Fundamentos Matemáticos para Teoría de la Computación

Miguel Angel Norzagaray Cosío

30 de agosto de 2016

Índice general

1. Conjuntos **7**
1.1. Definiciones y propiedades básicas 7
1.2. Operaciones entre Conjuntos 10

2. Relaciones y Funciones **15**
2.1. Relaciones 15
2.2. Funciones 17
2.3. Axioma de elección 17
2.4. Funciones inversas y biyectivas 18
2.5. Hipótesis del continuo 21
2.6. Composición de Funciones 22
2.7. Funciones computables 23
2.7.1. Incompletitud de las matemáticas 23

3. Inducción Matemática **25**
3.1. La falsa prueba de los casos particulares 25
3.2. Inducción matemática 26
3.2.1. Inducción más fuerte 35
3.3. Inducción como herramienta constructiva 37
3.4. Inducción estructural 41

Introducción

Las matemáticas son un lenguaje formale para representar y demostrar la veracidad de alguos conceptos y sus propiedades. Como si eso fuera poco, también son de gran ayudan para desarrollar el pensamiento analítico y las habilidades de abstracción de los estudiantes, competencias indispensables para su buen desempeño como estudiantes y profesionales.

Se presentan aquí los elementos de matemáticas básicos que se requiren para poder comprender el contenido de la asignatuira Teoría de la Computación, en las carreras del Departamento de Sistemas Computacionales de la UABCS.

Se cubren los temás mínimos para un buen desarrollo de la teoría, presentando resultados más que suficientes. Cada vez que se define un concepto se *enfatiza* utilizando un tipo de letra que lo distinga. En algunos párrafos se ha colocado un símbolo $\star$ al margen, indicando que la idea es importante y que vale la pena su estudio cuidadoso.

El contenido cubre tres temas centrales: *conjuntos*, pues un lenguaje es un conjunto de cadenas y se clasifican por jerarquías donde cada clase de lenguajes contiene a otras clases menores; *funciones*, ya que cada programa de computadora puede modelarse como una función o bien una función puede ser una computadora misma; finalmente *inducción matemática*, pues es el recurso constructivo que nos permite comprobar muchas aseveraciones que dan tanto seguridad como algoritmos para resolver problemas, tanto teóricos como prácticos.

Los conceptos y proposiciones sobre teoría de conjuntos e inducción matemática, ofrecen el material necesario para estudiar lenguajes, pero, al mismo tiempo, las proposiciones presentadas (y demostradas) son medulares para el estudio de la computabilidad. Estos materiales corresponden principalmente a un curso de Matemáticas Discretas y por tanto pueden emplearse ahí como material complementario.

Se incluye algunas nociones adicionales y comentarios de carácter histórico que siempre son interesantes para quuienes gustan saber un poco más que la disciplina. Estudiar con cuidado los ejemplos y discutir/resolver ejercicios es necesario para madurar las ideas. Adicionalmente, sirva de pretexto para repasar otros temas, como álgebra, grafos, estructuras de datos y algorítmica.

La Teoría de la Computación constituye los cimientos que sostienen con firmeza los conocimientos del área de la computación. Comprende dos grande rubros, íntimamente ligados:

1. la teoría de los lenguajes y

2. la computabilidad y factibilidad.

Estas notas fueron elaboradas (y son mantenidas) utilizando LaTeX, la distribución MikTeX 2.9, editando con TeXnicCenter 2.0 Beta y VauCanSon-G 0.4 para los diagramas de los autómatas.

Código fuente disponible a estudiantes y maestros del DASC solicitándolo a: `manc@uabcs.mx`.

Capítulo 1

Conjuntos

Un *conjunto* es una colección, familia o clase de elementos concretos o abstractos que puede ser vacío, finito o infinito. Es un concepto tan básico en matemáticas que es imposible dar una definición más precisa, las palabras colección, familia o clase son un simple remplazo por sinonimia de lo que se quiere definir. Es lo mismo que pasa en geometría, donde no se puede dar una definición de punto o recta.

