Notas de Combinatoria

github.com/danimalabares/combi

July 31, 2023

Índice

Parte I

Conteo

1. Conjuntos y multiconjuntos

Proposición. La cantidad de k-subconjuntos de un n-conjunto es

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

Definición. Escoger k objetos de n tipos sin orden ni límite de repetición produce un **multiconjunto** de tamaño k. Se trata de un conjunto formado por elementos en $[n]$ donde podemos considerar cualquier elemento más de una vez.

Observación. Denotemos a cada elección de k números del conjunto $[n] = \{1, \ldots, n\}$ por el vector $(x_1, \ldots, x_n)$ donde x_i es la cantidad de veces que se tomó el i-ésimo objeto, es decir, la **multiplicidad** de cada elemento. Entonces, $\sum_{i=1}^{n} = k$.

Teorema 1. El número de k-multiconjuntos de $[n]$ (equivalentemente, la cantidad de soluciones enteras no negativas de $\sum_{i=1}^{n} x_i = k$) es $\binom{k+n-1}{n-1} = \binom{k+n-1}{k}$.

Ahora enumeramos los trucos de conteo:

1. Las n-tuplas binarias con k 1's (hay $\binom{n}{k}$ de ellas) están en biyección con los caminos de latiz del $(0, 0)$ al $(k, n-k)$.

2. La de Pascal:
$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

3. La de Newton:
$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \qquad \text{y} \qquad (1+r)^n = \sum_{k=0}^{n} \binom{n}{k} r^k$$

4. Las de las diagonales en el triángulo de Pascal:
$$\sum_{k=0}^{n} \binom{k}{r} = \binom{n+1}{r+1} \qquad \text{y} \qquad \sum_{k=0}^{n} \binom{m+k}{k} = \binom{m+n+1}{n}$$

5. La del comité y la silla y la del comité y el subcomité

$$\binom{n}{k} = n\binom{n-1}{k-1} \qquad \text{y} \qquad \binom{n}{k}\binom{k}{\ell} = \binom{n}{\ell}\binom{n-\ell}{k-\ell}$$

6. Las de los subgrupos de un grupo de personas vistos en dos partes:

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2 \qquad \text{y} \qquad \binom{n+m}{r} = \sum_{k=0}^{r} \binom{n}{k}\binom{m}{r-k}$$

2. Relaciones de recurrencia

2.1 Obteniendo recurrencias

Definición. Una **relación de recurrencia** para una sucesión $a_0, a_0, \ldots$ es una expresión de la forma $a_n = g(n, a_{n-1}, a_{n-2}, \ldots, a_0)$, y tiene **orden** k si sólo depende de los k términos anteriores a a_n, es decir, de $a_{n-1}, \ldots, a_{n-k}$.

La recurrencia

$$a_n = g_1(n)a_{n-1} + g_2(n)a_{n-2} + \ldots + g_k a_{n-k} + f(n)$$

es **lineal** si las funciones g_i y f no dependen de ningún elemento en el espacio lineal generado por la sucesión, $\langle a \rangle$. Si f es cero, es una relación **homogénea**.

Definición. Los **números de Fibonacci** están dados por la recurrencia

$$F_{n+2} = F_{n+1} + F_n \qquad F(0) = 0, F(1) = 1$$

y los **números de Fibonacci ajustados** por

$$\hat{F}_{n+2} = \hat{F}_{n+1} + \hat{F}_n \qquad \hat{F}_0 = \hat{F}_1 = 1$$

Por último, los **números de Lucas** son la misma relación de recurrencia pero con

$$L_1 = 1, L_2 = 3$$

(El término "números de Fibonacci" fue popularizado por Lucas).

Definición. Un **desarreglo** es una permutación sin puntos fijos.

2.2 Métodos para encontrar soluciones

2.2.1 Relaciones homogéneas

Definición. Para una relación de recurrencia lineal con coeficientes constantes

$$a_n = c_1 a_{n-1} + \ldots + c_k a_{n-k} \tag{2.1}$$

definimos el **polinomio característico** como $\phi(x) = x^k - c_1 x^{k-1} - \ldots - c_k x^0$, y la **ecuación característica** como $\phi(x) = 0$, es decir

$$x^k = c_1 x^{k-1} + \ldots + c_k x^0$$

cuyas soluciones son las **raíces características**.

Para entender cómo se usan estos conceptos, primero revisamos el caso sencillo de la recurrencia

$$a_n = \alpha a_{n-1}$$

Sustituyendo una y otra vez, obtenemos que $a^n = \alpha a_{n-1} = \alpha^2 a_{n-2} = \ldots = \alpha^n a_0$. O sea que la solución al final depende de una constante A determinada por la condición inicial y el valor α, que es justamente uns raíz de la ecuación característica $x = \alpha$.

En el caso que nos interesa, la ecuación (2.1), tomemos una raíz característica α y sustituyámosla en la ecuación característica para obtener

$$\alpha^k = c_1 \alpha^{k-1} + \ldots + c_k \alpha^0$$

Y multiplicando por α^{n-k},

$$\alpha^n = c_1 \alpha^{n-1} + \ldots + c_k \alpha^{n-k}$$

O sea que una solución es $a_n = \alpha^n$. Y como al multiplicar por cualquier constante A se sigue preservando la igualdad, de hecho $a_n = A\alpha^n$ es una solución.

Y si hay otra raíz característica β con una solución asociada $a_n = B\beta^n$, de hecho cualquier expresión de la forma $a_n = A\alpha^n + B\beta^n$ también es una solución. (Ver la primera proposición del Deja Vu).

Y para encontrar los valores de A y B, es buena idea sustituir en $n = 0$.

O sea que la receta es:

1. Busco una constante α tal que $a_n = \alpha^n$ sea una solución. Esto naturalmente me lleva a la ecuación característica.
2. Las raíces me dan las soluciones de la recurrencia en la siguiente forma:

   Teorema 2 (Solución General)**.** Una recurrencia homogénea lineal de orden k con coeficientes constantes cuyas raíces características son $\alpha_1, \ldots, \alpha_r$, todas distintas y con multiplicidades $d_1, \ldots, d_r$, tiene solución

   $$a_n = \sum_i P_i(n)\alpha_i^n$$

   donde cada P_i es un polinomio de grado menor que d_i.

   (De hecho, todas las soluciones son de esta forma cambiando la elección de los P_i.)
3. Encuentro los valores de los polinomios (muchas veces son constantes, cuando las multiplicidades son 1) sustituyendo en las condiciones iniciales que nos dieron.

2.2.2 Relaciones no homogéneas

Literalmente es lo mismo que para ecuaciones diferenciales: las soluciones de una relación de recurrencia no homogénea están dadas por

$$a_n = p_n + h_n$$

donde p_n es una solución particular (que no depende de las condiciones iniciales) y h_n es una solución del sistema homogéneo asociado.

Para encontrar la solución particular consulté estas notas hawaiianas. Resulta que para una recurrencia de la forma

$$a_n = c_1 a_{n-1} + \ldots + c_k + F(n)$$

donde $F(n) = (b_d n^d + \ldots + b_1 n + b_0)s^n$ para ciertos números reales $b_d, \ldots, b_0, s$, hay de dos sopas:

1. Cuando s no es una raíz del polinomio característico de la homogénea. En este caso hay una solución particular de la forma

$$(\alpha_d n^d + \ldots + \alpha_1 n + \alpha_0)s^n$$

2. Cuando s es una raíz de multiplicidad m del polinomio característico de la homogénea. En este caso hay una solución particular de la forma

$$n^m(\alpha_d n^d + \ldots + \alpha_1 n + \alpha_0)s^n$$

Siguiendo a West:

Teorema 3. Tomemos una recurrencia de la forma $a_n = (\sum_{i=1}^{k} c_i a_{n-i}) + F(n)\alpha^n$ donde $n \geq k$, F es un polinomio de grado d, y α es una raíz de multiplicidad r (r puede ser cero, que en las notas hawaiianas es cuando s no es una raíz) de la recurrencia homogénea asociada.

Entonces existe una solución de la forma $a_n = P(n)n^r\alpha^n$ donde P es un polinomio de grado a lo más d.

2.2.3 Usando funciones generatrices

Definición. Dada una sucesión (a_n), una **función generatriz** es la serie formal $\sum_{n\geq 0} a_n x^n$. Y el operador $[x^n]$ nos devuelve el coeficiente que acompaña a x^n en la serie.

El método para solucionar recurrencias es como sigue:

1. Multiplicar simbólicamente por potencias de x^n y sumar todos los términos de la recurrencia en el dominio en el que sea válida.

