Índice general

Capítulo 0

Prefacio

Este texto surge como un borrador de las clases del curso de Combinatoria realizada los años 2014 y 2015 en la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile y puede ser usado como un apunte o guía de referencia para cursos futuros. El texto está en gran medida basado en la versión del curso realizada por Martín Matamala los dos años anteriores y complementado con material usado en cursos para profesores de educación media en combinatoria organizados en conjunto con el CMAT (campeonato nacional de matemática). También incluye bastante material no visto explícitamente en clase, sino que discutido con alumnos y auxiliares fuera de clase.

El material está pensado para ser usado por alumnos de pregrado que ya hayan alcanzado cierta madurez matemática. El ritmo del apunte es mucho más lento que el ritmo de un curso: en una clase es posible cubrir muchas páginas de material, esto es particularmente cierto para las secciones introductorias. No obstante lo anterior, gran parte del material puede ser adaptado a un nivel avanzado de enseñanza media preuniversitaria. Asímismo, este material puede ser usado para un curso inicial de combinatoria a nivel de postgrado.

De vez en cuando aparecerán comentarios que relacionan este texto con material más avanzado o con otras áreas de la Matemática. Estos comentarios aparecerán en texto azul y/o en secciones de discusión al final de cada capítulo. **Recomiendo *fuertemente* saltarse estas secciones en una primera lectura y solo volver a ellas en caso de interés ya que en la mayoría de los casos, éstos son absolutamente ortogonales al objetivo del curso.**

Ota advertencia: muchos de los ejemplos iniciales de cada sección son rudimentarios y simples. Estos no deben ser usado como una medida de la dificultad de los problemas que pretendemos atacar, sino más bien como una forma de *digerir* nociones nuevas.

Este borrador puede (con alta probabilidad) contener errores de tipeo y formato. Si usted encuentra alguno por favor infórmeme al correo electronico jsoto@dim.uchile.cl.

José A. Soto.
Junio 2015.

Capítulo 1

Principios Básicos.

La combinatoria es un área de la matemática muy amplia, por lo cual es difícil definirla con detalle. Habitualmente se le asocia el estudio de *estructuras finitas* o *discretas*. Aspectos de la combinatoria incluyen el *conteo* de estructuras de cierto tipo y tamaño, decidir la *existencia* de alguna estructura que satisfaga ciertas condiciones, encontrar estructuras *optimas* y el estudio de estructuras que aparecen en contextos *algebraícos*.

En estas notas nos enfocaremos, en un principio, en problemas de *combinatoria enumerativa*. Es decir, problemas relacionados con determinar la cardinalidad de ciertos conjuntos o secuencias de conjuntos.

1.1. Terminología

En este curso supondremos conocidas estructuras básicas en matemáticas, como el uso de conjuntos, funciones y relaciones. Asimismo, usaremos elementos básicos de álgebra, cálculo y probabilidades, sin llegar a ser estos requisitos fuertes. Cada vez que necesitemos notación especial la definiremos. Por ahora, damos la notación que usaremos con mayor frecuencia y aclarar ciertos vicios de notación

Definición 1.1 (Conjuntos típicos)**.** Usaremos los siguientes símbolos para denotar conjuntos.

$\mathbb{N}$: Conjunto de números naturales (usando la convención habitual que $0 \in \mathbb{N}$).
$\mathbb{Z}$: Conjunto de números enteros.
$\mathbb{Q}$: Conjunto de números racionales.
$\mathbb{R}$: Conjunto de números reales.
$\mathbb{C}$: Conjunto de números complejos.

Para un conjunto X cualquiera, usamos

$$\mathcal{P}(X) = \{A \colon A \subseteq X\}, \text{ para denotar su conjunto potencia.}$$

Además, para $n \in \mathbb{N}$, denotamos:

$$[n] = \{j \in \mathbb{N} \colon 1 \leq j \leq n\} = \{1, 2, \ldots, n\}.$$
$$\mathbb{Z}_n = \{j \in \mathbb{N} \colon j < n\} = \{0, 1, \ldots, n-1\}.$$

Notamos en particular que $\mathbb{Z}_0 = [0] = \emptyset$. Finalmente, si deseamos restringirnos a los números positivos de un conjunto usamos el super-índice $+$, así, $\mathbb{N}^+ = \mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$ denotan el conjunto de los enteros positivos, racionales positivos y reales positivos respectivamente.

Otra notación que aparece con tanta frecuencia que es mejor definirla de inmediato es el corchete de Iverson:

Definición 1.2 (Corchete de Iverson)**.** La expresión $[\![P]\!]$ vale 1 si P es una proposición verdadera, y vale 0 en cualquier otro caso.

Es increíble la versatilidad que provee esta notación. Por ejemplo, la función $f \colon \mathbb{N} \to \mathbb{N}$, dada por

$$f(x) = \begin{cases} (x+1) & \text{si } x \text{ es par,} \\ x & \text{si } x \text{ es impar,} \end{cases}$$

se puede escribir simplemente como $f(x) = x + [\![x \text{ es par}]\!]$. La primera forma de definir f es mejor en claridad, mientras que la segunda es más compacta

Otro ejemplo de su utilidad es que permite manipular sumas multiples con facilidad:

$$\sum_{i=0}^{N}\sum_{j=0}^{i} j = \sum_{i\in\mathbb{N}}\sum_{j\in\mathbb{N}} j[\![j \le i]\!][\![i \le N]\!] = \sum_{i\in\mathbb{N}}\sum_{j\in\mathbb{N}} j[\![j \le i \le N]\!] = \sum_{j\in\mathbb{N}}\sum_{i\in\mathbb{N}} j[\![j \le N]\!][\![j \le i \le N]\!] = \sum_{j=0}^{N} j\sum_{i=j}^{N} 1.$$

1.2. Cardinales finitos y principio biyectivo.

Cuando le pedimos a alguien que *cuente* los elementos de un conjunto probablemente esta persona comenzará a marcar cada elemento diciendo iterativamente por cada elemento marcado un número: *uno, dos, tres,...* hasta terminar con los elementos. De seguro responderá que la cantidad de elementos corresponde al último número, digamos n, dicho[1]. Ahora bien lo que en verdad está haciendo esta persona es encontrar una correspondencia entre los objetos a contar y un conjunto básico de referencia (el conjunto $[n]$). Este proceso se puede hacer ciertamente sin necesidad de usar este conjunto de referencia: Al contar un conjunto pequeño, un niño pequeño habitualmente no dirá su cantidad de elementos sino que, por ejemplo, levantará *tantos dedos* como elementos ha visto.

Asi, vemos que la definición más básica para contar no es la de "declarar una cardinalidad" sino más bien la de "poner en correspondencia dos conjuntos".

Definición 1.3. Equipotencia.

Dos conjuntos A y B se dicen *equipotentes* o *equinumerosos* si existe $f\colon A \to B$ función biyectiva. Anotamos en este caso $|A| = |B|$. También decimos (informalmente) que A y B tienen el mismo número de elementos.

Otra forma de interpretar la definición de equipotencia es la siguiente

Definición 1.4. Principio Biyectivo. Probar que dos conjuntos tienen el mismo número de elemento equivale a encontrar una biyección entre ambos.

Deseamos también poder declarar cuantos elementos tiene un conjunto. Para esto usamos la siguiente definición.

Definición 1.5. Cardinales finitos.

Sea A es un conjunto y $n \in \mathbb{N}$. Decimos que $|A| = n$ si $|A| = |\,[n]\,|$. En este caso decimos que *la cardinalidad de* A *es* n o que *el cardinal* de A es n.
Decimos que el conjunto A es *finito* si existe $n \in \mathbb{N}$ tal que $|A| = n$. De otro modo decimos que A es infinito.

Observación 1.6. Para que la expresión $|A| = n$ esté bien definida, se hace necesario probar que n es el único número natural para el cual $|A| = |\,[n]\,|$. De otra forma la notación deja de ser útil ya que podríamos tener que $|A| = n \neq m = |A|$. Dejamos esta demostración como ejercicio al final de la sección.

Informalmente, podemos pensar que $|\cdot|$ es una función "cardinalidad" cuyo valor, al menos para conjuntos finitos, está bien definido.

Comentario 1.7. La definición anterior es poco rigurosa y no es útil para cardinales infinitos. En este curso podemos suponer que existe un conjunto *universal* U cuyos elementos son todos los conjuntos *finitos* que se usarán en nuestro estudio (este no es un conjunto de "todos los conjuntos finitos posibles", ya que es *demasiado grande* para ser conjunto), y declarar que existe una función de cardinalidad $|\cdot|\colon U \to \mathbb{N}$ que satisface la definición dada más arriba. Esta solución es más que suficiente para la combinatoria que necesitamos pero es muy limitante para el estudio de cardinales generales. Otra solución, un poco mejor, es pensar que la equipotencia es una relación de equivalencia y que $|A|$ no es más que un representante de la clase de A. Esto funciona salvo por el hecho que la colección de conjuntos equipotentes con A no puede ser un conjunto. Hay maneras de corregir esto, pero hacerlo no es el objetivo de este curso. En la sección de discusión al final del capítulo damos una pincelada sobre la definición moderna de cardinales (no finitos), y algunas referencias para los interesados.

[1] Si no alcanza a decir nada, entonces responderá que hay cero elementos.

Observación 1.8. Cuando decimos que A tiene n elementos, lo que en verdad estamos haciendo es afirmar que existe una biyección entre A y $[n]$. En varias ocasiones es útil *numerar* los elementos de A, es decir escribir $A = \{a_1, a_2, \ldots, a_n\}$. Esto no es otra cosa que enunciar la existencia de una biyección $[n] \to A$ dada por $i \mapsto a_i$.

Veamos un par de ejemplos para ejercitar las nociones anteriores.

Ejemplo 1.9. Pruebe que $|\mathbb{Z}_n| = n$.

Solución. En efecto, la función $\mathbb{Z}_n \to [n]$ dada por $i \mapsto i + 1$ es biyectiva (su inversa es $j \mapsto j - 1$). □

Ejemplo 1.10. En un campeonato de fútbol juegan n equipos en una modalidad de eliminación: cada vez que un equipo pierde un partido, sale del campeonato. Además, cada partido debe tener un ganador y un perdedor (no hay empates). ¿Cuál el número mínimo y máximo de partidos que se deben jugar para que quede un solo equipo no eliminado?

Solución. La pregunta está formulada de manera que no entregue pistas hacia su solución. La verdad es que la respuesta es que se deben jugar exactamente $n - 1$ partidos. Para ver esto, basta notar que existe una biyección entre el conjunto de partidos jugados y el conjunto de equipos eliminados (hay un perdedor por cada partido que es eliminado, y estos no se pueden repetir). Por lo tanto si deseamos que hayan $n - 1$ eliminados, deberán jugarse $n - 1$ partidos. □

El ejemplo anterior muestra lo simple, pero poderoso, que es el principio biyectivo. Otro ejemplo similar se encuentra en el primer ejercicio de este capítulo.

1.3. Principios de la suma y el producto.

En esta sección enunciamos dos principios básicos para el conteo: el principio de la suma y el principio del producto.

Definición 1.11. Principio de la suma. Sean A y B conjuntos finitos *disjuntos* entonces

$$|A \cup B| = |A| + |B|.$$

Definición 1.12. Principio del producto. Sean A y B conjuntos finitos.

$$|A \times B| = |A| \cdot |B|.$$

Los principios de la suma y el producto tradicionalmente se enuncian de manera intuitiva de la siguiente manera.

Definición 1.13. Principio de la suma (informal) Si una actividad se puede realizar de a maneras y una segunda actividad se puede realizar de b maneras, y ambas actividades no se pueden hacer a la vez, entonces existe un total de $a + b$ maneras de realizar alguna de las dos actividades.

Definición 1.14. Principio del producto (informal) Si hay a formas de hacer una actividad y b maneras de hacer una segunda actividad entonces existen $a \cdot b$ formas de realizar ambas actividades.

A continuación damos una demostración simple de ambos principios.

Demostración del principio de la suma. Sean $A = \{a_1, \ldots, a_n\}$ y $B = \{b_1, \ldots, b_m\}$ conjuntos finitos disjuntos. La función $f\colon [n+m] \to A \cup B$ dada por $f(i) = \begin{cases} a_i & \text{si } i \in [n], \\ b_{i-n} & \text{si } n+1 \leq i \leq n+m \end{cases}$ es una biyección. □

Demostración del principio del producto. Sean $A = \{a_1, \ldots, a_n\}$ y $B = \{b_1, \ldots, b_m\}$ conjuntos finitos. La función $f\colon A \times B \to [n \cdot m]$ dada por $f(a_i, b_j) = (i-1)m + j$ es una biyección. □

Ejemplo 1.15.

1. Una alumna debe elegir un ramo electivo para llenar su curriculum. El departamento de matemáticas ofrece 12 ramos electivos que ella puede tomar y el departamento de física ofrece 9. Como los cursos son distintos, el principio de la suma nos dice que ella $12 + 9 = 21$ opciones.

2. Un menú simple en el casino consiste de un plato de entrada y un plato de fondo. El casino ofrece cada dia 3 opciones de platos de entrada y 2 de platos de fondo. Luego el número de menús simples distintos es $3 \cdot 2 = 6$.

Los principios de la suma y del producto se generalizan inmediatamente a múltiples conjuntos.

Proposición 1.16 (Principio de la Suma)**.** *Si* $\{A_1, \ldots, A_k\}$ *es una partición finita de un conjunto finito* A *entonces* $|A| = \sum_{i=1}^{k} |A_i|$.

Proposición 1.17 (Principio del Producto)**.** *Si* $(A_1, \ldots, A_k)$ *es una secuencia finita de conjuntos finitos y* $A = (\ldots((A_1 \times A_2) \times A_3) \times \ldots) \times A_k$ *entonces* $|A| = \prod_{i=1}^{k} |A_i|$.

Los principios anteriores se prueban por inducción.

Ejemplo 1.18.

1. ¿Cuántos números naturales entre 1 y 1000 comienzan por la cifra 6?
   Solución: Separemos estos números por cantidad de cifras. De una cifra, hay 1 número que comienza por 6 (el 6). De dos cifras, tenemos los 10 números entre 60 y 69. De tres cifras tenemos los 100 números entre 600 y 699. Luego en total hay $1 + 10 + 100 = 111$ números que satisfacen lo pedido.

2. ¿Cuántos números naturales de a lo más 5 cifras se escriben sin usar la cifra 5?
   Solución: Hay al menos dos formas de contar este conjunto. Una de ellas involucra contar mediante el principio de producto la cantidad de números de i cifras que se escriben sin el 5, y luego sumar las cardinalidades sobre todo i. Esta manera si bien es válida, es algo larga y merece cuidado: Se debe recordar que los números de i cifras (con $i \geq 2$) no pueden empezar con la cifra 0.

   Una solución alternativa es hacer una biyección entre el conjunto contado y las secuencias $(a_1, a_2, a_3, a_4, a_5)$ donde cada a_i puede ser uno de los 9 elementos de $\mathbb{Z}_{10} \setminus \{5\}$. La biyección consiste en completar cada número con 0's a la izquierda. El principio del producto nos garantiza entonces que hay 9^5 números.

La notación de producto cartesiano iterado usado en la Proposición 1.17 si bien es correcta, es algo tediosa de utilizar. En rigor, en el último ejemplo $(a_1, a_2, a_3, a_4, a_5)$ no es un elemento de un producto cartesiano iterado, sino que una *secuencia*. Formalizamos los conceptos de *secuencias* y *palabras sobre un alfabeto* en la siguiente sección.

1.4. Secuencias y palabras sobre un alfabeto

Definición 1.19. Sea A un conjunto finito o infinito. Una *secuencia* o *palabra* sobre A, de largo $k \in \mathbb{N}$, es una función $w\colon [k] \to A$. Usamos la notación w_i en vez de $w(i)$ para la evaluación de w en i, y decimos que w_i es el i-ésimo simbolo de w. Formalmente no hay diferencia entre secuencias y palabras, más allá de la notación: Para escribir w como secuencia se usa $w = (w_1, w_2, \ldots, w_k) = (w_i)_{i=1}^{k}$. Para escribir w como palabra, se escriben sus símbolos sin separadores entre ellos: $w = w_1 w_2 \ldots w_k$.

Denotamos $A^k = \{w = w_1 w_2 \ldots w_k\colon w_i \in A\}$ al conjunto de las palabras (secuencias) sobre A de largo k. En este curso denotaremos a la palabra vacía (el único elemento de A^0) por $\emptyset$ ó ε indistintamente.

Por ejemplo, si $A = \{a, b, c, d\}$, se tiene que $aba \in A^3$, $cada \in A^4$, etc. Además, es importante aclarar qué pasa para $A = \emptyset$. En dicho caso,

$$\emptyset^k = \begin{cases} \emptyset, & \text{si } k \geq 1. \\ \{\varepsilon\}, & \text{si } k = 0. \end{cases}$$

Definición 1.20. El conjunto de todas las palabras sobre un alfabeto A se denota por A^*. Es decir

$$A^* = \bigcup_{k \in \mathbb{N}} A^k.$$

Si $w \in A^*$, denotamos al largo de w como $|w|$.

Teniendo el concepto de palabra podemos ahora reemplazar el producto cartesiano iterado por el de *producto indexado* siguiente. Sean $A_1, \ldots, A_k$ una secuencia de conjuntos y $B = \bigcup_{i=1}^{k} A_i$ su unión, entonces se define el producto de la secuencia de conjuntos como todas las palabras sobre B, de largo k, tal que su i-ésimo símbolo está en A_i. Es decir,

$$\prod_{i=1}^{k} A_i = \{w \in B^k \colon w_i \in A_i, \forall i \in [k]\}.$$

Siempre será importante detenernos a entender *para que valores de* k tiene sentido la definición anterior. Ciertamente tiene sentido para $k \geq 1$. El caso $k = 0$ se ve un poco extraño pero también funciona:

$$\prod_{i=1}^{0} A_i = \{w \in B^0 \colon w_i \in A_i, \forall i \in [0]\} = \{\varepsilon\}.$$

En otras palabras el producto vacío de conjuntos resulta tener un elemento: la palabra vacía.

Observación 1.21. En particular, si todos los A_i son iguales a un conjunto dado, digamos A, entonces se obtiene la siguiente propiedad natural. Para todo $k \in \mathbb{N}$

$$\prod_{i=1}^{k} A = A^k.$$

Usando la biyección natural $f \colon (\ldots((A_1 \times A_2) \times A_3) \times \ldots) \times A_k \to \prod_{i=1}^{k} A_i$ dada por $f((((a_1, a_2), a_3), \ldots), a_k) = a_1 a_2 \ldots a_k$ y el principio del producto, se concluye la siguiente proposición.

Proposición 1.22. *Para toda secuencia de conjuntos finitos* $(A_1, \ldots, A_k)$,

$$\left|\prod_{i=1}^{k} A_i\right| = \prod_{i=1}^{k} |A_i|.$$

En particular, si A *es finito y* $k \in \mathbb{N}$*, entonces*

$$\left|A^k\right| = \prod_{i=1}^{k} |A| = |A|^k.$$

Ejemplo 1.23.

1. ¿Cuántas palabras de A^* tienen a lo más k símbolos?
   Solución: Estamos buscando $\left|\bigcup_{i\in 0}^{k} A^i\right| = \sum_{i=0}^{k} |A|^i$. La cantidad anterior depende del cardinal de A y se simplifica usando suma geométrica a ser:
   $$[\![|A| \neq 1]\!] \frac{|A|^{k+1} - 1}{|A| - 1} + [\![|A| = 1]\!](k+1).$$

2. ¿Cuántas números naturales de a lo más k cifras se escriben sin usar la cifra 0?
   Solución: El conjunto que deseamos contar está en biyección con las palabras en $[9]^*$ que tienen entre 1 y k símbolos. Usando el ejercicio anterior, éstas son exactamente
   $$\frac{9^{k+1} - 1}{9 - 1} - |[9]|^0 = \frac{9^{k+1} - 9}{8}.$$

3. Una palabra es palíndroma si al leerse de derecha a izquierda se obtiene la misma palabra. ¿Cuántas palabras palíndromas hay en A^k?
   Solución: La solución depende de si k es par o impar.
   Si k es par, entonces toda palabra palíndroma en A^k se escribe como ww^R, con $w \in A^{k/2}$, donde w^R es la palabra w escrita de derecha a izquierda.
   Si k es impar, entonces toda palabra palíndroma en A^k se escribe como wxw^R, con $w \in A^{(k-1)/2}$, $x \in A$.
   Luego la cantidad pedida es:
   $$[\![k \text{ par}]\!] \cdot |A^{k/2}| + [\![k \text{ impar}]\!] \cdot |A^{(k-1)/2}| \cdot |A| \;=\; A^{\lceil k/2 \rceil}.$$

1.5. Demostraciones Combinatoriales

Una aplicación importante de los principios anteriores es que nos permiten en varios casos demostrar identidades usando argumentos combinatoriales.

Para probar una identidad del tipo $r = s$, donde r y s son expresiones aritméticas que se evalúan a números naturales, podemos encontrar conjuntos R y S, con $|R| = r$ y $|S| = s$ y luego encontrar una biyección entre R y S. A este tipo de demostraciones se le conoce como **demostración combinatorial.**

En esta sección damos un par de ejemplos muy básicos. El poder de este tipo de demostraciones se verá más adelante.

Ejemplo 1.24. Probar combinatorialmente que para todo número $n \in \mathbb{N}^+$,

$$n^2 = (n+1)(n-1) + 1.$$

Solución: El lado derecho es la cardinalidad de $Y = [n]^2$, mientras que el lado izquierdo es la cardinalidad del conjunto $X = ([n+1] \times [n-1]) \cup \{(n+1, n)\}$ Se puede obtener una biyección de X en Y notando que

$$X = [n] \times [n-1] \cup \{n+1\} \times [n].$$
$$Y = [n] \times [n-1] \cup [n] \times \{n\}.$$

es fácil entonces escribir la biyección

$$(x, y) \mapsto \begin{cases} (x, y) & \text{si } (x, y) \in [n] \times [n-1], \\ (y, n) & \text{si } (x, y) = (n+1, y) \in \{n+1\} \times [n]. \end{cases}.$$

La demostración anterior es algo forzada, ya que realmente es muchísimo más simple probarla de manera algebraica. En un ejercicio anterior, usamos la suma geométrica para encontrar la cardinalidad de un conjunto. Veamos que, de hecho, la fórmula para la suma geométrica se puede probar combinatorialmente.

Ejemplo 1.25. Pruebe combinatorialmente que para todo n, m números naturales con $m \geq 2$, se tiene

$$\sum_{i=0}^{n} m^i = \frac{m^{n+1} - 1}{m - 1}.$$

Solución: Demostraremos la expresión equivalente $(m-1) \cdot \sum_{i=0}^{n} m^i = m^{i+1} - 1$.
El lado izquierdo cuenta el conjunto $X = \{w = w'a \colon w' \in [m]^*, 0 \leq |w'| \leq n, a \in [m-1], \}$. Mientras que el lado derecho cuenta el conjunto $Y = [m]^{n+1} \setminus \{(m, m, \ldots, m)\}$. Considere la función $\varphi \colon X \to Y$, que toma cada palabra de X y le agrega al final símbolos m hasta que la palabra tenga largo $n+1$, es decir:

$$\varphi(w) = wm^{n+1-|w|}.$$

Como la palabra w termina en un simbolo distinto de m, φ es biyectiva (su inversa consiste en eliminar letras m del final de la palabra hasta que ésta no termine en m).

Un ejemplo importante de demostración combinatorial consiste en probar que el conjunto potencia de $[n]$ tiene exactamente 2^n elementos.

Ejemplo 1.26. Probar que para todo $n \in \mathbb{N}$

$$|\mathcal{P}(n)| = 2^n.$$

Solución: Considere la biyección $\varphi \colon \mathcal{P}(n) \to \{0,1\}^n$ dada por

$$\varphi(X)_i = [\![i \in X]\!].$$

Con esto, $|\mathcal{P}(n)| = |\{0,1\}^n| = 2^n$. ■

Observamos que A^k no es más que una notación agradable para denotar al conjunto de funciones de $[k]$ en A. Esta notación es muy flexible y se puede extender un poco.

Definición 1.27. El conjunto de funciones de A en B se denota como B^A.

Proposición 1.28. *Para A y B finitos,*

$$|B^A| = |B|^{|A|}.$$

Demostración. Sea $A = \{a_1, \ldots, a_n\}$, con $n = |A|$. La función $\varphi\colon B^A \to B^n$ dada por $\varphi(f)_i = f(a_i)$ es una biyección. □

1.6. Ejercicios

Ejercicio 1.29. Felipe tiene una barra de chocolate pre-picada en nm cuadritos (n filas y m columnas). Esta barra es bastante dura por lo cual para comerla debe antes separar los cuadritos. Felipe puede en cada paso romper una de las piezas que tenga (él parte con una sola) y, mediante un fuerte golpe, dividirla a través de una de las filas horizontales o verticales. ¿Cuál es el número mínimo de pasos que Felipe debe realizar para separar la barra completamente en nm cuadritos?

Ejercicio 1.30. Sean $n, m \in \mathbb{N}$. Demuestre que $n = m$ si y solo si existe biyección entre $[n]$ y $[m]$. Concluya que si un conjunto A es finito entonces existe un solo valor n tal que $|A| = n$. **Indicación:** Suponga que $n \leq m$ y pruebe la afirmación por inducción en m.

Ejercicio 1.31. Sea A un conjunto. Demuestre que si A es finito entonces

$$(\forall B \subseteq A), \quad |A| = |B| \iff A = B.$$

Comentario 1.32. Este ejercicio da una manera alternativa de definir conjuntos finitos que no depende de la existencia del conjunto de los números naturales. Se dice que un conjunto es *Dedekind-finito* si no es equipotente con ninguno de sus subconjuntos propios. El ejercicio anterior dice que todo conjunto finito es Dedekind-finito. La recíproca también es cierta pero requiere asumir el axioma de elección.

Ejercicio 1.33. Demostrar combinatorialmente (no por inducción) que para todo $a, b, c \in \mathbb{N}$,

$$(a^b \cdot a^c) = a^{b+c}.$$
$$(a^b)^c = a^{b \cdot c}.$$

Discusiones

jsoto. Sección en construcción

Capítulo 2

Principios generales y selecciones de elementos.

jsoto. Hablar del principio general del producto

2.1. Principio general del producto

jsoto. Incluir ejemplo de Winkler de izquierda a derecha

2.2. Selecciones de objetos de un conjunto fijo

Hay dos parámetros importantes a considerar para clasificar selecciones de elementos de un conjunto dado A. (1) Si se permiten repetir elementos. (2) Si el orden importa. Cuando el orden importa, hablamos de **listas** o *secuencias* sobre A y usamos notación de palabras (ej: $abc \neq acb$). Cuando el orden no importa hablamos de **combinaciones** sobre A y usamos notación de conjuntos (si no se permite repetir) o de multiconjuntos. En particular, cuando deseemos considerar elementos repetidos, es útil poner los elementos en un paréntesis cuadrado (ej: $[a,a,b] = [a,b,a]$). La siguiente tabla nos ayudará a introducir notación.