En el siglo XIX se intentó formalizar todas las matemáticas a partir de una teoría axiomática de conjuntos. A los intentos iniciales del matemático italiano Giuseppe Peano, siguieron los de los matemáticos alemanes George Cantor y Friedrich Ludwig Gottlob Frege. De cierta manera, parecieron fracasar, pues el matemático y filósofo británico Bertrand Russell encontró una famosa contradicción: *la paradoja de Russell*. Esta formula el conjunto X de todos aquellos conjuntos que no se contienen a sí mismos. Es una paradoja pues si X no pertenece a este conjunto, por definición debe estar allí, lo que es una contradicción.

De los intentos axiomáticos posteriores, el más exitoso es el de los matemáticos alemanes Ernst Zermelo y Adolf Fraenkel. De hecho son conocidos como los axiomas de Zermelo–Fraenkel (ZFC). La teoría de conjuntos que se definirá, no se presenta formalmente como axiomas, sino como propiedades o definiciones sobre conjuntos, pero en su mayoría son la base fundamental de las matemáticas.

1.1. Definiciones y propiedades básicas

Es natural definir primero una relación de pertenencia a un conjunto. Se dice que un elemento x está contenido en un conjunto X o que pertenece a X y se escribe como $x \in X$. Si el elemento x NO está en el conjunto X entonces se escribe[1] como $x \notin X$. El conjunto vacío es un conjunto al que no pertenece

[1] El origen del símbolo $\in$ viene desde la formulación de los axiomas de Peano, cuando el lenguaje de la lógica símbólica estaba en su infancia. Peano utilizaba la letra griega épsilon, ϵ, para indicar pertenencia.

ningún elemento y se de nota por el símbolo, $\emptyset$.

Esta definición de la pertenencia a un conjunto se dice que es dura, en contraparte a la pretenencia difusa, donde ocurre que la pertenencia es gradual. En los conjuntos difusos, un elemento tiene pertenencia 0 si no está en X y pertenencia 1 si está completamente en X, pero tal pertenencia puede tomar cualquier valor intermedio. Esto permite modelar mejor muchos fenómenos reales, pero para la teoría de lenguajes, la pertenencia dura es la que se empleará. No se dirá más sobre conjuntos difusos.

Definición 1. *La cantidad de elementos en un conjunto A se llama* cardinalidad *y se denota por $|A|$.*

Se pueden definir conjuntos de varias maneras. Una muy frecuente es indicando la propiedad que cumplen sus elementos, diciendo por ejemplo los números que al mismo tiempo son múltiplos de 5 y de 7, lo que se escribe $A = \{x|x = 5k \text{ y } x = 7k\}$. En vez del símbolo $|$, que se entiende al leer como la expresión *tal que*, muchos usan los dos puntos, como en $A = \{x : x = 5k \text{ y } x = 7k\}$. A continuación se definen tres conjuntos de distinta manera:

1. mostrando todos sus elementos, como en $A = \{a, b, c, d\}$ que define 4 elementos;

2. mostrando una parte que permita identificarlos a todos, como en $P = \{2, 4, 6, 8, \ldots\}$ que define a todos los números pares positivos y

3. describiéndolos mediante alguna regla. Por ejemplo

$$C = \{x \in \mathbb{R} | x \text{ múltiplo de } 7\}.$$

   Esto se lee "*C es el conjunto de los números x que pertenecen ($\in$) al conujunto de los números reales tales que ($|$) son múltiplos de 7*". Esta forma de indicar las características de los elementos de un conjunto es lo más común. Otra variante es $C = \{x \in \mathbb{R} \mid x = 7 \times k \ \wedge \ k \in \mathbb{Z}\}$.

Algunos conjuntos importantes y de uso frecuente, además del conjunto vacío son:

- $\mathbb{N} = \{1, 2, 3, 4, \ldots\ldots\}$, el conjunto de los números naturales.
- $\mathbb{Z}$ el onjunto de los números enteros. Son los naturales con los negativos y el cero.
- $\mathbb{Q}$ el conjunto de los números racionales, es decir, $\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z} \text{ y } q \neq 0\}$.
- $\mathbb{R}$ el conjunto de todos los números reales[2].

[2]En este texto no analizaremos el conjunto de los números reales, compuestos por números racionales, números algebraicos y números trascendentes

El conjunto $\mathbb{N}$ es particularmente importante en Teoría de la Computación. Tanto en la vida diaria como en la ciencia, se utiliza para contar. Si se puede poner los elementos de un conjunto infinito X de manera ordenada al lado de los números naturales, se dice que X es *contable* o *numerable*, en el sentido que la asociación de elementos de uno y otro conjunto establece una *numeración*. Si esto es posible, entonces $|\mathbb{N}| = |X|$.