   Por ejemplo, si tenemos $a_n = a_{n-1} + n$ para $n \geq 1$ y $a_0 = 1$, multiplicamos por potencias de x^n y sumamos para obtener

$$\sum_{n\geq 1} a_n x^n = \sum_{n\geq 1} a_{n-1} x^n + \sum_{n\geq 1} n x^n$$

Si $A(x) = \sum_{n\geq 0} a_n x^n$, el lado izquierdo es $A(x) - 1$. El primer sumando del lado derecho es $xA(x)$.

El segundo sumando se simplifica así: como

$$1 + x + x^2 + x^3 + \ldots = \sum_{n\geq 0} x^n = \frac{1}{1-x}$$

al derivar esta expresión obtenemos que

$$1 + 2x + 3x^2 + \ldots = \frac{d}{dx}\frac{1}{1-x} = -\frac{1}{(1-x)^2}$$

así que el segundo término de la suma es $-\frac{x}{(1-x)^2}$. Tenemos que

$$\begin{aligned}
A(x) - 1 &= xA(x) - \frac{x}{(1-x)^2} \\
A(x) - xA(x) &= 1 - \frac{x}{(1-x)^2} \\
A(x)(1-x) &= 1 - \frac{x}{(1-x)^2} \\
A(x) &= \frac{1}{1-x} - \frac{x}{(1-x)^3} \\
A(x) &= \sum_{n\geq 0} x^n - \sum_{n\geq 0} \binom{n+2}{2} x^n \\
&= \sum_{n\geq 1} x^n - \sum_{n\geq 1} \binom{n+2}{2} x^n
\end{aligned}$$

Suponiendo que conocemos la expansión de $\frac{x}{(1-x)^3}$. En fin, $a_n = 1 - \binom{n+2}{2}$.

Ejercicio. Resolver la recursión de Fibonacci con este método. (Ver **generating-functionology**, p. 9)

3. Funciones generatrices

3.1 Ordinarias

Definición. Dada una sucesión (a_n), una **función generatriz ordinaria** es la serie formal $\sum_{n\geq 0} a_n x^n$. Y el operador $[x^n]$ nos devuelve el coeficiente que acompaña a x^n en la serie. Si el número a_n representa la cantidad de cosas u en cierto universo U que tienen peso $w(u)$ igual a n, decimos que la función generatriz es el **enumerador dado por** w **para** U.

Ejemplo. La función generatriz de la sucesión $a_n = n$ es $\sum_{n=0}^{\infty} nx^n$, que, como vimos en la sección de solución de recurrencias, se puede ver como $x\frac{d}{dx}\frac{1}{1-x} = \frac{x}{(1-x)^2}$. Esta clase de expresiones nos permiten manipular y extraer información de las sucesiones.

Definición. La **suma** y el **producto** de las funciones generatrices ordinarias $\sum_{n=0}^{\infty} a_n x^n$ y $\sum_{n=0}^{\infty} b_n x^n$ están dados por

$$\sum_{n=0}^{\infty}(a_n + b_n)x^n \qquad \text{y} \qquad \sum_{n=0}^{\infty}\left(\sum_{i+j=n} a_i b_j\right)x^n = \sum_{n=0}^{\infty}\left(\sum_{j=0}^{n} a_j b_{n-j}\right)x^n$$

Lema. Si las funciones generatrices de (a_n) y (b_n) cuentan los objetos que tienen peso n en los universos A y B (son enumeradores), entonces su producto es el enumerador de las parejas de objetos en $A \times B$ tales que sus pesos suman n.

Corolario. Haciendo inducción sobre el lema anterior, vemos que si $(a_n^1), \ldots, (a_n^r)$ son sucesiones que representan cuántos objetos con peso n hay en los conjuntos $A_1, \ldots, A_r$, entonces, el k-ésimo coeficiente de la función generatriz del producto cuenta las r-tuplas tales que la suma de los pesos es k.

Ejemplo. Recordemos que un k-multiconjunto construido a partir de n elementos está determinado por una n-tupla donde cada entrada es la multiplicidad de cada elemento, y estas multiplicidades deben sumar k.

Para encontrar un enumerador de los k-multiconjuntos formados con n números, podemos contar estas tuplas. Cada entrada cuenta las apariciones del i-esimo número, que

puede aparecer $0, 1, \ldots, k$ veces, así que queremos que nuestra función generatriz tenga el factor $\sum_{j=0}^{k} x^j$. Cuando variamos la k, obtenemos que el enumerador del i-ésimo número es $\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$. Luego, el enumerador de las n-tuplas es $\left(\frac{1}{1-x}\right)^n$

Y recordando el teorema que mostramos en el capítulo 1, concluimos que

$$(1 + x + x^2 + \ldots)^n = \sum_{k=0}^{\infty} \binom{k+n-1}{n} x^k$$

Llevemos un poco más lejos este razonamiento: el producto de $1 - x$ y $\sum_{k=0}^{\infty} x^k$ es 1, así que $(1-x)^n \left(\sum_{k=0}^{\infty} x^k\right)^n = 1^n = 1$. Luego,

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

... ¿qué no era más fácil sólo decir $(1 + x + x^2 + \ldots) = \frac{1}{1-x}$?

Ejemplo (Multiplicidades restringidas)**.** A veces queremos restringir alguno de los elementos a que aparezca cierta cantidad de veces. En estos casos, el enumerador individual de este elemento debe ser $\sum_{k \in S} x^k$.

Por ejemplo, si todos los elementos se deben usar al menos una vez, tenemos:

$$(x + x^2 + x^3 + \ldots)^n = \left(\frac{x}{1-x}\right)^n$$

Y luego:

$$[x^k] \left(\frac{x}{1-x}\right)^n = [x^{k-n}] \frac{1}{(1-x)^n} = \binom{k-n+n-1}{n-1} = \binom{k-1}{n-1}$$

es la cantidad de k-multiconjuntos tales que cada elemento de $[n]$ se usa por lo menos una vez. ... ¿cierto?

Agregemos aquí:

Teorema 4 (Regla 5)**.** Si $f \overset{ops}{\longleftrightarrow} \{a_n\}_0^\infty$

$$\frac{f}{1-x} \overset{ops}{\longleftrightarrow} \left\{\sum_{j=0}^{n} a_j\right\}_{n \geq 0}$$

3.2 F.g. exponenciales

Definición. La **función generatriz exponencial (fge)** de una sucesión (a_n) es $\sum a_n x^n / n!$.

Ejemplo. La cantidad de palabras de longitud n formadas con un alfabeto de k letras es k^n. La función generatriz exponencial correspondiente tiene la expresión muy sencilla e^{kx}.

Teorema 5. Siguiendo la notación del libro **generatingfunctionology**, si tenemos dos funciones generatrices exponenciales $f \overset{egf}{\longleftrightarrow} \{a_n\}_0^\infty$ y $g \overset{egf}{\longleftrightarrow} \{b_n\}_0^\infty$, entonces su producto está dado por

$$fg \overset{egf}{\longleftrightarrow} \left\{ \sum_k \binom{n}{k} a_k b_{n-k} \right\}_0^\infty$$

En comparación con las funciones generatrices ordinarias, en cuyo caso tenemos que:

$$fg \overset{ogf}{\longleftrightarrow} \left\{ \sum_k a_k b_{n-k} \right\}_0^\infty$$

De hecho podemos generalizar este resulado:

Teorema 6. Para $f \overset{egf}{\longleftrightarrow} \{a_n\}_0^\infty$, $g \overset{egf}{\longleftrightarrow} \{b_n\}_0^\infty$ y $h \overset{egf}{\longleftrightarrow} \{c_n\}_0^\infty$

$$fgh \overset{egf}{\longleftrightarrow} \left\{ \sum_{r+s+t=n} \frac{n!}{r!s!t!} a_r b_s c_t \right\}_0^\infty$$

Teorema 7. Para $f \overset{egf}{\longleftrightarrow} \{a_n\}_0^\infty$,

$$f^k \overset{egf}{\longleftrightarrow} \left\{ \sum_{r_1+r_2+\ldots+r_k=n} \frac{n!}{r_1!r_2!\ldots r_k!} a_{r_1} a_{r_2} \ldots a_{r_k} \right\}_0^\infty$$

Definición. El **número de Stirling del segundo tipo** $S(n,k)$, también denotado $\left\{ {n \atop k} \right\}$, es la cantidad de particiones de $[n]$ en k bloques no vacíos.

Teorema 8.

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

Demostración. Primero notemos que las particiones de $[n]$ en k bloques no vacíos se pueden ordenar de acuerdo a los elementos que tienen. Así, podemos ordenar los bloques en la lista $[k]$, y entonces las particiones *ordenadas* $[n]$ en k bloques no vacíos se pueden ver como funciones suprayectivas de $[n]$ en $[k]$. *Esta prueba me pareció sumamente confusa*

□

Definición. El **número de Bell** $B(n)$ cuenta la cantidad de particiones de $[n]$.

Ejemplo (¿Cuántos desarreglos hay?)**.** Recordemos que un **desarreglo** es una permutación sin puntos fijos. Denotemos por D_n a la cantidad de desarreglos de n elementos.