Selecciones de k objetos.	Sin repetición	Con repetición
Importa el orden (Listas)	k-variaciones. $A^{\underline{k}}$.	k-secuencias. A^k.
No importa el orden (Combinaciones)	k-conjuntos. $\binom{A}{k}$.	k-multiconjuntos. $\left(\!\binom{A}{k}\!\right)$.

Nota: En varios textos, $A^{\underline{k}}$ se denota por $(A)_k$. Usamos la primera notación para evitar confusión con el uso de subindices.

Ejemplo 2.1. Para $A = \{a,b,c\}$, listamos a continuación las k-variaciones, k-conjuntos y k-multiconjuntos de A, para $k \in \{2,3,4\}$.

$$A^{\underline{2}} = \{ab, ac, ba, bc, ca, cb\}, \qquad A^{\underline{3}} = \{abc, acb, bac, bca, cab, cba\}, \qquad A^{\underline{4}} = \emptyset.$$

$$\binom{A}{2} = \{\{a,b\},\{a,c\},\{b,c\}\}, \qquad \binom{A}{3} = \{\{a,b,c\}\}, \qquad \binom{A}{4} = \emptyset.$$

$$\left(\!\binom{A}{2}\!\right) = \{[a,a],[a,b],[a,c],[b,a],[b,b],[b,c],[c,a],[c,b],[c,c]\}.$$

$$\left(\!\binom{A}{3}\!\right) = \{[a,a,a],[a,a,b],[a,a,c],[a,b,b],[a,b,c],[a,c,c],[b,b,b],[b,b,c],[b,c,c],[c,c,c]\}.$$

$$\left(\!\binom{A}{4}\!\right) = \{[a,a,a,a],[a,a,a,b],[a,a,a,c],\dots\}.$$

Observación 2.2. Caso especial: $k = 0$.
Para todo A, $A^0 = A^{\underline{0}} = \binom{A}{0} = \left(\!\binom{A}{0}\!\right) = \{\varepsilon\}$ donde ε representa la lista/combinación vacía.

Observación 2.3. Caso especial: $A = \emptyset$.
Para todo $k \geq 1$, $\emptyset^k = (\emptyset)_k = \binom{\emptyset}{k} = \left(\!\binom{\emptyset}{k}\!\right) = \emptyset$.

En lo que resta de la sección estudiaremos la cardinalidad de los conjuntos anteriormente definidos. Para ello, la siguiente notación es de utilidad.

Definición 2.4. Para todo $n, k \in \mathbb{N}$, definimos

$$n^k := \left| [n]^k \right| \qquad \text{(Potencias naturales)}$$

$$n^{\underline{k}} := \left| [n]^{\underline{k}} \right| \qquad \text{(Factorial decreciente)}$$

$$\binom{n}{k} := \left| \binom{[n]}{k} \right| \qquad \text{(Combinatorio de } n \text{ sobre } k\text{, o coeficiente binomial de } n \text{ sobre } k\text{)}$$

$$\left(\!\binom{n}{k}\!\right) := \left| \left(\!\binom{[n]}{k}\!\right) \right| \qquad \text{(Multicombinatorio de } n \text{ sobre } k\text{)}$$

$$n! := n^{\underline{n}} \qquad (n \text{ factorial})$$

Observación 2.5. Si $|A| = n$ entonces $|A^k| = n^k$, $|A^{\underline{k}}| = n^{\underline{k}}$, $\left|\binom{A}{k}\right| = \binom{n}{k}$ y $\left|\left(\!\binom{A}{k}\!\right)\right| = \left(\!\binom{n}{k}\!\right)$. Estas igualdades se prueban usando la biyección entre A y $[n]$.

Puede parecer extraño que hayamos *definido* las potencias naturales siendo una operación tan habitual (para algunos detalles ver la discusión al final de la sección anterior). Sin embargo al hacerlo de esta manera respondemos de inmediato la siguiente duda natural ¿Cómo definimos 0^0? En general, ¿como definimos los valores anteriores cuando $n = 0$?

Observación 2.6. Usando las definiciones y observaciones anteriores, se concluye que para todo $n \in \mathbb{N}$:

$$n^0 = n^{\underline{0}} = \binom{n}{0} = \left(\!\binom{n}{0}\!\right) = 1.$$

En particular,

$$0^0 = 0^{\underline{0}} = \binom{0}{0} = \left(\!\binom{0}{0}\!\right) = 1,$$

y

$$0! = 0^{\underline{0}} = 1.$$

Por otro lado, para todo $k \geq 1$

$$0^k = 0^{\underline{k}} = \binom{0}{k} = \left(\!\binom{0}{k}\!\right) = 0.$$

Como es de esperar, la definición de potencias naturales coincide con la definición habitual.

Proposición 2.7.

$$(\forall n, k \in \mathbb{N}) \quad n^k = \prod_{i=1}^{k} n.$$

Demostración. Aplicación directa de $n^k = |[n]^k|$, de la biyección natural entre $[n]^k$ y el producto cartesiano de $[n]$ consigo mismo k veces. □

2.3. Variaciones y permutaciones de un conjunto.

Prosigamos con las variaciones de un conjunto. Recordamos que si A es un conjunto con n elementos, entonces directamente $\left|A^{\underline{k}}\right| = n^{\underline{k}}$. La próxima proposición da una fórmula para esta cantidad.

Proposición 2.8.

$$\forall n, k \in \mathbb{N} : \ n^{\underline{k}} = n \cdot (n-1) \cdot \cdots \cdot (n-k+1) = \prod_{i=n-k+1}^{n} i.$$

En particular,

$$\forall n \in \mathbb{N} : \ n! = n^{\underline{n}} = n \cdot (n-1) \cdot \cdots \cdot 1 = \prod_{i=1}^{n} i.$$

y luego,

$$\forall n, k \in \mathbb{N} : \ n! = n^{\underline{k}} = [\![k \leq n]\!] \frac{n!}{(n-k)!}.$$

Demostración. Considere la biyección

$$[n] \times [n-1] \times \cdots \times [n-k+1] \to [n]^{\underline{k}},$$

donde la secuencia $c_1 c_2 c_3 \ldots c_{n-k+1}$ es llevada a la k-variación cuyo i-ésimo símbolo es el c_i-ésimo elemento de $[n]$ que no haya sido usado aún. La segunda parte es directa de la anterior. Y la tercera se obtiene pues $[n]^{\underline{k}} = \emptyset$ para $k \geq n+1$, y de combinar las dos expresiones anteriores para el caso $k \leq n$. □

Al igual que las secuencias están en biyección con cierto conjunto de funciones, las variaciones están en biyección con cierto conjunto de funciones inyectivas.

Definición 2.9. El conjunto de funciones inyectivas de A en B se denota como $\mathrm{Iny}(A, B) = \{f \in B^A \mid f \text{ inyectiva}\}$.

Proposición 2.10. *Para A y B finitos,*

$$|Iny(A, B)| = |B|^{\underline{|A|}}.$$

Demostración. Sea $A = \{a_1, \ldots, a_n\}$, con $n = |A|$. La función $\varphi \colon \mathrm{Iny}(A, B) \to B^{\underline{n}}$ dada por $\varphi(f)_i = f(a_i)$ es una biyección. □

Definición 2.11. Una permutación de A es una función biyectiva de A en si misma. Denotamos al conjunto de permutaciones de A como $\mathcal{S}_A = \{f \in A^A \mid f \text{ biyectiva}\}$. Además, denotamos $\mathcal{S}_n := \mathcal{S}_{[n]}$.

Proposición 2.12. *Para A finito,*

$$|\mathcal{S}_A| = |A|\,!$$

Demostración. Directo del hecho que $\mathcal{S}_A = \mathrm{Iny}(A, A)$, y de la definición de factorial. □

Observación 2.13. Como las permutaciones de un conjunto A de cardinal n están en biyección con las n-variaciones de A, es común llamar también permutación de A a las n-variaciones de A, es decir a las palabras que se pueden obtener ordenando los elementos de A.

Dadas las proposiciones anteriores, es tentador denotar $\mathrm{Iny}(A, B)$ como $B^{\underline{A}}$, y $\mathcal{S}_A$ como $A!$. Nos resistiremos a esa tentación pues la última notación no es estándar.

2.4. Combinaciones: subconjuntos y multiconjuntos

Prosigamos con las combinaciones de un conjunto. Al igual que antes notamos que si A tiene n elementos, entonces directamente $\left|\binom{A}{k}\right| = \binom{n}{k}$. La próxima proposición nos da una fórmula para esta cantidad.

Proposición 2.14.

$$\forall n, k \in \mathbb{N}: \ \binom{n}{k} = \frac{n^{\underline{k}}}{k!} = [\![k \leq n]\!] \frac{n!}{(n-k)!k!}.$$

Demostración. Considerar la biyección natural: $\binom{[n]}{k} \times \mathcal{S}_k \to [n]^{\underline{k}}$, donde cada k-variación en $[n]^{\underline{k}}$ se obtiene eligiendo primero un subconjunto de $[n]$ de tamaño k y luego eligiendo un orden de dicho subconjunto. □

Antes de proseguir con los multiconjuntos, detengámonos a resolver algunos problemas.

Ejercicios resueltos 2.15. De una demostración combinatorial de las siguientes identidades-

1. $\forall 0 \leq k \leq n: \ \binom{n}{k} = \binom{n}{n-k}$.
2. $\forall k, n \in \mathbb{N}: \ \binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}$.
3. $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Demostración.

1. Usar la biyección $\binom{[n]}{k} \to \binom{[n]}{n-k}$ dada por $X \mapsto [n] \setminus X$ (complemento).
2. Basta notar que $\binom{[n+1]}{k+1} = \underbrace{\binom{[n]}{k+1}}_{\text{Conjuntos sin } n+1} \cup \left\{\{n+1\} \cup Y : Y \in \binom{[n]}{k}\right\}$ y que la unión es disjunta.
3. Directo de $\mathcal{P}([n]) = \bigcup_{k=0}^{n} \binom{[n]}{k}$, y del hecho que $2^n = |\mathcal{P}([n])|$. □

Uno de los ejercicios anteriores nos permite dar una definición alternativa de los coeficientes binomiales en función de una recurrencia. Esto aparecerá con cierta frecuencia en el curso.

Proposición 2.16. *Los números* $\left(\binom{n}{k}\right)_{n,k\geq 0}$ *están definidos por la siguiente recurrencia:*

$$\forall k, n \geq 1: \ \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

con valores de borde, $\binom{n}{0} = 1$, *para* $n \geq 0$ *y* $\binom{0}{k} = 0$, *para* $k \geq 1$.

Tratemos ahora los multiconjuntos. Un multiconjunto de A es una selección de objetos de A donde cada elemento puede aparecer más de una vez y el orden no importa. Así $[a, b, a]$ es un multiconjunto donde a aparece 2 veces y b aparece 1 vez. Para poder tratar con ellos necesitamos una definición formal.

Definición 2.17. Un multiconjunto x de A es una función $x\colon A \to \mathbb{N}$, donde $x(a)$ representa el número de veces que se selecciona $a \in A$. La cantidad $\sum_{a \in Dom(x)} x(a)$ se denomina *tamaño* de x.

Recordemos que $\left(\!\binom{A}{k}\!\right)$ es la familia de multiconjuntos de A de tamaño k, y que si $A = [n]$, $\left(\!\binom{n}{k}\!\right)$ representa su cardinalidad. En particular, es directo notar que $\left(\!\binom{0}{0}\!\right) = 1$, $\left(\!\binom{n}{0}\!\right) = \left(\!\binom{0}{k}\!\right) = 0$ si $n, k > 0$. Ahora estamos listos para encontrar el valor de $\left(\!\binom{n}{k}\!\right)$.

Proposición 2.18.

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

Demostración. Considere la biyección que a un multiconjunto x de $[n]$ de tamaño k le asocia la palabra $x' \in \{\bullet, |\}^{n+k-1}$ dada por

$$x' = \underbrace{\bullet \dots \bullet}_{x(1)} | \underbrace{\bullet \dots \bullet}_{x(2)} | \cdots | \underbrace{\bullet \dots \bullet}_{x(n-1)} | \underbrace{\bullet \dots \bullet}_{x(n)}.$$

La asignación $x \mapsto x'$ es una biyección entre los multiconjuntos de $[n]$ de tamaño k, $\left(\!\binom{[n]}{k}\!\right)$ y las palabras en $\{\bullet, |\}^{n+k-1}$ con exactamente k símbolos $\bullet$ y $n-1$ separadores $|$. El último conjunto, a su vez, está en biyección con $\binom{[n+k-1]}{k}$, ya que cada palabra x' está definida exactamente por el conjunto de índices i en $[n+k-1]$ tales que $x'_i = \bullet$. □

Al igual que antes, podemos dar una definición alternativa de los números $\left(\!\binom{n}{k}\!\right)$ via una recurrencia.

Proposición 2.19. *Los números* $\left(\quad \left(\!\binom{n}{k}\!\right) \quad\right)_{n,k\geq 0}$ *están definidos por la siguiente recurrencia:*

$$\forall k, n \geq 1 : \ \left(\!\binom{n}{k}\!\right) = \left(\!\binom{n}{k-1}\!\right) + \left(\!\binom{n-1}{k}\!\right).$$

con valores de borde, $\left(\!\binom{n}{0}\!\right) = 1$*, para* $n \geq 0$ *y* $\left(\!\binom{0}{k}\!\right) = 0$*, para* $k \geq 1$*.*

Demostración. Propuesta. □

Gracias a las proposiciones anteriores podemos completar el siguiente cuadro con las cardinalidades de las selecciones de k objetos de un conjunto A de n elementos.

Selecciones de k objetos.	Sin repetición	Con repetición
Importa el orden (Listas)	k-variaciones. $\lvert A^{\underline{k}}\rvert = n^{\underline{k}} = \prod_{i=n-k+1}^{n} i.$	k-secuencias. $\lvert A^k\rvert = n^k.$
No importa el orden (Combinaciones)	k-conjuntos. $\left\lvert\binom{A}{k}\right\rvert = \binom{n}{k}.$	k-multiconjuntos. $\left\lvert\left(\!\binom{A}{k}\!\right)\right\rvert = \left(\!\binom{n}{k}\!\right) = \binom{n+k-1}{k}.$

2.5. Ejercicios

Ejercicio 2.20. Probar combinatorialmente. Es decir, encuentre biyecciones (explícitas o implícitas) entre 2 conjuntos con las cardinalidades requeridas. Para todo $n, m, k \in \mathbb{N}$:

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

$$\sum_{i=k}^{n} \binom{i}{k} = \binom{n+1}{k+1}.$$

$$\sum_{i\in\mathbb{N}} i\binom{n}{i} = n2^{n-1}.$$

$$\sum_{i\in\mathbb{N}} \binom{n}{2i} = \sum_{i\in\mathbb{N}} \binom{n}{2i+1}.$$

$$\sum_{i=0}^{m} \left(\!\binom{n}{i}\!\right) = \left(\!\binom{n+1}{m}\!\right).$$

Capítulo 3

Composiciones y Particiones de enteros

3.1. Composiciones de un entero.

Definición 3.1. Una **composición** de n en k partes es una solución a la ecuación $x_1 + x_2 + \cdots + x_k = n$ con $x_i \in \mathbb{N}^+$.
Una **composición débil** de n en k partes es una solución a la ecuación $x_1 + \cdots + x_k = n$ con $x_i \in \mathbb{N}$.
Al conjunto de los $x\colon [k] \to [n]$ composiciones de n en k partes lo denotamos por $\mathrm{COM}(n,k)$.
Al conjunto de los $x\colon [k] \to [n] \cup \{0\}$ composiciones débiles de n en k partes lo denotamos por $\mathrm{CD}(n,k)$.

Notemos que $\mathrm{CD}(n,k) = \left(\!\binom{[k]}{n}\!\right)$. Gracias a esto prodemos probar el siguiente resultado.

Proposición 3.2. *Para todo $n, k \in \mathbb{N}$,*

$$|\,\mathrm{CD}(n,k)| = \binom{n+k-1}{n}.$$

$$|\,\mathrm{COM}(n,k)| = |\,\mathrm{CD}(n-k,k)| = [\![k \leq n]\!]\binom{n-1}{n-k}.$$

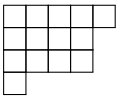
Demostración. La primera igualdad viene del hecho que cada multiconjunto de $[k]$ largo n se puede ver como una composición débil de n en k partes. La segunda igualdad sale de que al restar uno de cada parte de una composición de $n+k$ se obtiene una composición débil de n. □

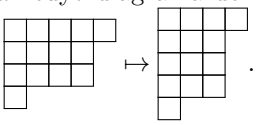
Observación 3.3. No es bueno tentarse a usar la identidad $\binom{n-1}{n-k} = \binom{n-1}{k-1}$ y escribir que $|\,\mathrm{COM}(n,k)| = \binom{n-1}{k-1}$ pues la expresión de la izquierda tiene sentido para todo $k \geq 0$ pero la expresión de la derecha no está definida cuando $k = 0$. Por otro lado la expresión $\binom{n-1}{n-k}$ tiene sentido incluso para $k = 0$ (más adelante le daremos un sentido al caso $n = k = 0$ donde tendremos $\binom{-1}{0} = 1$).

3.2. Particiones de un entero

Definición 3.4. Una **partición**[1] de $n \in \mathbb{N}$ es un vector $(a_1, \ldots, a_k)$ con $\sum_{i=1}^{k} a_i = n$, $a_1 \geq a_2 \geq \ldots a_k \geq 1$. Denotamos por $p_k(n)$ al número de particiones de n en **exactamente**[2], y al total lo denotamos $p(n)$.

Definición 3.5. El **Diagrama de Ferrers** (también conocido como **Diagrama de Young**) de una partición $a = (a_1, \ldots, a_k)$ de n es un arreglo de cajas cuadradas ordenadas en k filas horizontales (justificadas a la izquierda) de tamaños $a_1, \ldots, a_k$ respectivamente ordenadas verticalmente.

Por ejemplo, el diagrama de Ferrers de $(5,4,4,1)$ es  .

Definición 3.6. La partición **conjugada** de a es la partición a^* cuyo diagrama de Ferrers es el transpuesto del diagrama de a. Por ejemplo, $(5,4,4,1)^* = (4,3,3,3,1)$.  .

[1] ¡Cuidado! El nombre es similar a las particiones de un conjunto pero el sentido es distinto.
[2] Ojo, algunos autores llaman $p_k(n)$ a las particiones en a lo más k partes.

Notemos que $(\cdot)^*$ es una biyección (de hecho una involución) del conjunto de particiones de n.

Proposición 3.7. *El número de particiones de n en k partes es igual al número de particiones de n cuya parte más grande tiene largo k.*

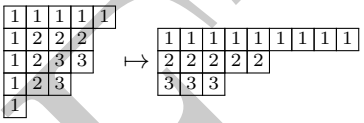
Demostración. Basta notar que $()^*$ es una biyección entre ambos conjuntos. □

Podemos usar Diagramas de Young para probar otras relaciones sorprendentes.

Lema 3.8. *El número de particiones de n autoconjugadas es igual al número de particiones de n con todas sus partes impares y distintas.*

Demostración. Sea π una partición autoconjugada. Crearemos una nueva partición $f(\pi)$ con todas sus partes impares. Borremos el primer gancho (primera fila y columna) y agreguemos los cuadrados borrados como primera fila de $f(\pi)$. Repitamos el proceso borrando (borrar ganchos y agregar filas). Con esto el objeto creado $f(\pi) = (2\pi_1 - 1, 2\pi_2 - 3, \dots)$ (donde el número de partes es tal que su última entrada no es 0), es una particion con todas sus partes impares y distintas. Claramente el proceso es reversible.

Ejemplo: $(5,4,4,3,1) \mapsto (9,5,3)$ y gráficamente



□

jsoto. Codificación de una partición a de n como un vector de multiplicidades: a'.

Proposición 3.9. *El número de soluciones enteras de $\sum_{k=1}^{n} kx_i = n$ es exactamente $p(n)$*

3.3. Ejercicios

Ejercicio 3.10. Muestre que la siguientes recurrencia definen a $\mathrm{CD}(n,k)_{n,k\geq 0}$

$$\forall n,k \geq 1 : \ \mathrm{CD}(n,k) = \mathrm{CD}(n,k-1) + \mathrm{CD}(n-1,k).$$

con valores de borde, $\mathrm{CD}(0,k) = 1$, para $k \geq 0$ y $\mathrm{CD}(n,0) = 0$, para $n \geq 1$.

Muestre además que la siguientes recurrencia definen a $\mathrm{COM}(n,k)_{n,k\geq 0}$

$$\forall n \geq k \geq 1 : \ \mathrm{COM}(n,k) = \mathrm{COM}(n-1,k-1) + \mathrm{COM}(n-1,k).$$

con valores de borde, $\mathrm{COM}(0,0) = 1$, y $\mathrm{COM}(n,0) = \mathrm{COM}(0,k) = 0$ para $n,k \geq 1$.

Ejercicio 3.11. Muestre que la siguiente recurrencia define a $(p_k(n))_{n,k\geq 0}$

$$\forall n \geq k \geq 1 : \ p_k(n) = p_k(n-k) + p_{k-1}(n-1).$$

con valores de borde, $p_0(0) = 1$, y $p_0(n) = 0$ para $n \geq 1$, y $p_k(n) = 0$ para $0 \leq n < k$.

Capítulo 4

Permutaciones de palabras. Particiones de conjuntos

4.1. Permutaciones de palabras

En esta sección nos interesa estudiar cuantas palabras se pueden obtener al permutar las letras de una palabra dada.

Definición 4.1. Sea $w \in A^*$ una palabra, y $a \in A$ un símbolo. Denotamos por $|w|$ al largo de w es decir, el único valor k tal que $w \in A^k$ y por $|w|_a$ al número de veces que a aparece en w, es decir $|w|_a = |\{i \in [|w|] : w_i = a\}|$.

Definición 4.2. Sea $w \in A^*$. Llamamos *permutación de* w a toda palabra w' que se puede obtener de w al permutar sus letras, y usamos $\text{Per}(w)$ para denotar al conjunto de todas las permutaciones de w. Es decir

$$\text{Per}(w) = \{w' \in A^* : |w'|_a = |w|_a \, \forall a \in A\}.$$

Proposición 4.3. *Para toda palabra $w \in A^*$,*

$$|Per(w)| = \frac{|w|!}{\prod_{a\in A} |w|_a!}.$$

Daremos dos demostraciones de esta propiedad. Una por inducción y una combinatorial

Demostración.
(Inducción en $|A|$)|1| Para $|A| \leq 1$, la demostración es directa, pues $\text{Per}(w) = \{w\}$ y $1 = \frac{1!}{1} = \frac{0!}{1}$, así que supongamos que $|A| \geq 2$. Sea a^* un símbolo cualquiera de A y sea $B = A \setminus \{a^*\}$. Para una palabra $v \in \text{Per}(w)$, llamemos $v' \in B^*$ a la subpalabra de v obtenida al borrar las apariciones de a^*, y $\sigma(v) \in \binom{[|w|]}{|w|_{a^*}}$ al conjunto de posiciones j tal que $v_j = a^*$. La asignación $v \mapsto (v', \sigma(v))$ es una biyección entre $\text{Per}(w)$ y $\text{Per}(w') \times \binom{[|w|]}{|w|_{a^*}}$. Usando principio del producto e inducción tenemos que

$$|\text{Per}(w)| = \frac{|w'|!}{\prod_{a\in B} |w'|_a!} \cdot \binom{|w|}{|w|_{a^*}} = \frac{|w'|!}{\prod_{a\in B} |w'|_a} \cdot \frac{|w|!}{|w'|!|w|_{a^*}!} = \frac{|w|!}{\prod_{a\in A} |w|_a!}.$$

(Demostración combinatorial),
Colguemos a cada letra a de w un índice i que representando el número de aparición de la letra a en w. Más formalmente, para todo $k \in [|w|]$ sea $\varphi(k) = (a, j)$ donde la j-ésima aparición de a en la palabra w se encuentra en la k-ésima posición de w. Con esto, $P := \varphi([|w|])$ es un conjunto de $|w|$ pares ordenados distintos.

Considere la función

$$\varphi : P^{\underline{|w|}} \to \text{Per}(w) \times \prod_{a\in A} [|w|_a]^{\underline{|w|_a}}$$

dada por

$$\varphi((v_1, i_1)(v_2, i_2) \cdots (v_{|w|}, i_{|w|})) = (v, (s_a)_{a\in A})$$

donde $v = v_1 v_2 \dots v_{|w|}$, y para cada $a \in A$, s_a es la subpalabra de $i_1 i_2 \dots i_{|w|}$ obtenida al quedarse solo con los i_j tales que $v_j = a$. Esta función es biyectiva y prueba que

$$|w|! = |\varphi : P^{\underline{|w|}}| = |\text{Per}(w)| \prod_{a\in A} |[|w|_a]^{\underline{|w|_a}}| = |\text{Per}(w)| \prod_{a\in A} |w|_a!$$

□

La expresión calculada en la proposición anterior aparece con relativa frecuencia, por lo cual recibe una notación especial.

Definición 4.4. Si $(n_1, n_2, \ldots, n_k)$ es una composición débil de $n \in \mathbb{N}$, definimos

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{\prod_{i=1}^{k} n_i!}.$$

La proposición anterior indica que $\binom{n}{n_1,n_2,\ldots,n_k}$ es exactamente el número de permutaciones de una palabra con n_i símbolos de un tipo i.

4.2. Particiones de un conjunto

Definición 4.5. Una secuencia $(A_1, \ldots, A_k)$ de conjuntos **no vacíos** y disjuntos par a par tal que $\bigcup_{i=1}^{k} A_i = A$ se conoce como *partición ordenada* de A.

Las partes de una partición se conocen como bloques.

Definición 4.6. A cada partición ordenada $\Pi = (A_1, \ldots, A_k)$ de A en k bloques le asociamos la composición x de $|A|$ en k partes que satisface $x_i = |A_i|$, para $i \in [k]$.

Proposición 4.7. *Sea $c = (c_1, \ldots, c_k)$ una composición de $[n]$. El número de particiones ordenadas $(A_1, \ldots, A_k)$ de $[n]$ asociadas a la composición c es igual a*

$$\binom{n}{c_1, \ldots, c_k}.$$

Demostración. Basta notar que cada partición ordenada descrita se puede codificar de manera única como una permutación w de la palabra $1^{c_1} 2^{c_2} \cdots k^{c_k}$, donde $w_j \in [k]$ representa el único índice tal que $j \in A_{w_j}$. □

Definición 4.8. Un conjunto $\{A_1, \ldots, A_k\}$ formado por conjuntos **no vacíos** y disjuntos par a par tal que $\bigcup_{i=1}^{k} A_i = A$ se conoce como *partición* (no ordenada) de A.

