Notas de Combinatoria

Dani
github.com/danimalabares/combi

July 17, 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 $\binom{k+n-1}{n-1} = \binom{k+n-1}{k}$.

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 $\phi(x) = x^k - c_1x^{k-1} - \ldots - c_kx^0$, y la **ecuación característica** como $\phi(x) = 0$, es decir

$$x^k = c_1x^{k-1} + \ldots + c_kx^0$$

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. Escribir la ecuación característica.
2. Encontrar las raíces características $\alpha_1, \ldots, \alpha_k$. Entonces las soluciones son de la forma
$$A_1\alpha_1^n + \ldots + A_k\alpha_k^n$$
3. Sustituir en las condiciones iniciales $a_0, a_1, \ldots, a_{k-1}$ (que nos fueron proporcionadas) para encontrar los valores de $A_1, ..., A_k$.

Y dejamos el teorema por si acaso:

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.

2.2.2 Déjà Vu de Ecuaciones diferenciales

Referencias: esto y esto.

Definición. Un sistema de ecuaciones diferenciales lineales

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{f} \tag{2.2}$$

se llama **homogéneo** si el vector $\mathbf{f} = 0$.

Definición. El **polinomio característico** de $\mathbf{A}$ es una función de λ dada por $\det(\lambda\mathbf{Id} - \mathbf{A})$. Las raíces de este polinomio son los **valores propios** de $\mathbf{A}$, y los **vectores propios** son las soluciones de $(\mathbf{A} - \lambda\mathbf{Id})\mathbf{v} = 0$.

Teorema 3. Si los valores propios de una matriz $\mathbf{A}$ de $n \times n$ son reales y diferentes, entonces la matriz formada por cualquier conjunto de vectores propios $\mathbf{v}_1, \ldots, \mathbf{v}_n$, digamos $\mathbf{P} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ es invertible y

$$\mathbf{P}\mathbf{A}\mathbf{P}^{-1} = \mathbf{\Lambda}$$

es diagonal.

Para el problema homogéneo

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} \tag{2.3}$$

consideremos el cambio de coordenadas

$$\mathbf{z} = \mathbf{P}^{-1}\mathbf{x}$$

que al derivar nos lleva a que

$$\dot{\mathbf{z}} = \mathbf{P}^{-1}\dot{\mathbf{x}} = \mathbf{P}^{-1}\mathbf{A}\mathbf{x} = \mathbf{P}\mathbf{A}\mathbf{P}^{-1}z = \mathbf{\Lambda}\mathbf{z}$$

Así que si $\lambda_1, \ldots, \lambda_n$ son los valores propios, el problema en las nuevas coordenadas se reduce a

$$z_i = \lambda_i z_i$$

que tiene solución

$$z_i = z_i(0)e^{\lambda_i t}$$

Proposición. Si $\mathbf{x}_1$ y $\mathbf{x}_2$ son soluciones de (2.3), entonces

$$c_1\mathbf{x}_1 + c_2\mathbf{x}_2$$

también lo es.

Proposición. Si $\mathbf{x}_1, \ldots, \mathbf{x}_n$ son soluciones de un sistema de ecuaciones diferenciales de $n \times n$ tales que

$$\det((\mathbf{x}_1, \ldots, \mathbf{x}_n)) \neq 0$$

entonces, se trata de un **conjunto fundamental de soluciones** y de hecho cualquier solución es de la forma

$$c_1\mathbf{x}_1 + \ldots + c_n\mathbf{x}_n$$

2.2.3 Déjà Vu de Ecuaciones diferenciales 2

Usando estas notas como guía, consideremos la siguiente ecuación diferencial no homogénea:

$$\ddot{y} + p(t)\dot{y} + q(t)y = f(t) \tag{2.4}$$

y la ecuación homogénea asociada:

$$\ddot{y} + p(t)\dot{y} + q(t)y = 0 \tag{2.5}$$

Resulta que:

Teorema 4. Si $Y_1(t), Y_2(t)$ son soluciones de (2.4) y $y_1(t), y_2(t)$ son un conjunto fundamental de soluciones de (2.5), entonces

$$Y_1(t) - Y_2(t)$$

también es solución de (2.5) así que se puede escribir como

$$Y_1(t) - Y_2(t) = c_1 y_1(t) + c_2 y_2(t)$$

Para aplicar este teorema, necesitamos una solución particular de (2.4), digamos $Y_P(t)$. Supongamos que $y(t)$ es la solución general que buscamos. Luego,

$$Y_P(t) - y(t)$$

es una solución del sistema homogéneo asociado, así que se puede escribir como

$$\begin{aligned} y(t) - Y_P(t) &= c_1 y_1(t) + c_2 y_2(t) \\ \iff y(t) &= c_1 y_1(t) + c_2 y_2(t) + Y_P(t) \end{aligned}$$

para algún conjunto fundamental de soluciones del homogéneo.

2.2.4 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 y h_n es una solución del sistema homogéneo asociado. Parece que en la práctica usaremos que:

Teorema 5. 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 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.

2.2.5 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 considerar el producto de n enumeradores que cuentan los k-multiconjuntos construidos a partir de cada uno de los n elementos.

Pero claro, sólo hay un k-multiconjunto que se puede formar a partir de un elemento: el que está formado por k copias del elemento. Así, el enumerador de los multiconjuntos formados a partir de un sólo elemento es $\sum_{k=0}^{\infty} x^k$.

Luego, el enumerador de los k-multiconjuntos es $\left(\sum_{k=0}^{\infty} x^k\right)^n$. 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:

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

Agregemos aquí:

Teorema 6 (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 7. 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 8. 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 9. 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 10.

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

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 $[k]$.

También podemos pensar que son palabras de tamaño n en el alfabeto $[k]$, con la restricción de que cada letra debe aparecer al menos una vez. Así, la función generatriz exponencial que cuenta la multiplicidad de cada bloque es $\frac{x^1}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots = e^x - 1$, y en total, $(e^x - 1)^k$ para los k bloques.

Entonces la función generatriz exponencial que cuenta las particiones ordenadas de n elementos en k bloques es $(e^x - 1)^k$. Hay $k!$ maneras de ordenar cada k particiones, así que tenemos la ecuación

$$\sum_{n=0}^{\infty} k! \left\{ n \atop k \right\} \frac{x^n}{n!} = (e^x - 1)^k$$

De donde

□

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

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

Diviendo entre $n!$ factorial, 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

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

Y para acordarse:

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

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 11. 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":

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

Que de hecho es exactamente lo que West denota por $f(\emptyset)$.

5. Enumeración bajo acciones de grupo

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 $g \in G$.

Teorema 12 (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. Po ahora no lo escribimos.

Definición. El índice de ciclos 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

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

□

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.

- 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.

Teorema 13 (Dilworth, 1950)**.** Sea P un orden parcial. El tamaño de la anticadena más grande es igual al mínimo número de cadenas que necesitamos para cubrir a todos los elementos de P.

En la demostración se usa Hall.

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 14 (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 15 (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.

Teorema 16 (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 $\lceil \frac{n}{2} \rceil$.

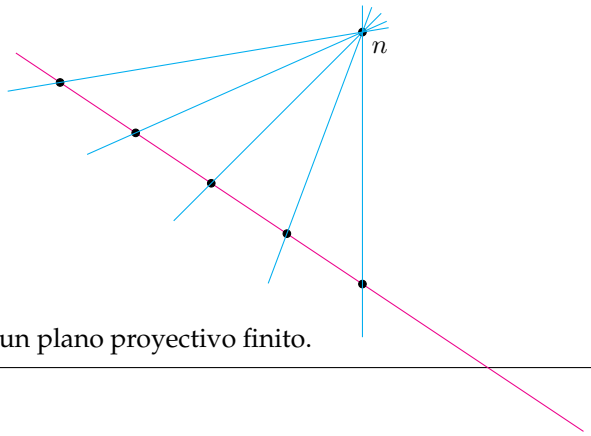
8.3 De Bruijn-Erdős

Teorema 17 (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 18. 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 19 (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 20. 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 21. 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 $t-(v,k,\lambda)$**-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. $bk = vr$
2. $r(k-1) = \lambda(v-1)$

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.