La cantidad de permutaciones de n elementos, que es $n!$, se puede ver como la suma de las cantidades de permutaciones que no fijan elementos, las que fijan 1 elemento, 2 elementos, etc., hasta la identidad. Cada una de estas cantidades es justamente D_{n-k}.

En cada caso hay $\binom{n}{k}$ elecciones de subconjuntos de k elementos que pueden quedar fijos, así que

$$n! = \sum_{k=0}^{n} \binom{n}{k} D_{n-1}$$

Diviendo entre $n!$, multiplicando por x^n y sumando sobre todos los naturales, obtenemos las funciones generatrices exponenciales:

$$\frac{1}{1-x} = e^x D(x)$$

Usando la regla del producto exponencial, donde $D(x)$ es la función generatriz exponencial, es decir, $D(x) = \sum_{n\geq 0} \frac{D_n}{n!} x^n$.

Usando la regla 5 en la expresión $e^{-x}/(1-x)$ obtenemos que $D \overset{egf}{\longleftrightarrow} \{\sum_k (-1)^k/k!\}$, es decir,

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

Y para acordarse:

$$D_n \approx \frac{n!}{e}$$

Definición. Los **números de Catalan** C_n cuentan la cantidad de expresiones de n parejas de paréntesis bien balanceadas.

Por ejemplo, $C_3 = 5$ ya que sólo hay:

$$((())) \qquad (()()) \qquad ()()() \qquad ()(()) \qquad (())()$$

Los números de Catalan también cuentan:

- Los caminos en una cuadrícula de $n \times n$ partiendo de la esquina inferior izquierda a la esquina superior derecha sin pasar por arriba de la diagonal.
- Triangulaciones de un $n+2$-ágono usando líneas que no se cruzan.
- Y muchas otras cosas más.

Teorema 9.

$$C_n = \frac{1}{n+1}\binom{2n}{n}$$

4. Principio de inclusión-exclusión

La siguiente fórmula es sumamente familiar:

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

Y también la generalización para tres conjuntos:

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

Que captura la esencia del Principio de Inclusión Exclusión (PIE): *overcounting*, o "contar de más".

La fórmula general es de alguna manera obvia: la cardinalidad de la unión es igual a la suma de la cardinalidad de cada conjunto, menos las cardinalidades de las intersecciones de a dos, más las intersecciones de a tres, menos las de a cuatro, ..., hasta que sumamos o restamos la intersección de todos (esto depende de la paridad).

Escribir esto puede no ser algo laborioso. Matousek nos da una buena solución de acuerdo a la notación de que $\binom{X}{k}$ denota la colección de *subconjuntos* de X de tamaño k:

Teorema 10. Para cualquierquiera conjuntos finitos $A_1, \ldots, A_n$,

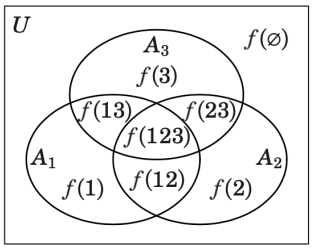
$$\left|\bigcup_{i=0}^{n} A_i\right| = \sum_{i=1}^{n} (-1)^{i+1} \sum_{\mathcal{A} \in \binom{\{A_1, \ldots, A_n\}}{i}} \left|\bigcap \mathcal{A}\right|$$

Y hay otra expresión "almost devilish":

$$\left|\bigcup_{i=0}^{n} A_i\right| = \sum_{\emptyset \neq \mathcal{A} \subseteq \{A_1, \ldots, A_n\}} (-1)^{|\mathcal{A}|-1} \left|\bigcap \mathcal{A}\right|$$

Que de hecho se parece mucho a lo que West denota por $f(\emptyset)$. Veamos un poco más el planteamiento de West:

Dado un subconjunto del conjunto de índices $T \subseteq [n]$, denotaremos por $f(T)$ a la cantidad de elementos x tales que $x \in A_i$ si y sólo si $i \in T$. De alguna manera estamos partiendo el espacio de acuerdo a todas las posibles intersecciones de los conjuntos:



Teorema 11 (PIE)**.**

$$f(T) = \sum_{S \supseteq T} (-1)^{|S|-|T|} \left| \bigcap_{i \in S} A_i \right|$$

Muchas veces se usa el PIE en su forma complementaria, que es justamente lo que West denota por $f(\varnothing)$. Una fórmula más accesible es:

$$\begin{aligned} \left| U - \bigcup_{i=0}^{n} A_i \right| &= |U| - \sum_{i=1}^{n} |A_i| + \ldots + (-1)^n |A_1 \cap \ldots \cap A_n| \\ &= \left| U - \bigcup_{i=0}^{n} A_i \right| \\ &= |U| - \sum_{i=1}^{n} (-1)^{i+1} \sum_{\mathcal{A} \in \binom{\{A_1, \ldots, A_n\}}{i}} \left| \bigcap \mathcal{A} \right| \end{aligned}$$

y en particular, si las intersecciones de los A_i son todas del mismo tamaño, tenemos la expresión

$$\left| U - \bigcup_{i=0}^{n} A_i \right| = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \alpha_k$$

donde α_k es el tamaño de las intersecciones de a k, y $\alpha_0 = |U|$.

Una clara aplicación de esta fórmula nos da una prueba muy directa de un resultado conocido

Teorema 12.

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

Demostración. Recordemos que las particiones de $[n]$ en k bloques no vacíos se pueden ordenar de acuerdo a los elementos que tienen, así que podemos ordenar los bloques en la lista $[k]$ y pensar que las particiones *ordenadas* $[n]$ en k bloques no vacíos son funciones suprayectivas de $[n]$ en $[k]$.

Usando PIE, podemos contar estas funciones calculando el número de funciones de $[n]$ en $[k]$ menos la unión de las funciones que no le pegan a $1, 2, \ldots k$. Todas las intersecciones son del mismo tamaño, así que esta cantidad es $\sum_{i=0}^{k}(-1)^i\binom{k}{i}(k-i)^n$. Al "revolverlas" para que ya no sean las particiones ordenadas, dividimos entre $k!$ y listo. $\square$

5. Enumeración bajo acciones de grupo

Teorema 13 (Lema que no es de Burnside)**.** Dada una acción de un grupo finito G en un conjunto X,

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix} g|$$

donde X/G es el conjunto de órbitas y $\operatorname{Fix} g$ es el conjunto de puntos fijos de $g \in G$.

Demostración. Primero notemos que

$$\sum_{g \in G} |\operatorname{Fix} g| = \sum_{x \in X} |\operatorname{Stab} x|$$

ya que ambos lados cuentan la cantidad de parejas (g, x) tales que g fija a x.

Ahora notemos que, dado x, hay tantos elementos en su órbita como clases laterales $G/\operatorname{Stab} x$. En efecto: la correspondencia $gx \mapsto g+\operatorname{Stab} x$ está bien definida y es biyectiva. Agregando a esto el teorema de Lagrange,

$$|G \cdot x| = [G : \operatorname{Stab} x] = |G|/|\operatorname{Stab} x|$$

Invirtiendo este cociente y sumando sobre $x \in X$, casi terminamos. Sólo falta notar que como las órbitas son una partición de X,

$$\sum_{x \in X} \frac{1}{|G \cdot x|} = \sum_{G \cdot x \in G/X} \left(\sum_{y \in G \cdot x} \frac{1}{|G \cdot y|} \right) = \sum_{G \cdot x \in G/X} 1 = |X/G|$$

□

Teorema 14 (de enumeración de Pólya-Redfield)**.** Sea X un conjunto finito, G un grupo de permutaciones de X y Y un conjunto finito de colores. Entonces,

$$|Y^X/G| = \frac{1}{|G|} \sum_{g \in G} |Y|^{c(g)}$$

donde:

- Y^X es el conjunto de coloraciones de X, formalmente el conjunto de funciones $X \to Y$.
- Como G actúa en X, también actúa en Y^X, así que hay un espacio de órbitas Y^X/G.
- $c(g)$ es la cantidad de ciclos que tiene g cuando lo vemos como una permutación de X.

Observación. Hay una versión con pesos de este teorema, que demuestra West. Por ahora no lo escribimos.

Definición. El **índice de ciclo** es un polinomio

$$Z_G(x_1, x_2, \ldots) = \frac{1}{|G|}(\text{la función que enlista los elementos en } G \text{ de acuerdo a sus ciclos})$$

es decir, cada x_i representa un ciclo de longitud i.

Por ejemplo, el polinomio

$$\frac{1}{12}(x_1^4 + 8x_1x_3 + 3x_2^2)$$

Es el índice de ciclos del subgrupo de rotaciones de las simetrías de un tetraedro regular, ya que la identidad tiene cuatro 1-ciclos, las rotaciones por el centro de las caras tienen un 1-ciclo y un 3-ciclo, y las rotaciones por los puntos medios de las aristas tienen dos 2-ciclos. Los coeficientes enteros simplemente nos dicen cuántas hay de cada una.

