circ \circlearrowleft_n(a_1\, a_2) ;$$

y, en general, para un ciclo de cualquier longitud (véase el ejercicio 3.2.4):

$$f = \circlearrowleft_n(a_1\, a_2\, \dots\, a_{k-1}\, a_k) = \circlearrowleft_n(a_1\, a_k) \circ \circlearrowleft_n(a_1\, a_{k-1}) \circ \cdots \circ \circlearrowleft_n(a_1\, a_3) \circ \circlearrowleft_n(a_1\, a_2) ,$$

El método descrito conduce a una descomposición de una permutación general en trasposiciones. Pero ya hemos visto que esta descomposición no es única (y aquí no nos referimos sólo a que haya varias maneras distintas de escribirla, como ocurría con los ciclos). Además, las distintas trasposiciones utilizadas en la descomposición no serán, en general, disjuntas.

¿Dónde reside el interés, entonces, de este tipo de descomposiciones? Por un lado, claro, está la sencillez de las piezas utilizadas: trasposiciones, siempre ciclos de orden 2. Pero además, como comprobaremos en un momento, el *número* de trasposiciones utilizadas para descomponer una permutación dada es *siempre* par o impar. Así que este tipo de descomposición nos llevará a descubrir una nueva característica de las permutaciones que, a veces, será muy relevante.

La clave para demostrar este resultado es la siguiente observación: sea $g \in S_n$ una permutación cualquiera con α_j ciclos de longitud j, de manera que $\sum_{j=1}^n \alpha_j$ es el número total de ciclos de que consta. Sea π una trasposición que, digamos, intercambia los elementos a y b. ¿Cuántos ciclos tiene la permutación $\pi \circ g$? Hay que distinguir dos casos, dependiendo de si a y b pertenecen al mismo ciclo o no (nótese que π no actúa sobre los elementos que pertenezcan a ciclos en los que no estén ni a ni b):

$\boxed{\text{Caso 1:}}$ si a y b pertenecen al mismo ciclo de g, entonces

$$g = \circlearrowleft_n(a\, x_2\, \dots\, x_{r-2}\; b\; x_r\, \dots x_l) \circ \text{ (resto de ciclos de } g) .$$

(podemos suponer que a es el primer elemento de ese ciclo). En este caso, la acción sucesiva de g y π sobre los elementos del ciclo viene dada por

$$\begin{array}{cccccccccc}
 & a & x_2 & \dots & x_{r-2} & b & x_r & & \dots & x_l \\
g & \downarrow & \downarrow & & \downarrow & \downarrow & \downarrow & & & \downarrow \\
 & x_2 & x_3 & \dots & b & x_r & x_{r+1} & & \dots & a \\
\pi & \downarrow & \downarrow & & \downarrow & \downarrow & \downarrow & & & \downarrow \\
 & x_2 & x_3 & \dots & a & x_r & x_{r+1} & & \dots & b
\end{array}$$

Y la conclusión es que se forman dos ciclos a partir del original:

$$\pi \circ g = \circlearrowleft_n(a\, x_2\, \dots\, x_{r-2}) \circ \circlearrowleft_n(b\, x_r\, \dots\, x_l) \circ \text{ (resto de ciclos de } g) .$$

$\boxed{\text{Caso 2:}}$ Si a y b están en ciclos distintos,

$$g = \circlearrowleft_n (a\,a_2\,\ldots\,a_l) \circ \circlearrowleft_n (b\,b_2\,\ldots b_s) \circ \text{(resto de ciclos de } g\text{)}\,,$$

entonces

$$\begin{array}{ccccccccc} & a & a_2 & \ldots & a_l & b & b_2 & \ldots & b_s \\ g & \downarrow & \downarrow & & \downarrow & \downarrow & \downarrow & & \downarrow \\ & a_2 & a_3 & \ldots & a & b_2 & b_3 & \ldots & b \\ \pi & \downarrow & \downarrow & & \downarrow & \downarrow & \downarrow & & \downarrow \\ & a_2 & a_3 & \ldots & b & b_2 & b_3 & \ldots & a \end{array}$$

Y ahora tenemos un único ciclo a partir de los dos de partida:

$$\pi \circ g = \circlearrowleft_n (a\,a_2\,\ldots\,a_l\,b\,b_2\,\ldots\,b_s) \circ \text{(resto de ciclos de } g\text{)}\,.$$

Reuniendo estos dos casos, concluimos que, si π es una trasposición,

$$\#\,\text{ciclos de } (\pi \circ g) = \#\,\text{ciclos de } g \pm 1\,.$$

Esto es suficiente para demostrar el siguiente resultado:

Teorema 3.2 *Dada una permutación $g \in S_n$, si podemos escribir g como composición de s y t trasposiciones, entonces s y t tienen la misma paridad (es decir, son simultáneamente pares o impares).*