Definición 4.9. A cada partición no ordenada $P = \{A_1, \ldots, A_k\}$ de A en k bloques le asociamos la partición (entera) x de $|A|$ que codifica los tamaños (ordenados de mayor a menor) de los bloques de P. Además, si m_i denota el número de bloques de tamaño i en P (es decir, $(m_i)_{i\in\mathbb{N}}$ es el vector de multiplicidades de x), diremos que P tiene *tipo* $m = (m_i)_{i\in\mathbb{N}}$.

Proposición 4.10. *Sea $a = (a_1, \ldots, a_k)$ una partición de n y sea $m = (m_i)_{i\in\mathbb{N}}$ su vector de multiplicidades (es decir, número de veces que aparece i en a). El número de particiones de $[n]$ de tipo m (o equivalentemente, el número de particiones de $[n]$ asociadas a la partición a) es*

$$\binom{n}{a_1, \ldots, a_k} \frac{1}{m_1! \cdots m_n!}.$$

Demostración. Hay $\binom{n}{a_1,\ldots,a_k}$ formas de elegir una partición ordenada de $[n]$, (es decir, la parte i tiene a_i elementos). Sin embargo si reordenamos las partes que tienen el mismo tamaño obtenemos la misma partición de $[n]$. □

Estudiemos un poco más las particiones.

Definición 4.11. Denotemos por $\mathcal{P}(n, k)$ al conjunto de todas las particiones no ordenadas de $[n]$ en k bloques no vacíos.

Definición 4.12. Números de Stirling del segundo tipo. Los valores $S(n, k) = |\mathcal{P}(n, k)|$ se conocen como números de Stirling del segundo tipo[1].

Calcular estos números no es una tarea directa. Algunos casos son simples:

[1] Esta cantidad también se denota en algunos libros como $\left\{ {n \atop k} \right\}$.

Observación 4.13. Se cumple que:

1. Para todo $n \in \mathbb{N}$, $S(n,n) = 1$.
2. Para $n, k > 0$, $S(n,0) = S(0,k) = 0$.
3. Para todo $k > n$, $S(n,k) = 0$.
4. Para todo $n > 1$, $S(n, n-1) = n$.

Proposición 4.14. *Los números* $\left(\quad S(n,k) \quad \right)_{n,k\geq 0}$ *están definidos por la siguiente recurrencia:*

$$\forall k, n \geq 1 : \ S(n,k) = kS(n-1,k) + S(n-1,k-1).$$

con valores de borde, $S(0,0) = 1$, $S(n,0) = S(0,k) = 0$ *para* $n, k \geq 1$.

Demostración. Sea A el conjunto de las particiones de $\mathcal{P}(n,k)$ donde $\{n\}$ es un bloque en sí mismo y $B = \mathcal{P}(n,k) \setminus A$. Claramente A está en biyección con $\mathcal{P}(n-1,k-1)$ (borrando el bloque $\{n\}$). Además, hay una función k a 1 desde B hasta $\mathcal{P}(n,k+1)$ (dada por la operación "borrar n de su bloque"). □

La siguiente propiedad relaciona las particiones no ordenadas con las particiones ordenadas

Proposición 4.15. *El número de particiones ordenadas de* n *en* k *bloques es* $k!S(n,k)$.

Demostración. Cada partición ordenada de $[n]$ en k bloques se obtiene tomando una partición (normal) en $\mathcal{P}(n,k)$ y luego ordenando las k partes. □

En particular, concluimos la siguiente importante propiedad:

Proposición 4.16. *El número de funciones sobreyectivas de* $[n] \to [k]$ *es* $k!S(n,k)$.

Demostración. Cada función f sobreyectiva se puede ver como $(f^{-1}(1), \ldots, f^{-1}(k))$ que es una partición ordenada de $[n]$ en k bloques. □

Discutamos un poco más las particiones de $[n]$.

Definición 4.17. Llamamos $B(n)$ al número total de particiones de $[n]$. Los números $(B(n))_{n\in\mathbb{N}}$ se conocen como números de Bell

Tenemos $B(0) = 1$ y $B(n) = \sum_{k=0}^{n} S(n,k)$. La siguiente proposición nos da otra recurrencia para calcular $B(n)$.

Proposición 4.18. *Los números* $B(n)_{n\geq 0}$ *estan definidos por la siguiente recurrencia:*

$$\forall n \geq 1 : \ B(n) = \sum_{k=0}^{n-1} \binom{n-1}{k} B(k).$$

con valor de borde $B(0) = 1$.

Demostración. Para Π partición de $[n]$ llamemos $\varphi(\Pi)$ al bloque que contiene a n.

$$\begin{aligned} B(n) &= |\{\Pi\text{: partición de } [n]\} \\ &= \sum_{k=0}^{n-1} \sum_{A\subseteq\binom{[n-1]}{k}} |\{\Pi\text{: partición de } [n], \varphi(\Pi) = A \cup \{n\}\}| \\ &= \sum_{k=0}^{n-1} \sum_{A\subseteq\binom{[n-1]}{k}} B(|[n-1] \setminus A|) = \sum_{k=0}^{n-1} \binom{n-1}{k} B(n-1-k) = \sum_{k=0}^{n-1} \binom{n-1}{k} B(k). \end{aligned}$$

□

Definición 4.19. Llamamos $T(n)$ al número total de particiones ordenadas de $[n]$. Los números $(T(n))_{n\in\mathbb{N}}$ se conocen como números ordenados de Bell o números de Fubini.

4.3. Ejercicios

Ejercicio 4.20. Sea $(n_1, \ldots, n_k) \in \mathrm{CD}(n)$. Demuestre que:

$$\binom{n}{n_1, \ldots, n_k} = \binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n_k}{n_k}.$$

Ejercicio 4.21. Pruebe que los números de Fubini $T(n)_{n\geq 0}$ están definidos por la siguiente recurrencia:

$$\forall n \geq 1 : \; T(n) = \sum_{k=1}^{n}\binom{n}{k}T(n-k) = \sum_{k=0}^{n-1}\binom{n}{k}T(k).$$

con valor de borde $T(0) = 1$

Capítulo 5

Las doce formas de repartir n pelotas en k cajas.

Queremos estudiar las maneras de repartir n pelotas en k cajas. Lo que hace el problema interesante es si las pelotas son todas iguales o no (distinguibles o indistinguibles), si las cajas son distinguibles o indistinguibles, y si imponemos alguna condición sobre la asignación. Las tres condiciones más interesantes son si la asignación es libre (irrestricta), sobreyectiva (en cada caja hay al menos una pelota) o inyectiva (en cada caja hay a lo más una pelota).

Con lo que llevamos estudiado en el curso podemos llenar la siguiente tabla.

Libre	Pelotas distintas	Pelotas iguales
Cajas distintas	k^n (k-variaciones de $[n]$)	$\lvert \mathrm{CD}(n,k)\rvert = \binom{\binom{k}{n}}{} = \binom{n+k-1}{n}$ (composiciones débiles de n en k partes)
Cajas iguales	$\sum_{i=0}^{k} S(n,i)$ (particiones de $[n]$ en a lo más k bloques)	$\sum_{i=0}^{k} p_i(n)$ (particiones de n en a lo más k partes)

Sobreyectiva	Pelotas distintas	Pelotas iguales
Cajas distintas	$S(n,k)k!$ (funciones sobreyectivas)	$\lvert \mathrm{COM}(n,k)\rvert = \binom{n-1}{n-k}$ (composiciones de n en k partes)
Cajas iguales	$S(n,k)$ (particiones de $[n]$ en k bloques)	$p_k(n)$ (particiones de n en k partes)

Inyectiva	Pelotas distintas	Pelotas iguales
Cajas distintas	$(k)_n$ (funciones inyectivas)	$\binom{k}{n}$ (elegir las n cajas con 1 pelota)
Cajas iguales	$[\![n \leq k]\!]$ (todas son iguales)	$[\![n \leq k]\!]$ (todas son iguales)

Observación 5.1. Muchas de las expresiones anteriores se simplifican cuando $n = k$.

Libre	Pelotas distintas	Pelotas iguales
Cajas distintas	n^n	$\binom{2n-1}{n}$
Cajas iguales	$B(n)$	$p(n)$

Inyectiva=Sobreyectiva	Pelotas distintas	Pelotas iguales
Cajas distintas	$n!$	1
Cajas iguales	1	1

jsoto. También tiene sentido hacerse la pregunta, si debo repartir n pelotas en un número arbitrario de cajas, de manera sobreyectiva

jsoto. Ejercicio sobre multiasignaciones

Capítulo 6

Permutaciones y ciclos

En esta sección estudiaremos un poco más las permutaciones de $[n]$.

Definición 6.1. Decimos que $(a_1, a_2, \ldots, a_k)$ es un **ciclo** de $\pi \in \mathcal{S}_n$ si $\pi(a_1) = a_2$, $\pi(a_2) = a_3, \ldots$, $\pi(a_k) = a_1$.

Sea $\pi \in \mathcal{S}_n$. Es fácil ver que cada elemento $i \in [n]$ pertenece a exactamente un ciclo de π. Esta observación nos dice que cada permutación está definida por sus ciclos.

Definición 6.2. Las permutaciones de $\mathcal{S}_n$ que contienen un solo ciclo se conocen como *permutaciones circulares*

Proposición 6.3. *Sea $n \geq 1$. El número de permutaciones circulares de $\mathcal{S}_n$ es $(n-1)!$.*

Demostración. Sea $\mathcal{C}(n,1)$ el conjunto de todas las permutaciones circulares de $\mathcal{S}_n$. Consideremos la función

$$\begin{aligned} \varphi &: \mathcal{S}_n \to \mathcal{C}(n,1) \\ \varphi(\pi) &= (\pi_1, \ldots, \pi_n) \end{aligned}$$

La función φ no es inyectiva. Notamos que para cada $(\tau) := (\tau_1, \ldots, \tau_n) \in \mathcal{C}(n,1)$, las únicas palabras π tal que $\varphi(\pi)$ es igual a τ son *rotaciones* de la palabra $\tau_1 \ldots \tau_n$. De aquí se concluye que $|\varphi^{-1}((\tau))| = n$, y usando que $\mathcal{S}_n = \bigcup_{(\tau) \in C(n,1)} \varphi^{-1}((\tau))$ se deduce que $n! = |\mathcal{C}(n,1)|n$, es decir, $|\mathcal{C}(n,1)| = (n-1)!$. □

Consideremos ahora el siguiente problema: Sean $c_1, c_2, \ldots, c_n$ números naturales. ¿De cuántas formas podemos ubicar $n = \sum_{i=1}^{k} ic_i$ personas en c_1 mesas redondas para 1 persona, c_2 mesas redondas para dos personas, etc.; donde dos configuraciones se consideran iguales si en ambas configuraciones cada persona tiene el mismo vecino a su derecha y el mismo vecino a la izquierda? En el lenguaje de permutaciones, lo que estamos preguntando es cuantas permutaciones tienen exactamente c_i ciclos de tamaño i para cada $i \in [n]$.

Definición 6.4. El **tipo** de una permutación $\pi \in \mathcal{S}_n$ es el vector $(m_1, \ldots, m_n)$ donde m_i es la cantidad de ciclos de tamaño i en π.

Notar que directamente se tiene que

$$\sum_{i=1}^{n} ic_i = n.$$

Proposición 6.5. *El número de permutaciones de tipo $m = (m_1, \ldots, m_n)$ es*

$$\frac{n!}{m_1! \cdots m_n!} \frac{1}{1^{m_1} 2^{m_2} \cdots n^{m_n}}.$$

Demostración. Daremos dos demostraciones de este hecho. Sea $\mathcal{S}(m)$ el conjunto de permutaciones de tipo m. En la primera demostración codificamos cada permutación π como

$$\pi = \underbrace{(*)\cdots(*)}_{m_1}\underbrace{(*,*)\cdots(*,*)}_{m_2}\cdots\underbrace{(*,\ldots,*)\cdots(*,\ldots,*)}_{m_n}, \tag{6.1}$$

donde los paréntesis codifican los ciclos de π. Si reemplazamos los asteriscos por una palabra $w \in \mathcal{S}_n = ([n])_n$ obtenemos una permutación $\varphi(w)$ con el tipo deseado. Sin embargo cada permutación puede provenir de varias palabras. De esta forma

$$\mathcal{S}_n = \bigcup_{\pi \in \mathcal{S}(m)} \varphi^{-1}(\pi).$$

Calculemos $|\varphi^{-1}(\pi)|$. Notemos que si permutamos los ciclos de largo i de w entre si obtenemos la misma permutación. Esta operación se puede hacer de $m_1!m_2!\dots m_n!$ maneras. Finalmente, podemos *rotar* cada ciclo individual decidiendo quien es su primer elemento $(1325) = (3251) = (2513) = (5132)$. Esto se puede hacer para cada ciclo de largo i de i maneras. Esto muestra que $|\varphi^{-1}(\pi)| = (m_1!m_2!\cdots m_n!)\cdot 1^{m_1}2^{m_2}\cdots n^{m_n}$.

De la fórmula arriba se obtiene que $n! = (m_1!m_2!\cdots m_n!)\cdot 1^{m_1}2^{m_2}\cdots n^{m_n}\cdot|\mathcal{S}(m)|$, lo que prueba lo pedido.

En la segunda demostración notamos que cada permutación de tipo m se puede obtener seleccionando primero una partición de tipo m y luego eligiendo una permutación circular de cada uno de sus bloques. Sea $a = (a_1,\dots,a_k)$ la partición de n asociada al vector de multiplicidades m, es decir a_1 es el tamaño del bloque más grande, a_2 es el siguiente y así sucesivamente. Lo anterior nos dice que

$$\begin{aligned}|\mathcal{S}(m)| &= \binom{n}{a_1,\dots,a_k}\frac{1}{m_1!\cdots m_n!}\cdot(a_1-1)!\cdots(a_k-1)!\\ &= \frac{n!}{m_1!\cdots m_n!}\frac{1}{a_1\cdots a_k} = \frac{n!}{m_1!\cdots m_n!}\frac{1}{1^{m_1}2^{m_2}\cdots n^{m_n}}.\end{aligned}$$

□

Estudiemos un poco más las permutaciones con un número fijo de ciclos.

Definición 6.6. Sea $\mathcal{C}(n,k)$ el conjunto de permutaciones de $[n]$ con k ciclos.

Definición 6.7. Números de Stirling sin signo.
Llamamos $\left[{n \atop k}\right]$ (algunos autores usan $c(n,k)$) al conjunto de permutaciones en $\mathcal{S}_n$ con exactamente k ciclos. La familia $\left(\left[{n \atop k}\right]\right)_{n,k\in\mathbb{N}}$ se conoce como números de Stirling sin signo.

Definición 6.8. Números de Stirling del primer tipo. Los valores $s(n,k) = (-1)^{n-k}\left[{n \atop k}\right]$ se conocen como números de Stirling del primer tipo.

Al igual que con los números de Stirling del segundo tipo, estos números no son necesariamente simples de calcular.

Observación 6.9. Se cumple que:

1. Para todo $n\in\mathbb{N}$, $\left[{n \atop n}\right] = 1$.
2. Para $n,k>0$, $\left[{n \atop 0}\right] = \left[{0 \atop k}\right] = 0$.
3. Para todo $k>n$, $\left[{n \atop k}\right] = 0$.
4. Para todo $n>1$, $\left[{n \atop n-1}\right] = \binom{n}{2}$.

La siguiente recurrencia define los números de Stirling sin signo.

Proposición 6.10. *Los números* $\left({n \atop k}\right)_{n,k\geq 0}$ *están definidos por la siguiente recurrencia:*

$$\forall n,k\geq 1:\ \begin{bmatrix}n\\k\end{bmatrix} = (n-1)\begin{bmatrix}n-1\\k\end{bmatrix} + \begin{bmatrix}n-1\\k-1\end{bmatrix}$$

con valores de borde, $\left[{0 \atop 0}\right] = 1$, $\left[{n \atop 0}\right] = \left[{0 \atop k}\right] = 0$ *para* $n,k\geq 1$.

Demostración. Sea A el conjunto de de permutaciones en $C(n+1,k+1)$ donde $n+1$ es un ciclo en si mismo y $B = C(n+1,k+1)\setminus A$.

Para cada permutación $\pi\in\mathcal{C}(n+1,k+1)$, definamos $\varphi(\pi)$ como la permutación obtenida de eliminar el símbolo $n+1$ del ciclo en el que está. Notemos que $\varphi(\pi)$ tiene k ciclos (si $\pi\in A$) o $k+1$ ciclos (si $\pi\in B$). Es fácil ver que $\varphi\colon A\to\mathcal{C}(n,k)$ es biyectiva. Por otro lado, cada $\tau\in\mathcal{C}(n,k+1)$ puede provenir de varias permutaciones en $\mathcal{C}(n+1,k+1)$. ¿De cuántas? Si τ está escrita como una lista de ciclos en orden entonces podemos insertar $n+1$ en n lugares: justo antes de cada símbolo. De aquí se tiene que $\varphi\colon B\to\mathcal{C}(n,k+1)$ es una función n a 1 (i.e. $|\varphi^{-1}(\tau)| = n$). Con esto $|\mathcal{C}(n+1,k+1)| = |A|+|B| = |\mathcal{C}(n,k)| + n|\mathcal{C}(n,k+1)|$. □

Ejercicio 6.11. Pruebe que la siguiente recurrencia define los números de Stirling del primer tipo.

$$\forall n,k\geq 1:\ s(n,k) = (1-n)s(n-1,k) + s(n-1,k-1).$$

con valores de borde, $s(0,0) = 1$, $s(n,0) = s(0,k) = 0$ para $n,k\geq 1$.

Capítulo 7

Polinomios

7.1. Polinomios formales.

Hemos definidos varios objetos de manera combinatorial: $((n)_k, \binom{n}{k}, \left(\binom{n}{k}\right), \dots)$. Estas definiciones tienen sentido para todo n y k natural. Hay formas naturales de extender estas nociones a otros dominios. La más natural es usar polinomios. Supondremos cierta familiaridad con polinomios a coeficientes reales o complejos. Si necesitamos algún resultado específico de álgebra abstracta, lo enunciaremos.

Recordemos que $\mathbb{C}[x]$ denota el anillo de los polinomios en la variable x a coeficientes en $\mathbb{C}$. Más precisamente suponemos que existe una variable indeterminada x, y su conjunto infinito de *potencias naturales* $\{1, x, x^2, \dots\}$ llamados *monomios*. Los elementos de $\mathbb{C}[x]$ se llaman *polinomios*. Cada polinomio $p(x)$ se obtiene como una combinación lineal con coeficientes en $\mathbb{C}$ de un subconjunto *finito* de monomios. Es decir, para cada polinomio $p(x)$, existe un entero $k \in \mathbb{N}$ tal que

$$p(x) = \sum_{n=0}^{k} a_n x^n,$$

donde $a_i \in \mathbb{C}$ es el coeficiente i-ésimo de p. En otras palabras, cada polinomio esta definido por una secuencia infinita $(a_0, a_1, \dots)$ de coeficientes donde solo una cantidad finita de ellos son distintos de 0, y sin pérdida de generalidad escribimos $p(x) = \sum_{n\geq 0} a_n x^n$. Decimos que dos polinomios $p(x)$ y $q(x)$ en $\mathbb{C}[x]$ se dicen **iguales como polinomios** si todos sus coeficientes son iguales. La suma y producto de dos polinomios se define de la manera natural

$$\sum_{n\geq 0} a_n x^n + \sum_{n\geq 0} b_n x^n = \sum_{n\geq 0} (a_n + b_n) x^n$$

$$\sum_{n\geq 0} a_n x^n \cdot \sum_{n\geq 0} b_n x^n = \sum_{n\geq 0} x^n \sum_{i=0}^{n} (a_n b_{n-i})$$

Las operaciones anteriores convierten a $\mathbb{C}[x]$ en un anillo conmutativo con unidad (el neutro del producto es el polinomio 1), donde los únicos elementos invertibles son las constantes distintas de 0. $\mathbb{C}[x]$ también es un espacio vectorial sobre $\mathbb{C}$, cuya base canónica es, precisamente, la base de monomios.

Observamos que si $p(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{C}[x]$, entonces podemos definir para todo $\lambda \in \mathbb{C}$, la evaluación de $p(x)$ en λ, como $p(\lambda) = \sum_{i=0}^{k} a_i \lambda^i$. En otras palabras podemos interpretar p como una función de $\mathbb{C}$ en $\mathbb{C}$. De hecho, el siguiente resultado de álgebra abstracta es muy útil:

Proposición 7.1. *Sean $p(x), q(x) \in \mathbb{C}[x]$. Se tiene que $p(x) = q(x)$ **como polinomios** si y solo si $p = q$ **como funciones**.*

Comentario 7.2. Es posible definir polinomios sobre cualquier anillo conmutativo con unidad R. El conjunto resultante no es un espacio vectorial necesariamente (para esto necesitamos que R sea un cuerpo), sino que solo un anillo, llamado $R[x]$. Sus elementos son de la forma $p(x) = \sum_{i=0}^{n} a_n x^n$ con $a_n \in R$. Al igual que antes, dos polinomios son iguales si y solo si todos sus coeficientes son iguales. También podemos evaluar polinomios en elementos de R pero no es necesario que la proposición 7.1 se tenga. Por ejemplo, si $R = \mathbb{Z}_2$, los polinomios $p(x) = x + x^2$ y $q(x) = 0$ son distintos, pero sus evaluaciones son iguales en $\mathbb{Z}_2$: $p(0) = 0 + 0 = 0 = q(0), p(1) = 1 + 1 = 0 = q(1)$.

Es importante notar que si R es un anillo conmutativo **infinito** y **sin divisores de 0**, por ejemplo, $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, entonces dos polinomios son iguales si y solo si sus funciones de evaluación son iguales.

7.2. Teoremas del binomio y multinomio

Para los siguientes teoremas, será también útil el uso de polinomios a varias variables, es decir elementos del anillo $\mathbb{C}[x,y] := \mathbb{C}[x][y]$, o en general $\mathbb{C}[x_1,\dots,x_k]$. En estos anillos las operaciones de suma y producto son análogas al caso univariado y similarmente, dos polinomios son iguales si y solo si el coeficiente que acompaña a cada posible monomio $x_1^{\alpha_1}\cdots x_k^{\alpha_k}$ son iguales.

Proposición 7.3. *Teorema del binomio y del multinomio. Para todo $n \in \mathbb{N}$, se tienen las siguientes igualdades de polinomios.*

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}.$$

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{a \in \mathrm{CD}(n,k)} \binom{n}{a_1, a_2, \dots, a_k} x_1^{a_1} x_2^{a_2} \cdots x_k^{a_k}.$$

Demostración. Notemos que

$$\sum_{a \in \mathrm{CD}(n,2)} \binom{n}{a_1, a_2} x^{a_1} y^{a_2} = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i},$$

por lo que nos basta probar la segunda identidad. En efecto, sea el alfabeto $X = \{x_1,\dots,x_k\}$. Luego:

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{y \in X^k} y_1 y_2 \dots y_n = \sum_{(a_1,\dots,a_k)\in\mathbb{N}^k} \sum_{\substack{y \in X^k: \\ y_1 y_2 \cdots y_n = x_1^{a_1}\cdots x_k^{a_k}}} x_1^{a_1}\cdots x_k^{a_k},$$

En la segunda suma interpretamos la igualdad $y_1 y_2 \cdots y_n = x_1^{a_1}\cdots x_k^{a_k}$ no como igualdad de palabras, sino como igualdad de producto de variables asociativas y conmutativas (por ejemplo, si los y_i y los x_j son números naturales entonces la igualdad es simplemente verificar que los productos en $\mathbb{N}$ son iguales).

Ahora bien, notemos que si $y \in X^k$, e $y_1 \cdots y_n = x_1^{a_1}\cdots x_k^{a_k}$, debemos tener que $a_1 + a_2 + \cdots + a_k = n$, i.e. $a \in \mathrm{CD}(n,k)$. Con esto tenemos que:

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{a \in \mathrm{CD}(n,k)} x_1^{a_1}\cdots x_k^{a_k} \cdot \left|\{y \in X^n : \ y_1 y_2 \cdots y_n = x_1^{a_1}\cdots x_k^{a_k}\}\right|.$$

Para concluir, notemos que $\{y \in X^k : \ y_1 y_2 \cdots y_n = x_1^{a_1}\cdots x_k^{a_k}\} = \mathrm{Per}(x_1^{a_1}\cdots x_k^{a_k}) = \binom{n}{a_1,\dots,a_k}$. □

Ejercicio 7.4. jsoto. Agregar ejercicios sobre el teo del binomio y multinomio

7.3. Bases factoriales y números de Stirling

Recordamos que el *grado* de un polinomio $p(x) \in \mathbb{C}[x] \setminus \{0\}$ es el mayor entero i tal que el coeficiente que acompaña a x^i es distinto de 0. El grado del polinomio 0 es $-\infty$.

Definición 7.5. Definimos los siguientes polinomios de grado k:

$$x^{\underline{k}} := (x)_k := x(x-1)(x-2)\cdots(x-k+1). \qquad \binom{x}{k} := \frac{x^{\underline{k}}}{k!}.$$

$$x^{\overline{k}} := (x)^k := x(x+1)(x+2)\cdots(x+k-1). \qquad \left(\!\binom{x}{k}\!\right) := \frac{x^{\overline{k}}}{k!}.$$

Donde naturalmente definimos $x^{\underline{0}} = x^{\overline{0}}$ como el polinomio $x^0 = 1$.

Comentario 7.6. Las definiciones anteriores también tienen sentido en un anillo conmutativo abstracto R. Pero para ello, necesitamos definir objetos como 1, 2, etc. Aquí $1 := 1_R$ es el neutro multiplicativo de R, $2 = 1_R + 1_R$, y en general para $k \in \mathbb{N}$ es la suma de 1_R consigo mismo k veces. De este modo, $x^{\underline{k}}$ y $x^{\underline{k}}$ están bien definidos en la medida que R tenga unidad. Por otro lado, para que $\binom{x}{k}$ y $\left(\!\binom{x}{k}\!\right)$ tengan sentido, necesitamos que $k!$ sea invertible. Esto ocurre por ejemplo, si R es un cuerpo infinito.

Al evaluar los polinomios recién definidos en números naturales recuperamos los objetos que teníamos antes. Pero ahora se permite escribir cosas como

$$(-10)^{\overline{3}} = (-10)(-9)(-8) = -720.$$
$$(1+i)^{\underline{3}} = (1+i)i(i-1) = i(i^2-1) = 0.$$
$$\binom{-5}{2} = \frac{(-5)(-6)}{2} = 15.$$
$$\left(\!\binom{-5}{2}\!\right) = \frac{(-5)(-4)}{2} = 20.$$
$$\binom{-1/2}{k} = \frac{(-1/2)(-3/2)(-5/2)\dots(-1/2-(k-1))}{k!} = \frac{(-1)\cdot(-3)\cdots(1-2k)}{2^k k!} = \frac{(-1)^k 1\cdot 3\cdots(2k-1)}{2^k k!}.$$
$$= \frac{(-1)^k}{2^k k!}\frac{(2k-1)!}{2\cdot 4\cdots(2k-2)} = \frac{(-1)^k}{2^k k!}\frac{(2k-1)!}{2^{k-1}(k-1)!} = 2\binom{-1}{4}^k\binom{2k-1}{k}.$$

Ejercicio 7.7. Encuentre fórmulas cerrada para

$$\binom{m+1/2}{k}$$

para todo $m, k \in \mathbb{N}$ en función de coeficientes binomiales con parámetros naturales.