6. Ejercicios

Los ejercicios vienen de dos libros: W=West, C=Cameron.

W 1.1.1 Después de tirar k dados, ¿cuál es la probabilidad de que la suma sea par?

Solución. La probabilidad es $1/2$. Denotemos por P_i la probabilidad de que la suma sea par cuando tiramos i dados, y I_i cuando la suma es impar. Entonces, la probabilidad que buscamos, P_k, se obtiene de dos formas: cuando al tirar $k-1$ la suma fue par y el k-ésimo también salió par, o bien cuando al tirar $k-1$ la suma salió impar y el k-ésimo también salió impar. Es decir,

$$P_k = P_{k-1}\frac{1}{2} + I_{k-1}\frac{1}{2}$$

Para encontrar P_{k-1}, y todos los anteriores, sucederá exactamente lo mismo:

$$P_i = P_{i-1}\frac{1}{2} + I_{i-1}\frac{1}{2}$$

Y de hecho algo análogo pasa con la probabilidad de que la suma sea impar: tiene que ser cierto que los $i-1$ dados anteriores suman par y el i-ésimo impar, o bien que los $i-1$ anteriores sumaron impar y el i-ésimo par. Es decir,

$$I_i = P_{i-1}\frac{1}{2} + I_{i-1}\frac{1}{2}$$

Hasta que lleguemos a P_2, que se obtiene sólo si los dos primeros dados sumaron par, o si los dos sumaron impar, así que $P_2 = \frac{1}{2}\frac{1}{2} + \frac{1}{2}\frac{1}{2} = \frac{1}{2}$. Y de hecho $I_2 = \frac{1}{2}\frac{1}{2} + \frac{1}{2}\frac{1}{2} = \frac{1}{2}$. Sustituyendo, notemos que $P_3 = \frac{1}{2}\frac{1}{2} + \frac{1}{2}\frac{1}{2} = \frac{1}{2}$. Y de hecho esto sigue sucediendo conforme subimos el índice hasta llegar a k, es decir, $P_k = \frac{1}{2}\frac{1}{2} + \frac{1}{2}\frac{1}{2} = \frac{1}{2}$ □

W 1.1.2 Cuente la cantidad de rectángulos con área positiva formados por una retícula con m rectas horizontales y n verticales

Solución. Si contamos sólo los rectángulos actoados, es fácil convencerse de que son $(n-1)(m-1)$. Y los rectángulos no acotados que se forman son $2(m+n)$. □

W 1.1.3 El alfabeto romano tiene 21 consonantes y 5 vocales. ¿Cuántas palabras se pueden formar con r consonantes y s vocales?

Solución. Una colección de r consonantes entre las 21, sin importar el orden y con posibilidad de repetición es un r-multiconjunto de $[21]$, de los que, como sabemos, hay $\binom{r-21-1}{21-1} = \binom{r-20}{20}$. Análogamente, hay $\binom{s+4}{4}$ posibles colecciones de vocales que podemos escoger. Ahora sólo queda ordenar los $r+s$ elementos que tenemos.

La respuesta es

$$\binom{r-20}{20}\binom{s+4}{4}(r+s)!$$

□

W 1.1.8 ¿Cuántas manos de 6 cartas se puede formar con una baraja de 52 cartas de forma que haya al menos una carta de cada palo?

Solución. $13 \cdot 13 \cdot 13 \cdot 13 \cdot 48 \cdot 47$ □

W 1.1.9 Cuente la cantidad de números enteros del 0 al 99,999 en los que cada dígito se repite a lo más dos veces.

Solución. La cantidad de números del 0 al 99,999 es 100,000. Para resolver nuestro problema, basta descartar los números en los que hay al menos un dígito que se repite tres veces. Veamos:

- La cantidad de números de 5 dígitos tales que todos son diferentes es $10 \cdot 9 \cdot 8 \cdot 7 \cdot 6$.
- Si dos números son iguales: $10 \cdot 9 \cdot 8 \cdot 7 \cdot 4$.
- Si tres números son iguales: $10 \cdot 9 \cdot 8 \cdot 3$.

La respuesta es: $100,000 - 10 \cdot 9 \cdot 8 \cdot 3$. □

W 1.1.11 Dada una bolsa con muchísimas canicas de 4 colores distintos, ¿de cuántas formas podemos escoger 12 canicas? Cuente las distintas formas de ordenarlas en una línea.

Solución. Una elección de 12 canicas de la bolsa corresponde a un 12-multiconjunto de $[4]$. Sabemos que hay $\binom{12+3}{3} = 455$ tales multiconjuntos. Contar las formas de ordenarlas en una línea es como contar las funciones de $[12]$ en $[4]$, que son 4^{12} (es un número muy grande). □

W 2.2.14 Resuelva las siguientes recurrencias, dado que $a_0 = a_1 = 1$.

(a) $a_n = 4a_{n-1} - 4a_{n-2} - n + 6$

(b) $a_n = 5a_{n-1} - 6a_{n-2} + 2n - 1 + 2^n$

Solución.

(a) Multiplicando por x^n y sumando sobre los naturales a partir de 2, obtenemos:

$$\sum_{n\geq 2} a_n x^n = 4\sum_{n\geq 2} a_{n-1}x^n - 4\sum_{n\geq 2} a_{n-2}x^n - \sum_{n\geq 2} nx^n + 6\sum_{n\geq 2} x^n$$

Suponiendo que $A(x) = \sum_{n\geq 0} a_n x^n$, y tomando en cuenta que $a_0 = a_1 = 1$, la expresión de arriba se puede expresar como:

$$A(x) - x - 1 = 4(xA(x) - x) - 4x^2A(x) - \left(\frac{x}{(1-x)^2} - x\right) + \frac{6}{1-x} - x - 1$$

$$\iff A(x) = 4xA(x)(1-x) - 3x - \frac{x}{(1-x)^2} + \frac{6}{1-x}$$

$$\iff A(x)(1 - 4x(1-x)) = \frac{6}{1-x} - \frac{x}{(1-x)^2} - 3x$$

$$\iff A(x)(1-2x)^2 = \frac{6}{1-x} - \frac{x}{(1-x)^2} - 3x$$

Como $\frac{1}{1-2x} = \sum_{n\geq 0}(2x)^n$, al derivar obtenemos que $\frac{2}{(1-2x)^2} = \sum_{n\geq 0}(n+1)2^{(n+1)}x^n$

$$\begin{aligned} A(x) &= \frac{1}{2}\frac{2}{(1-2x)^2}\left(\frac{6}{1-x} - \frac{x}{(1-x)^2} - 3x\right) \\ &= \frac{1}{2}\sum_{n\geq 0}(n+1)2^{(n+1)}x^n\left(6\sum_{n\geq 0}x^n - \sum_{n\geq 0}nx^n - 3x\right) \\ &= \frac{1}{2}\left(6\sum_{n\geq 0}\left(\sum_{j=0}^{n}(j+1)2^{(j+1)}\right)x^n - \sum_{n\geq 0}\left(\sum_{j=0}^{n}(j+1)2^{(j+1)}(n-j)\right)x^n - 3\sum_{n\geq 0}(n+1)2^{(n+1)}x^{n+1}\right) \end{aligned}$$

Ahora veamos si sí da 1 en a_0 y a_1:

$$a_0 = \text{no da}$$

□

W 4.1.9 Usa PIE para demostrar que $\sum(-1)^k\binom{n}{k}(n-k)^n = n!$.

Solución. Consideremos $A_i := \{f : [n] \to [n] : i \notin \operatorname{img} f\}$. Las permutaciones de n elementos son las funciones suprayectivas de $[n]$ en $[n]$ así que

$$n! = \left|\{f : [n] \to [n]\} - \bigcup A_i\right|$$

Usando la fórmula de West, esta cantidad es

$$\begin{aligned} f(\varnothing) &= \sum_{S\subseteq[n]}(-1)^{|S|}\left|\bigcap_{i\in S}A_i\right| \\ &= \sum_{k=0}^{n}(-1)^k\binom{n}{k}(n-k)^n \end{aligned}$$

Ya que cada subcolección de k de los conjuntos A_i tiene intersección de tamaño $(n-k)^n$, ya que son las palabras de longitud n en $n-k$ símbolos, y hay $\binom{n}{k}$ elecciones en cada caso. Cuando $k=0$ contamos todas las funciones de $[n]$ en $[n]$, de las que hay n^n. □

C 3.13.10 Demuestre las siguientes identidades:

(a) $\binom{n}{k}\binom{k}{\ell} = \binom{n}{\ell}\binom{n-\ell}{k-\ell}$

(b) $\sum_{i=0}^{k}\binom{m}{i}\binom{n}{k-i} = \binom{m+n}{k}$ donde $\binom{n}{k} = 0$ si $k<0$ o $k>n$.