Demostración. Escribimos g como composición de s trasposiciones:

$$g = \pi_s \circ \pi_{s-1} \circ \cdots \circ \pi_2 \circ \pi_1\,.$$

Como trasposición que es, π_1 tiene $n-1$ ciclos. Éste es nuestro punto de partida. Ahora, cada sucesiva trasposición hace que el número de ciclos aumente o disminuya en una unidad. Digamos que, tras las $s-1$ trasposiciones, hemos tenido α aumentos y β disminuciones. Obsérvese que

$$\left\{ \begin{array}{rcl} \alpha + \beta & = & s - 1\,, \\ (n-1) + \alpha - \beta & = & \#\,\text{ciclos de } g. \end{array} \right.$$

Sumando estas dos expresiones y despejando s del resultado, llegamos a que

$$s = n + 2\,\alpha - \#\,\text{ciclos de } g\,.$$

Ahora escribimos g de la otra manera,

$$g = \widetilde{\pi}_t \circ \widetilde{\pi}_{t-1} \circ \cdots \circ \widetilde{\pi}_2 \circ \widetilde{\pi}_1\,,$$

y aplicamos el mismo argumento para obtener que

$$t = n + 2\widetilde{\alpha} - \#\,\text{ciclos de } g\,,$$

donde $\widetilde{\alpha}$ es el número de aumentos en las sucesivas aplicaciones. Restando ambas cantidades,

$$s - t = 2\,(\alpha - \widetilde{\alpha})\,,$$

que es un número par. Por tanto, s y t tienen la misma paridad. ■

Ahora que tenemos este resultado, podemos hablar de que una permutación es **par** si se escribe como composición de un número par de trasposiciones. E **impar** en caso contrario. De hecho, se suele hablar del **signo** (o signatura) de una permutación: será 1 si la permutación es par, y -1 si es impar:

$$\text{signo}(g) = (-1)^t \,,$$

donde t es el número de trasposiciones en una descomposición (en trasposiciones) cualquiera de g. Para calcular el signo de una permutación, es decir, para determinar si la permutación es par o impar, debemos, en principio, descomponer la permutación en producto de trasposiciones (de la manera que queramos), y contar cuántas hay. Pero muchas veces tenemos información adicional sobre la permutación que facilita el cálculo de la signatura (veánse los ejercicios 3.2.5—3.2.9). De entre las $n!$ permutaciones de S_n, exactamente la *mitad* son permutaciones pares, y la otra mitad impares (véase el ejercicio 3.2.10).

3.2.3. Permutaciones y matrices de ceros y unos

Otra manera de describir una permutación es con una matriz de ceros y unos. Supongamos que tenemos una permutación del conjunto $\mathcal{X} = \{1, \dots, n\}$ dada por

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}.$$

Formamos entonces una matriz $n \times n$ con filas y columnas etiquetadas con $\{1, \dots, n\}$. En la primera columna pondremos un 1 en la fila que nos indique a_1 (y así esta primera columna nos informa de la imagen del 1 con la permutación, a_1): en la segunda columna, pondremos el 1 en la posición que nos indique a_2, etc. En el resto de las posiciones situamos ceros.

Ejemplo 3.2.3 *Sea el conjunto $\mathcal{X} = \{1, 2, 3\}$ y consideremos las permutaciones dadas por*

$$g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Siguiendo las indicaciones que exponíamos antes, obtenemos

$$g_1 \longrightarrow \begin{array}{c|ccc} & 1 & 2 & 3 \\ \hline 1 & 1 & 0 & 0 \\ 2 & 0 & 0 & 1 \\ 3 & 0 & 1 & 0 \end{array} \qquad g_2 \longrightarrow \begin{array}{c|ccc} & 1 & 2 & 3 \\ \hline 1 & 0 & 0 & 1 \\ 2 & 0 & 1 & 0 \\ 3 & 1 & 0 & 0 \end{array} \qquad g_3 \longrightarrow \begin{array}{c|ccc} & 1 & 2 & 3 \\ \hline 1 & 0 & 0 & 1 \\ 2 & 1 & 0 & 0 \\ 3 & 0 & 1 & 0 \end{array}$$

Este procedimiento establece una aplicación biyectiva entre el conjunto de las permutaciones de $\{1, \dots, n\}$ y el de las matrices $n \times n$ con ceros y unos con un único 1 por columna y un único 1 por fila. ♣

En este nuevo lenguaje podemos reinterpretar algunos conceptos ya vistos; por ejemplo, un elemento fijo de la permutación se corresponde con un 1 en la diagonal. Y un desbarajuste tendrá asociado una matriz cuya diagonal sólo tenga ceros (de manera que no fije elemento alguno). El ejercicio 3.2.11 sugiere un procedimiento para construir las matrices correspondientes a un tipo especial de desbarajustes, las permutaciones cíclicas.