Proposición 7.8. *Una propiedad interesante que será usada con cierta frecuencia es la siguiente. Para todo $k \in \mathbb{N}$, se tiene las siguientes igualdades de polinomios en $\mathbb{C}[x]$,*

$$(-1)^k(-x)^{\underline{k}} = x^{\overline{k}} = (x+k-1)^{\underline{k}}.$$
$$(-1)^k\binom{-x}{k} = \left(\!\binom{x}{k}\!\right) = \binom{x+k-1}{k}.$$

Demostración. Notamos que la segunda serie de igualdades se deduce de la primera dividiendo por $k!$. Para ver la primera basta notar que

$$(-1)^k(-x)^{\underline{k}} = (-1)^k(-x)(-x-1)\dots(-x-(k-1)) = x(x+1)\dots(x+k-1).$$

y que el lado derecho es, por definición igual a $x^{\overline{k}}$ y a $(x+k-1)^{\underline{k}}$. □

Ejercicio 7.9.

1. Dos puntos x e y en $\mathbb{Z}^k$ se dicen *adyacentes* si $\|x-y\|_1 := \sum_{i=1}^k |x_i - y_i| = 1$. Un paseo de largo ℓ en $\mathbb{Z}^k$ es una secuencia $x^0, x^1, \dots, x^\ell$ donde cada punto es adyacente al anterior. Si el paseo no repite vértices, decimos que es un camino. Si además tenemos que para cada $i \geq 1$, $x^{i-1} \leq x^i$ coordenada a coordenada, decimos que el paseo es un camino creciente. Encuentre:
   a) El número de paseos de largo ℓ en $\mathbb{Z}^k$ que parten en el origen.
   b) El número de caminos crecientes de largo ℓ en $\mathbb{Z}^k$ que parten en el origen.
   c) El número de caminos crecientes en $\mathbb{Z}^k$ de $(0,0)$ a $x = (x_1, \dots, x_k)$, donde $x_i \geq 0$ para todo i.
2. Encuentre el número de soluciones de la ecuación $x_1 + x_2 + \cdots + x_k = n$ con: *a*) $x_i \geq 2$. *b*) $x_i \geq i$.

Recordemos que $\mathbb{C}[x]$ es un espacio vectorial sobre $\mathbb{C}$ con base canónica $\{1, x, x^2, \dots\}$. Observamos además que $\{1, x^{\underline{1}}, x^{\underline{2}}, \dots, x^{\underline{n}}\}$ y $\{1, x^{\overline{1}}, x^{\overline{2}}, \dots, x^{\overline{n}}\}$ son dos bases del espacio generado por $\{1, x, x^2, \dots, x^n\}$. Una pregunta interesante resulta ser como expresar los polinomios anteriores en la base canónica de $\mathbb{C}[x]$, es decir como hacer un cambio de base.

Sorprendentemente, los números de Stirling que definimos en capítulos anteriores aparecerán de manera natural.

Proposición 7.10.

$$x^{\overline{n}} = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} x^k.$$

Demostración. Demostremos esta proposición por inducción, usando la recurrencia $\begin{bmatrix} n \\ k \end{bmatrix} = (n-1)\begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$ que se demostró anteriormente.

Para $n = 0$, tenemos que $\begin{bmatrix} 0 \\ 0 \end{bmatrix} x^0 = 1 = x^{\overline{0}}$. Por otro lado para $n \geq 0$,

$$\begin{aligned} x^{\overline{n+1}} = x^{\overline{n}}(x+n) &= \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} x^k (x+n) \\ &= \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} x^{k+1} + \sum_{k=0}^{n} n \begin{bmatrix} n \\ k \end{bmatrix} x^k \\ &= \sum_{k=1}^{n+1} \begin{bmatrix} n \\ k-1 \end{bmatrix} x^k + \sum_{k=0}^{n} n \begin{bmatrix} n \\ k \end{bmatrix} x^k \\ &= \begin{bmatrix} n \\ n \end{bmatrix} x^{n+1} + \sum_{k=1}^{n} \begin{bmatrix} n+1 \\ k \end{bmatrix} x^k + n \begin{bmatrix} n \\ 0 \end{bmatrix} x^0 \\ &= \sum_{k=0}^{n+1} \begin{bmatrix} n+1 \\ k \end{bmatrix} x^k, \end{aligned}$$

donde usamos que $\begin{bmatrix} n \\ n \end{bmatrix} = 1 = \begin{bmatrix} n+1 \\ n+1 \end{bmatrix}$ y que $n\begin{bmatrix} n \\ 0 \end{bmatrix} = 0 = (n+1)\begin{bmatrix} n+1 \\ 0 \end{bmatrix}$. □

La proposición anterior dice que la matriz de coeficientes asociadas a los números de Stirling sin signo $\begin{bmatrix} n \\ k \end{bmatrix}$ es la matriz de cambio de base de la base de factoriales ascendientes a la base de monomios.

Proposición 7.11.

$$x^{\underline{n}} = \sum_{k=0}^{n} s(n,k) x^k.$$

Demostración. Notemos que $x^{\underline{n}} = (-1)^n (-x)^{\overline{n}}$. Luego, aplicando la proposición anterior a $(-x)$ obtenemos:

$$\begin{aligned} x^{\underline{n}} = (-1)^n (-x)^{\overline{n}} &= (-1)^n \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} (-x)^k \\ &= \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} (-1)^{n-k} x^k \\ &= \sum_{k=0}^{n} s(n,k) x^k. \end{aligned}$$

□

Lo anterior dice que la matriz de números de Stirling del primer tipo $s(n,k)$ es la matriz de cambio de base de la base de factoriales descendientes a la base de monomios.

Observación: Gracias a las proposiciones anteriores tenemos demostraciones alternativas de ciertas igualdades que se pueden probar combinatorialmente (tomando $x = 1$):

$$\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} = n! \qquad \text{y} \qquad \sum_{k=0}^{n} s(n,k) = [\![n \in \{0,1\}]\!].$$

Proposición 7.12.

$$x^n = \sum_{k=0}^{n} S(n,k) x^{\underline{k}}.$$

Demostración. Esta proposición se puede probar usando la recurrencia 4.14 e inducción. En vez de hacer eso, daremos una demostración "semicombinatorial". Probaremos que la igualdad de la propoxición 7.12 se tiene para

todo x natural. Como dos polinomios en $\mathbb{C}[x]$ que son iguales en infinitos puntos son iguales como polinomios concluimos la igualdad. Notemos que si $x \in \mathbb{N}$,

$$\begin{aligned} x^n &= |[x]^n| = |\{f\colon [n] \to [x] \text{ función}\}| \\ &= \sum_{k=0}^{x} \sum_{Y \subseteq \binom{[x]}{k}} |\{f\colon [n] \to Y \text{ función sobreyectiva}\} \\ &= \sum_{k=0}^{x} \binom{x}{k} k! S(n,k) \\ &= \sum_{k=0}^{x} x^{\underline{k}} S(n,k). \end{aligned}$$

□

Corolario 7.13. *Para todo $0 \leq a, b \leq n$,*

$$\delta_{a,b} := [\![a = b]\!] = \sum_{k=0}^{n} S(a,k)s(k,b) = \sum_{k=0}^{\infty} S(a,k)s(k,b).$$

Alternativamente, si tomamos las matrices de $n \times n$, $\mathbf{S}_n = (S(i,j))_{1 \leq i,j \leq n}$ y $\mathbf{s}_n = (s(i,j))_{1 \leq i,j \leq n}$ entonces $\mathbf{S}_n$ y $\mathbf{s}_n$ son inversas: $I_n = \mathbf{S}_n \cdot \mathbf{s}_n$.

La demostración consiste en notar que $\mathbf{S}_n$ y $\mathbf{s}_n$ son las matrices de cambio de base entre $\{1, x, \ldots, x^n\}$ y $\{1, x, \ldots, x^{\underline{n}}\}$.

Ejercicio 7.14.

1. De una demostración alternativa de la Proposición 7.12 usando la Proposición 4.14 e inducción.
2. Encuentre una demostración semicombinatorial para la Proposición 7.10. Para esto siga los siguientes pasos. Sean $n, x \in \mathbb{N}$. Una n-permutación x-coloreada es un par (f, g) donde f es una permutación de $[n]$ y $g\colon [n] \to [x]$ es una funcion de "coloreo" tal que cada ciclo de f_1 recibe el mismo color (igual valor de g). Pruebe que ambos lados de la igualdad en el lema cuentan las n-particiones x-coloreadas. Para la parte difícil piense en como pasar de una $(n-1)$-partición x-coloreada a una n-permutación x-coloreada.

Capítulo 8

Principio de Inclusión-Exclusión

El principio de Inclusión-Exclusión es una extensión del principio de la suma aplicado a conjuntos que no son necesariamente disjuntos. En lo que sigue sean $A_1, \ldots, A_n$ una secuencia de conjuntos finito. Para todo $I \subseteq [n]$, llamemos A_I al conjunto $\bigcap_{i \in I} A_i$, donde interpretamos $A_\emptyset$ como $\bigcup_{i=1}^n A_i$.

Teorema 8.1 (Principio de Inclusión-Exclusión)**.**

$$0 = \sum_{I \subseteq [n]} (-1)^{|I|} |A_I|.$$

En particular,

$$\begin{aligned} |\bigcup_{i=1}^n A_i| &= \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|+1} |A_I| \\ &= |A_1| + \cdots + |A_n| - |A_1 \cap A_2| - \cdots - |A_{n-1} \cap A_n| + |A_1 \cap A_2 \cap A_3| + \ldots \end{aligned}$$

Demostración. Probaremos algo un poco más general. Veamos que para todo x,

$$[\![x \in A_\emptyset]\!] - 1 = \sum_{I \subseteq [n]} (-1)^{|I|} [\![x \in A_I]\!].$$

Si sumamos la expresión anterior sobre todos los posibles $x \in A_\emptyset$ tendremos la igualdad que queremos probar. Sea x elemento cualquiera, y sea $I(x) = \{i \in [n] : x \in A_i\}$ los índices de los conjuntos que contienen a x. Notar que para $I \neq \emptyset$, $x \in A_I$ si y solo si $I \subseteq I(x)$. Con esto tenemos que la expresión de la derecha es

$$\begin{aligned} (-1)^{|\emptyset|} [\![x \in A_\emptyset]\!] + \sum_{\emptyset \subsetneq I \subseteq [n]} (-1)^{|I|} [\![I \subseteq I(x)]\!] &= [\![x \in A_\emptyset]\!] + \sum_{\emptyset \neq I \subseteq I(x)} (-1)^{|I|} \\ &= [\![x \in A_\emptyset]\!] - 1 + \sum_{j=0}^{|I(x)|} \sum_{I \in \binom{I(x)}{j}} (-1)^{|I|} \\ &= [\![x \in A_\emptyset]\!] - 1 + \sum_{j=0}^{|I(x)|} (-1)^j \binom{|I(x)|}{j} \\ &= [\![x \in A_\emptyset]\!] - 1 + (-1+1)^{|I(x)|}, \end{aligned}$$

donde la última igualdad viene del teorema del binomio.

Para concluir, notamos que si $x \in A_\emptyset$, entonces $I(x) \neq \emptyset$ y luego la expresión de arriba se evalúa a $1 - 1 + 0 = 0$. Por otro lado, si $x \notin A_\emptyset$ entonces $0^{|I(x)|} = 0^0 = 1$ y luego la expresión de arriba se evalúa a $0 - 1 + 1 = 0$. □

Observación 8.2. La demostración anterior usa el teorema del binomio. Más adelante daremos una segunda demostración que no requiere de este teorema.

Es fácil extender la demostración anterior a contextos más generales como lo muestra las siguientes proposiciones.

Proposición 8.3. *Sean $A_1, \dots, A_n$ conjuntos finitos y $w\colon X = \bigcup_{i=1}^n A_i \to G$, donde $(G, +)$ es un grupo abeliano. Para todo $Y \subseteq X$, llame $w(Y) = \sum_{x\in Y} w(x)$ donde la suma es la operación de G. Entonces:*

$$w(\bigcup_{i=1}^n A_i) = \sum_{\emptyset\neq I\subseteq[n]} (-1)^{|I|+1} w(A_I),$$

donde para todo $g \in G$, $(-1)g = -g$ es el inverso aditivo de g en G.

Proposición 8.4. *Sean $A_1, \dots, A_n$ eventos en un espacio de probabilidad, luego*

$$\Pr(\bigcup_{i=1}^n A_i) = \sum_{\emptyset\neq I\subseteq[n]} (-1)^{|I|+1} \Pr(A_I).$$

Demostración de las proposiciones 8.3 y 8.4. Anteriormente demostramos que

$$[\![x \in A_\emptyset]\!] - 1 = \sum_{I\subseteq[n]} (-1)^{|I|} [\![x \in A_I]\!]. \tag{8.1}$$

donde $A_\emptyset = X$. Para todo $x \in X$, el lado izquierdo vale 0. Luego, podemos multiplicar por $w(x)$ para $x \in X$, la igualdad anterior. Sumando sobre $x \in X$ se tiene

$$0 = \sum_{x\in X}\sum_{I\subseteq[n]} (-1)^{|I|} [\![x \in A_I]\!] w(x) = \sum_{I\subseteq[n]} (-1)^{|I|} \sum_{x\in X} [\![x \in A_I]\!] w(x) = \sum_{I\subseteq[n]} (-1)^{|I|} \sum_{x\in X} w(A_I),$$

lo que concluye la demostración de la primera proposición.

Para la segunda proposición basta integrar (8.1) sobre todo x en $A_\emptyset$.

$$0 = \sum_{I\subseteq[n]} (-1)^{|I|} \Pr(A_I).$$

□

Veamos un ejemplo de uso del Principio de Inclusión y Exclusión (PIE).

Ejercicio resuelto 8.5. Sean $p_1, \dots, p_k$ primos y $n \in \mathbb{N}$. Contar el conjunto de elementos menores que n que no son múltiplos de ningún p_i.

Definamos A_i como el conjunto de multiplos de p_i en $[n]$. Luego lo pedido es exactamente $n - |\bigcup_{i\in[k]} A_k|$. Aplicando el PIE tenemos que esto es igual a

$$n - \sum_{I\subseteq[k]} (-1)^{|I|+1} |A_I| = n + \sum_{\emptyset\neq I\subseteq[k]} (-1)^{|I|} \Big\lfloor \frac{n}{\prod_{i\in I} p_i} \Big\rfloor.$$

Por ejemplo si queremos contar los elementos menores que 10000 que no son multiplos de 2, 3 ni 5 obtenemos

$$\begin{aligned} 10000 - \lfloor 10000/2\rfloor - \lfloor 10000/3\rfloor \lfloor 10000/5\rfloor + \lfloor 10000/6\rfloor + \lfloor 10000/10\rfloor + \lfloor 10000/15\rfloor - \lfloor 10000/30\rfloor \\ = 10000 - 5000 - 3333 - 2000 + 1666 + 1000 + 666 - 333 = 2666. \end{aligned}$$

Un corolario simpático es que si llamamos $f(n; p_1, \dots, p_k)$ como la proporción de elementos en $[n]$ que no son múltiplos de p_i satisface

$$\lim_{n\to\infty} f(n; p_1, \dots, p_k) = 1 + \sum_{\emptyset\neq I\subseteq[k]} (-1)^{|I|} \frac{1}{\prod_{i\in I} p_i} = \sum_{I\subseteq[k]} \prod_{i\in I} \frac{-1}{p_i} \prod_{i\in[k]\setminus I} 1 = \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right).$$

Notemos que si n es suficientemente grande y elegimos un número $i \in [n]$ uniformemente al azar, la probabilidad de que ese número no sea múltiplo de p_i es esencialmente $1 - 1/p_i$. La fórmula recién descrita nos dice que los eventos "no ser múltiplo de p_i" son esencialmente independientes. Por otro lado, notemos que el estimado es bastante útil incluso para valores relativamente pequeños de n. Por ejemplo para el caso de $(2, 3, 5)$ tenemos que la proporción es $\frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = \frac{4}{15} = 0{,}2666\dots$

Para concluir el capítulo, veamos una última aplicación del P.I.E: una fórmula exacta para los números de Stirling del segundo tipo.

Proposición 8.6.

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

Demostración. Recordemos que $k!S(n,k)$ es la cantidad de funciones sobreyectivas de $[n]$ a $[k]$. Llamemos A_i al conjunto de funciones f de $[n]$ a $[k]$ tal que $f^{-1}(i) = \emptyset$. Con esto $k!S(n,k) = k^n - |\bigcup_{i=1}^{n} A_i|$. Al igual que en el caso anterior llamemos $A_I = \bigcap_{i\in I} A_i$. En este caso A_I es el conjunto de funciones $f\colon [n] \to [k]$ tal que ningún elemento de I tiene preimagen. Es decir A_I son las funciones de $[n] \to [k] \setminus I$ y luego $|A_I| = (k - |I|)^n$. El P.I.E. nos dice que

$$\begin{aligned} k!S(n,k) &= k^n - \sum_{i=1}^{n}\sum_{I\in\binom{[k]}{i}}(-1)^{i+1}|A_I| \\ &= k^n + \sum_{i=1}^{n}\binom{k}{i}(-1)^i(k-i)^n = \sum_{i=0}^{n}\binom{k}{i}(-1)^i(k-i)^n. \end{aligned}$$

□

Ejercicio 8.7. Sean $k, \ell, n \in \mathbb{N}$. Pruebe que:

1. El número de soluciones de la ecuación $x_1 + x_2 + \cdots + x_k = n$ con $1 \le x_i \le \ell$ es

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

2. El número de soluciones de la ecuación $x_1 + x_2 + \cdots + x_k = n$ con $\ell \ge x_1 \ge x_2 \ge \cdots \ge x_1 \ge 1$ es

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

Indicación: Puede resolver los dos problemas simultaneamente, llamando $f(n-\ell i, k)$ al coeficiente que acompaña a $\binom{k}{i}(-1)^i$ en cada caso e interpretando f de acuerdo al problema.
Concluya que

$$\sum_{i=0}^{k}(-1)^i\binom{k}{i}\binom{n-1-2i}{k-1} = \binom{k}{n-k}.$$

$$\sum_{i=0}^{k}(-1)^i\binom{k}{i}p_k(n-2i) = [\![1 \le k \le n]\!].$$

jsoto. Desigualdades de Bonferroni

Capítulo 9

Más principios básicos

9.1. Principio Inyectivo y Principio Sobreyectivo

En esta sección enunciamos dos extensiones naturales del principio biyectivo.

Proposición 9.1 (Principio Inyectivo)**.** *Sean A y B conjuntos donde B es finito.*

A es finito y $|A| \leq |B|$ si y solo si existe una función inyectiva de A a B.

Demostración. La dirección hacia la derecha es simple. Sean $f\colon A \to [m]$ y $g\colon [n] \to B$ biyecciones, donde $m \leq n$. Como ambas funciones son inyectivas, la función $h\colon A \to B$ dada por $h(x) = g(f(x))$ es inyectiva.

Veamos ahora la otra dirección. Probemos primero por inducción en n que todos los subconjuntos de $[n]$ son finitos. En efecto, esto es cierto para $n = 0$ pues el único subconjunto de $[0] = \emptyset$ es $[0] = \emptyset$. Sea entonces $n \geq 1$, y sea $X \subseteq [n]$. Si $X = [n]$ entonces $|X| = n$ y X es finito. Asi que supongamos que existe $a \in [n] \setminus X$. Si $a = n$ entonces $X \subseteq [n-1]$, y por inducción X es finito y $|X| \leq n-1$. Luego supongamos $a < n$ y sea $Y = X \setminus \{n\} \cup \{a\}$. La biyección $f\colon X \to Y$ dada por $f(n) = a$ y $f(x) = x$ para todo $x \in X \setminus \{n\}$ muestra que $|X| = |Y|$. Por otro lado $Y \subseteq [n-1]$, Y es finito. Por lo tanto X es finito y $|X| = |Y| \leq n-1$.

Terminemos la demostración de la proposición. Sea $h\colon A \to B$ una función inyectiva y sea $g\colon B \to [n]$ una biyección. Luego la función $f = g \circ h\colon A \to [n]$ es inyectiva. Usando que $f(A) \subseteq [n]$ y que f es biyección entre A y $f(A)$, tenemos $|A| = |f(A)| \leq n = |B|$. □

Comentario 9.2. El principio inyectivo enunciado anteriormente para cardinales finitos, puede ser modificada a una *definición* de orden para cardinales generales: $|A| \leq |B|$ se define como la existencia de una función inyectiva de A en B.

Otra forma de interpretar el principio anterior es el siguiente.

> (**Principio Inyectivo**) Para probar que un conjunto (finito) tiene una cantidad menor o igual de elementos que otro, basta encontrar una inyección (i.e., una función inyectiva) del primer conjunto al segundo.
>
> En particular, si se encuentra una inyección de A en B, y una inyección de B en A, entonces A y B tienen el mismo cardinal.

Comentario 9.3. La última afirmación también es cierta para conjuntos infinitos, y se conoce como el Teorema de Cantor-Schröder–Bernstein (este teorema no requiere del axioma de elección).

Una variante del principio anterior es la siguiente

Proposición 9.4 (Principio Sobreyectivo)**.** *Sean A y B conjuntos donde B es finito.*

A es finito y $|A| \leq |B|$ si y solo si existe una función sobreyectiva de B a A.

Demostración. La dirección hacia la derecha es similar a la de la proposición anterior. Sean $f\colon [n] \to A$ y $g\colon B \to [m]$ biyecciones, donde $n \leq m$. Definamos además la función $f'\colon [m] \to A$ como $f'(x) = f(\text{mín}(x, n))$. Como f es sobreyectiva, f' también lo es. Como la composición de funciones sobreyectivas es sobreyectiva, concluimos que $f' \circ g\colon B \to A$ es sobreyectiva.

Para la otra dirección sea $B = \{b_1, \ldots, b_m\}$ y $f\colon B \to A$ una función sobreyectiva. La función $h\colon A \to B$ dada por $h(a) = b_i$ donde i es el mínimo índice tal que $f(b_i) = a$ está bien definida (siempre existe este índice pues $f^{-1}(a)$ es no vacío y $\mathbb{N}$ es bien ordenado). Además es fácil ver que h es inyectiva. Por la proposición anterior A es finito y $|A| \leq |B|$. □

Comentario 9.5. El principio sobreyectivo también funciona para conjuntos infinitos, pero su demostración requiere el uso del axioma de elección (interesantemente, es equivalente al axioma de elección).

Podemos rescribir el principio sobreyectivo de una manera más coloquial como sigue.

> (**Principio Sobreyectivo**) Para probar que un conjunto tiene una cantidad menor o igual de elementos que un segundo conjunto (finito), basta encontrar una sobreyección (i.e., una función sobreyectiva) del segundo conjunto al primero.
>
> En particular, si se encuentra una sobreyección de A en B, y una sobreyección de B en A, entonces A y B tienen el mismo cardinal.

Los principios anteriores nos permiten dar distintas maneras de probar que dos conjuntos tienen el mismo cardinal.

Corolario 9.6. *Sean A y B dos conjuntos finitos. Los siguientes son equivalentes.*

1. $|A| = |B|$.
2. *Existe una inyección de A en B y una inyección de B en A.*
3. *Existe una sobreyección de A en B y una sobreyección de B en A.*
4. *Existe una inyección de A en B y una sobreyección de A en B.*

Demostración. Directo. □

9.2. Ejemplo: Principio del palomar y metodo probabilista

Al principio del curso estabamos interesados en saber contar conjuntos finitos. En esta seccion nos interesa algo mucho mas debil, determinar si un conjunto es vacio o no.

El principio del palomar (o de Dirichlet, o de los casilleros) es una herramienta muy util para probar la existencia de un conjunto. Enunciamos y demostramos varias versiones del mismo a continuacion.

Teorema 9.7. *Sean n objetos distintos repartidos en m casilleros (llamemos $f\colon [n] \to [m]$ a la funcion tal que $f(i)$ es el casillero en el cual i es asignado).*

1. *Si $n \geq m + 1$ entonces hay un casillero que recibe al menos 2 objetos (i.e. f no es sobreyectiva).*
   Si $n \leq m + 1$ entonces hay un casillero vacio (i.e. f no es inyectiva).
   ***Ejemplos basicos**: Si hay 367 personas en un salon, hay 2 de cumpleaños el mismo dia.*
   Si S es un conjunto de 5 puntos en $\mathbb{Z}^2$, entonces hay un par cuyo promedio esta en $\mathbb{Z}^2$.
   En cualquier grupo de n personas hay al menos 2 con el mismo numero de amigos.
   Si se tira un par de dados 10 veces existe una suma que no ha salido
2. *Si $n \geq km + 1$ entonces hay un casillero que recibe al menos $k + 1$ objetos.*
   Si $n \leq km - 1$ entonces hay un casillero que recibe a lo mas $k - 1$ objetos.
   En Santiago hay un conjunto de 6000 personas con las mismas iniciales.
   Hay un dia del año donde no mas de 20000 personas de Santiago estan de cumpleaños.
3. *Existe un casillero con $\geq \lceil n/m \rceil$ objetos y un casillero con $\leq \lfloor n/m \rfloor$ objetos.*

4. *Si* $a_1 + \cdots + a_m \leq n-1$ *entonces existe un casillero* i *con al menos* $a_i + 1$ *objetos.*
   Si $a_1 + \cdots + a_m \geq n+1$ *entonces existe un casillero* i *con a lo más* $a_i - 1$ *objetos.*

En general todas las versiones (finitas) del principio del palomar son corolarios del llamado principio probabilista del primer momento que dice lo siguiente:

Sea X una variable aleatoria real sobre un espacio de probabilidad Ω, luego siempre existe $\omega \in \Omega$ tal que $X(\omega) \geq \mathbb{E}[X]$ y siempre existe $\omega \in \Omega$ tal que $X(\omega) \leq \mathbb{E}[X]$.

Demostración.

$$\mathbb{E}[X] = \int_{\omega \in \Omega} X(\omega) dP(\omega)$$

Si para todo $\omega \in \Omega$, $X(\omega) \leq \mathbb{E}[X] - \epsilon$ para $\epsilon > 0$, tendriamos que

$$\mathbb{E}[X] \leq (\mathbb{E}[X] - \epsilon) \left(\int_{\omega \in \Omega} dP(\omega) \right) \leq \mathbb{E}[X] - \epsilon,$$

lo cual es una contradiccion. □

Con esto podemos probar los PP.