Ejemplo 1. *Hay tantos números naturales ($\mathbb{N}$) como números enteros ($\mathbb{Z}$). la forma de relacionarlos es simple:*

$$\begin{aligned} 1 &\longleftrightarrow 0 \\ 2 &\longleftrightarrow 1 \\ 3 &\longleftrightarrow -1 \\ 4 &\longleftrightarrow 2 \end{aligned}$$

de tal manera que la regla que asocia naturales con enteros es

$$n \longleftrightarrow \begin{cases} \frac{n}{2} & \textit{si } n \textit{ es par} \\ -\left\lfloor \frac{n}{2} \right\rfloor & \textit{si } n \textit{ es impar} \end{cases}$$

y considerando 1 asociado al 0 como caso particular.

Ejemplo 2. *Los números naturales $\mathbb{N}$ son tantos como los múltiplos de 7, (o $7\mathbb{N}$). Aunque esto no es evidente, es posible organizar las parejas de elementos de cada conjunto como*

$$\{(1,7),\ (2,14),\ (3,21),\ldots,(n,7\times n),\ldots\}$$

y continuar hasta el infinito. Por ello, como para cada número natural se hace corresponder un múltiplo de 7, se concluye que hay tantos números naturales como múltiplos de 7, así que $|\mathbb{N}| = |7\mathbb{N}|$.

El ejemplo anterior va contra el sentido común, pero es correcto. Con ese argumento, los números naturales son tantos como los múltiplos de cualquier número. Se puede probar el resultado aún más insólito de que $|\mathbb{N}| = |\mathbb{Q}|$, enumerando las fracciones p/q. La numeración inicia con el 0, que es un racional y continúa con las fracciones en las que $p + q$ suma 2: $\frac{1}{1}$, luego las que suman 3: $\frac{1}{2}, \frac{2}{1}$, las que suman 4: $\frac{1}{3}, \frac{2}{2}, \frac{3}{1}$, siempre comenzando con 1 en el numerador y $q - 1$ en el denominador. Por último, intercalar los negativos no representa problema, como en ejemplo 1. Así y de esa manera se establece la numeración que garantiza que $\mathbb{Q}$ es contable.

Para los conjuntos se definen varias propiedades y operaciones importantes. Dados dos conjuntos A y B, con elementos del universo U, se dice que A es *subconjunto* de B si para cada $x \in A$, ocurre que $x \in B$ y se escribe $A \subset B$. También se puede decir que B es un *superconjunto* de A.

Se dice que dos conjuntos son iguales $A = B$ cuando poseen los mismos ★ elementos, es decir, ocurre al mismo tiempo que $A \subset B$ y $B \subset A$. Esto se conoce como *contención mutua*. Generalmente se demuestra la igualdad entre conjuntos con dos pasos:

1. $A \subset B$: se toma cualquier $x \in A$ y se prueba que está en B y luego
2. $B \subset A$: se toma cualquier $x \in B$ y se prueba que está en A.

En caso de querer probar que dos conjuntos NO son iguales, sólo se necesita mostrar un elemento en uno de los conjuntos tal que no esté contenido en el otro.

Se dice que A es un *subconjunto propio* de B si $A \subset B$ y $A \neq B$, es decir, existe al menos une elemento $x \in B$ que no está en A. En ese caso se puede escribir $A \subsetneq B$ y se entiende que $|A| < |B|$.

El conjunto vacío es subconjunto de todos los conjuntos: $\emptyset \subset A$, cualquiera que sea el conjunto A. Un conjunto siempre es subconjunto de sí mismo.

Debe ser claro que si $A \subset B$ y $B \subset C$ entonces $A \subset C$, es decir, *ser subconjunto de* es una propiedad (o relación) transitiva.

1.2. Operaciones entre Conjuntos

Las más básicas: *unión*, *intersección* y *complemento*, que se definen para conjuntos contenidos en un universo U de la siguiente manera.