Estas matrices son también apropiadas para representar la acción de una permutación (como aplicación biyectiva). Tomemos, por ejemplo, la matriz

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

correspondiente a la permutación $(1,3,2)$ que escribíamos antes. Si lo que nos dan es la matriz, podemos recuperar la permutación a la que representa multiplicándola (con las reglas de multiplicación de matrices habituales) por el vector de los elementos de $\{1,2,3\}$ en el orden natural:

$$(1,2,3)\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = (1,3,2)$$

Lo mismo ocurriría con las otras matrices. Más aún, si queremos obtener la composición de las permutaciones g_1 y g_2 del ejemplo, $g_1 \circ g_2$ (en este orden), el resultado es

$$g_1 \circ g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

precisamente la tercera permutación g_3 que considerábamos en el ejemplo. Y ahora podemos comprobar que la acción sucesiva de las permutaciones se puede describir también mediante el producto (en el orden adecuado) de sus correspondientes matrices de ceros y unos:

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}}_{g_1}\underbrace{\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}}_{g_2} = \underbrace{\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}}_{g_1 \circ g_2 = g_3}$$

Podemos entender esta representación matricial de las permutaciones desde otro punto de vista: cada matriz es una posible disposición de n torres en un tablero $n \times n$ de manera que ninguna de ellas amenace a cualquier otra (con los movimientos legales de la torre del ajedrez, claro). Parece sólo una curiosidad, pero en la sección 10.6 veremos que se trata de una interpretación muy útil.

3.2.4. Desbarajustes

Queremos contar el número de desbarajustes de $\{1,\dots,n\}$, las permutaciones de $\{1,\dots,n\}$ que no fijan elemento alguno (no contienen ciclos de longitud 1). Llamaremos D_n a este número de desbarajustes. Este número es, por supuesto, $\leq n!$. Pero también sabemos (véase el argumento de la página 170) que permutaciones cíclicas, que son un caso particular de desbarajustes (tienen un único ciclo de orden n), hay $(n-1)!$.

El valor de D_n, entonces, estará entre $(n-1)!$ y $n!$. Queremos calcular, o al menos estimar, la proporción que los desbarajustes ocupan entre todas las permutaciones; es decir, $D_n/n!$. O, si se quiere, la probabilidad de que si escogemos una permutación al azar, ésta sea un desbarajuste.

En el planteamiento clásico del problema, se han escrito n cartas y preparado los n sobres con las direcciones correspondientes, cada uno al lado de su carta. Pero alguien los ha descolocado, de manera que no queda más remedio que introducir las cartas en los sobres al azar. Hecho esto, ¿cuál será la probabilidad de no acertar ninguna?

Antes de empezar a analizar el problema, quizás el lector debería meditar un momento sobre la cuestión y apelar a su intuición para al menos arriesgar una respuesta aproximada: ¿una probabilidad cercana a 0, cercana a 1?; ¿qué ocurre cuando el número de cartas y sobres es muy grande? Parece difícil no acertar ninguna...

Para calcular el valor de D_n emplearemos los argumentos ya habituales del principio de inclusión/exclusión. Si una permutación no es un desbarajuste, ocurrirá que al menos uno de los símbolos está en su posición natural. Así que consideramos los conjuntos

$$\begin{aligned} A_1 &= \{\text{permutaciones de } \{1,\dots,n\} \text{ con el símbolo 1 en la posición 1}\}\,, \\ A_2 &= \{\text{permutaciones de } \{1,\dots,n\} \text{ con el símbolo 2 en la posición 2}\}\,, \\ &\ \vdots \\ A_n &= \{\text{permutaciones de } \{1,\dots,n\} \text{ con el símbolo } n \text{ en la posición } n\}\,. \end{aligned}$$

Como hay $n!$ listas en total,

$$D_n = n! - |A_1 \cup \cdots \cup A_n|\,.$$

Apliquemos el principio de inclusión/exclusión. El tamaño de cualquiera de los conjuntos A_j es $(n-1)!$, porque serán listas en las que el símbolo j está en la posición j, y para contarlas bastará ordenar (permutar) los $n-1$ símbolos restantes. El tamaño de las intersecciones dos a dos (hay $\binom{n}{2}$ de ellas), con el mismo argumento —ahora hay dos símbolos ya colocados en sus posiciones correspondientes—, resulta ser $(n-2)!$. Y así con el resto de los casos. Tendremos entonces que

$$D_n = n! - \left[\binom{n}{1}(n-1)! - \binom{n}{2}(n-2)! + \cdots \pm \binom{n}{n}(n-n)!\right] = \sum_{j=0}^{n} \binom{n}{j}(n-j)!(-1)^j\,.$$

Esto es,

$$\boxed{D_n = n! \sum_{j=0}^{n} \frac{(-1)^j}{j!}}$$

Sabemos que la suma de la derecha es prácticamente igual al número $e^{-1} = 1/e$ en cuanto n es grande. Así que este resultado nos dice que el número de desbarajustes es una proporción *casi* fija del número total, en concreto $n!/e$.

En términos de proporciones, o quizás probabilidades, la cantidad de interés es

$$\frac{D_n}{n!} = \sum_{j=0}^{n} \frac{(-1)^j}{j!}.$$

Este número depende del valor de n con el que estemos tratando. Pero, a todos los efectos, y en cuanto n es grande (un “grande” relativo, quizás basta $n = 10$), el número es casi indistinguible de $1/e$. Así que, como conclusión: primero, la probabilidad de obtener un desbarajuste es prácticamente independiente de n (si n es suficientemente grande); y segundo, es una probabilidad grande, mayor que un tercio, quizás más de lo que hubiéramos apostado al principio (véase también el ejercicio 3.2.13).