1. Sea $g(i) = f^{-1}(i)$, y $\mathbb{E}[g] = \frac{1}{m} \sum_{i=1}^{m} g(i)$. Entonces existe un i con $g(i) \geq \lceil \mathbb{E}[g] \rceil$ y un i con $g(i) \leq \lfloor \mathbb{E}[g] \rfloor$.
2. Sea $g(i) = f^{-1}(i)/a_i$, y sean $\lambda_i = a_i / \sum_{i=1}^{m} a_i$. De modo que $\mathbb{E}_\lambda[g] = \sum_{i=1}^{m} \lambda_i g(i) = \sum_{i=1}^{m} f^{-1}(i) / \sum_{i=1}^{m} a_i = n / \sum_{i=1}^{m} a_i$. Entonces existe un i con $g(i) \geq \lceil \mathbb{E}[g] \rceil$ y un i con $g(i) \leq \lfloor \mathbb{E}[g] \rfloor$.

Veamos algunos ejemplos interesantes del principio del palomar y del principio prob. del primer momento.

Teorema 9.8 (Teorema de Erdos-Szekeres)**.** *Sea* $s \in \mathbb{R}^{mn+1}$ *una secuencia de* $mn+1$ *números reales. Entonces existe una subsecuencia (debilmente) creciente de* s *con* $m+1$ *numeros o una subsecuencia (debilmente) decreciente de* s *con* $n+1$ *numeros.*

Demostración. Supongamos que el resultado es falso. Para todo $i \in [mn+1]$ defina a_i como el largo de la subsecuencia creciente mas larga que parte en la posicion i y b_i como el largo de la subsecuencia decreciente mas larga que termina en la posicion i.

Como supusimos que el resultado es falso que los pares $(a_i, b_i) \in [n] \times [m]$. Como hay $mn+1$ posibles i, el ppio del palomar dice que existen $i < j$ con $(a_i, b_i) = (a_j, b_j)$.

Si $s_i \leq s_j$ entonces la secuencia s_i concatenada con la secuencia creciente mas larga que parte en la posicion j es creciente y de largo $a_j + 1 = a_i + 1$ y empieza en i lo que contradice la defn. de a_i. Similarmente si $s_i \geq s_j$ entonces la secuencia decreciente que termina en la posicion i concatenada con s_j es decreciente de largo $b_i + 1 = b_j + 1$ y termina en la posicion j lo que contradice la definición de b_j. □

Otro ejemplo infinito del principio del palomar.

Lema 9.9. *Sea* n *un numero natural cualquiera y* b *un numero coprimo con 10. Probar que existen infinitas potencias positivas de* b *que termina (en decimal) en la secuencia* $0^n 1$.

Demostración. Consideremos los casilleros $B = \mathbb{Z}_{10^{n+1}}$ y $A = \mathbb{N}$. Defina $f \colon A \to B$ como $f(m)$ es igual al resto de dividir m por 10^{n+1}. Claramente (ppio del palomar ïnfinito") f no es inyectiva y de hecho debe existir un $j \in B$ tal que $f^{-1}(j)$ es un conjunto infinito.

Sean $a_1, a_2, \ldots,$ los elementos de $f^{-1}(j)$ ordenados de menor a mayor. Para todo $j \geq 1$,

Luego $0 \equiv_{10^{n+1}} b^{a_j} - b^{a_1} = b^{a_1}(b^{a_j - a_1} - 1)$. Como b es coprimo con 10^{n+1}, tenemos que

$$b^{a_j - a_1} \equiv_{10^{n+1}} 1,$$

es decir, para todo $j \geq 1$ $b^{a_j - a_1}$ termina en la secuencia $0^n 1$.

□

Nota: Lo anterior prueba una versión débil del pequeño teorema de Fermat: Si b y m son coprimos, existen infinitas potencias de b congruentes con 1 modulo m.

Capítulo 10

Conjuntos Parcialmente Ordenados: Introducción y Fórmulas de Inversión

jsoto. Este capítulo está sin tocar desde el 2014

10.1. Definiciones básicas

[Def]

$P = (X, \leq_P)$ es un orden parcial si $\leq$ es refleja, transitiva y antisimétrica.
[Def]

$P = (X, <_P)$ es un orden estricto si $<$ es irreflexiva y transitiva (y por lo tanto, asimétrica).
Obs 1: A veces escribiremos $x \in P$ en vez de $x \in X$ (cuando no hay confusión confundiremos P y X)
Obs 2: En ocasiones diremos "sea P un orden" para denotar al orden parcial $(P, \leq_P)$.
Obs 3: Hay una relación natural entre ordenes parciales y ordenes estrictos.
En efecto, dado $\leq_P$ orden parcial se puede definir $x <_P y \iff x \leq_P y \wedge x \neq y$ orden estricto asociado. Similarmente si $x <_P y$ es orden estricto entonces definiendo $x \leq_P y \iff x <_p y \vee x = y$ se obtiene un orden parcial asociado.

Ejemplos 10.1. En adelante usamos X^* para referirnos al conjunto $\bigcup_{i \in \mathbb{N}} X^i$ de todas las palabras sobre el alfabeto X.

- $(\mathbb{R}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{N}, \leq)$, $([n], \leq)$, etc. donde $\leq$ es el orden habitual de $\mathbb{R}$.
- $D_n := (\{t \in [n] \colon (t|n)\}, |)$ donde $p|q$ si p divide a q.
- $B_n := (\mathcal{P}([n]), \subseteq)$ (se conoce como orden booleano).
- $\Pi_n :=$ (particiones de $[n], \leq$) donde $\alpha \leq \beta$ si α refina a β.
- $(X^*, \trianglelefteq)$ donde $\alpha \trianglelefteq \beta$ si $\beta = \gamma\alpha\delta$ con $\gamma, \delta \in X^*$ (decimos que α es **factor** de β).
- $(X^*, \leq)$ donde $\alpha \leq \beta$ si $\alpha = x_1 x_2 \dots x_k$, $x_i \in X$ y $\beta = \gamma_1 x_1 \gamma_2 x_2 \dots \gamma_k x_k \gamma_{k+1}$, con $\gamma_i \in X^*$ (decimos que α es **subsecuencia** de β).
- Genéricamente, si hay una relación sub* hay un orden subyacente (subgrupos, subespacios vectoriales, etc).

Es costumbre llamar a los órdenes "poset" (del inglés, partially ordered set).

Conceptos en órdenes parciales

Sea P un orden. En lo que sigue daremos varias definiciones con subindice P, si no produce ambigüedad, dichos subindices se pueden borrar.

- Si $x \leq_P y$ ó $y \leq_P x$ decimos que x e y son comparables y anotamos $x \sim_P y$. Si no, decimos que son incomparables y anotamos $x \perp_P y$.
- [Def]

  Una **anticadena** en P es un conjunto de elementos incomparables dos a dos en P.
- [Def]

  Una **cadena** en P es un conjunto de elementos comparables dos a dos en P (muchas veces lo anotamos como una secuencia, más que como un conjunto).

- Un elemento $x \in P$ es máximal si no existe $y \neq x$ con $x \leq_P y$. $x \in P$ es minimal si no existe $y \neq x$ con $y \leq_P x$. Al conjunto de maximales y minimales se les denota por máx P y mín P.
- Definimos el intervalo $[x, y]_P := \{z \in P \mid x \leq_P z \wedge z \leq_P y\}$ (consideramos $[x, y]_P$ como un orden con relación $\leq_P |_{[x,y]_P \times [x,y]_P}$).
- Decimos que P es **localmente finito** si $|[x, y]_P| < \infty$.
- Decimos que y cubre a x si $x <_P y$ y además $[x, y]_P = \{x, y\}$. En ese caso escribiremos $x \lessdot_P y$.
- **Diagrama de Hasse** de P. Es una representación de P en el plano donde si $x \lessdot_P y$ entonces x aparece más abajo que y y hay una flecha (o una línea) desde x a y.

Observaciones.

1. Si $x \leq y$ no es necesariamente cierto que existe z tal que $x \lessdot z$. El ejemplo más claro es $(\mathbb{R}, \leq)$.
2. Si P es localmente finito entonces $\lessdot_P$ **define** a $\leq_P$. En efecto, $\leq_P$ es la **envoltura transitiva** de $\lessdot_P$ (la intersección de todas las relaciones transitivas que contienen a $\lessdot_P$). Otra forma de decir esto es que $x \leq_P y$ si y solo si existe una secuencia $x = z_0 \lessdot_P z_1 \lessdot_P \cdots \lessdot_P z_k = y$.

Funciones monótonas

Una función $\varphi\colon P \to Q$ se dice

1. **monótona** (que preserva el orden) si $x \leq_P y \implies \varphi(x) \leq_Q \varphi(y)$.
2. **fuertemente monótona** (incrustación de orden) si $x \leq_P y \iff \varphi(x) \leq_Q \varphi(y)$.
3. **isomorfismo** si φ es monótona fuerte y sobreyectiva.

Ejemplos:

1. $\varphi\colon B_n \to [n]$, $\varphi(X) = \text{máx}(X)$ es una función monótona pero no fuertemente monótona. (Esto es decir, $X \subseteq Y$ implica $\text{máx}(X) \leq \text{máx}(Y)$).
2. $\varphi\colon [n] \to B_n$, $\varphi(x) = [x]$ es una función fuertemente monótona (decimos que $[n]$ se incrusta en $B(n)$).
3. $\varphi\colon B_3 \to D_{30}$, $\varphi(X) = 2^{[\![1 \in X]\!]} 3^{[\![2 \in X]\!]} 5^{[\![3 \in X]\!]}$ es un isomorfismo.

Decimos que P es un **suborden (débil)** de Q si $\forall x, y \in P$, $x \leq_P y \implies x \leq_Q y$. En otras palabras, la identidad en P es una **función monotona de P en Q**.

¡Cuidado! La existencia de una función monótona y biyectiva de P a Q no garantiza que P sea isomorfo a Q. (Pensar en un ejemplo infinito)

10.2. Particiones en cadenas y anticadenas

Proposición 10.2. *Si C es una cadena de P y A es una anticadena, entonces $|A \cap C| \leq 1$..*

Demostración. Trivial □

Observemos que de cualquier forma podemos tener cadenas y anticadenas maximales que no se intersectan.

Lo siguientes vale en órdenes parciales finitos.
[Def]

El **alto** de P es la cardinalidad de su cadena más larga. Esto se denota por $h(P)$.
[Def]

El **ancho** de P es la cardinalidad de su cadena más larga. Esto se denota por $w(P)$.
Siempre podemos particionar un orden parcial en cadenas (resp. en anticadenas) pues los singletons son simultáneamente cadenas y anticadenas.

Proposición 10.3. *Sea $\mathcal{P}$ una partición en cadenas de P, $\mathcal{Q}$ una partición en anticadenas de P. Entonces*

$$|\mathcal{P}| \geq |A| \quad \forall A \text{ anticadena}$$
$$|\mathcal{Q}| \geq |C| \quad \forall C \text{ cadena}$$

Demostración. Se deduce de la observación que $|C \cap A| \leq 1$ para toda C cadena y A anticadena. □

En particular, se tiene que

$$h(P) \leq |\mathcal{P}| \quad \forall \mathcal{P} \text{ partición de } P \text{ en cadenas,}$$
$$w(P) \leq |\mathcal{Q}| \quad \forall \mathcal{Q} \text{ partición de } P \text{ en anticadenas.}$$

Teorema 10.4.

(1) ***Teorema de Mirsky***

$$h(P) = \min\{|\mathcal{Q}| \colon \mathcal{Q} \textit{ partición de } P \textit{ en anticadenas.}\}$$

(2) ***Teorema de Dilworth***

$$w(P) = \min\{|\mathcal{P}| \colon \mathcal{P} \textit{ partición de } P \textit{ en cadenas.}\}$$

Demostración. (1) Debemos probar que todo orden se puede particionar en $h(P)$ anticadenas. El teorema es trivialmente cierto si $h(P) = 1$ (pues entonces P es una anticadena), así que supongamos que $h(P) \geq 1$. Notemos que el conjunto $A = \max P$ consistente en los elementos maximales de P es una anticadena. Tomemos el suborden $P' = P \setminus A$, entonces $h(P') = h(P) - 1$, pues $|A \cap C| = 1$ para toda cadena C maximal.

Por inducción, existe una partición de P' en a lo más $h(P) - 1$ anticadenas. Esto junto a A muestra una partición de P en a lo más $h(P)$ anticadenas. Por la proposición anterior, debe ser en exactamente $h(P)$ anticadenas.

(2) Debemos probar que todo orden se puede particionar en $w(P)$ anticadenas. La demostración anterior funcionó pues existe una anticadena especial A que intersecta a todas las cadenas maximales. Esto no ocurre para cadenas necesariamente (¿Puede encontrar un ejemplo de un orden donde para toda cadena C existe una anticadena maximal que no la intersecta?)

Continuemos la demostración. El teorema es cierto si $w(P) = 1$ pues P es una cadena. Así que supondremos que $w(P) \geq 2$. Sea C una cadena maximal. Notemos que

$$w(P) - 1 \leq w(P \setminus C) \leq w(P).$$

Si $w(P \setminus C) = w(P) - 1$ entonces podemos usar inducción y obtener una partición de $P \setminus C$ en $w(P) - 1$ anticadenas, lo que junto a C termina la demostración. Luego podemos suponer en lo que sigue que $w(P \setminus C) = w(P)$ y que $A = \{a_1, \ldots, a_{w(P)}\}$ es una anticadena de tamaño máximo en $P \setminus C$.

Definamos $A^+ = \{x \in P \mid \exists a \in A, a \leq x\}$ y $A^- = \{x \in P \mid \exists a \in A, x \leq a\}$.

Observemos que:

a) $A^+ \cup A^- = P$ pues A es maximal. (si existiera $x \in P \setminus (A^+ \cap A^-)$ entonces $A \cup \{x\}$ sería anticadena).
b) $A^+ \cap A^- = A$, pues si existiera $x \in (A^+ \cap A^-) \setminus A$, entonces también existirían $a_1 \in A$ y $a_2 \in A$ con $a_1 \leq_P x \leq_P a_2$ lo que implica que $a_1 \neq a_2$ y que ambos son comparables.
c) $A^+ \neq P$ y $A^- \neq P$.

La tercera propiedad se cumple pues el elemento máximo x^+ de C está fuera de A^- (si estuviera dentro, existiría $a \in A$ con $x^+ \leq a$ y luego $C \cup \{a\}$ sería cadena contradiciendo su maximalidad). Análogamente, el elemento mínimo de C está fuera de A^+.

Gracias a la última propiedad podemos usar hipótesis de inducción en A^-. Sea $C_1^-, \ldots, C_{w(P)}^-$ una partición de A^- en cadenas, enumeradas de tal forma que $a_i \in C_i^-$ (y luego a_i debe ser el máximo de C_i^-). Hagamos

exactamente lo mismo para A^+. Por razonamiento análogo podemos encontrar una partición de A^+ en cadenas $C_1^+, C_2^+, \ldots, C_{w(P)}^+$ de modo que $a_i \in C_i^+$ (y luego a_i es el mínimo de C_i^+).

Como a_i es el máximo de C_i^- y el mínimo de C_i^+ podemos definir la cadena $C_i = C_i^- \cup C_i^+$. Con esto, $C_1, \ldots, C_{w(P)}$ es una partición de P en exactamente $w(P)$ cadenas.

□

En auxiliar verán aplicaciones de los teoremas de Mirsky y Dilworth.

Ejercicio 10.5.

1. Demuestre que en todo orden parcial finito
$$h(P) \cdot w(P) \geq |P|.$$
2. Demuestre la desigualdad de LYM siguiente. Sea $\mathcal{F}$ una anticadena del orden booleano B_n. Pruebe que
$$\sum_{A \in \mathcal{F}} \binom{n}{|A|}^{-1} \leq 1.$$
Indicación: Para cada $A \in \mathcal{F}$, defina el conjunto $\mathrm{Cad}(A) = \{\mathcal{C} \text{ cadena maximal en } B_n \mid A \in \mathcal{C}\}$. Calcule el tamaño de $\mathrm{Cad}(A)$ en función de n y $|A|$. Luego pruebe de otra forma que $\sum_{A \in \mathcal{F}} |\mathrm{Cad}(A)| \leq n!$ y concluya.

10.3. Álgebra de Incidencias y función de Moebius

En esta sección hablaremos de una poderosa técnica que, en particular, implica el P.I.E.

Definimos las incidencias de un orden parcial **localmente finito** P sobre los complejos como el conjunto de funciones f que mandan intervalos $[x,y]_P$ de P a números complejos. Por tradición, se prefiere escribir $f(x,y)$ en vez de $f([x,y]_P)$.

Para nuestros propósitos
$$I(P) = \{f \colon P \times P \to \mathbb{C} \mid x \not\leq_P y \implies f(x,y) = 0\}$$
con operaciones
$$\begin{aligned} (f+g)(x,y) &= f(x,y) + g(g,y), && \forall f, g \in I(P), \\ (cf)(x,y) &= cf(x,y), && \forall f \in I(P), c \in \mathbb{C}, \\ f * g(x,y) &= \sum_{z \in [x,y]_P} f(x,z) g(z,y) && \forall f, g \in I(P). \end{aligned}$$

Nota: ¡Como el orden es localmente finito todas las sumas son finitas!

Es fácil ver que la suma, ponderación y convolución son operaciones cerradas en $I(P)$. Por otro lado la suma hereda todas las propiedades de $(\mathbb{C}, +)$ (i.e., es una operación de grupo).

La convolución puede ser interpretada como multiplicación de matrices cuadradas posiblemente infinitas. Para ver esto, asocien a cada $f \in I(P)$ una matriz $M(f)$ de $P \times P$ de modo que la entrada x, y de $M(f)$ es igual a $f(x,y)$. Con esto es sencillo ver que $M(f * g) = M(f)M(g)$. De aquí se deduce que la convolución es asociativa, distribuye sobre la suma y tiene como identidad la función delta de Kronecker
$$\delta_P(x,y) = [\![x = y]\!].$$
En otras palabras, $f * (g * h) = (f * g) * h$, $f * (g + h) = f * g + f * h$, y $\delta_P * f = f * \delta_P = f$.

Obs: Para los más algebristas, la estructura $(I(P), +, *)$ se conoce como álgebra asociativa sobre $\mathbb{C}$.

No todos los elementos de $I(P)$ tienen inversa. Pero de nuestros cursos de álgebra sabemos que si f tiene una inversa izquierda y f tiene una inversa derecha entonces son iguales, y en ese caso la inversa es única. De hecho, f tiene inversa izquierda ssi f tiene inversa derecha (¿Por qué?).

Notemos que $f * g = \delta_P = g * f$ si y solo si para todo $x \leq y$,

$$\sum_{z\colon x\leq z\leq y} f(x,z)g(z,y) = \delta_P(x,y),$$

o alternativamente,

$$g(x,y) = \frac{1}{f(x,x)}\left(\delta_P(x,y) - \sum_{z\colon x<z\leq y} f(x,y)g(z,y)\right).$$

Esto nos da una fórmula para la inversa g de f en la medida que $f(x,x) \neq 0$ para todo $x \in P$.

Obs: De hecho, pruebe que f es invertible si y solo si $f(x,x) \neq 0$. Anotamos $g = f^{-1}$ a la inversa de f para la convolución.

En $I(P)$ hay dos elementos muy especiales llamadas la función zeta ζ_P y la función μ_P de Moebius.

$$\zeta_P(x,y) = [\![x \leq_P y]\!], \quad \mu_P = \zeta_P^{-1}.$$

Si usamos la fórmula de más arriba tenemos que para $x \leq y$,

$$\mu_P(x,y) = \left(\delta(x,y) - \sum_{z\colon x<_P z\leq_P y} \mu_P(z,y)\right)$$

Es decir,

$$\mu_P(x,y) = \begin{cases} 0 & \text{si } x \not\leq y, \\ 1 & \text{si } x = y, \\ -\sum_{z\colon x<_P z\leq_P y} \mu_P(z,y) & \text{si } x < y \end{cases}$$

Ejemplo 1. Tenemos que $M(\zeta_{[n]}) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & 1 \\ & & \ddots & \\ 0 & 0 & \ddots & 1 \\ 0 & 0 & \cdots & 1 \end{pmatrix}$, y luego $M(\mu_{[n]}) = M(\zeta_{[n]})^{-1} = \begin{pmatrix} 1 & -1 & 0 & \cdots & 0 \\ 0 & 1 & -1 & \cdots & 0 \\ & \ddots & \ddots & \ddots & \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & & 0 & 1 & -1 \\ 0 & \cdots & 0 & 0 & 1 \end{pmatrix}$.

En otras palabras, $\mu_{[n]}(x,y) = \begin{cases} 1 & \text{si } x = y \\ -1 & \text{si } y = x+1 \\ 0 & \text{en otro caso} \end{cases}$.

De hecho, esta expresión también describe la función de Möbius para el orden localmente finito $(\mathbb{N}, \leq)$.

Teorema 10.6 (Fórmula de Inversión de Möbius.)**.** *Sea $(P, \leq)$ un orden parcial localmente finito con elemento mínimo $\hat{0}$. Para todo $f, g\colon P \to \mathbb{C}$.*

$$f(x) = \sum_{y\colon \hat{0}\leq y\leq x} g(y) \qquad \Longleftrightarrow \qquad g(y) = \sum_{x\colon \hat{0}\leq x\leq y} f(y)\mu(x,y).$$

Demostración. Tomemos la matriz $M[\zeta]$. Notemos que la primera expresión dice que $f = M[\zeta] \cdot g$ (como producto matriz vector). La segunda dice que $g = M[\mu] \cdot f$. El resultado sigue del hecho que $\mu = \zeta^{-1}$ y luego $M[\mu] = (M[\zeta])^{-1}$. □

Veamos que dice esto de nuestro ejemplo para $[n]$. Sean $f, g\colon [n] \to \mathbb{C}$. Luego

$$f(k) = \sum_{l=0}^{k} g(l) \iff g(l) = \sum_{k=0}^{l} \mu_{[n]}(k,l) f(k) = \sum_{k=0}^{l} \mu_{[n]}(k,l) f(k) = f(l) - f(l-1)[\![l \geq 0]\!]$$

Recupramos la propiedad "telescópica" de las diferencias sucesivas.

Esto no es muy sorprendente. Veamos que pasa para B_n.

Proposición 10.7.

$$\mu_{B_n}(S,T) = \begin{cases} (-1)^{|T\setminus S|} & \text{si } S \subseteq T \\ 0 & \text{si no} \end{cases}.$$

Demostración. Sea $S \subseteq T$. Probemos la proposición por inducción en $|T \setminus S|$. Si $|T \setminus S| = 0$ entonces $T = S$ y luego, $\mu_{B_n}(S,T) = 1 = (-1)^0$, así que la proposición es cierta. Supongamos entonces que $|T \setminus S| = k \geq 1$.

Tenemos que para todo $S \subset R \subseteq T$, $|T \setminus R| < k$ y luego $\mu_{B_n}(R,T) = (-1)^{|T\setminus R|}$. Usando la fórmula para calcular μ tenemos que:

$$\begin{aligned}
\mu_{B_n}(S,T) &= -\sum_{R\colon S\subset R\subseteq T} \mu_{B_n}(R,T) \\
&= -\sum_{R\colon S\subset R\subseteq T} (-1)^{|T\setminus R|} \\
&= -\sum_{W\colon \emptyset\subset W\subseteq T\setminus S} (-1)^{|(T\setminus S)\setminus W|} && \text{(Tomando } R = W \dot\cup S\text{)} \\
&= -(-1)^{|T\setminus S|} \sum_{W\colon \emptyset\subseteq W\subset T\setminus S} (-1)^{|W|} \\
&= -(-1)^{|T\setminus S|} \sum_{w=1}^{|T\setminus S|} \binom{|T\setminus S|}{w} (-1)^{w} \\
&= -(-1)^{|T\setminus S|}((-1+1)^{|T\setminus S|} - 1) = (-1)^{|T\setminus S|}. && \square
\end{aligned}$$

En otros órdenes parciales, la fórmula de inversión resulta sumamente útil para combinatoria y teoría de números.

Lo interesante son los corolarios de la fórmula de Inversión:

Corolario 10.8.

1. *Fórmula de Inversión sobre B_n.*
$$f(T) = \sum_{S\subseteq T} g(S) \iff g(T) = \sum_{S\subseteq T} (-1)^{|T|-|S|} f(T).$$
2. *Fórmula de Inversión binomial.*
$$f(n) = \sum_{i=0}^{n} \binom{n}{i} g(i) \iff g(n) = \sum_{i=0}^{n} \binom{n}{i} (-1)^{n-i} f(i).$$

Ejercicio 10.9. Se define la función de Möbius numérica como $\mu\colon \mathbb{N} \to \mathbb{R}$ tal que $\mu(t) = 0$ si t es múltiplo de un primo al cuadrado, y $\mu(t) = (-1)^t$ si t es libre de cuadrados y tiene exactamente t factores primos distintos.

Pruebe que para todo $t|n$, $\mu(n/t) = \mu_{D_n}(t,n)$, donde μ_{D_n} es la función de Möbius asociada al orden D_n.

Concluya la fórmula de Möbius siguiente:

$$f(n) = \sum_{d|n} g(d) \iff g(n) = \sum_{d|n} \mu(n/d) f(d).$$

Definamos ahora el orden dual de P, llamado P^* como $x \leq_{P^*} y$ ssi $y \leq_P x$. Un corolario interesante del Teorema de Inversión es el siguiente.

Corolario 1. *Sea P orden parcial localmente finito con elemento máximo $\hat{1}$. Para todo $f, g \colon P \to \mathbb{C}$.*

$$f(x) = \sum_{y \colon x \leq_P y \leq_P \hat{1}} g(y) \qquad \Longleftrightarrow \qquad g(y) = \sum_{x \colon x \leq_P y \leq_P \hat{1}} f(y)\mu(x,y).$$

Demostración. Basta ver que $\mu_{P^*}(x,y) = \mu_P(y,x)$ (ejercicio). □

Veamos que el corolario anterior, aplicado al orden B_n, implica el principio de inclusión exclusión (P.I.E.).

Demostración (Fórmula de Inversión implica P.I.E.).

Sean $A_1, \ldots, A_n$ conjuntos finitos cualquiera. Para $S \subseteq I$ definamos $A(S) = \bigcap_{i \in S} A_i \cap \bigcap_{i \in [n] \setminus S} A_i^c$, donde el complemento es con respecto a cualquier universo finito $\mathbf{U}$ que contenga a $\bigcup_{i \in [n]} A_i$.

Notemos que $A(S)$ es el conjunto de los elementos del universo que están exactamente en los conjuntos con índice en S.

Nota: Es útil hacer un diagrama de Venn con $n = 3$, darse cuenta que cada zona indivisible del diagrama corresponde a un conjunto de índices $S \subseteq [3]$.