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

(d) $\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}$

(e) $\sum_{k=0}^{n}(-1)^k\binom{n}{k}^2 = \begin{cases} 0 & \text{si } k \text{ es impar} \\ (-1)^m\binom{2m}{m} & \text{si } n = 2m \end{cases}$

Solución.

(a) Ambos lados cuentan los subcomités de tamaño ℓ de los comités de tamaño k de un grupo de n personas.

(b) Ambos lados cuentan los k-subconjuntos de $m+n$.

(c)

(d) Ambos lados cuentan la cantidad de parejas (m, M) con $m \in [n]$ y $M \subseteq [n]$ tales que $m \in M$.

□

C 3.13.10 ¿Cuántas palabras se pueden formar con las letras en la palabra STATE?

Solución. Tenemos cinco símbolos, así que la cantidad de permutaciones en total es de $5! = 120$. Sin embargo, cada intercambio de la letra T nos lleva a la misma palabra. Para tomar esto en cuenta consideremos el siguiente razonamiento. Renombrando los símbolos como T_1 y T_2, la cantidad de permutaciones se puede dividir en dos bloques: los que tienen primero a T_1 y los que tienen primero a T_2. Así, la cantidad total de permutaciones salvo permutaciones de las Ts es $5!/2 = 60$. □

C 3.13.10 ¿Cuántas palabras se pueden formar con n letras si m de ellas son iguales?

Solución. Ahora tenemos $n!$ posibles palabras, y para cada una, hay $m!$ maneras equivalentes de acomodar las letras que son iguales. Hay $n!/m!$ palabras diferentes. □

Parte II

Acomodos

7. Conjuntos parcialmente ordenados

Definición. Una **relación** R en un conjunto X es un subconjunto del producto cartesiano $X \times X$. Escribimos xRy para denotar $(x, y) \in R$. Un **orden parcial** en X es una relación

reflexiva: xRx para toda $x \in X$.

antisimétrica: si xRy y yRx, entonces $x = y$.

transitiva: si xRy y yRz entonces xRz.

Si dos elementos no se pueden comparar mediante un orden parcial, escribimos $x||y$.

Definición (Conceptos básicos)**.**

- Una **cadena** es un conjunto linealmente ordenado. El **alto** de un orden parcial es el tamaño de la cadena más grande.
- Una **anticadena** es un conjunto donde no hay dos elementos comparables. El **ancho** de un orden parcial es el tamaño de la anticadena más grande.
- Un elemento en un conjunto parcialmente ordenado es **maximal** (**minimal**) si no hay elementos mayores (menores) que él.
- Un elemento es el **máximo** (**mínimo**) si es mayor (menor) o igual que todos los demás. El máximo y el mínimio son únicos.
- Dos conjuntos parcialmente ordenados son **isomorfos** si existe una biyección entre ellos que preserva el orden.
- El **producto** de dos COPOS está construido en el producto cartesiano de los conjuntos y la relación de orden está dada entrada a entrada.

Definición. Un **diagrama de Hasse** es una gráfica cuyos puntos son los elementos del COPO y hay una arista entre dos elementos comparables si no hay ninguno entre ellos.

El elemento mayor está literalmente arriba (coordenada y mayor). El diagrama determina completamente el COPO: $u < v$ si y sólo si existe un camino "vertical" entre u y v.

Definición (Latices)**.**

- Una **latiz** es un COPO en el que cualquier pareja de elementos tiene una máxima cota inferior (**glb**) y una mínima cota superiot (**lub**).

  Un conjunto totalmente ordenado es una latiz, ya que cualesquiera dos elementos son comparables, así que podemos tomar la máxima cota inferior el menor de ellos, y la mínima cota superior el mayor de ellos. También el conjunto potencia es una latiz, donde la glb es la intersección y la lub la unión.

  Usamos la notación $a \wedge b$ para la glb de a y b, y $a \vee b$ para la lub.

- Una latiz es **distributiva** si

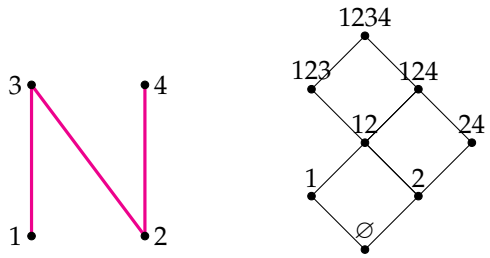
$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$
$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

- Un subconjunto $Y \subseteq P$ de un COPO es un **down-set** si para cualesquiera $y \in Y$ y $z \in P$ tales que $z \leq y$, se tiene que $z \in Y$. Es decir, todo lo que está abajo de cualquier elemento de Y está en Y.

  La colección de down-sets es una latiz distributiva, que denotamos $L(P)$. Cualquier latiz distributiva finita se puede representar como la $L(P)$ de un COPO en $[n]$:

Teorema 15. Sea L una latiz distributiva finita. Entonces hay un único COPO finito tal que L es isomorfo a $L(P)$.

Por ejemplo, el COPO N tiene la siguiente latiz distributiva:



Lema. Cualquier COPO finito no vacío tiene un elemento maximal.

Teorema 16 (Dilworth, 1950)**.** Sea P un orden parcial. El tamaño de la anticadena más grande es igual al mínimo número de cadenas que forman una partición de P.

Demostración. Inducción sobre el tamaño de P. La condición es obvia para un conjunto vacío, así que podemos tomar un elemento maximal $a \in P$.

Supongamos que cualquier subconjunto con menos elementos que P puede ser cubierto por tantas cadenas y como elementos en la anticadena más grande. Tomemos $P\backslash\{a\}$, y supongamos que hay k cadenas $C_1, \ldots, C_k$ que lo cubren y una anticadena A_0 con k elementos. Como $A_0 \cap C_i \neq \varnothing$, podemos escoger un elemento maximal en C_i que esté en alguna anticadena de tamaño k para definir $A := \{x_1, \ldots, x_k\}$.

Veamos que A es una anticadena. Tomemos dos elementos $x_i \neq x_j \in A$. Hay una anticadena A_i de tamaño k en la que está x_i, y de hecho $A_i \cap C_j \neq \varnothing$ ya que las C's cubren todo el copo. Escojamos $y \in A_i \cap C_j$. Como y está en la cadena cuyo elemento maximal es x_j, tenemos que $y \leq x_j$. Pero y está en una anticadena donde está x_i, así que no es posible que $y \leq x_i$ ni que $x_i \leq y$. Luego, si $x_j \leq x_i$ se obtiene una contradicción. Intercambiando los roles de i y j se obtiene el otro lado.

Ahora volvamos a P. Primero supongamos que $a \geq x_i$ para alguna i y definamos $K := \{a\} \cup \{x \in C_i : x \leq x_i\}$. ¿Qué tan grande puede ser una anticadena en $P\backslash K$? Como las C's son una partición de $P\backslash\{a\}$, cualquier anticadena de tamaño máximo en $P\backslash\{a\}$ debe contener algún elemento de C_i. Pero x_i es el elemento maximal que está en alguna anticadena de $P\backslash\{a\}$, y ya no está en $P\backslash K$. Así que $P\backslash K$ no puede tener una anticadena con k elementos.

Como $A\backslash\{x_i\}$ es una anticadena de tamaño $k-1$ en $P\backslash K$, por hipótesis inductiva hay $k-1$ cadenas disjuntas que lo cubren. Luego, la anticadena de mayor tamaño en P tiene tantos elementos como la partición de C's con la K.

Por último, si $x_i \not\leq a$ para toda i, entonces $A \cup \{a\}$ es una anticadena, pues, al ser maximal tampoco podría ser que $a \leq x_i$. Luego, la partición $\{a\}, C_1, \ldots, C_k$ consiste de $k+1$ cadenas, el tamaño de la anticadena más grande en P. □

De hecho, el teorema de Hall se puede deducir de éste:

Corolario (Teorema de Hall)**.** Si X es un conjunto finito y $A_1, \ldots, A_n$ son subconjuntos de X tales que $\left|\bigcup_{i\in J} A_i\right| \geq |J|$ para cualquier $J \subseteq [n]$, entonces existe un sistema de representantes distintos de los A_i.

Demostración. Consideremos el orden parcial en el conjunto de los elementos de X y los símbolos $y_1, \ldots, y_n$ con la relación $x \leq y_i$ si y sólo si $x \in A_i$. Tanto $Y = \{y_i\}$ como X son anticadenas. De hecho, la anticadena más grande es X. Para verlo, supongamos que S es otra anticadena y consideremos $J = \{i \in [n] : y_i \in S\}$. Entonces ningún elemento en los A_j para $j \in J$ puede estar en S. Luego,

$$|S| \leq |J| + |X| - \bigcup_{i\in J} A_i \leq |X|$$

por la condición de Hall.