¿Cuál es la explicación[14] de este aparentemente paradójico resultado? Llamemos, para cada $j = 1, \ldots, n$, B_j al complementario de A_j en S_n. Esto es, B_j contiene a las permutaciones de $\{1, \ldots, n\}$ en las que el símbolo j no está en la posición j. Desde luego,

$$Prob(B_j) = 1 - Prob(A_j) = 1 - \frac{(n-1)!}{n!} = 1 - \frac{1}{n}.$$

La intersección de todos los conjuntos B_j son, precisamente, los desbarajustes. Si los B_j *fueran independientes* entre sí (dos a dos), entonces tendríamos que

$$Prob\Big(\bigcap_{j=1}^{n} B_j\Big) = \Big(1 - \frac{1}{n}\Big)^n \sim \frac{1}{e} \quad \text{si } n \text{ es grande.}$$

Sin entrar en los detalles del significado exacto de la noción de independencia, apelemos únicamente a la intuición: el que el símbolo j esté fuera de su posición, ¿"influye" en que el símbolo k esté fuera de su posición? Por ejemplo, si tenemos permutaciones de dos elementos $\{1, 2\}$, la respuesta es sí: si el símbolo 1 está fuera de su posición, el 2 ha de estar necesariamente descolocado. Si tenemos tres símbolos, el que el símbolo 1 no esté en su posición también influye en que, por ejemplo, el 2 no esté en la segunda posición (aunque "menos"). Pero si n es grande, podríamos decir que la respuesta es (aproximadamente) no. Es decir, los B_j son (aproximadamente) independientes[15], lo que explica que la probabilidad de obtener un desbarajuste sea $\approx 1/e$.

3.2.5. Coaliciones, poder de voto y permutaciones

Tenemos un conjunto de personas que votan y toman decisiones por mayoría (un consejo de administración de una empresa, un tribunal judicial, el Congreso o el Senado,...). La mayoría a la que nos referimos podría ser absoluta (la "mitad" más uno de los votos), de dos tercios, etc. Además, cada persona podría tener distinto número de votos (por ejemplo, alguien en quien otros votantes hubieran delegado el voto, un miembro de un consejo de administración de una empresa representando a un grupo de accionistas o un presidente con poderes especiales). Incluso cabe la posibilidad de que alguno de los votantes tuviera derecho de veto (recuérdese el funcionamiento del Consejo de Seguridad de la ONU) o la posibilidad de deshacer empates (el presidente de un tribunal judicial suele tener esa prerrogativa).

Lo que nos interesa es dar una medida de la influencia que cada persona puede tener en un contexto como éste. Si no se indica lo contrario, en lo que sigue supondremos que las votaciones se ganan por mayoría absoluta. Empecemos definiendo una coalición de votantes

[14] La explicación que aquí sugerimos requiere una cierta familiaridad con conceptos de probabilidad. Quizás el lector quiera consultar antes el capítulo 7. Véanse, por ejemplo, el ejercicio 7.3.7 y el ejemplo 7.5.12.

[15] Se puede dar un argumento riguroso de esta afirmación, véase el ejercicio 3.2.12.

ganadora como aquélla que reúne suficientes votos como para ganar una votación. Si los votantes que no están en una cierta coalición pueden ganar, entonces diremos que esa coalición es **perdedora**. Si una coalición no es ni ganadora ni perdedora, entonces se dice que es **bloqueadora**.

Nos van a interesar, por supuesto, las coaliciones ganadoras con el menor número de votantes posible: una coalición ganadora se dice **minimal** si la retirada de la misma de cualquiera de sus miembros hace que deje de ser ganadora. Por supuesto, toda coalición que incluya una ganadora minimal es también ganadora. Y toda coalición ganadora contiene, al menos, a una ganadora minimal. Un caso especial y que merece un nombre rotundo es aquél en el que un único votante forma una coalición (una coalición muy simple, eso sí) ganadora: diremos que entonces ese votante es un **dictador**.

Ejemplo 3.2.4 *Tenemos n personas, cada una con 1 voto, y las decisiones se toman por mayoría absoluta.*

Una coalición es ganadora si reúne, al menos, a $\lfloor n/2 \rfloor + 1$ de los votantes. Si n es par, cualquier coalición de $n/2$ personas es bloqueadora (si n es impar no puede haber coaliciones bloqueadoras). ♣

Ejemplo 3.2.5 *Tenemos un número par $2k$ de votantes, cada uno con 1 voto. Se necesita mayoría absoluta para tomar una decisión; pero, en caso de empate, hay uno (el presidente) que decide.*

En este caso, cualquier coalición de k personas entre las que se encuentre el presidente es ganadora; y si no está el presidente, es perdedora. ♣

Ejemplo 3.2.6 *Hay cuatro votantes, a, b, c y d, con 3, 2, 1 y 1 votos, respectivamente.*

Las decisiones se toman por mayoría absoluta, lo que en este caso exige 4 votos. Podemos listar todas las $2^4 - 1 = 15$ posibles coaliciones (excluyamos al $\emptyset$) y decidir cuáles de ellas son ganadoras (aparecen en negrita):

Coalición	$\{a\}$	$\{b\}$	$\{c\}$	$\{d\}$	$\{a,b\}$
Votos	3	2	1	1	**5**
Coalición	$\{a,c\}$	$\{a,d\}$	$\{b,c\}$	$\{b,d\}$	$\{c,d\}$
Votos	**4**	**4**	3	3	2
Coalición	$\{a,b,c\}$	$\{a,b,d\}$	$\{a,c,d\}$	$\{b,c,d\}$	$\{a,b,c,d\}$
Votos	**6**	**6**	**5**	**4**	**7**

De entre las coaliciones ganadoras, $\{a,c\}$, $\{a,d\}$ y $\{b,c,d\}$ son, además, minimales. Obsérvese que todas reúnen el mínimo número de votos indispensable, 4.