En particular, si $S \neq T$, $S, T \subseteq [n]$, se tiene que $A(S) \cap A(T) = \emptyset$. Además, para todo $S \subseteq [n]$,

$$\bigcup_{T \colon T \supseteq S} A(T) = \bigcap_{i \in S} A_i.$$

Definamos ahora las funciones $g, f \colon \mathcal{P}([n]) \to \mathbb{R}$ como

$$g(S) = |A(S)|, \text{ y}$$
$$f(S) = \sum_{T \supseteq S} g(T) = \left| \bigcup_{T \supseteq S} A(T) \right| = \left| \bigcap_{i \in S} A_i \right|.$$

La fórmula de inversión nos permite despejar g en función de f:

$$g(S) = \sum_{T \colon T \supseteq S} (-1)^{|T \setminus S|} f(T).$$

En particular, tomando $S = \emptyset$,

$$g(\emptyset) = f(\emptyset) + \sum_{\emptyset \neq T \subseteq [n]} (-1)^{|T|} f(T).$$

Recordando que $g(\emptyset) = |A(\emptyset)| = |\bigcap_{i \in [n]} A_i^c| = |\mathbf{U}| - |\bigcup_{i \in [n]} A_i|$, que $f(\emptyset) = |\mathbf{U}|$, y reordenando tenemos

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

que es el principio de inclusión-exclusión. □

10.4. Operaciones en órdenes

Sean P y Q dos órdenes. Definimos:

1. $P + Q$: Suma cardinal (o disjunta) de P y Q es el orden sobre el conjunto $P \dot\cup Q$ (copias disjuntas de P y Q) $x \leq_{P+Q} y$ ssi $(x, y \in P, x \leq_P y)$ o $(x, y \in Q, x \leq_Q y)$. La suma de P consigo mismo n veces se denota nP.

   El diagrama de Hasse de $P+Q$ se obtiene dibujando los diagramas de Hasse de P y de Q independientemente.

2. $P \oplus Q$: Suma ordinal de P y Q es el orden sobre $P \dot\cup Q$ dado por $x \leq_{P+Q} y$ ssi $x \leq_{P+Q} y$ o $(x \in P$ e $y \in Q)$

   Notar que la suma ordinal no es conmutativa: En $P \oplus Q$, todos los elementos de P son menores que los elementos de Q.

3. $P \times Q$: Producto cartesiano de P y Q es el orden en el conjunto $P \times Q$ dado por $(x, y) \leq_{P\times Q} (x', y')$ ssi $x \leq_P x'$ e $y \leq_Q y'$. El producto de un orden P consigo mismo n veces se denota P^n.

4. $P \cap Q$: Intersección de P y Q es el orden dado por $x \leq_{P\cap Q} y$ ssi $x \leq_P$ y $x \leq_Q y$. Esta operación típicamente se usa en ordenes sobre el mismo conjunto.

5. $P^{\bullet Q}$: Funciones monótonas de Q en P. Este es el orden sobre el conjunto $\{f\colon Q \to P,$ monótona $\}$ donde $f \leq_{P^{(Q)}} g$ si y solo si $f(t) \leq g(t)$ para todo $t \in Q$.

Obs: La suma disjunta, el producto y la intersección de familias arbitrarias de órdenes se definen análogamente.
Obs: El "punto" en el exponente está alli para diferenciarlo de P^Q que son todas las funciones de Q en P. Pero muchos autores no hacen la diferencia y escriben P^Q en vez de $P^{\bullet Q}$.

Nota: Como ejercicio, ilustrar las 3 primeras operaciones con $P = [2]$ y $Q = [3]$ (cadenas de 2 y 3 elementos) dibujando los diagramas de Hasse de $[2] + [3]$, $[2] \oplus [3]$ y $[2] \times [3]$.

Veamos un par de ejemplos para entender la última operación:

Ejemplo 1:
Sean $P = n[1]$ y $Q = k[1]$ (Es decir, P y Q son anticadenas de largo n y k resp.). Entonces $P^{\bullet Q}$ es isomorfo a $n^k[1]$.

En efecto, toda función de Q a P es trivialmente monótona. Además, si $f, g \in P^{\bullet Q}$ tenemos que $f \leq g$ ssi $f(t) \leq g(t)$, para todo $t \in Q$. Como Q es una anticadena, ésto es si y solo si $f = g$. En otras palabras los elementos de $P^{\bullet Q}$ son par a par incomparables.

Ejemplo 2:
El orden $[2]^{\bullet[2]}$ es isomorfo a $[3]$.
Hay solo 3 funciones monótonas de $[2]$ a $[2]$: f_1, la función constante igual a 1; f_2, la identidad; y f_3, la función constante igual a 2. Y tenemos que $f_1 \leq f_2 \leq f_3$.

Ejercicio 10.10. Escribimos $P \cong Q$ si P es isomorfo a Q como orden.

- Probar que $[2]^n \cong B_n$.
- Probar que $[2]^{\bullet[n]} \cong [n+1]$.
- Probar que $P^{\bullet(Q+R)} \cong P^{\bullet Q} \times P^{\bullet R}$.
- Probar que $(P^{\bullet Q})^{\bullet R} \cong P^{\bullet(Q\times R)}$.

Capítulo 11

Introducción a funciones generatrices. Recurrencias lineales

El concepto de función generatriz es una de las invenciones más útiles y sorprendentes en Matemáticas Discretas. De una manera informal, las funciones generatrices nos permiten aplicar herramientas analíticas sobre problemas de sucesiones $a\colon \mathbb{N} \to \mathbb{C}$.

11.1. Sucesiones y funciones generatrices

Normalmente podemos codificar un problema de conteo parametrizado por un número natural, mediante una **sucesión**. Por ejemplo, las siguientes sucesiones, a, b y c son las **sucesiones** asociadas a la cardinalidad de $[n]$, al número de permutaciones de $[n]$ y al número de subconjuntos de tamaño n de un conjunto fijo de tamaño 3:

$$\begin{aligned} a &= (0,1,2,3,\dots,n,\dots) & a_n &= n,\\ b &= (1,1,2,6,\dots,n!,\dots) & b_n &= n!,\\ c &= (1,3,3,1,0,\dots) & c_n &= \binom{3}{n}. \end{aligned}$$

En el caso que una sucesión tenga sólo un número finito de valores no nulos, es costumbre cortar la sucesión en el último término distinto de 0. En este caso decimos que la sucesión es finita. Por ejemplo, la sucesión c definida antes se escribe $c = (1,3,3,1)$. La sucesión constante igual a 0, se puede escribir como (0) o como $()$.

Definición 11.1. El conjunto de todas las sucesiones es $\mathbb{C}^{\mathbb{N}} = \{a\colon \mathbb{N} \to \mathbb{C}\}$. El grado[1] de una sucesión $a \in \mathbb{C}^{\mathbb{N}}$ es el máximo n tal que $a_n \neq 0$. Si a no es finita entonces decimos que tiene grado infinito. Denotamos el grado de a como $\deg(a)$. El grado de la sucesión 0 se define como $-\infty$.

A toda sucesión s de grado $k \leq +\infty$ le podemos asociar un **polinomio** a coeficientes complejos, $F_s(x) = \sum_{i=0}^{k} s_i x^i$ de grado k (usando la notación estándar de grado de polinomio donde el grado del polinomio 0 es $-\infty$ y el grado de un polinomio no nulo es la mayor potencia de x que aparece con coeficiente no nulo). Por ejemplo la sucesión $c = (1,3,3,1)$ de grado 3 se puede identificar con el polinomio $1 + 3x + 3x^2 + x^3$, el que podemos escribir compactamente usando el producto estándar de polinomios como $(1+x)^3$. Extendemos esta notación a secuencias infinitas de la siguiente manera.

Definición 11.2. (**Función generatriz ordinaria**). Dada una variable indeterminada x, y una sucesión $a \in \mathbb{C}^{\mathbb{N}}$, llamamos **función generatriz ordinaria** (FGO) asociada a a a la serie formal

$$F_a(x) = \sum_{n \geq 0} a_n x^n.$$

Algunos autores denotan $G(a;x)$ a la FGO de la secuencia a con indeterminada x. Denotamos por $\mathbb{C}[[x]]$ al conjunto de FGO a coeficientes complejos, con indeterminada x.

[1] Esta definición no es estándar, pero su uso se justifica en el siguiente párrafo.

Los objetos en $\mathbb{C}[[x]]$ son *series formales* pues están definida como un concepto algebraico (abstracto), no como un concepto analítico donde tenga sentido *evaluar*. Por ejemplo, para la sucesión b definida al principio del capítulo, $F_b(x) = \sum_{n\in\mathbb{N}} n!x^n$. Esta expresión, vista como función de $\mathbb{C}$ en $\mathbb{C}$ sólo converge si $x = 0$: $F_b(0) = 1$. Lo mismo pasa con la expresión $G(x) = \sum_{n\in\mathbb{N}}(2n)!x^n$. Es decir, F_b y G son iguales como funciones pero nosotros las consideraremos como objetos distintos pues tienen distintos coeficientes. La siguiente notación será util para aclarar esto.

Definición 11.3. Dada una serie formal $F(x) \in \mathbb{C}[[x]]$ y un número $k \in \mathbb{N}$, denotamos por $[x^k]F(x)$ al coeficiente asociado a x^k

Definición 11.4. Dos elementos $F, G \in \mathbb{C}[[x]]$ son iguales si y solo si $[x^k]F(x) = [x^k]G[x]$ para todo $k \in \mathbb{N}$.

Definición 11.5. La sucesión asociada a $F \in \mathbb{C}[[x]]$ es la sucesión $s(F) = ([x^k]F(x))_{k\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$. Es decir, la única sucesión tal que F es FGO de s.

Definición 11.6. A pesar que no evaluaremos simbólicamente $F(x)$, denotamos por conveniencia $F(0) = [x^0]F(x)$.

En otras palabras (hasta ahora) una FGO no es más que otra forma de expresar sucesiones. Desde el punto de vista de la combinatoria, las series formales más interesantes son las FGO de secuencias asociadas a las secuencias que cuentan la cardinalidad de familias de conjuntos (en particular, todos los coeficientes son números naturales).

Como ya dijimos, normalmente no veremos las series formales como funciones sino como objetos abstractos sobre los cuales podemos hacer ciertas operaciones.

Definición 11.7. (**Operaciones sobre sucesiones y series formales**) Las siguientes operaciones unarias y binarias se definen en $\mathbb{C}^{\mathbb{N}}$ y en $\mathbb{C}[[x]]$. Sean a y b en $\mathbb{C}^{\mathbb{N}}$, y sus FGO asociadas F_a y F_b. Sea además $\lambda \in \mathbb{C}$.

Operación	En secuencias	En FGO
Suma	$(a+b)_n = a_n + b_n$	$(F_a + F_b)(x) = \sum_{n\geq 0}(a_n + b_n)x^n$.
Ponderación	$(\lambda a)_n = \lambda a_n$	$\lambda F_a(x) = \sum_{n\geq 0} \lambda a_n x^n$
Convolución/Producto	$(a \cdot b)_n = \sum_{k=0}^{n} a_k b_{n-k}$	$(F_a F_b)(x) = \sum_{n\geq 0} (\sum_{k=0}^{n} a_k b_{n-k})\, x^n$
Escalamiento	$--$	$F_a(\lambda x) = \sum_{n\geq 0} a_n \lambda^n x^n$.

Observación 11.8. La multiplicación está definida de modo que las reglas habituales de álgebra de polinomios se cumplan, por ejemplo $x^i x^j = x^{i+j}$. Notemos que la suma y multiplicación de series están definidas de tal forma que el coeficiente que aparece frente a x^k en el resultado se obtiene operando una cantidad finita de coeficientes de los dos operandos. Por esta razon uno puede sumar y multiplicar sin preocuparse de las típicas preguntas de convergencia absoluta, condicional o uniforme que son tipicas en cálculo y análisis.

Dadas las operaciones anteriores, tiene sentido definir ciertas secuencias especiales.

Definición 11.9.
Llamamos 0 a la secuencia $(0) \in \mathbb{C}^{\mathbb{N}}$ y también a su FGO asociada.
Llamamos 1 a la secuencia $(1) \in \mathbb{C}^{\mathbb{N}}$ y también a su FGO asociada.
Llamamos Δ a la secuencia $(0, 1) \in \mathbb{C}^{\mathbb{N}}$. Su FGO asociada es $F_\Delta(x) = x$.
Para $\lambda \in \mathbb{C}$, llamamos

$$\underline{\lambda} = (1, \lambda, \lambda^2, \dots),$$

a la secuencia con $(\underline{\lambda})_n = \lambda^n$.

Proposición 11.10. *La estructura $(\mathbb{C}[[x]], +, \cdot)$ es un anillo conmutativo con unidad. Es decir, la suma es asociativa, conmutativa, tiene neutro aditivo 0, y todo elemento F tiene inverso $-F := (-1)F$, el producto es asociativo, conmutativo, tiene neutro multiplicativo 1, y distribuye sobre la suma.*

Además, no hay divisores de 0 (si $F(x)G(x) = 0$ entonces $F(x) = 0$ o $G(x) = 0$) por lo cual, en particular hay cancelación*: si $F(x)G(x) = F(x)H(x)$ entonces $G(x) = H(x)$, sin importar si $F(x)$ tiene o no inverso.*

$(\mathbb{C}[[x]], +)$ es un espacio vectorial sobre $\mathbb{C}$ (es decir, la ponderación por escalar es compatible con el producto, y también distribuye sobre la suma), cuya base canónica (infinita) es $(x^0, x^1, x^2, \dots)$. Gracias a esto $(\mathbb{C}[[x]], +, \cdot)$ es un álgebra sobre $\mathbb{C}$.

Demostración. Propuesta como ejercicio. □

Veamos una caracterización de los elementos invertibles de $\mathbb{C}[[x]]$.

Proposición 11.11. *$F(x)^{-1}$ existe si y solo si $F(0) \neq 0$.*

Demostración. Sean $F = F_a$, $G = F_b$ para $a, b \in S$, tales que $F(x)G(x) = 1$. Entonces, $a_0 b_0 = 1$, y para todo $n \geq 1$, $\sum_{k=0}^{n} a_k b_{n-k} = 0$. De aquí se tiene que $b_0 = 1/a_0$ y que $b_n = \frac{-1}{a_0} \sum_{k=1}^{n} a_k b_{n-k}$. □

Cuando $F(x)^{-1}$ existe, la escribimos como $1/F(x)$ sin problemas. También lo hacemos para la sucesión asociada.

Enunciamos algunas propiedades de las series formales.

Antes de estudiar más propiedades de las series formales. Veamos mediante ejemplos que sucede al multiplicar una sucesión por una sucesión finita. Sea $a \in \mathbb{C}^{\mathbb{N}}$.

$$\begin{aligned}(a \cdot (1,-1))_n &= a_n - a_{n-1}\\ (a \cdot (1,-1,-1))_n &= a_n - a_{n-1} - a_{n-2}.\\ (a \cdot (1,-2,1))_n &= a_n - 2a_{n-1} + a_{n-2}.\end{aligned}$$

Donde estamos suponiendo que $a_n = 0$, para $n < 0$. De aquí se ve que si el último término no nulo de b es b_k, entonces el término n-ésimo de $(a \cdot b)$ es combinación lineal de los términos $a_n, \ldots, a_{n-k}$. Es decir:

Proposición 11.12. *Sean $a, f \in \mathbb{C}^{\mathbb{N}}$ dos sucesiones, donde a es una sucesión finita de grado k*

jsoto. Introducir el concepto de grado y orden antes

. Entonces

$$(a \cdot f)_n = f_n a_0 + f_{n-1} a_1 + \cdots + f_{n-k} a_k,$$

donde interpretamos $f_t = 0$ si $t < 0$.

Lo interesante de lo anterior es que nos permite escribir de manera compacta **recurrencias lineales** como ecuaciones.

11.2. Recurrencias lineales

jsoto. Agregar definición de recurrencia lineal

Proposición 11.13. *Toda recurrencia lineal para a se puede escribir como una ecuación en secuencias $ab = c$. Luego, su solución es $a = cb^{-1}$.*

Ejemplo 11.14.

$$\left.\begin{aligned} a_n - a_{n-1} &= 0\\ a_0 &= k.\end{aligned}\right\} \quad a \cdot (1,-1) = (k). \tag{R1}$$

$$\left.\begin{aligned} a_n - 2a_{n-1} + a_{n-2} &= 0\\ a_0 &= k\\ a_1 &= \ell\end{aligned}\right\} \quad a \cdot (1,-2,1) = (k, \ell - 2k). \tag{R2}$$

$$\left.\begin{aligned} a_n - a_{n-1} - a_{n-2} &= m\\ a_0 &= k\\ a_1 &= \ell\end{aligned}\right\} \quad a \cdot (1,-1,-1) = (k, \ell - k, m, m, \ldots) = (k-m, \ell - k - m) + m(\underline{1}). \tag{R3}$$

Calcular el inverso de una secuencia puede llevar a resolver una nueva recurrencia. Sin embargo en ocasiones resulta ser simple.

Proposición 11.15. $(\underline{\lambda})^{-1} = (1, -\lambda)$. *O equivalentemente* $\frac{1}{1-\lambda x} = \sum_{n \geq 0} \lambda^n x^n$.

Demostración.

$$((1,-\lambda) \cdot (\underline{\lambda}))_n = (\underline{\lambda})_n - \lambda(\underline{\lambda})_{n-1} = \begin{cases} \lambda^n - \lambda^n = 0, & \text{para } n \geq 1,\\ \lambda^0 = 1, & \text{para } n = 0.\end{cases}$$ □

De aquí tenemos la solución a nuestra la recurrencia trivial (R1): $a = (k) \cdot (1,-1)^{-1} = (k) \cdot (\underline{1}) = k(\underline{1})$. También pudimos haberla resuelto usando FGO's como sigue: $F_a(x) \cdot (1-x) = k$ implica que $F_a(x) = k \sum_{n\geq 0} n^k$. Por lo cual $a_n = [x^n]F_a(x) = k$.

Veamos como resolver (R2). Es fácil ver que $(1,-2,1) = (1,-1)^2$. Y que $((1,-1)^{-2})_n = ((\underline{1})^2)_n = n+1$. Luego la segunda recurrencia tiene por solución $a = (k, \ell - 2k) \cdot (1,-1)^{-2} = (k, \ell-2k) \cdot (\underline{1}^2)$. Es decir $a_n = k(\underline{1}^2)_n + (\ell - 2k)(\underline{1}^2)_{n-1} = k(n+1) + (\ell - 2k)n = k + n\ell - kn$.

Resolveremos (R3) mediante FGO. Sabemos que

$$\begin{aligned} F_a(x) &= \frac{1}{(1-x-x^2)} \left(k - m + (\ell - k - m)x + m \sum_{n\geq 0} x^n \right) \\ &= \frac{1}{1-x-x^2} \left(k - m + (\ell - k - m)x + m/(1-x) \right) \\ &= \frac{A + Bx + Cx^2}{(1-\alpha x)(1-\beta x)(1-x)}, \end{aligned}$$

donde A, B, C son constantes en $\mathbb{C}$ y $(1-\alpha x)(1-\beta x) = (1-x-x^2)$. Es decir, α, β son las raices de $x^2 - x - 1$. ($\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}$).

Usando fracciones parciales, $F_a(x)$ se puede escribir como

$$\begin{aligned} F_a(x) &= \frac{A'}{(1-\alpha x)} + \frac{B'}{(1-\beta x)} + \frac{C'}{1-x} \\ &= \sum_{n\geq 0} (A'\alpha^n + B'\beta^n + C')x^n. \end{aligned}$$

Con A', B', C' constantes a determinar de las condiciones iniciales.

Por ejemplo, para la sucesión de Fibonacci, $f_0 = 0, f_1 = 1, f_n = f_{n-1} + f_{n-2}$. La FGO nos da

$$F(x) = \frac{x}{1-x-x^2} = \frac{1}{\alpha - \beta} \left(\frac{1}{1-\alpha x} - \frac{1}{1-\beta x} \right) = \sum_{n\geq 0} \frac{(\alpha^n - \beta^n)}{\alpha - \beta} x^n.$$

De aquí uno deduce la fórmula de Binet:

$$f_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

Cabe notar que la deducción de la función generatriz asociada a una recurrencia lineal no requiere mucho trabajo. No es necesario deducir la convolución como lo hicimos antes sino que podemos manipular la ecuación formalmente.

Por ejemplo, para la recurrencia $a_n = Ca_{n-1} + Da_{n-2} + E$, podemos escribir la FGO de a como sigue

$$\begin{aligned} F_a(x) &= \sum_{n\geq 0} a_n x^n = a_0 + a_1 x + \sum_{n\geq 2} a_n x^n \\ &= a_0 + a_1 x + \sum_{n\geq 2} (Ca_{n-1} + Da_{n-2} + E)x^n \\ &= a_0 + a_1 x + Cx \sum_{n\geq 2} a_{n-1} x^{n-1} + Dx^2 \sum_{n\geq 2} a_{n-2} x^{n-2} + E \sum_{n\geq 2} x^n \\ &= a_0 + a_1 x + Cx(F_a(x) - a_0) + Dx^2 F_a(x) + \frac{E}{1-x}. \end{aligned}$$

Despejando, se tiene

$$F_a(x) = \frac{a_0 + x(a_1 - Ca_0) + E/(1-x)}{1 - Cx - Dx^2}.$$

Usando la técnica anterior podemos resolver cualquier recurrencia lineal, en la medida que sepamos invertir polinomios (es decir, series formales con finitos términos).

Sea $a = (a_0, \dots, a_k)$ con $a_0 \neq 0$ y $F_a(x)$ su FGO (polinomio) asociado. Como $F_a(x) \in \mathbb{C}[x] \subseteq \mathbb{C}[[x]]$ (es decir es un polinomio complejo), se puede factorizar completamente en términos lineales. De hecho es más conveniente factorizarlo de la siguiente manera.

$$F_a(x) = C(1 - \lambda_1 x)^{m_1}(1 - \lambda_2 x)^{m_2} \cdots (1 - \lambda_s x)^{m_s},$$

De aquí,

$$F_a(x)^{-1} = \frac{1}{C}\prod_{j=1}^{s}(x - \lambda_j)^{-m_j} = \frac{1}{C}\prod_{j=1}^{s}\left(\sum_{n\geq 0}\lambda_j^n x^n\right)^{m_j} = \frac{1}{C}\prod_{j=1}^{s}F_{\underline{(\lambda_j)}}(x)^{m_j} = \frac{1}{C}\prod_{j=1}^{s}F_{\underline{(1)}}(\lambda x)^{m_j}$$

Es útil entonces estudiar las potencias de $F_{\underline{1}}(x) = \sum_{n\geq 0} x^n$.

$$\begin{aligned}[x^j]\Big(\sum_{n\geq 0}x^n\Big)^m &= [x^j] \sum_{(\alpha_1,\dots,\alpha_m)\in\mathbb{N}^m,\sum_{i=1}^m \alpha_i = j} x^{\alpha_1}x^{\alpha_2}\cdots x^{\alpha_m} \\ &= |\operatorname{CD}(j,m)| = \left(\!\!\binom{m}{j}\!\!\right).\end{aligned}$$

Luego

$$\Big(\sum_{n\geq 0}x^n\Big)^m = \sum_{j\geq 0}\left(\!\!\binom{m}{j}\!\!\right)x^j.$$

En otras palabras, para $m \geq 1$,

$$(1-x)^{-m} = \sum_{n\geq 0}\left(\!\!\binom{m}{n}\!\!\right)x^n = \sum_{n\geq 0}\binom{n+m-1}{n}x^n.$$

O bien, escalando x por -1 y usando que $\left(\!\!\binom{m}{n}\!\!\right) = \binom{-m}{n}(-1)^n$, concluimos que

$$(1+x)^{-m} = \sum_{n\geq 0}\left(\!\!\binom{m}{n}\!\!\right)(-x)^n = \sum_{n\geq 0}\binom{-m}{n}x^n.$$

Esta es una generalización del teorema del binomio para exponentes negativos.

Proposición 11.16. *Para todo $m \in \mathbb{Z}$:*

$$(1+x)^m = \sum_{n\geq 0}\binom{m}{n}x^n.$$

Sigamos nuestra discusión de FGO con un problema de caminos.

Problema. Encuentre el número de caminos en el reticulado $\mathbb{Z}^2$ con n pasos, que partan en $(0,0)$, cuyos pasos sean del tipo $N = (0,1)$, $E = (1,0)$, u $O(-1,0)$ y que no se autointersecten.

Demostración. Codifiquemos los caminos pedidos como palabras sobre $\{N, E, O\}$. Como en la dirección vertical el camino es monótono, la condición que no se autointersecte es equivalente a que la palabra no posea a EO ni a OE como factor.

Sea a_n el número pedido. Sea b_n el número de palabras válidas de largo n que no empiezan por E (= a las que no empiezan por O). Condicionando en el primer símbolo, hay a_{n-1} palabras válidas de largo n que empiezan por N, hay b_{n-1} que empiezan por E y b_{n-1} que empiezan por O. Luego, para $n \geq 1$,

$$a_n = a_{n-1} + 2b_{n-1}.$$

Además, por un razonamiento análogo, para $n \geq 1$,

$$b_n = a_{n-1} + b_{n-1}.$$

Luego, $a_{n-1} = b_n - b_{n-1}$. De la primera ecuación iterada dos veces tenemos que para $n \geq 2$:

$$\begin{aligned} a_n - a_{n-1} &= (a_{n-1} + 2b_{n-1}) - (a_{n-2} + 2b_{n-2}) \\ &= a_{n-1} - a_{n-2} + 2(b_{n-1} - b_{n-2}) \\ &= a_{n-1} - a_{n-2} + 2a_{n-2} = a_{n-1} + a_{n-2}. \end{aligned}$$

Luego, a satisface la recurrencia, $a_n = 2a_{n-1} + a_{n-2}$, para $n \geq 2$, $a_0 = 1$, $a_1 = 3$. O bien, $a(1, -2, -1) = (1, 1)$.

Resolviendo tenemos que

$$F_a(x) = \frac{1+x}{1-2x-x^2} = \frac{1+x}{(1-\alpha x)(1-\beta x)}, \text{ donde } \alpha = 1-\sqrt{2},\ \beta = 1+\sqrt{2}$$

Es decir,

$$\begin{aligned} F_a(x) &= \left(\sum_{n\geq 0} \alpha^n x^n\right)\left(\sum_{n\geq 0} \beta^n x^n\right)(1+x) \\ &= (1+x)\sum_{n\geq 0} x^n \sum_{i=0}^{n} \alpha^i \beta^{n-i} = (1+x)\sum_{n\geq 0} (x\beta)^n \sum_{i=0}^{n} (\alpha/\beta)^i \\ &= (1+x)\sum_{n\geq 0} x^n \beta^n \frac{1-(\alpha/\beta)^{n+1}}{1-\alpha/\beta} \\ &= (1+x)\sum_{n\geq 0} x^n \frac{\beta^{n+1}-\alpha^{n+1}}{\beta-\alpha} \end{aligned}$$

O bien,

$$\begin{aligned} a_n &= \frac{\beta^{n+1}-\alpha^{n+1}}{\beta-\alpha} + \frac{\beta^n - \alpha^n}{\beta-\alpha} = \frac{\beta^n(1+\beta) + \alpha^n(1+\alpha)}{2\sqrt{2}} \\ &= \frac{\beta^n(\sqrt{2}\beta) + \alpha^n(\sqrt{2}\alpha)}{2\sqrt{2}} = \frac{\beta^{n+1}+\alpha^{n+1}}{2}. \end{aligned}$$

□

Capítulo 12

Operatoria en series formales

Como ya hemos dicho, es bastante útil trabajar con funciones generatrices debido a nuestra experiencia con series de potencias (A posteriori, sería más adecuado didácticamente primero aprender a usar series y polinomios formales y luego trabajar con funciones seriales o funciones polinomiales). Por ejemplo, podemos definir la serie formal

$$\exp(x) = \sum_{n\geq 0} \frac{x^n}{n!}.$$

Y deducir que exp satisface que $\exp(x)\exp(-x) = \exp(0) = 1$. En efecto en $\mathbb{C}[[x]]$,

$$[x^n]\exp(x)\exp(-x) = \sum_{j=0}^{n} \frac{1}{j!}\frac{(-1)^{n-j}}{(n-j)!} = \frac{1}{n!}\sum_{j=0}^{n}(-1)^{n-j}\binom{n}{j} = \frac{(1-1)^n}{n!} = \delta_{0,n}$$

que se prueba ¡mediante el teorema del binomio!