Así que hay una descomposición del COPO en tantas cadenas como elementos en X. Entonces, para cada y_i hay al menos una cadena $x_i < y_i$ que lo contiene. Como hay tantas cadenas como elementos en X, no puede haber dos y_i que contengan al mismo elemento, ya que cada x debe estar en una única cadena. □

Y de hecho la otra implicación también es cierta: los dos teoremas son equivalentes. Aquí sólo probaremos este caso particular:

Ejercicio. Hall implica Dilworth para COPOS de dos niveles.

- Un COPO de dos niveles está formado por dos anticadenas U and L de forma que las únicas relaciones son de la forma $\ell \leq u$ para $u \in U$ y $\ell \in L$.
- Conviene usar esta variante de Hall: si $A_1, \ldots, A_n$ son subconjuntos de un conjunto finito X tales que $\left|\bigcup_{i \in J} A_i\right| \geq |J| - r$ para un número r y cualquier $J \subseteq [n]$, entonces hay una subfamilia de tamaño $n - r$ con un sistema de prepresentantes distintos.

Definición (Extensiones)**.**

- Una **extensión** de un COPO P es un orden parcial en los elementos de P que contiene todas las relaciones de P. Es decir, si $\leq$ y $\preccurlyeq$ son órdenes parciales en un conjunto P, $\preccurlyeq$ es una extensión de $\leq$ si $a \leq b \implies a \preccurlyeq b$.
- Una **extensión lineal** es una extensión que es una cadena.
- La **intersección** de dos órdenes parciales es la colección de relaciones que aparecen en ambos, es decir, la intersección de $(P, \leq)$ y $(P, \preccurlyeq)$ es el orden $(P, \leq^*)$ dado por $a \leq^* b$ si y sólo si $a \leq b$ y $a \preccurlyeq b$.

Teorema 17. Un COPO finito es la intersección de todas sus extensiones lineales.

Teorema 18. Todo COPO tiene una extensión lineal. Más aún, si a y b no son comparables, hay una extensión lineal $\preccurlyeq_1$ tal que $x \preccurlyeq_1 y$ y otra $\preccurlyeq_2$ tal que $y \preccurlyeq_2 x$.

Definición (Orden y dimensión)**.**

- Un **realizador** de un COPO P es un es una colección de órdenes lineales cuya intersección es P.
- La **dimensión** de un COPO P es el mínimo número de órdenes lineales cuya intersección es P.

Aprovechemos para citar algo de Matousek:

Definición. Un **encaje** de COPOS es una función inyectiva que preserva el orden.

Teorema 19. Cualquier COPO $(P, \leq)$ se puede encajar en $(2^X, \subseteq)$.

8. Teoría extremal de conjuntos

En este capítulo consideraremos familias de subconjuntos de algún conjunto con ciertas propiedades, y trataremos de acotar su tamaño.

8.1 Erdős-Ko-Radó

Un ejemplo de una familia de r-subconjuntos de un n-conjunto que se intersectan dos a dos se obtiene al tomar un punto del conjunto total y considerar todos los r-subconjuntos que lo contienen. Sólo cuando $n \geq 2r$ el problema es no trivial, y de hecho en este caso nuestro ejemplo es la cota mayor para el tamaño de una subfamilia intersectante. Si $n = 2r$ hay otros conjuntos que realizan esta cota, y si $n > 2r$, éste es el único.

Teorema 20 (Erdós-Ko-Rado)**.** Supongamos que $n \geq 2r$ y $\mathcal{A}$ es una familia de r-subconjuntos de un conjunto de n elementos tal que la intersección de cualesquiera dos de ellos es no vacía. Entonces

$$|\mathcal{A}| \leq \binom{n-1}{r-1}$$

Para ver que cuando $n < 2r$ el problema es trivial, simplemente notamos que cualesquiera dos elementos se deben intersectar. Luego, la cantidad de ellos es a lo más $\binom{n}{r} > \binom{n-1}{r-1}$.

Teorema 21 (Erdós-Ko-Rado Generalizado)**.** Si $n \geq (t+1)(r-t+1)$ para un número t tal que la intersección de cualesquiera dos elementos tiene al menos t elementos, entonces

$$|\mathcal{A}| \leq \binom{n-t}{r-t}$$

8.2 Teorema de Sperner

Definición. Una **familia de Sperner** es una familia de conjuntos tal que ninguno contiene propiamente a otro. Es justamente una anticadena.

Por ejemplo, la colección de todos los k-subconjuntos de $[n]$ es una familia de Sperner, porque ninguno puede estar propiamente contenido en el otro ya que esto implicaría que uno tiene más elementos que el otro. El valor de k con el que esta familia puede ser lo más grande posible es $n/2$ si n es par, y cualquiera de $\lfloor n/2 \rfloor$ o $\lceil n/2 \rceil$ si n es impar. El teorema de Sperner nos dice que éstos son los tamaños más grandes de las familias de Sperner en general.

Teorema 22 (de Sperner)**.** Si $\mathcal{F}$ es una familia de Sperner de subconjuntos de un conjunto con n elementos, entonces

$$\mathcal{F} \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$$

Y si la igualdad se cumple, entonces $\mathcal{F}$ consiste de todos los subconjuntos de tamaño $\lfloor \frac{n}{2} \rfloor$ o bien de todos los de tamaño $\lceil \frac{n}{2} \rceil$.

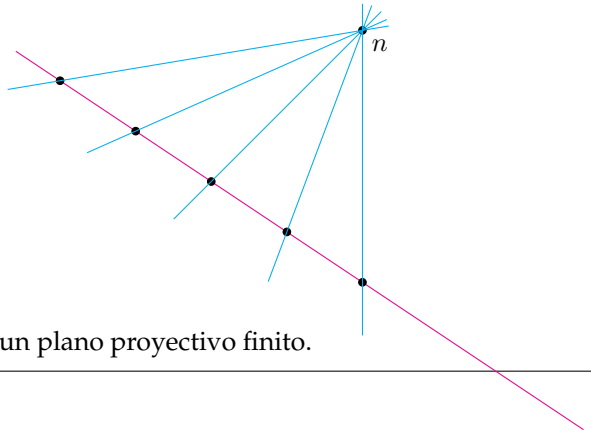
8.3 De Bruijn-Erdős

Teorema 23 (de Bruijn-Erdős)**.** Supongamos $\mathcal{F}$ es una familia de de subconjuntos de un conjunto de tamaño n tal que la intersección de cualesquiera dos contiene exactamente un elemento. Entonces

$$|\mathcal{F}| \geq n$$

y si $|\mathcal{F}| = n$, entonces se tiene alguno de los siguientes casos:

- Hay un punto distinguido, digamos n, tal que $A_i = \{i, n\}$ y A_n es o bien $\{n\}$ o bien $\{1, \ldots, n-1\}$. En este caso tenemos un "near pencil".



- $\mathcal{F}$ son las líneas de un plano proyectivo finito.

9. Cuadrados latinos

Definición. Un **cuadrado latino** de **orden** n es una matrix de $n \times n$ tal que cada entrada está en un único renglón y una única columna. Dos cuadrados latinos son **ortogonales** si al sobreponerlos, ninguna de las n^2 entradas es igual. Una **familia ortogonal** de cuadrados latinos es una colección de cuadrados latinos mutualmente ortogonales, y se denota $\mathrm{MOLS}(n, k)$ donde n es el orden k el tamaño de la familia.

Lema. Una familia ortogonal de cuadrados latinos de orden n tiene como máximo $n - 1$ elementos.

Demostración. Primero renombramos todos los cuadrados de la familia para que el primer renglón tenga los símbolos en orden ascendente. Esto hace que cualquier pareja de cuadrados sobrepuestos tenga las entradas $(1, 1), (2, 2), \ldots, (n, n)$ en el primer renglón.

Ahora tomemos un cuadradito abajo del primer renglón en cualquier cuadrado latino. Cuando le ponemos encima otro cuadrado de la familia, ese cuadradito debe tener una entrada de la forma (i, j) con $i \neq j$, porque todas las entradas iguales ya fueron consideradas en el primer renglón. Luego, hay uno tipo de entrada distinto para cada cuadrado en la familia, y hay $n - 1$ posibles entradas. □

Definición. Una familia de cuadrados latinos de orden n se llama **completa** si tiene $n-1$ elementos.

Teorema 24. Para cualquier n potencia de primo, hay una $\mathrm{MOLS}(n, n - 1)$.

10. Teorema de Hall

Definición. Sean $A_1, \ldots, A_n$ conjuntos. Un **sistema de representantes distintos (SDR)** es una n-tupla $(x_1, \ldots, A_n)$ tal que:

(a) $x_i \in A_i$ para toda i.