Pero esto no ocurre siempre. En un sistema general, toda coalición que reúna exactamente el número mínimo de votos necesario para ganar es, desde luego, minimal. Pero no al revés: por ejemplo, si tenemos 6 votantes, con 3, 2, 2, 2, 1 y 1 votos respectivamente (11 votos en total), entonces la coalición de los tres primeros es ganadora minimal y reúne 7 votos, uno más de los necesarios para ganar. ♣

Planteeemos la cuestión en general. Tenemos un conjunto de n votantes, cada uno con un cierto número de votos, y con unas reglas dadas (sistema de mayoría, reglas de veto, etc.). Los datos son la lista de los votos de cada uno,

$$(v_1, v_2, \dots, v_n)\,,$$

el número total de votos $v = \sum v_j$ y el número (mínimo) de votos necesario para ganar las votaciones, q.

Queremos "medir" el poder que, en ese sistema, tiene un votante cualquiera. Lo primero que se nos ocurre, por supuesto, es utilizar como medida el número de votos (o más bien, la proporción de votos) que tiene esa persona. Pero éste no será, en general, un buen indicador: por ejemplo, si hay dos votantes, uno con 51 votos y otro con 49, y las decisiones se toman por mayoría absoluta, el segundo votante, pese a tener una proporción muy alta (¡casi la mitad!) de votos, no tiene influencia alguna. O, en el otro sentido, si hay tres votantes, a, que cuenta con 50 votos, b con 49 y c con 1, aunque b cuenta con una proporción de votos mucho mayor que c, su poder decisorio es exactamente el mismo: cualquier estrategia que siga b para formar coaliciones ganadoras o bloqueadoras la puede seguir también c, con los mismos resultados. Finalmente, para el caso $(50, 49, 2)$, los tres votantes tienen el mismo poder, pese a la disparidad de los votos de que disponen.

Vamos a analizar un índice (debido a Shapley y Shubik), de definición algo extraña, pero que recoge la idea de que, en realidad, lo importante no es sólo que un individuo esté en el "equipo ganador", sino que su participación sea *decisiva* para que el equipo sea ganador. El concepto clave es el de **pivote**: ordenamos los votantes, $(x_1, \dots, x_n)$, y diremos que, *respecto de ese orden*, x_i es pivote si $\{x_1, \dots, x_{i-1}\}$ no es una coalición ganadora, pero $\{x_1, \dots, x_i\}$ sí lo es. Obsérvese que, una vez decidida la ordenación de los votantes, hay un único pivote.

El **índice de poder** de un votante a, $I(a)$, se define entonces de la siguiente manera: de todas las posibles ordenaciones (permutaciones) de los votantes, la proporción de ellas en las que a es pivote. En fórmula,

$$I(a) = \frac{1}{n!}\,\#\{\text{permutaciones en las que } a \text{ es pivote}\}\,.$$

El índice $I(a)$ mide con qué frecuencia a es indispensable para ganar. Como en cada permutación hay un único pivote, si llamamos V al conjunto de los votantes, se tendrá que

$$\sum_{v\in V} I(v) = 1\,,$$

así que este índice nos proporciona una medida (en tantos por uno) del poder de cada votante. Veamos en algunos ejemplos que es una medida adecuada.

Ejemplo 3.2.7 *Volvamos al ejemplo de tres votantes, a con 50 votos, b con 49 y c con 1.*

Listamos las seis posibles permutaciones e identificamos el pivote en cada una de ellas:

Permutación	abc	acb	bac	bca	cab	cba
Pivote	b	c	a	a	a	a

Así que tendremos que

$$I(a) = \frac{4}{6}, \qquad I(b) = \frac{1}{6}, \qquad I(c) = \frac{1}{6}.$$

Y esta asignación recoge, efectivamente, la observación de que b y c tienen al final la misma influencia en el sistema (pese a que la cantidad de sus votos es muy diferente). ♣

Ejemplo 3.2.8 *Consideremos un conjunto de n votantes, cada uno con un voto.*

Por simetría (el papel de cada votante es intercambiable), es claro que

$$I(v) = \frac{1}{n}, \quad \text{para cada votante } v.$$

Y si no nos convence este argumento, pensemos que cada votante es pivote en las listas en que ocupe una situación especial, la posición en la que se sumen la "mitad" más uno de los votos (en realidad, cuando se sumen $\lfloor n/2 \rfloor + 1$ votos). De estas listas hay $(n-1)!$, como corresponde a ordenar el resto de los votantes en las demás posiciones. Así que, para cada votante v,

$$I(v) = \frac{(n-1)!}{n!} = \frac{1}{n}.$$

Ejemplo 3.2.9 *¿Cuál es el índice de un dictador?*

Un dictador a es pivote en cualquier permutación (porque con sólo sumar sus votos ya obtenemos mayoría), así que

$$I(a) = 1,$$

y el resto de los votantes tiene índice 0 (como corresponde a su influencia en este sistema).♣