Así uno está "tentado" a usar todo lo que sabe de series de potencias convergentes y aplicarlo aquí. Sin embargo, hay que ser cuidadoso como lo muestra el siguiente ejemplo.

Ejemplo: La identidad

$$\sum_{n\geq 0}\frac{(x+1)^n}{n!} = e\sum_{n\geq 0}\frac{x^n}{n!},$$

que uno reconoce como $e^{x+1} = e^x \cdot e$, no tiene sentido en $\mathbb{C}[[x]]$, pues $\sum_{n\geq 0}\frac{(x+1)^n}{n!} \notin \mathbb{C}[[x]]$.

Para ver esto, notar que el término constante de la suma anterior es $\sum_{n\geq 0}\frac{1}{n!}$, cuya interpretación como número complejo requiere **conceptos de convergencia en** $\mathbb{C}$ que nosotros no usaremos (propiedades de variable compleja pueden ser útiles en algunos casos, pero para nuestros propósitos, trataremos de evitarlos).

A pesar que no usaremos convergencia en $\mathbb{C}$, necesitaremos en el futuro hablar de ciertos procesos infinitos en $\mathbb{C}[[x]]$, el más importante es que queremos **componer** series. Para esto vamos a tener que introducir un concepto muy estricto de convergencia en $\mathbb{C}[[x]]$.

[Def]

La sucesión $F_i(x) \in \mathbb{C}[[x]]$ **converge**[1] a $F(x) \in \mathbb{C}[[x]]$ si para cada k, la sucesión $[x^k]F_i(x)$ es, a medida que i se va a infinito, eventualmente constante e igual a $[x^k]F(x)$. Es decir, para todo k, existe $m(k)$ tal que para todo $i \geq m(k)$, $[x^k]F_i(x) = [x^k]F(x)$. Nuestra definición de convergencia es muy estricta. Por ejemplo, $(1+x/j)^j$ no converge a $\exp(x)$, pues para $n \geq 2$, $[x^n](1+x/j)^j = \binom{j}{n}/j^n$ no se estabiliza (no es eventualmente constante) cuando $j \to \infty$.

Ahora que sabemos escribir sucesiones convergentes de FGO, podemos definir sumas infinitas de elementos de $\mathbb{C}[[x]]$.

[1] Para los más topológicos o analistas: dotamos a $\mathbb{C}[[x]]$ con la topología producto de $\mathbb{C}^{\mathbb{N}} \cong \mathbb{C}[[x]]$ donde en cada factor usamos la topología discreta de $\mathbb{C}$.

[Def]

Decimos que $\sum_{j\geq 0} F_j(x)$ **vale** $F(x)$, si la secuencia $\sum_{j=0}^{i} F_j(x)$ converge a $F(x)$ en $\mathbb{C}[[x]]$ cuando $i \to \infty$.

Dicho de otra forma, la suma $\sum_{j\geq 0} F_j(x)$ tiene sentido solo cuando para cada k, el coeficiente $[x^k]\sum_{j=0}^{i} F_j(x)$ es eventualmente constante a medida que i se va a infinito. Es decir, $[x^k]\sum_{j\geq 0} F_j(x) = \sum_{j\geq 0}[x^k]F_j(x)$ es en realidad una suma con un número finito de terminos no nulos.

Ejercicio 12.1. [Def]

El orden de $F(x)$ (denotado $\operatorname{ord}(F(x))$) es el índice k más pequeño tal que $[x^k]F(x) \neq 0$. Ejemplo, $x^2 + x^3 + x^4 + \dots$ tiene orden 2. Notar que $\operatorname{ord}(F(x)G(x)) = \operatorname{ord}(F(x)) + \operatorname{ord}(G(x))$.

- Pruebe que $(F_i(x))_i$ converge a $F(x)$ en $\mathbb{C}[[x]]$ ssi
$$\lim_{i\to\infty} \operatorname{ord}(F(x) - F_i(x)) = \infty.$$
- Pruebe que $(F_i(x))_i$ converge en $\mathbb{C}[[x]]$ ssi
$$\lim_{i\to\infty} \operatorname{ord}(F_{i+1}) - \operatorname{ord}(F_i) = \infty.$$
- Pruebe que $\sum_{j\geq 0} F_j(x)$ converge ssi $\lim_{j\to\infty} \operatorname{ord}(F_j(x)) = \infty$.

Ahora estamos listos para definir correctamente la composición de series como sigue.

Sean $F(x), G(x) \in \mathbb{C}[[x]]$ con $F(x) = \sum_{n\geq 0} a_n x^n$, y $G(0) = 0$. Definimos la composición $(F \circ G)(x) = F(G(x))$ como la suma infinita
$$\sum_{n\geq 0} a_n G(x)^n.$$

Esto es lo que uno espera. Notar que como $\operatorname{ord}(G(x)^n) = n\operatorname{ord}(G(x)) \geq n$, tenemos, por el ejercicio que $F(G(x))$ está bien definido como serie formal y por lo tanto, cada coeficiente de $F(G(x))$ se calcula mediante una suma finita.

Por ejemplo, como la serie "$G(x) = x + x^2 + x^3 + \cdots = \frac{x}{1-x}$" no tiene término constante, podemos escribir
$$\exp\left(\frac{x}{1-x}\right) = \sum_{n\geq 0} \frac{1}{n!}\left(\sum_{m\geq 1} x^m\right)^n$$

Comprobemos que los coeficientes se expresan como sumas finitas en $\mathbb{C}$:
$$[x^i]\exp\left(\frac{x}{1-x}\right) = \sum_{n\geq 0} \frac{[x^i]}{n!}\left(\sum_{m\geq 1} x^m\right)^n =$$
$$= \sum_{n\geq 0} \frac{1}{n!}|\operatorname{COM}(i,n)| = \sum_{n=0}^{i} \frac{\binom{i-1}{i-n}}{n!}.$$

La restricción que $G(0) = 0$ es importante para que la composición esté bien definida. Por ejemplo, ya vimos que la expresión $\exp(x+1)$ no tiene sentido pues su suma no estabiliza ni siquiera para el coeficiente asociado a $n = 0$.

Ahora que tenemos la composición podemos usar nuestros teoremas del binomio anteriores para decir que para todo $F(x) \in \mathbb{C}[[x]]$ con $F(0) = 0$, y todo $m \in \mathbb{Z}$
$$(1 + F(x))^m = \sum_{n\geq 0} \binom{m}{n} F(x)^n,$$

Lo último que nos falta en nuestra caja de herramientas es una operación natural que tienen las series de potencias y que nosotros podemos definir en $\mathbb{C}[[x]]$ que es la **derivada formal**.

Si $F(x) = \sum_{n\geq 0} a_n x^n$ entonces $F'(x) = \sum_{n\geq 1} n a_n x^{n-1} = \sum_{n\geq 0}(n+1)a_{n+1}x^n$.

Es fácil ver que tenemos las reglas habitual de derivación:

$$(F(x)+G(x))' = F'(x)+G'(x).$$
$$(F(x)G(x))' = F'(x)G(x)+F(x)G'(x).$$
$$F(G(x))' = F'(G(x))G'(x).$$

Y de hecho, tenemos que cada serie formal es igual a su **serie de Taylor** en el origen, es decir

$$F(x) = \sum_{n\geq 0} \frac{F^{(n)}(0)}{n!}x^n.$$

Aprovechemos este momento para definir la **potencia compleja**. Vimos que para todo $m \in \mathbb{Z}$,

$$(1+x)^m = \sum_{n\geq 0} \binom{m}{n} x^n.$$

Demos un paso más y **definamos** para $\lambda \in \mathbb{C}$,

$$(1+x)^\lambda = \sum_{n\geq 0} \binom{\lambda}{n} x^n. \tag{12.1}$$

Usando composición, esta definición se extiende a

$$(1+F(x))^\lambda = \sum_{n\geq 0} \binom{\lambda}{n} F(x)^n.$$

en la medida que $F(0) = 0$. Notemos que,

$$((1+x)^\lambda)' = \sum_{n\geq 1} \binom{\lambda}{n} n x^{n-1} = \sum_{n\geq 1} \frac{(\lambda)_n}{(n-1)!}x^{n-1} = \lambda \sum_{n\geq 1} \frac{(\lambda-1)_{n-1}}{(n-1)!}x^{n-1} = \lambda(1+x)^{\lambda-1}$$

y en general, la n-ésima derivada de $(1+x)^\lambda$ es $\binom{\lambda}{n} n!(1+x)^{\lambda-n}$.

Este es el único momento de nuestra discusión sobre $\mathbb{C}[[x]]$ en que usaremos "evaluación". Damos la siguiente propiedad cuya demostración omitimos.

Propiedad: Si $F(x)$, $G(x)$ son dos series formales en $\mathbb{C}[[x]]$ tales que, vistas como funciones satisfacen $F(x) = G(x)$ para todo $x \in \mathbb{C}$ en un abierto (en la topología habitual de $\mathbb{C}$) alrededor del cero. Entonces $F(x) = G(x)$ como series formales.

Ojo que la recíproca no es cierta pues existen series formales $F(x) \in \mathbb{C}[[x]]$ que vistas como funciones **sólo convergen** para $x = 0$. Un ejemplo es $\sum_{n\geq 0} n!x^n$. De la propiedad anterior se desprende que para todo $\lambda, \mu \in \mathbb{C}$:

$$(1+x)^{\lambda+\mu} = (1+x)^\lambda (1+x)^\mu$$
$$((1+x)^\lambda)^\mu = (1+((1+x)^\lambda - 1))^\mu = (1+x)^{\lambda\mu}$$

pues ambas expresiones son válidas para $x \in \mathbb{C}$, con $|x| \leq 1$, interpretando ambos lados como sus series de Taylor.

Como corolario, tenemos que las mismas propiedades valen si reemplazamos x por cualquier serie $F(x) \in \mathbb{C}[[x]]$ con $F(0) = 0$ (aquí estamos usando composición).

La discusión anterior nos permite interpretar cualquier función que tenga serie de Taylor convergente en un abierto alrededor del origen como una serie formal que satisface sus mismas propiedades (en la medida que todas las expresiones involucradas estén en $\mathbb{C}[[x]]$). Así podemos definir, por ejemplo

$$L(x) := \ln(1+x) = \sum_{n\geq 1} \frac{(-1)^{n+1}x^n}{n} = -\sum_{n\geq 1} \frac{(-x)^n}{n}$$
$$\operatorname{sen}(x) = \sum_{n\geq 0} \frac{(-1)^n}{(2n+1)!}x^{2n+1}$$
$$\cos(x) = \sum_{n\geq 0} \frac{(-1)^n}{(2n)!}x^{2n},$$

y tenemos que $\text{sen}^2(x) + \cos^2(x) = 1$, $\ln(\exp(x)) = 1$, y $\exp(\ln(1+x)) = 1$, pero curiosamente, no podemos escribir $\ln(x)$ pues esto no está en $\mathbb{C}[[x]]$.

Usando potencias complejas podemos dar una demostración alternativa de la identidad de Chu-Vandermonde siguiente:

Proposición 12.2. *Para $\alpha, \beta \in \mathbb{C}$, $n \in \mathbb{N}$.*

$$\sum_{i=0}^{n} \binom{\alpha}{i}\binom{\beta}{n-i} = \binom{a+b}{n}.$$

Demostración.

$$\begin{aligned}\sum_{i=0}^{n} \binom{\alpha}{i}\binom{\beta}{n-i} &= [x^n]\left((\sum_{m\geq 0}\binom{\alpha}{m}x^m)(\sum_{m\geq 0}\binom{\beta}{m}x^m)\right)\\ &= [x^n]((1+x)^\alpha(1+x)^\beta)\\ &= [x^n](1+x)^{\alpha+\beta}\\ &= \binom{\alpha+\beta}{n}.\end{aligned}$$

□

Binomiales

En ocasiones es útil considerar series formales en más de una variable (es decir, trabajar en el anillo $\mathbb{C}[[x,y]]$ o en $\mathbb{C}[[x_1,\ldots,x_k]]$, etc.)

Ya sabemos que la FGO de la secuencia $a_k = \binom{n}{k}$ es $(1+x)^k$. ¿Cuál es la FGO de $a_n = \binom{n}{k}$?

Para esto es mejor definir $b_{k,n} = \binom{n}{k}$ y trabajar con

$$\begin{aligned}A(x,y) &= \sum_{n\geq 0}\sum_{k\geq 0} b_{k,n}x^k y^n = \sum_{n\geq 0}\sum_{k\geq 0}\binom{n}{k}x^k y^n\\ &= \sum_{n\geq 0}(1+x)^n y^n\\ &= \sum_{n\geq 0}((1+x)y)^n\\ &= \frac{1}{1-(1+x)y} = \frac{1}{1-y-xy}.\end{aligned}$$

Veamos que se deduce de aquí.

1.
$$[x^k]A(x,y) = \sum_{n\geq 0} y^n[x^k y^n]A(x,y) = \sum_{n\geq 0} y^n\binom{n}{k}.$$

Luego $[x^k]A(x,y)$ es la FGO que buscamos. Desarrollemos tratando de aislar x^k.

$$\begin{aligned}A(x,y) &= \frac{1}{(1-y)-xy} = \frac{1/(1-y)}{1-xy/(1-y)}\\ &= \frac{1}{1-y}\sum_{k\geq 0}\left(\frac{xy}{1-y}\right)^k = \sum_{k\geq 0}\frac{1}{1-y}\left(\frac{y}{1-y}\right)^k x^k.\end{aligned}$$

Es decir, la FGO de $a = (\binom{0}{k}, \binom{1}{k}, \ldots, \binom{n}{k}, \ldots)$ es

$$[x^k]A(x,y) = \frac{y^k}{(1-y)^{k+1}}.$$

(Notar que los términos a_n son 0 para $n < k$).

2. Un corolario interesante se obtiene evaluando $A(x, y)$ en $x = y$:

$$\frac{1}{1-x-x^2} = A(x,x) = \sum_{n\geq 0}\sum_{k\geq 0}\binom{n}{k}x^{n+k} = \sum_{m\geq 0} x^m \sum_{i\geq 0}\binom{m-i}{i}$$

Recordando que $\frac{x}{1-x-x^2}$ es la FGO de los números de Fibonacci tenemos que:

$$f_{m+1} = [x^m]A(x,x) = \sum_{i\geq 0}\binom{m-i}{i}.$$

Números de Catalán.

Problema:
Encontrar la única sucesión $a \in S$ que satisface $a_0 = 1$, y

$$\sum_{k=0}^{n} a_k a_{n-k} = 1.$$

Demostración. El lado izquierdo de la expresión anterior es igual a $(a^2)_n$. En otras palabras, la ecuación anterior es igual a $(a^2) = (\underline{1})$ o equivalentemente,

$$(F_a(x))^2 = \sum_{n\geq 0} x^n = \frac{1}{1-x}.$$

Luego, hay dos opciones para $F_a(x)$,

$$\begin{aligned} F_a(x) &= \pm(1-x)^{-1/2} \\ &= \pm\sum_{n\geq 0}\binom{-1/2}{n}(-1)^n x^n. \end{aligned}$$

Como $F_a(0) = 1$ tenemos que el signo correcto es el positivo. Es decir,

$$\begin{aligned} a_n &= (-1)^n\binom{-1/2}{n} \\ &= (-1)^n\frac{(-\frac{1}{2})(-\frac{3}{2})(-\frac{5}{2})\cdots(-\frac{2n-1}{2}}{n!} \\ &= \frac{1\cdot 3\cdot 5\cdots(2n-1)}{2^n n!} \\ &= \frac{(2n)!}{(2\cdot 4\cdot 6\cdots(2n))2^n n!} \\ &= \frac{(2n)!}{n!^2 2^{2n}} = \binom{2n}{n}\frac{1}{4^n}. \end{aligned}$$

□

Problema: Determine el número C_n de formas de triangular un polígono regular de $(n+2)$ lados usando $(n+1)$ diagonales que no se intersecten. Por conveniencia, defina además $C_0 = C_1 = 1$.

Lo primero que debemos hacer es encontrar una recurrencia para C_n. Sea $n \geq 1$, sea P el polígono de $n+2$ lados y sea ℓ un lado cualquiera. Cualquier triangulación deja a ℓ en un triángulo T_ℓ fijo. Al remover ℓ obtenemos dos poligonos triangulados, el "superior" de i lados y el "inferior" de j lados, con $i+j = n+3$, es decir, $(i-2)+(j-2) = n-1$. De aquí se tiene que

$$C_n = C_0C_{n-1} + C_1C_{n-2} + \cdots + C_{n-1}C_0 = \sum_{k\geq 0} C_kC_{n-1-k} = (C\cdot C)_{n-1}.$$

Es decir, si llamamos $F(x)$ a la FGO de C, tenemos que

$$xF(x)^2 = x\sum_{n\geq 0} x^n \sum_{k\geq 0} C_kC_{n-k} = \sum_{n\geq 0} x^{n+1}C_{n+1} = -C_0 + \sum_{n\geq 0} x^nC_n = -1 + F(x).$$

Es decir, $xF^2 = F - 1$. O bien, $xF^2 - F + 1 = 0$. De aquí se tiene que

$$F(x) = \frac{1 \pm \sqrt{1-4x}}{2x}.$$

Como $F(0) = C_0 = 1$, el signo correcto es el menos. (La expresión no es del todo corecta, pues estamos dividiendo por x. Sin embargo, al elegir el signo menos todo sale bien pues el numerador tiene orden 1. Es decir, no tiene termino constante)

De aquí tenemos por el Teorema del Binomio que

$$\begin{aligned}
\frac{1-\sqrt{1-4x}}{2x} &= \frac{-1}{2x}\sum_{n\geq 1}\binom{1/2}{n}(-4x)^n = \frac{-1}{2x}\sum_{n\geq 1}\frac{(1/2)}{n}\binom{-1/2}{n-1}(-4x)^n \\
&= \frac{-1}{4x}\sum_{n\geq 0}\frac{1}{n+1}\binom{-1/2}{n}(-4x)^{n+1} \\
&= \sum_{n\geq 0}\frac{1}{n+1}\binom{2n}{n}x^n.
\end{aligned}$$

Es decir, $C_n = \frac{1}{n+1}\binom{2n}{n}$. Los números de Catalan aparecen en todas partes. Por ejemplo cuentan las palabras sobre $\{(,)\}$ que están "bien parentizadas".

Capítulo 13

Método simbólico para objetos no etiquetados

Definición 13.1. Una **clase combinatorial** es un conjunto finito o numerable $\mathcal{A}$, junto a una función de tamaño $|\cdot|_{\mathcal{A}}\colon \mathcal{A} \to \mathbb{N}$ que satisface que para cada $i \in \mathbb{N}$,

$$\mathcal{A}_{(i)} = \{x \in \mathcal{A}\colon |x|_{\mathcal{A}} = i\}$$

es finito. Normalmente anotamos $|\cdot|_{\mathcal{A}}$ simplemente como $|\cdot|$.

Definición 13.2. La **secuencia de conteo** de $\mathcal{A}$ es $(a_n)_{n\in\mathbb{N}}$ con $a(i) = |\mathcal{A}_i|$. La FGO

$$A(x) = \sum_{n\geq 0} a_n x^n = \sum_{a\in\mathcal{A}} x^{w(a)},$$

se conoce como la FGO de la clase $\mathcal{A}$.

Observación 13.3. Por comodidad, usaremos la siguiente convención. La clase, su secuencia de conteo y su FGO son denotadas con la misma letra pero en distinta fuente. La clase se denota con letra caligráfica, la secuencia de conteo con letra en minúscula, y la FGO con la misma letra en mayúscula: Por ejemplo $(\mathcal{B}, b_n, B(x)), (\mathcal{C}, c_n, C(x))$

Ejemplo 13.4. Sea $N \in \mathbb{N}$. La clase combinatorial $\mathcal{P} := \mathcal{P}([N])$ con función de tamaño $w(X) = |X|$, tiene como secuencia de conteo $p_n = \binom{N}{n}$ y FGO $P(x) = (1+x)^N$.

Definimos dos clases combinatoriales especiales

Definición 13.5. La clase neutra $\mathcal{E}$ tiene un solo elemento, llamado ε, de peso 0.
La clase atómica $\mathcal{Z}$ tiene un solo elemento, llamado $\bullet$, de peso 1.

En ocasiones nos convendrá definir varias clases atómicas (cuyos elementos recibirán diferentes nombres) por ejemplo podemos escribir $\mathcal{Z}_a = \{a\}$ donde a es un elemento de peso 1.

Las clases anteriores reciben su nombre del hecho que $E(x) = x^0 = 1$ y $Z(x) = x^1 = x$.

La gracia de usar clases combinatoriales es que podemos obtener nuevas clases a partir de clases más simples mediante algunas operaciones. Podemos definir la intersección de dos clases combinatoriales $\mathcal{A} \cap \mathcal{B}$ como su intersección a nivel de conjuntos *solamente* si la función de largos coincide en la intersección. Asimismo podemos definir la unión de dos clases combinatoriales $\mathcal{A} \cup \mathcal{B}$ de la manera natural en la medida que su función de largo coincida en la intersección de ambas clases. Las siguientes operaciones son más generales (y más utiles).

Definición 13.6. La suma de clases combinatoriales $\mathcal{A} + \mathcal{B}$ es simplemente la clase

$$\mathcal{A} + \mathcal{B} = \mathcal{A} \cup \mathcal{B},$$

suponiendo que ambas son disjuntas (si no, trabajamos con $\mathcal{A} \times \varepsilon_1$ y $\mathcal{A} \times \varepsilon_2$).

La gracia de la suma por sobre la unión es que está siempre definida. Se tiene directamente que si $\mathcal{C} = \mathcal{A} + \mathcal{B}$ entonces

$$C(x) = \sum_{c\in\mathcal{A}+\mathcal{B}} x^{w(c)} = \sum_{c\in\mathcal{A}} x^{w(c)} + \mathcal{B}x^{w(c)} = A(x) + B(x).$$

Definición 13.7. El producto (concatenación) de dos clases combinatoriales $\mathcal{A}$ y $\mathcal{B}$ es

$$\mathcal{A} \cdot \mathcal{B} = \{ab \colon a \in \mathcal{A}, b \in \mathcal{B}\}.$$

En general, el producto de una secuencia de clases combinatoriales $\mathcal{A}_1, \mathcal{A}_2, \ldots \mathcal{A}_k$ es el conjunto de palabras con i-ésimo simbolo en $\mathcal{A}_i$, es decir

$$\prod_{i=1}^{k} \mathcal{A}_i = \{w_1 w_2 \ldots w_k \colon w_i \in \mathcal{A}_i.$$

La función de tamaño de una secuencia $w \in \prod_{i=1}^{k} \mathcal{A}_i$ se define como

$$|w| = |w_1| + |w_2| + \cdots + |w_k|$$

Esta definición de largo se adecúa bien al concepto de palabra: El largo de la concatenación de dos palabras es la suma de las palabras que la componen.

Definición 13.8. El producto de dos clases combinatoriales $\mathcal{A}$ y $\mathcal{B}$ es

$$\mathcal{A} \times \mathcal{B} = \{ab \colon a \in \mathcal{A}, b \in \mathcal{B}\}.$$

En general, el producto de una secuencia de clases combinatoriales $\mathcal{A}_1, \mathcal{A}_2, \ldots \mathcal{A}_k$ es el conjunto de palabras con i-ésimo simbolo en $\mathcal{A}_i$, es decir

$$\prod_{i=1}^{k} \mathcal{A}_i = \{(w_1, w_2, \ldots, w_k) \colon w_i \in \mathcal{A}_i.$$

La función de tamaño de una secuencia $w \in \prod_{i=1}^{k} \mathcal{A}_i$ se define como

$$|w| = |w_1| + |w_2| + \cdots + |w_k|$$

Observación 13.9. Aclaración importante.

Si $w \in \prod_{i=1}^{k} \mathcal{A}_i$, entonces siempre podemos identificar los factores $w_i \in \mathcal{A}_i$ tal que $w = (w_1, \ldots, w_k)$. Esto es a diferencia de lo que pasa con la concatenación de palabras: Si $\mathcal{A} = \{1, 11\}$ y $\mathcal{B} = \{2, 12\}$ entonces la palabra 112 se obtiene de dos maneras como concatenación de una palabra de $\mathcal{A}$ con una palabra de $\mathcal{B}$: $(1, 12)$ y $(11, 2)$.

La **secuencia** de una clase combinatorial $\mathcal{A}$ se define como

$$\mathrm{Seq}(\mathcal{A}) = \varepsilon + \mathcal{A} + \mathcal{A}^2 + \cdots = \sum_{n \geq 0} \mathcal{A}^n.$$

Es fácil ver que $\mathrm{Seq}(\mathcal{A})$ es una clase combinatorial y que su FGO es $(1 - A(x))^{-1}$.

Ejemplos

Palabras de largo 1 **sobre el alfabeto** Σ**, (tamaño = largo):** Clase combinatorial Σ, con FGO, $|\Sigma|x$.

Palabras finitas sobre el alfabeto $[k]$**:** Clase combinatorial

$$\Sigma^* = \varepsilon + \Sigma + \Sigma^2 + \cdots = S(\Sigma), \text{con FGO } (1 - |\Sigma|x)^{-1}.$$

Ejemplo rebuscado: si $\Sigma = [k]$, entonces, el número de palabras de largo n sobre Σ es $[x^n](1 - kx)^{-1} = k^n$.

Problema: ¿Cuántas palabras de largo n sobre $[k]$ no tienen a $k1$ como subpalabra.