(b) $x_i \neq x_j$ para toda $i \neq j$.

Es claro que para cualquier subconjunto J de $\{1, \ldots, n\}$, $\left|\bigcup_{i \in J} A_i\right| \geq |J|$, pero el converso también es cierto:

Teorema 25 (de Hall)**.** Existe un SDR para los conjuntos finitos $A_1, \ldots, A_n$ si y sólo si

$$\left|\bigcup_{i \in J} A_i\right| \geq |J|$$

para cualquier $J \subseteq \{1, \ldots, n\}$.

Dados un conjunto de niñas y uno de niños, dado que cada niño conoce cierto subconjunto de niñas, es posible casar a cada niño con una niña que conoce si y sólo si cualquier k-subconjunto de niños corresponde hay al menos k niñas que todos ellos conocen. Es el teorema de matrimonio de Hall.

Teorema 26. Supongamos que los conjuntos $A_1, \ldots, A_n$ satisfacen la condición de Hall, y además $|A_i| \geq r$ para toda i y algún número r. Entonces, la cantidad de SDRs que hay es al menos:

$$\begin{cases} r! & \text{si } r \leq n \\ r(r-1)\ldots(r-n+1) = \frac{r!}{n!} & \text{si } r > n \end{cases}$$

Teorema 27. Supongamos que $A_1, \ldots, A_n$ son subconjuntos de $\{1, \ldots, n\}$ y r es un entero positivo tal que

(a) $|A_i| = r$ para toda i.

(b) Cualquier elemento de $\{1, \ldots, n\}$ está contenido en exactamente r de los subconjuntos.

Entonces, la familia satisface la condición de Hall, así que tiene un SDR.

Corolario. Esta familia tiene $r!$ SDRs.

Estos resultados se usan para completar cuadrados latinos. Ver Proofs from the Book.

11. Diseños de bloques

Definición. Un t-(v, k, λ)**-diseño de bloques** es una colección $\mathcal{B}$ de subconjuntos de algún conjunto V tales que:

- V tiene v elementos.
- Cada bloque en $\mathcal{B}$ tiene k elementos.
- Cualquier familia de t elementos en V está en exactamente λ bloques en común.

Definición. La **matriz de incidencia** de un diseño de bloques es una matriz de ceros y unos cuyos renglones son los elementos de V y las columnas son los bloques que indica si un elemento está en ese bloque.

Proposición. Un (v, k, λ)-diseño de bloques que tiene b bloques y cualquier elemento de V aparece en r bloques satisface que:

1. $vr = kb$
2. $\lambda(v - 1) = r(k - 1)$

Demostración.

1. Ambos lados de la igualdad son formas de contar la cantidad de 1's en la matriz de incidencia.
2. Dado $x \in V$, ambos lados de la igualdad son formas de contar la cantidad de elementos que hay en cada bloque sin contar a x.

□

Hay una generalización de la proposición anterior para diseños de bloques con $t \neq 2$:

Proposición. Si un t-(v, k, λ)-diseño de bloques existe, entonces el siguiente número es un entero para $0 \leq s \leq t$:

$$\lambda \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}} = \lambda \frac{(v-s)(v-s-1)\dots(v-t+1)}{(k-s)(k-s-1)\dots(k-t+1)}$$

Los casos $s = 0$ y $s = 1$ corresponden a los incisos 1 y 2 de la primera proposición.

Teorema 28 (Desigualdad de Fisher)**.** Si $k < v$, entonces $b \geq v$.

Demostración. Consideramos la matriz de incidencia A, cuya entrada i, j es

$$a_{ij} = \begin{cases} 1 & \text{si } x_i \in B_j \\ 0 & \text{si } x_i \notin B_j \end{cases}$$

Luego, la matriz AA^T tiene entrada i, j

$$m_{ij} = \sum_{k=1}^{b} a_{ik} a_{jk}$$

que representa la cantidad de bloques en donde están al mismo tiempo los elementos x_i y x_j. Por definición, esta cantidad es

$$m_{ij} = \begin{cases} \lambda & \text{si } i \neq j \\ r & \text{si } i = j \end{cases}$$

Esta matriz tiene determinante distinto de cero (usando la hipótesis $k < v$, haciendo cuentas), por lo que al ser una matriz de $v \times v$ tiene rango, es decir, la dimensión del espacio lineal generado por las columnas, igual a v.

Para concluir notemos que (why?) si $b < v$, entonces el rango de A y de A^T sería menor estricto que v. Como el rango del producto es menor o igual al mínimo de los rangos de los factores, $\operatorname{ran} M < v$, que no es posible. □

Este teorema sirve para descartar la existencia de ciertos diseños de bloques, como por ejemplo $2 - (16, 6, 1)$.

En fin,

Definición. Un diesño de bloques es **simétrico** si $v = b$, que implica que $r = k$.

Va a resultar que podremos voltear el diseño. Ahí va:

Proposición. En un diseño de bloques simétrico, no sólo cada pareja de elementos está en λ bloques, sino que cada pareja de bloques se intersecta en λ elementos.

Demostración. Tomemos un bloque arbitrario B y veamos que su intersección con todos los demás es de tamaño λ. Denotemos por $x_1, \ldots, x_{v-1}$ el tamaño de la intersección de B con el i-ésimo bloque. Mostraremos que $\sum (x_i - \lambda)^2 = 0$.

Cada elemento de B está en $k - 1$ bloques además de B. Así que hay $k(k-1)$ elementos en la intersección de B con algún otro bloque, es decir, $\sum x_i = k(k-1) = \lambda(v-1)$ aplicando nuestra proposición.

Análogamente, cada pareja en B está en $\lambda-1$ bloques además de B, así que hay $\binom{k}{2}(\lambda-1)$ parejas en la intersección de B con otro bloque, es decir, $\sum \binom{x_i}{2} = \binom{k}{2}(\lambda-1)$. Podemos reescribir esto como $\sum x_i(x_i-1) = k(k-1)(\lambda-1) = \sum x_i^2 - x_i = \lambda(v-1)(\lambda-1)$.

Sumando las dos igualdades obtenemos que $\sum x_i^2 = \lambda(v-1)+\lambda(v-1)(\lambda-1) = \lambda^2(v-1)$. Y luego:

$$\begin{aligned}\sum (x_i-\lambda)^2 &= \sum x_i^2 - 2\sum \lambda x_i + \sum \lambda^2 \\ &= \lambda^2(v-1) - 2\lambda(\lambda(v-1)) + (v-1)\lambda^2 = 0\end{aligned}$$

□

Proposición. En un diseño de bloques simétrico, si v es par, entonces $k-\lambda$ es un cuadrado.

Teorema 29 (Bruck-Ryser-Chowla)**.** Si existe un (v,k,λ)-diseño de bloques simétrico, entonces

(a) Si v es par, $k-\lambda$ es un cuadrado.

(b) Si v es impar, entonces

$$z^2 = (k-\lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2$$

tiene una solución entera no cero en x, y, z.

12. Matrices de Hadamard

¿Qué tan grande puede ser el determinante de una martiz cuyas entradas están acotdadas?

Teorema 30 (de Hadamard)**.** Sea A una matriz de $n \times n$ de números reales tal que $|a_{ij}| \leq 1$ para toda i, j. Entonces, $\det A \leq n^{n/2}$, y la igualdad se satisface si y sólo si $a_{ij} = \pm 1$ y $AA^T = nId$.

Demostración. El determinante es el volumen del paralelepípedo n-dimensional cuyos lados son los renglones de A. Este volumen es menor o igual al producto del tamaño de los lados, que es $\sqrt{\sum_{j=1}^{n} a_{ij}^2}$ para el i-ésimo renglón. Este número es menor o igual que $\sqrt{n}$, así que se sigue la desigualdad. La igualdad se tiene sólo cuando los lados son justo de ese tamaño, por lo que $|a_{ij}| = 1$, y además los lados del paralelepípedo son perpendiculares entre sí, de forma que $\sum_{k=1}^{n} a_{ik}a_{jk} = 0$. Esto es tanto como decir que $AA^T = nId$. □

Definición. Una matriz que satisface la igualdad en el teorema anterior es una **matriz de Hadamard**.

Proposición. Si existe una matriz de Hadamard de orden n, entonces $n = 1$ o 2, o bien $n \equiv 0 \mod 4$.

Teorema 31. Si $n > 4$, son equivalentes:

- Existe una matriz de Hadamard de orden n.
- Existe un 3-$(n, \frac{1}{2}n, \frac{1}{2}n - 1)$-diseño de bloques.
- Existe un 2-$(n - 1, \frac{1}{2}n - 1, \frac{1}{4}n - 1)$-diseño de bloques.