Aunque estos ejemplos certifican que estos índices son una medida correcta del poder de un votante, nos gustaría tener una descripción en términos del número de coaliciones ganadoras minimales a las que el votante pertenezca. Por ejemplo, si el índice de un votante a es $I(a) = 0$, será porque no pertenece a coalición ganadora minimal alguna. Si, por ejemplo, $\{a, b, c\}$ fuera una coalición minimal, entonces a sería pivote en la lista $(b, c, a, \dots)$ y su índice no sería 0. Fijémonos en que exigir que sea minimal es fundamental en este argumento; por ejemplo, un votante sin influencia alguna puede pertenecer a coaliciones ganadoras (sin ir más lejos, a aquélla que incluye a todos los votantes).

La relación que podemos obtener es la siguiente: supongamos que, en un sistema con n votantes, el elemento a pertenece a l_j coaliciones ganadoras minimales de tamaño j, para cada $j = 1, \dots, n$ (nótese que varios, o todos, los l_j pueden ser 0). Esto es, el votante a, tras un cuidadoso análisis, ha determinado todas las coaliciones minimales de las que forma parte. Entonces puede asegurar que su índice de poder es

$$I(a) \geq \sum_{j=1}^{n} \frac{l_j}{j} \frac{1}{\binom{n}{j}}.$$

Quizás no sea capaz de determinar exactamente su índice de poder, pero al menos tiene una estimación por debajo, que puede ser suficiente para muchas cuestiones.

Veámoslo: sea A una coalición ganadora minimal de tamaño j a la que a pertenece. Es claro entonces que el elemento a será pivote de todas las permutaciones en las que esté situado en la posición j y tenga por delante al resto de los elementos de A:

$$\overbrace{\boxed{\qquad\qquad\qquad}}^{\text{restantes elementos de } A}\boxed{\;a\;}\overbrace{\boxed{\qquad\qquad\qquad\qquad}}^{\text{demás votantes}}$$

De estas permutaciones hay, claro, $(j-1)!\,(n-j)!$, pues hay que ordenar, por un lado, los $j-1$ compañeros en A y, por otro, a los $n-j$ restantes votantes. Repitiendo el argumento para las restantes coaliciones minimales en las que a esté incluido, concluimos que a es, al menos, pivote en el siguiente número de permutaciones:

$$\sum_{j=1}^{n} l_j\,(j-1)!\,(n-j)!$$

Pero en realidad el índice de poder puede ser mayor que esa cantidad, es decir, que tenemos que

$$I(a) \geq \frac{1}{n!}\sum_{j=1}^{n} l_j\,(j-1)!\,(n-j)! = \sum_{j=1}^{n} \frac{l_j}{j}\,\frac{1}{\binom{n}{j}}\,,$$

como afirmábamos antes. Para convencernos de que se tiene un $\geq$ en lugar de la igualdad, consideremos el siguiente sistema: a tiene 2 votos, b tiene 1, c tiene 10 y d tiene otros 10. Hay 23 votos en total, y se necesitan 12 para ganar una votación. El votante c, por ejemplo, pertenece a las siguientes coaliciones ganadoras minimales: $\{a,c\}$ y $\{c,d\}$, que dan lugar, con el procedimiento explicado antes, a cuatro permutaciones en las que c es pivote: $(acbd)$, $(acdb)$, $(dcab)$ y $(dcba)$. Pero, por ejemplo, c es pivote también de la lista $(bacd)$, que no es ninguna de las anteriores.

EJERCICIOS.

3.2.1 *Compruébese que $f^s = id$ si y sólo si s es un múltiplo del orden de f.*

3.2.2 *Demuéstrese que*

$$\begin{aligned} f^2 = id &\iff f \text{ sólo tiene ciclos de longitud 1 y/o 2} \\ f^3 = id &\iff f \text{ sólo tiene ciclos de longitud 1 y/o 3} \end{aligned}$$

3.2.3 *Compruébese que el orden de una permutación $f \in S_n$ divide a $n!$.*

> **Sugerencia.** Sean $l_1, l_2, \dots, l_m$ son las longitudes (distintas) de los diversos ciclos de f. Utilícese que el producto $l_1 \cdot l_2, \cdots l_m$ divide a $n!$

3.2.4 *Compruébese que una permutación dada por $f = \circlearrowleft_n(a_1\,a_2\,\dots a_{k-1}\,a_k)$ se puede escribir como*

$$f = f_k \circ f_{k-1} \circ \cdots \circ f_3 \circ f_2\,,$$

donde, para $j = 2, \dots, k$, f_j es la trasposición que intercambia a_1 con a_j.