Sea $\mathcal{L}$ la clase combinatorial de las palabras sobre $[k]$ que no tienen a $k1$ como subpalabra. Llamemos $\mathcal{L}_0$ a la clase $[k-1]^*$ y $\mathcal{L}_1$ a la clase combinatorial de las palabras sobre $[k]$ que parten en k, su segundo símbolo esta en $[k-1] \setminus \{1\}$, y el resto de los simbolos están en $[k-1]$. Finalmente, sea $\mathcal{L}_2 = \{k\} + \mathcal{L}_1$

Notemos que toda palabra en $w \in \mathcal{L}$ se escribe de manera única como una palabra en $\mathcal{L}_0$ seguida de cero o más palabras en $\mathcal{L}_2$. Luego podemos verlo como

$$\mathcal{L} = \mathcal{L}_0 \times (\mathcal{L}_2)^* = [k-1]^* \times (\{k\} + \mathcal{L}_1)^*$$

De aquí tenemos que

$$L(x) = L_0(x) \cdot \frac{1}{1-(x+L_1(x))}$$

Como además

$$\mathcal{L}_1 = \{k\} \cdot ([k-1] \setminus \{1\}) \cdot \mathcal{L}_0$$

tenemos que

$$L_1(x) = L_0(x) \cdot (k-2)x^2$$

y luego

$$\begin{aligned} L(x) &= \frac{L_0(x)}{1-(x+(k-2)x^2L_0(x))} = \frac{L_0(x)}{1-x-(k-2)x^2L_0(x)} = \frac{1}{\frac{1-x}{L_0(x)}-(k-2)x^2} \\ &= \frac{1}{(1-x)(1-(k-1)x)-(k-2)x^2} = \frac{1}{1-x-(k-1)x+(k-1)x^2-(k-2)x^2} \\ &= \frac{1}{1-kx+x^2}. \end{aligned}$$

Alternativamente, podemos factorizar

$$\mathcal{L} = \mathcal{L}_0 \times \{k\} \times \{k^*\}(([k-1] \setminus \{1\}) \times \mathcal{L}_0 \times \{k\} \times \{k^*\})^*$$

Con lo que obtenemos

$$\begin{aligned} L(x) &= \frac{L_0(x)}{1-(\frac{x}{1-x} \cdot (k-2)x \cdot L_0(x))} = \frac{(1-x)L_0(x)}{1-x-(k-2)x^2L_0(x)} \\ &= \frac{(1-kx)}{(1-kx)(1-(k-1)x)-(k-2)x^2L_0(x)} = \frac{(1-kx)}{1-(2k-1)x+(k^2-2k+2)x^2} \end{aligned}$$

Problema: ¿Cuántas palabras de largo n sobre el alfabeto $[k]$ no tienen dos k consecutivos.

Sea L_k el conjunto de palabras sobre $[k]$ sin dos k consecutivos, y sea $F_k(x)$ su FGO. Partamos con el caso $k=2$. Sea x una palabra de L_2. Si x empieza con 1 entonces $x = 1y$ con $y \in L_2$. Si x empieza con 2 (y $x \neq 2$), entonces su siguiente simbolo debe ser 1, es decir $x = 21y$ con $y \in L_2$. De aquí deducimos que

$$L_2 = \varepsilon + \{2\} + \{1\} \times L_2 + \{21\} \times L_2$$

Y luego

$$F_2(x) = 1 + x + xF_2(x) + x^2F_2(X),$$

o bien

$$F_2(x) = \frac{1+x}{1-x-x^2}.$$

Recordando que $\frac{1}{1-x-x^2}$ es la FGO de Fibonacci, se deduce que $[x^n]L_2(x) = [x^n](1+x)F_f(x) = f_n + f_{n-1} = f_{n+1}$.

Para k general, no es un mucho más dificil. Tenemos que

$$L_k = \varepsilon + \{k\} + [k-1] \times L_k + \{k\} \times [k-1] \times L_k$$

O sea,

$$F_k(x) = 1 + x + (k-1)xF_k(x) + (k-1)x^2F_k(x),$$

o bien

$$F_k(x) = \frac{1+x}{1-(k-1)x-(k-1)x^2}$$

y la respuesta que buscamos es

$$[x^n]F_k(x) = [x^n]\frac{1+x}{1-(k-1)x-(k-1)x^2},$$

cuyo valor preciso se puede encontrar mediante fracciones parciales.

Ecuaciones en $\mathbb{N}^k$: ¿De cuántas formas se puede resolver la ecuación

$$x_1 + x_2 + \cdots + x_k = n,$$

donde $x_i \in \mathcal{A}_i$?

Las soluciones pertenecen a la clase combinatorial $\mathcal{A} = \mathcal{A}_1 \cdot \mathcal{A}_2 \cdot \cdots \cdot \mathcal{A}_k$, luego la respuesta es simplemente $[x^n] \prod_{i=1}^{k} A_i(x)$, donde $A_i(x)$ es la FGO de $\mathcal{A}_i$ usando $w(x_i) = x_i$.

Ejemplos: ¿De cuantas maneras podemos resolver

$$x_1 + x_2 + \cdots + x_k = n,$$

donde x_i es par ssi i es par?

Notar que si i es par, $A_i(x) = x^0 + x^2 + \cdots = \frac{1}{1-x^2}$, y si i es impar entonces, $A_i(x) = x^1 + x^3 + \cdots = \frac{x}{1-x^2}$. De aquí se tiene que

$$\begin{aligned} A(x) = \frac{x^{\lfloor k/2 \rfloor}}{(1-x^2)^k} &= x^{\lfloor k/2 \rfloor}(1-x^2)^{-k} = x^{\lfloor k/2 \rfloor} \sum_{m \geq 0} \binom{-k}{m} (-1)^m x^{2m} \\ &= \sum_{m \geq 0} \left(\!\!\binom{k}{m}\!\!\right) x^{2m + \lfloor k/2 \rfloor}. \end{aligned}$$

Luego,

$$[x^n]A(x) = \begin{cases} \left(\!\!\binom{k}{\frac{n-\lfloor k/2 \rfloor}{2}}\!\!\right), & \text{si } \dfrac{n - \lfloor k/2 \rfloor}{2} \in \mathbb{N} \\ 0, & \text{si no.} \end{cases}$$

Ejemplo: ¿De cuantas formas podemos llenar una bolsa con n frutas si debe haber un número par de manzanas, un número múltiplo de 5 de plátanos, a lo más 4 naranjas, a lo más una frutilla, al menos tres limones y sólo estas frutas se permiten?

Resolver este problema sin FGO, (por ejemplo por inclusión-exclusión) sería muy complejo. Naturalmente, creamos una FGO para cada tipo de frutas, de modo que la FGO del problema entero sea su producto.

$$\begin{aligned} F_m(x) &= x^0 + x^2 + \cdots = \frac{1}{1-x^2} \\ F_p(x) &= x^0 + x^5 + \cdots = \frac{1}{1-x^5} \\ F_n(x) &= 1 + x + x^2 + x^3 + x^4 = \frac{1-x^5}{1-x} \\ F_f(x) &= 1 + x \\ F_l(x) &= x^3 + x^4 + \cdots = \frac{x^3}{1-x} \end{aligned}$$

Luego,

$$\begin{aligned} F(x) &= \frac{1}{1-x^2}\frac{1}{1-x^5}\frac{1-x^5}{1-x}(1+x)\frac{x^3}{1-x} = \frac{x^3}{(1-x)^3} \\ &= x^3 \sum_{m \geq 0} \binom{-3}{m} (-x)^m = \sum_{m \geq 0} \left(\!\!\binom{3}{m}\!\!\right) x^{m+3} \end{aligned}$$

Bolas no etiquetadas en cajas etiquetadas - Composiciones

¿De cuantas formas podemos repartir n bolas no etiquetadas en k cajas:?
Igual a resolver la ecuación $x_1 + x_2 + \cdots + x_k = n$ con x_i libre. La fn. generatriz de la respuesta es

$$\left(\frac{1}{1-x}\right)^k = \sum_{n\geq 0} \binom{-k}{n}(-x)^n = \sum_{n\geq 0} \left(\!\binom{k}{n}\!\right) x^n.$$

¿Y si queremos sobreyectividad (sin cajas vacías)? Cada término es ahora $x + x^2 + \cdots = \frac{x}{1-x}$. Por lo que la respuesta es

$$\left(\frac{x}{1-x}\right)^k = \sum_{n\geq 0} x^k \binom{-k}{n}(-x)^n = \sum_{n\geq 0} \left(\!\binom{k}{n}\!\right) x^{n+k} = \sum_{n\geq k} \left(\!\binom{k}{n-k}\!\right) x^n.$$

Particiones
¿Cuántas particiones tiene el entero n? Recordemos que una partición es una solución de

$$x_1 + x_2 + \cdots + x_k = n, x_1 \geq x_2 \geq \cdots \geq x_k \geq 1$$

donde k es variable.

Otra forma de pensar en particiones es contar "cuantas veces se usa una parte con tamaño i". Es decir, si llamamos y_i al número de partes de tamaño i. Una partición es una solución de

$$y_1 + 2y_2 + 3y_3 + 4y_4 \cdots = n$$

con los $y_i \in \mathbb{N}$.

Notar que la FG de ky_k es $1 + x^k + x^{2k} + \cdots = \frac{1}{1-x^k}$. Con lo que tenemos que la FG. de las particiones es

$$P(x) = \sum_{n\geq 0} p_n x^n = \prod_{k\geq 0} \frac{1}{1-x^k}.$$

Ejemplo. Probar, usando FGO, que el número de particiones de n en partes impares es igual al número de particiones de n con partes distintas.

$$P_d(x) = \prod_{k\in\mathbb{N}} (1 + x^k)$$

$$P_i(x) = \prod_{k \text{ impar}} \frac{1}{1-x^k} = \frac{(1-x^2)(1-x^4)(1-x^6)\ldots}{(1-x)(1-x)^2(1-x)^3\ldots}$$
$$= \prod_{k\in\mathbb{N}} \frac{1-x^{2i}}{1-x^i} = \prod_{k\in\mathbb{N}} (1+x^i) = P_d(x).$$

Usando el mismo método que antes no es difícil concluir que el número de soluciones de la ecuación

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = n,$$

con $a_i \in \mathbb{N}$ números naturales dados y $x_i \in \mathbb{N}$ variables naturales es $[x^n]F(x)$, donde

$$F(x) = \prod_{i=1}^{k} \frac{1}{1-x^{a_i}}.$$

Capítulo 14

Método simbólico para objetos etiquetados.

[Def]

Sea $a \in S$ una secuencia. La función generatriz exponencial (FGE) de a es $\hat{F}(x) \in \mathbb{C}[[x]]$ dada por

$$\hat{F}(x) = \sum_{n \geq 0} f(n) \frac{x^n}{n!}.$$

[Def]

$[x^n/n!]F(x)$ recupera $f(n)$. Esto es lo mismo que $n![x^n]F(x)$.

Por ejemplo, la FGE de $(\underline{1})$ es $\exp(x)$. La FGE de (λ) es $\exp(\lambda x)$.

Las FGE nos servirán para atacar problemas donde cada objeto a ser contado tiene cierta estructura de conjunto etiquetado. Por ejemplo

1. Contar las particiones de $[n]$.
2. Contar las permutaciones de $[n]$.
3. Contar los árboles planares cuyos vértices reciben etiquetas distintas de $[n]$

La diferencia con los problemas anteriores radica en que ahora los objetos a contar están "etiquetados" por el conjunto $[n]$. En otras palabras recibimos un conjunto de n elementos (spg, $[n]$) y le damos alguna "estructura interna" (los ordenamos, partimos, asignamos a las hojas de un árbol, etc.)

En esta sección un "objeto" de tamaño n, será una estructura arbitraria (para fijar ideas, piensen en un "digrafo", es decir, un conjunto (V, E) donde $E \subseteq V \times V$) que tiene n vértices donde se pueden poner etiquetas.

Un objeto de tamaño n está **debilmente etiquetado** si todos sus vértices reciben etiquetas distintas de $\mathbb{N}$. El objeto está **bien etiquetado** si el conjunto de etiquetas usadas es exactamente $[n]$.

Una **clase etiquetada** es una clase combinatorial que consiste de objetos bien etiquetados. Dos objetos cuyas etiquetas son distintas, también son distintos.

Hablemos un poco de grafos y su notación.

Un **digrafo** (simple) es un par $G = (V, E)$ donde $E \subseteq V \times V$ es el conjunto de **arcos** y V es el conjunto de **nodos**. Todo digrafo se puede ver como una "relación binaria" sobre V donde $(v, w) \in E$ se representa como $v \to_E w$. Normalmente dibujamos un grafo como un conjunto de puntos (vértices) donde hay una flecha de v a w para todo $(v, w) \in E$.

Un **grafo** (simple) es un par $G = (V, E)$ donde $E \subseteq \binom{V}{2}$ es el conjunto de **aristas** y V es el conjunto de **vértices**. Todo grafo simple se puede ver como una "relación binaria simétrica irreflexiva" donde $\{v, w\} \in E$ se representa como $v \sim w$. Por comodidad, escribimos $vw \in E$ (pero recordando que $vw = wv$ en este caso). Normalmente dibujamos un grafo como un conjunto de puntos (vértices) donde dos puntos v y w se unen mediante una linea si $vw \in E$.

Un paseo en un grafo (resp. digrafo) es una secuencia de vertices (resp. nodos) $v_0 v_1 \dots v_k$ donde cada $v_i v_{i+1} \in E$, k es el largo del paseo. Un camino es un paseo que no repite vertices/nodos. Un ciclo es un paseo donde todos los vertices /nodos son distintos excepto v_0 y v_k que son iguales. A cada paseo asociamos el grafo/digrafo natural cuyos vertices/nodos son los que visita el paseo y sus aristas/arcos son las usadas por el paseo.

¿Cuántos grafos/digrafos (etiquetados) con $V = [n]$ existen?
Cualquier subconjunto de $\binom{[n]}{2}$ (o de V^2) nos da un grafo (digrafo), así que la respuesta es $2^{\binom{n}{2}}$ (2^{n^2}).

El problema es, en este caso más interesante sin etiquetas. Por ejemplo, si $n = 3$, hay $2^3 = 8$ grafos etiquetados diferentes. De estos 8 casos hay algunos que se "ven" igual pero están "reetiquetados". Si ignoramos las etiquetas hay solo 4 grafos no etiquetados distintos.

Si $\mathcal{A}$ es una clase etiquetada y a_n representa la cantidad de objetos (bien etiquetados) de tamaño n, entonces su FGE es

$$\hat{A}(x) = \sum_{n\geq 0} a_n x^n/n!.$$

En general todas (o casi todas) las clases combinatoriales etiquetadas que encontremos se pueden representar con (secuencias o conjuntos de) grafos, digrafos etiquetados con alguna propiedad. De hecho podemos "simular" grafos con digrafos poniendo arcos antiparalelos donde van las aristas asi que casi siempre es más fácil usar digrafos.

Advertencia: Los objetos sin etiquetas (o sea, de peso 0) a veces son considerados y a veces no (por ejemplo, normalmente se supone la existencia de la permutación vacía, pero no del ciclo vacío).

Algunas clases etiquetadas

1. Clase neutra: $\mathcal{E} = \{\varepsilon\}$ donde $w(\varepsilon) = 0$. Su FGE es $\hat{E}(x) = x^0 = 1$.
2. Clase atómica: $Z = \{\bullet\}$ donde $w(\bullet) = 1$. Su FGE es $\hat{Z}(x) = x$.
3. Clase de permutaciones: Cada permutación se puede representar como un digrafo $\pi(1) \to \pi(2) \to \pi(3) \to \cdots \to \pi(n)$. Su FGE es $\hat{P}(x) = \sum_{n\geq 0} n!x^n/n! = \frac{1}{1-x}$.
4. Clase de urnas / conjuntos: Una urna es un conjunto donde las etiquetas son distintas pero no hay relación entre ellas. Podemos pensarlo como los grafos (o digrafos) sin aristas. Su FGE es $\hat{S}(x) = \sum_{n\geq 0} 1x^n/n! = \exp(x)$.
5. Clase de ciclos dirigidos o no dirigidos. La FGE para ciclos dirigidos es $\hat{C}(x) = \sum_{n\geq 1}(n-1)!x^n/n! = \sum_{n\geq 1} x^n/n = -\ln(1-x)$.. Si son no dirigidos es $\hat{C}_N(x) = x + x^2 + \sum_{n\geq 1}(n-1)!/2 \cdot x^n/n!$ (esto es tomando un vértice como un ciclo de largo 0).

Principios de la suma y el producto

El principio de la suma es igual que en el caso no etiquetado (es la unión disjunta). Sin embargo para el producto tenemos algunos problemas con las etiquetas. Por ejemplo si $\mathcal{A}$ y $\mathcal{B}$ son clases combinatoriales etiquetadas, $\alpha \in \mathcal{A}$, $\beta \in \mathcal{B}$ y tratamos de "pegarlos" para obtener un par ordenado (α, β) (como lo haría el producto cartesiano), la etiqueta 1 aparecería en 2 vértices. Así que tenemos que permitir **re-etiquetar** para hacer que todo funcione.

En el caso no etiquetado, cuando tomábamos $\alpha \in \mathcal{A}$ y $\beta \in \mathcal{B}$, el par (α, β) era un objeto único de tamaño $w(\alpha) + w(\beta)$. (Es poner el digrafo de α al lado del digrafo de β, como unión disjunta, reconociendo en la unión quien es α y quien es β). En el caso etiquetado su "producto" generará un conjunto de objetos. Esencialmente el producto funciona como sigue: mantenemos la estructura (un par ordenado de digrafos) y generamos nuevas etiquetas que preserven el orden de las etiquetas en cada parte. Para explicarlo formalmente usamos la siguiente operacion:

Reducir etiquetas: Si γ es una estructura débilmente etiquetada con etiquetas $(e_1, e_2, \ldots, e_k)$, la reducción de γ es la misma estructura pero cuyas etiquetas son cambiadas al intervalo $[n]$, manteniendo el orden relativo de las etiquetas originales. Por ejemplo, si las etiquetas son $(7, 5, 1, 4)$, al reducirlas estas se cambian a $(4, 3, 1, 2)$. Denotemos esta operacion como $\rho(\gamma)$.

Dados dos objetos bien etiquetados α y β. Su producto etiquetado $\alpha \star \beta$ es el conjunto.

$$\alpha \star \beta = \{(\alpha', \beta') \colon (\alpha', \beta') \text{ bien etiquetado y } \rho(\alpha') = \alpha, \rho(\beta') = \beta\}.$$

Ejemplo: Si α es el camino $1 \mapsto 2$ y β es el triángulo $1 \to 2 \to 3 \to 1$. Entonces $\alpha \star \beta$ es un conjunto de digrafos con 5 vertices: $1 \to 2, 3 \to 4 \to 5 \to 3$; $1 \to 3, 2 \to 4 \to 5 \to 2$, etc.

¿Cuántos elementos tiene $\alpha \star \beta$? Hay $\binom{w(\alpha)+w(\beta)}{w(\alpha),w(\beta)}$. Pues de las $n = w(\alpha) + w(\beta)$ hay que elegir cuales van al objeto α (y son asignadas de manera única a sus vértices) y el resto son asignadas a β.

Producto etiquetado de clases

$$\mathcal{A} \star \mathcal{B} = \bigcup_{\alpha \in \mathcal{A}, \beta \in \mathcal{B}} (\alpha \star \beta).$$

Si a, b, c son las secuencias de conteo de $\mathcal{A}, \mathcal{B}, \mathcal{A} \star \mathcal{B}$, y $\hat{A}(x), \hat{B}(x), \hat{C}(x)$ son sus FGE, entonces:

$$c_n = \sum_{(n_1,n_2):n_1+n_2=n} \binom{n}{n_1, n_2} a_{n_1} b_{n_2} = \sum_{i=0}^{n} \binom{n}{i} a_i b_{n-i},$$

y además

$$\hat{C}(x) = \hat{A}(x) \cdot \hat{B}(x).$$

Demostremos la ultima parte:

$$\begin{aligned}
\hat{A}(x) \cdot \hat{B}(x) &= \sum_{n \geq 0} a_n \frac{x^n}{n!} \sum_{n \geq 0} b_n \frac{x^n}{n!} \\
&= \sum_{n \geq 0} x^n (\sum_{i=0}^{n} \frac{a_i}{i!} \frac{b_{n-i}}{(n-i)!} \\
&= \sum_{n \geq 0} x^n \binom{n}{i} \frac{a_i b_{n-i}}{n!}.
\end{aligned}$$

Nota: Si a y b son secuencias, la secuencia c con $c_n = \sum_{i=0}^{n} \binom{n}{i} a_i b_{n-i}$ se conoce como su **convolución binomial**.

Ejemplos: Permutaciones: Una permutación de $[n]$ se puede ver como el producto de n átomos.

En otras palabras, la clase $\mathcal{P}$ de permutaciones es $1 + Z + Z \star Z + Z \star Z \star Z + \ldots$, donde Z es la clase atomica. Su FGE es $1 + x + x^2 + \cdots = \frac{1}{1-x}$.

En otras palabas, el numero de permutaciones es $[x^n/n!](1-x)^{-1} = n![x^n](1-x)^{-1} = n!$.

En general, si $\mathcal{A}$ es una clase etiquetada cualquiera con FGE $\hat{A}(x)$, la clase de sus secuencias se denota por

$$\mathrm{Seq}(\mathcal{A}) = \sum_{n \geq 0} \mathcal{A}^{\star n}.$$

Y tenemos que la FGE de $\mathrm{Seq}(\mathcal{A})$ es $\frac{1}{1-\hat{A}(x)}$.

Para hacer cosas mas interesantes necesitamos el concepto de "construccion de conjuntos no ordenados".

La expresión $\mathcal{A}^{\star k}$ representa el producto etiquetado de A con si mismo n veces. Cada copia de $\mathcal{A}$ es una "componente", y sabemos quien es la primera componente, quien es la segunda, etc. Para contar secuencias de objetos donde el orden no importe necesitamos considerar la clase combinatorial

$$\mathrm{Set}_k(\mathcal{A}) = \mathcal{A}^{\star k}/R$$

donde cuocientamos por la relacion de equivalencia que identifica dos objetos si las etiquetas de uno se pueden obtener del otro "permutando componentes".

Si $\hat{A}(x)$ es la FGE de $\mathcal{A}$, entonces la FGE de $\mathcal{A}^{\star k}$ es $\hat{A}(x)^k$ y la FGE de $\mathrm{Set}_k(\mathcal{A})$ es $\hat{A}(x)^k/k!$.

Finalmente podemos definir $\mathrm{Set}(\mathcal{A})$ como la suma de las clases $\mathrm{Set}_k(\mathcal{A})$ con $k \in \mathbb{N}$. Luego, la FGE de $\mathrm{Set}(\mathcal{A})$ es

$$\sum_{k \geq 0} \frac{A(x)^k}{k!} = \exp(A(x)).$$

(para no tener problemas formales, esto solo se puede hacer si $A(0) = 0$).

Nota: Las construcciones de conjuntos también se pueden hacer para clases no etiquetadas, de la manera obvia.

En lo que sigue, si llamamos a una clase etiquetada con una letra caligráfica, llamaremos a su secuencia de conteo con la misma letra pero en minúscula y a su FGE con la letra mayúscula correspondiente.

Ejemplos:

1. Un **emparejamiento dirigido** es la unión disjunta de caminos de largo 1 (es decir, cada nodo es o bien cabeza o bien cola de un arco). ¿Cuántos emparejamientos dirigidos etiquetados con n vertices existen?

   Sea $\mathcal{A}$ la clase combinatorial de los emparejamientos dirigidos etiquetados. Y sea $\mathcal{B}$ la clase combinatorial de un camino de largo 1. Entonces $\mathcal{A} = \mathrm{Set}(\mathcal{B})$. La FGE de $\mathcal{B}$ es $\sum_{\beta\in\mathcal{B}} x^{w(\beta)}/w(\beta)! = 2x^2/2! = x^2$. Luego

   $$\hat{A}(x) = \exp(\hat{B}(x)) = \exp(x^2) = \sum_{n\geq 0} x^{2n}/n! = \sum_{n\geq 0,\mathrm{par}} x^n/(n/2)!.$$

   De aquí, el numero de emparejamientos dirigidos etiquetados es $n![x^n]\exp(x^2) = n!/(n/2)!$, donde n es par.

2. ¿Cuántos **emparejamientos no dirigidos** etiquetados con n vertices existen?

   Ahota tenemos $\hat{B}(x) = x^2/2$. Con lo cual el numero de emparejamientos es 0 si n es impar, y

   $$n![x^n]\hat{A}(x) = n![x^n]\exp(\hat{B}) = n![x^n]\exp(x^2/2) = \frac{n!}{(n/2)!2^{n/2}},$$

   para n par.

   O sea, si $n = 2m$, este numero es $(2m)!/(2^m m!) = (2m-1)(2m-3)\cdots 1$. Esto se conoce como $(2m-1)!!$.

3. Otra forma de ver **permutaciones** es como "conjuntos de ciclos dirigidos". Sea $C(x) = -\ln(1-x)$ la FGE de los ciclos dirigidos. Luego la FGE de las permutaciones es $\exp(C(x)) = 1/(1-x)$, que es lo mismo que antes.

4. **Involuciones**: Una involucion es una permutacion π tal que $\pi^2 = id$. En terminos de ciclos, todos los ciclos de π deben tener largo 1 o 2. Luego la clase de involuciones corresponde a la clase de conjuntos de ciclos de largo 1 o 2 (ojo que son dirigidos).

   Sea $\hat{C}_{1,2}(x)$ la FGE de los ciclos dirigidos de largo 1 o 2, es decir $\hat{C}_{1,2}(x) = x + x^2/2$. Con esto la FGE de las involuciones no es mas que $\hat{I}(x) = \exp(x + x^2/2)$, lo cual es igual a

   $$\begin{aligned}\sum_{k\geq 0}\frac{x^k}{k!}(1+x/2)^k &= \sum_{k\geq 0}\sum_{j=0}^{k}\binom{k}{j}\frac{x^{k+j}}{2^j k!}\\ &= \sum_{n\geq 0}\sum_{j=0}^{n}\binom{n-j}{j}\frac{x^n}{2^j(n-j)!}\end{aligned}$$

   Luego, el numero de involuciones de $[n]$ es

   $$\sum_{j=0}^{n}\binom{n-j}{j}\frac{n!}{2^j(n-j)!} = \sum_{j=0}^{\lfloor n/2\rfloor}\frac{n!}{2^j j!(n-2j)!}$$

5. **Desarreglos**: Son las permutaciones tal que $\pi(i) \neq i$ para todo i. Es decir, aquellas que son uniones de ciclos de largo 2 o mas. Sea $\hat{C}_{\geq 2}(x)$ la FGE de los ciclos de largo 2 o mas. Tenemos que $\hat{C}_{\geq 2}(x) = \hat{C}(x) - x = -\ln(1-x) - x$. Por lo tanto la FGE de los desarreglos es

   $$\begin{aligned}\exp(-\ln(1-x) - x) &= \frac{e^{-x}}{1-x}\\ &= \sum_{n\geq 0}\frac{(-1)^n x^n}{n!}\cdot\sum_{n\geq 0}x^n.\end{aligned}$$

O sea,

$$\hat{D}_n = n![x^n]\hat{C}_{\geq 2}(x) = n!\sum_{j=0}^{n}\frac{(-1)^j}{j!}.$$

Ejercicio 14.1. Encuentre una fórmula para las particiones de $[n]$ en partes de tamaño al menos 3 y a lo más 5.