□

Teorema 22 (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.

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

Teorema 23 (Bruck-Ryser-Chowla)**.** Si existe un (v, k, λ)-diseño de bloques, 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 24 (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 25. 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

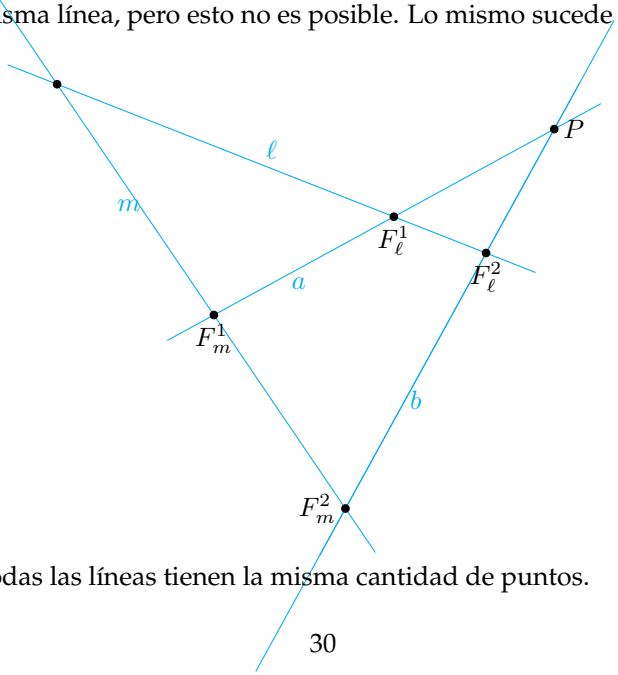
(P0) Hay cuatro puntos en posición general.

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

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

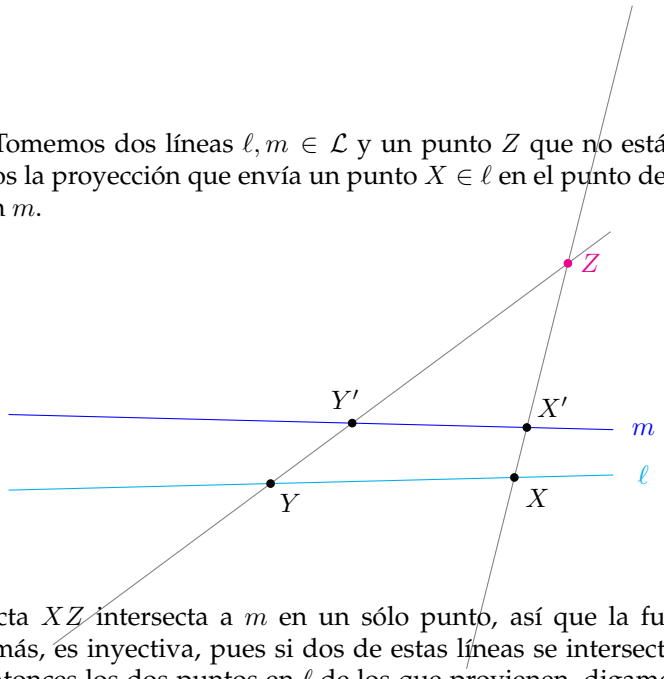
Lema. Dadas dos líneas, hay un punto que no está en ellas.

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.

($\Longrightarrow$) 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.

($\Longleftarrow$) 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.

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.

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

Teorema 26. Si un $\mathrm{STS}(v)$ eviste, entonces $v = 1, 3 \mod 6$