3.2.5 *Compruébese que la identidad en S_n, $n \geq 2$, es siempre una permutación par.*

3.2.6 *Pruébese que si g y h son permutaciones de S_n,*

1. *$signo(g \circ h) = signo(g)\, signo(h)$.*
2. *$signo(g^{-1}) = signo(g)$.*

3.2.7 *Compruébese que si $g \in S_n$ es una trasposición, entonces es una permutación impar.*

3.2.8 *Demuéstrese que si g es un ciclo de longitud k de S_n (esto es, fija $n-k$ elementos y mueve cíclicamente los k restantes), entonces g es par si k es un número impar; y es impar si k es par.*

3.2.9 *Pruébese que si $g \in S_n$ se escribe como composición de m ciclos disjuntos, de ciertas longitudes $l_1, l_2, \dots, l_m$, entonces*

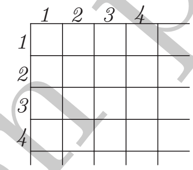
$$signo(g) = (-1)^t\,, \quad \text{donde } t = (l_1 - 1) + (l_2 - 1) + \cdots + (l_m - 1)\,.$$

O, de otra manera, agrupando los ciclos por longitudes: si g tiene α_1 ciclos de longitud 1, α_2 de longitud 2, etc., entonces

$$signo(g) = (-1)^{\alpha_2 + \alpha_4 + \cdots}\,.$$

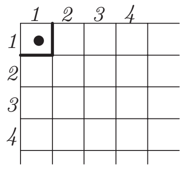
3.2.10 *Demuéstrese que, para $n \geq 2$, la mitad de las permutaciones de S_n son pares.*

3.2.11 *En este ejercicio describiremos un algoritmo gráfico para generar todas las permutaciones cíclicas (para cada valor de n). Se parte de una cuadrícula infinita, con los cuadrados etiquetados con los enteros positivos:*

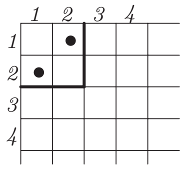


El primer paso es colocar una ficha en el cuadrado superior izquierdo. En el segundo se sitúan dos fichas según indica el dibujo:

$n = 1$



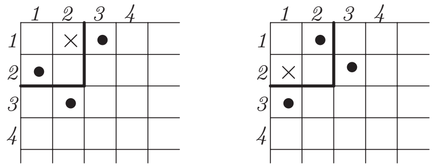
$n = 2$



Y ahora interpretamos la zona recuadrada como una permutación del conjunto $\{1, 2\}$: el 1 va al 2, y el 2 al 1, así que es el ciclo $\circlearrowleft_2(1\,2)$.

Para construir el paso $n = 3$, tomamos una cualquiera de las fichas y la sustituimos por otras dos, situadas una en la misma columna y en el cuadrado exterior al resaltado hasta el momento, y la otra en la misma fila y en el cuadrado exterior correspondiente. Se entiende bien en el dibujo (señalamos con un aspa la ficha que quitamos en cada caso):

$n = 3$



El de la izquierda representa a la permutación que lleva el 1 en 2, el 2 en 3 y el 3 en 1; esto es, el ciclo $\circlearrowleft_3(1\,2\,3)$. *La de la derecha representa al ciclo* $\circlearrowleft_3(1\,3\,2)$. *Y así sucesivamente, de manera que en el paso k sustituimos una ficha de coordenadas (i,j) por fichas en las posiciones (i,k) y (k,j).*

(a) Constrúyanse con este procedimiento las $3! = 6$ permutaciones cíclicas de $\{1,2,3,4\}$.

(b) Convencerse de que este procedimiento produce siempre matrices de permutaciones (esto es, en el paso k, una matriz $k \times k$ con una única ficha por fila y columna).

(c) Llamemos configuración factible a una disposición de fichas en el tablero construida con este procedimiento. Pruébese que una configuración es factible si y sólo si la configuración representa a una permutación cíclica.

(d) Compruébese que la equivalencia anterior nos permite recuperar el ya conocido resultado (véase la página 170) de que el número de permutaciones cíclicas de $\{1,\dots,n\}$ es $(n-1)!$.

3.2.12 *Recordemos que llamábamos B_j al conjunto de permutaciones de $\{1,\dots,n\}$ en las que el símbolo j no está en la posición j. Pruébese que*

$$\frac{Prob(B_i \cap B_j)}{Prob(B_i)\,Prob(B_j)} \xrightarrow[n\to\infty]{} 1$$

3.2.13 *Utilícese el teorema 10.1 sobre series alternadas para probar que*

$$\left|\frac{1}{e} - \frac{D_n}{n!}\right| = \left|\sum_{j=0}^{\infty}\frac{(-1)^j}{j} - \sum_{j=0}^{n}\frac{(-1)^j}{j}\right| \le \frac{1}{(n+1)!}\,.$$

Dedúzcase que, si $n > 1$, D_n es el entero más cercano a $n!/e$.