13. Planos proyectivos finitos

Definición. Un **plano proyectivo finito** es una pareja $(\mathcal{P}, \mathcal{L})$ donde $\mathcal{P}$ es un conjunto finito de *puntos* y $\mathcal{L}$ es una familia de *líneas*, subconjuntos de $\mathcal{P}$, tales que

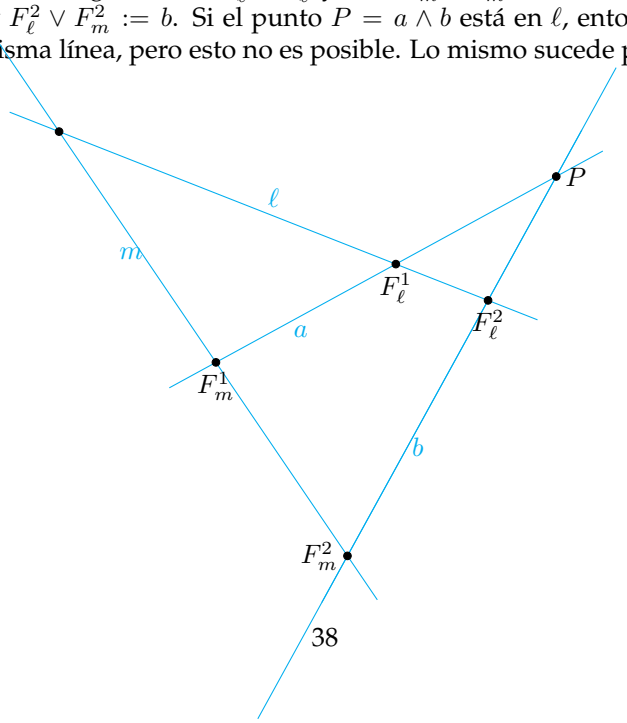
(P0) Hay cuatro puntos en posición general.

(P1) Cualesquiera dos líneas se intersectan en un único punto.

(P2) Por cualesquiera dos puntos pasa una única línea.

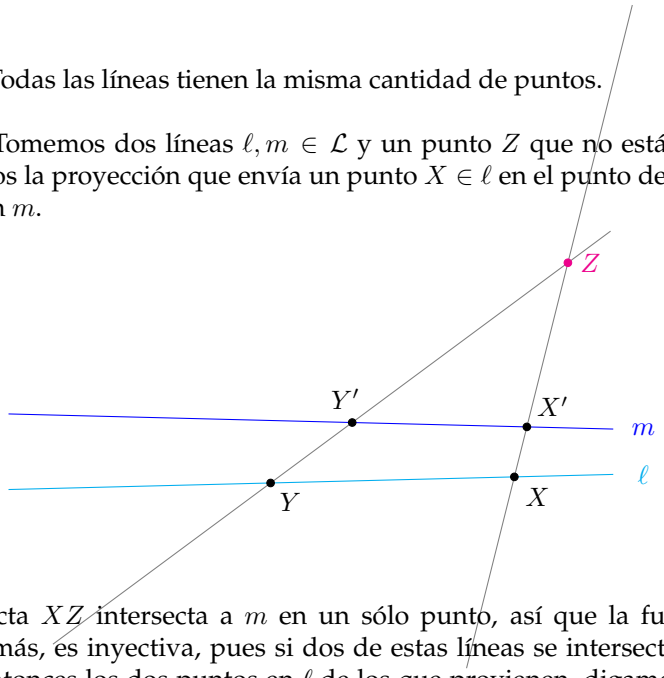
Lema. Dadas dos líneas, hay un punto que no está en ellas.

Demostración. Cada una de nuestras dos líneas puede intersectar al conjunto de cuatro puntos no colineales, llamémoslo F, en a lo más dos puntos. Si uno de estos cuatro puntos está fuera de las dos líneas, terminamos, y si no, nuestras dos líneas están generadas por dos parejas en F, digamos $\ell = F_\ell^1 \vee F_\ell^2$ y $m = F_m^1 \vee F_m^2$. Ahora tomemos las parejas $F_\ell^1 \vee F_m^1 := a$ y $F_\ell^2 \vee F_m^2 := b$. Si el punto $P = a \wedge b$ está en ℓ, entonces F_ℓ^1, F_ℓ^2 y F_m^1 estarían en la misma línea, pero esto no es posible. Lo mismo sucede para m. □



Proposición. Todas las líneas tienen la misma cantidad de puntos.

Demostración. Tomemos dos líneas $\ell, m \in \mathcal{L}$ y un punto Z que no está en ninguna de ellas. Definamos la proyección que envía un punto $X \in \ell$ en el punto de intersección de la recta XZ con m.



Por (P1), la recta XZ intersecta a m en un sólo punto, así que la función está bien definida. Además, es inyectiva, pues si dos de estas líneas se intersectan en el mismo punto de m, entonces los dos puntos en ℓ de los que provienen, digamos X y Y, de no ser iguales, obligarían a Z a estar en ℓ: sólo una línea pasa por ellos (P2). □

Proposición. La cantidad de puntos que hay en cada línea es igual para todos los puntos, y de hecho es igual a la cantidad de líneas que pasan por cada punto.

Demostración. Un momento por favor. □

Definición. El **orden** del plano proyectivo es el tamaño de las líneas menos 1.

Proposición. Una familia de conjuntos de tamaño $q+1$ es la colección de líneas de un plano proyectivo de orden q si y sólo si es un $(q^2+q+1, q+1, 1)$-diseño de bloques.

Demostración.

($\implies$) Las condiciones **2** y **3** de la definición se satisfacen trivialmente. Para ver la primera, tomemos una línea $\ell \in \mathcal{L}$. Para cada uno de los $q+1$ puntos en ella pasa una línea distinta de ℓ. Esto hace que haya exactamente $1+(q+1)q = q^2+q+1$ líneas.

($\impliedby$) La condición que cualesquiera dos elementos en V se intersecten en un sólo bloque nos da la propiedad **(P2)**. Usando las fórmulas $vr = kb$ y $\lambda(v-1)) = r(k-1)$, obtenemos que $v = b$ y $r = k$. Es decir, la cantidad de bloques es igual a la cantidad de puntos, y cada punto está en tantos bloques como puntos en cada bloque hay. Estas dos frases implican que el diseño de bloques es simétrico, luego, se sigue que cada pareja de bloques se intersecta en $\lambda = 1$ puntos. □

Proposición. El **dual** de un plano proyectivo, la esctructura que obtenemos al intercambiar los papeles de la líneas y los puntos preservando incidencia, también es un plano proyectivo.

Teorema 32. Para $q \geq 2$, existe un plano proyectivo de orden q si y sólo si existe una $\mathrm{MOLS}(q, q-1)$.

14. Ternas de Steiner

Los planos proyectivos son los diesños de bloques con k más grande. Las ternas de Steiner tienen el k más pequeño: tres.

Proposición (Cameron, 8.1.1)**.** Sea $\mathcal{B}$ una familia de m-subconjuntos de un n-conjunto tal que cualquier l-subconjunto está contenida en a lo más un elemento de $\mathcal{B}$. Entonces

$$|\mathcal{B}| \leq \binom{n}{l} \Big/ \binom{m}{l}$$

y la igualdad se da cuando cada l-subconjunto está contenido en exactamente un elemento de $\mathcal{B}$.

Demostración. Para la igualdad, se trata de un l-$(n, m, 1)$-diseño de bloques. Cualquier subconjunto de tamaño l está contenido en exactamente un m-bloque. En este caso, los l-subconjuntos del n-conjunto están en correspondencia con los l-subconjuntos de los bloques. Cada bloque tiene $\binom{m}{l}$ l-subconjuntos.

Si cada l subconjunto está en a lo más un elemento de $|B|$, puede haber más l-subconjuntos en total que los que les hacemos corresponder en los bloques. □

Definición. Una **terna de Steiner** es un $(v, 3, 1)$-diseño de bloques, denotado por $\mathrm{STS}(v)$.

Teorema 33. Si un $\mathrm{STS}(v)$ existe, entonces $v = 1, 3 \mod 6$

Demostración. Sustituyendo los valores conocidos en nuestras fórmulas, obtenemos que

$$\lambda(v-1) = r(k-1) \approx \frac{v-1}{2} = r \qquad \Longrightarrow \qquad vr = kb \approx \frac{v(v-1)}{6} = b$$

La primera igualdad quiere decir que v es impar, así que debe estar en alguna de las clases equivalencia $\bar{1}, \bar{3}$ o $\bar{5}$ en $\mathbb{Z}_6$. Para ver que no puede ser $\bar{5}$, supongamos que $v = 6m + 5$. Entonces tenemos:

$$\frac{(6m+5)(6m+4)}{6} = \frac{(6m+5)(3m+2)}{3}$$

pero ni $6m+5$ ni $3m+2$ son múltiplos de 3, así que esa fracción no podría ser un entero, que no es posible. $\square$

15. Ejercicios