3.2.14 *Sea $D_n(k)$ el número de permutaciones de $\{1,2,\dots,n\}$ que dejan fijos exactamente a k elementos de entre $\{1,2,\dots,n\}$. (Así que $D_n(0) = D_n$= número de desbarajustes de $\{1,2,\dots,n\}$.) Pruébese que*

$$D_n(k) = \binom{n}{k} D_{n-k}.$$

Si definimos $D_0 = 1$, dedúzcase que

$$\sum_{j=0}^{n}\binom{n}{j} D_j = n!$$

Sugerencia. Para (a), obsérvese que, una vez elegidos los que quedan fijos, el resto hay permutarlos a la manera de los desbarajustes. Para (b), utilícese el resultado del primero.

3.2.15 *Del ejercicio anterior se deduce que $D_n(1)$, el número de permutaciones de dejan fijo exactamente un elemento, es nD_{n-1}.*

(a) Utilícese el ejercicio 3.1.42 para dar una prueba alternativa de este resultado.

(b) Compruébese que la probabilidad de que una permutación no fije ningún elemento y la probabilidad de que fije exactamente uno son prácticamente iguales si n es muy grande.

(b) ¿Qué podemos decir de la probabilidad de que la permutación fije exactamente dos elementos? ¿Y sobre la de que fije tres?

3.2.16 *Tenemos n votantes, uno con b votos y el resto con 1. ¿Cuál es el índice de cada uno de los votantes?*

Sugerencia. Analícense por separado los casos $b \geq n$ y $b < n$.

Solución. Los índices son $\min\{b/n, 1\}$ para el votante con b votos y $\max\{(n-b)/(n(n-1)), 0\}$ para el resto.

3.2.17 *Hay cuatro votantes, a, b, c y d, con 45, 43, 8 y 4 votos, respectivamente. ¿Cuánto valen sus correspondientes índices de poder?*

3.2.18 *Hay 100 votantes, cada uno con un voto. En caso de empate, el presidente, p, decide. ¿Cuál es el poder de cada uno de los votantes? ¿Y si el presidente tiene derecho de veto?*

Sugerencia. Si el presidente puede romper empates, hay dos posiciones, la 50 y la 51, en las que es pivote. Si tiene derecho de veto, el pivote nunca puede estar antes de la posición del presidente, pues sin él la coalición nunca es ganadora. Así pues, en cualquier posición de la 51 a la 100, el presidente es pivote.

Solución. Si el Presidente deshace empates: $2/100$ para el presidente y $98/(99 \times 100)$ para el resto. Si el Presidente tiene derecho de veto: $49/100$ para el presidente y $51/(99 \times 100)$ para el resto.

3.2.19 ***La unión hace la fuerza***. *Tenemos n votantes. Compruébese que si b de ellos se alían para votar siempre juntos, su poder individual pasa de ser $1/n$ a ser $1/(n-b+1)$.*

Sugerencia. Considérese a esa alianza como si fuera un único votante con b votos.

3.2.20 *El Consejo de Seguridad de la ONU consta de 15 miembros: hay cuatro miembros permanentes, EEEUU, Reino Unido, Francia, Rusia y China, que tienen derecho de veto. Los otros 10 miembros van rotando de entre los países de la ONU. Las decisiones se toman por mayoría simple. Pruébese que este sistema es equivalente a*

$$(7,7,7,7,7,1,1,1,1,1,1,1,1,1,1)\,, \qquad \textit{donde 39 votos son necesarios.}$$

Calcúlense los índices de poder de los miembros del Consejo de Seguridad.

3.2.21 *Llamemos $\mathcal{J}_a$ a la colección de coaliciones ganadoras minimales que contienen al elemento a.*
(a) Compruébese que

$$I(a) \geq \frac{1}{n} \sum_{J \in \mathcal{J}_a} \frac{1}{\binom{n-1}{|J|-1}}\,.$$

(b) Compruébese que, si llamamos $\mathcal{J}$ a la colección de todas las coaliciones ganadoras minimales de nuestro sistema,

$$\sum_{J \in \mathcal{J}} \frac{1}{\binom{n}{|J|}} \leq 1 \qquad \textit{y que} \qquad |\mathcal{J}| \leq \binom{n}{\lfloor n/2 \rfloor}.$$

Sugerencia. Para la primera parte del apartado (b), sumése en todos los votantes del sistema. Para la segunda parte, recuérdese que el coeficiente binómico $\binom{n}{k}$ es máximo para $k = \lfloor n/2 \rfloor$.

3.2.22 *Una familia $\mathcal{S}$ de subconjuntos se dice que es* ***familia de Sperner*** *si ningún $A \in \mathcal{S}$ está contenido en algún otro $B \in \mathcal{S}$. Compruébese que la familia $\mathcal{J}$ de coaliciones ganadoras del ejercicio anterior es de Sperner.* ***Nota****: Toda familia $\mathcal{S}$ de Sperner cumple que $|\mathcal{S}| \leq \binom{n}{\lfloor n/2 \rfloor}$.*

3.2.23 *Sea $\mathcal{S}$ la colección de subconjuntos de tamaño 3 del conjunto $\{1,2,\dots,7\}$. Demuéstrese que $\mathcal{S}$ es un familia de Sperner. Compruébese que, sin embargo, no hay ninguna asignación de votos a $\{1,2,\dots,7\}$ para la que $\mathcal{S}$ sea el conjunto de coaliciones ganadoras minimales.*