Definición 2. *La* unión *de los conjuntos A y B se define como*

$$A \cup B = \{x | x \in A \text{ o } x \in B\}.$$

Definición 3. *La* intersección *de A y B como*

$$A \cap B = \{x | x \in A \text{ y } x \in B\}.$$

Es bastante sencillo aceptar las siguientes dos proposiciones.

Proposición 1. *Si el elemento x pertenece al conjunto A, entonces x también está en A unido con cualquier otro conjunto.*

Proposición 2. *Si el elemento x NO pertenece al conjunto A, entonces x tampoco está en A intersectado con cualquier otro conjunto.*

Definición 4. *El* complemento *de un conjunto A, se define como*

$$A^c = \{x \in U | x \notin A\}$$

y siempre es con respecto al mismo universo U prestablecido.

Debe ser claro que para todo $x \in U$, o $x \in A$ o $x \notin A^c$ pero no en ambos[3]. Es común que la operación *complemento* se denote por $\overline{A}$, que es más económico en algunas ocasiones, así: $(A \cup B)^c \equiv \overline{A \cup B}$.

A manera de ejemplo y formalidad, podemos establecer nuestras primeras proposiciones formales y demostrar que son ciertas. Hay muchos tipos de demostraciones, pero no hay reglas específicas de cuándo usar cada tipo. Lo importante es hacer ver de manera evidente, ya sea con lenguaje matemático o natural, que lo que se quiere probar es cierto.

★

[3] Al menos en la teoría clásica de conjuntos.

Proposición 3. *Las operaciones de unión e intersección son* conmutativas*, es decir,* $A \cup B = B \cup A$ *y* $A \cap B = B \cap A$.

Demostración. Consideremos primero la asociatividad de la unión. Probaremos dos cosas: $A \cup B \subset B \cup A$ y $B \cup A \subset A \cup B$.

Caso a: $A \cup B \subset B \cup A$. Sea $x \in A \cup B$.

$$x \in A \cup B \Rightarrow x \in A \text{ ó } x \in B.$$

Independientemente de a qué conjunto pertenece x, por la definición 2 también se cumple que $x \in B \cup A$.

Caso b: $B \cup A \subset A \cup B$. El razonamiento anterior aplica.

El caso de la conmutatividad de la intersección se deja como ejercicio. □

Proposición 4. *La unión e intersección son* asociativas*:* $(A \cup B) \cup C = A \cup (B \cup C)$ *y* $(A \cap B) \cap C = A \cap (B \cap C)$.

Demostración. Probaremos primero el caso de la unión, es decir que $(A \cup B) \cup C = A \cup (B \cup C)$. De nuevo probaremos con la contención mútua.

Caso a: $(A \cup B) \cup C \subset A \cup (B \cup C)$.

$$\begin{aligned} x \in (A \cup B) \cup C &\Rightarrow x \in A \cup B \text{ ó } x \in C \\ &\Rightarrow x \in A \text{ ó } x \in B \text{ ó } x \in C \\ &\Rightarrow x \in A \text{ ó } x \in B \cup C \end{aligned}$$

por lo que este caso se cumple.

Caso b: $A \cup (B \cup C) \subset (A \cup B)$. Es similar al anterior y se deja al lector su desarrollo.

El caso de la asociatividad de la intersección también se deja como ejercicio. □

La *diferencia* de conjuntos se define como $A - B = \{x | x \in A \text{ y } x \notin B\}$. Algunos autores consideran esto un abuso de notación y prefieren escribir su equivalencia:

$$A - B = A \cap B^c \tag{1.1}$$

empleando las operaciones previas. Ahora unos ejemplos de demostraciones con conjuntos.

El *producto cartesiano* de dos conjuntos, denotado por $A \times B$, se define como

$$A \times B = \{(a, b) | a \in \wedge b \in B\}$$

formado por todas las parejas posibles entre elementos de A y de B.

Las siguientes demostraciones hacen uso de lógica proposicional básica. Es de esperarse que el lector pueda entender la simbología empleada. De no ser así, solicite ayuda de un profesor o remítase a libros de lógica de nivel básico.

Ejemplo 3 (Ley de D'Morgan)**.** *Dados dos conjuntos A y B, se cumple que*

$$(A \cup B)^c = A^c \cap B^c.$$

Demostración. Sea $x \in (A \cup B)^c$.

$$\begin{aligned} x \in (A \cup B)^c &\Leftrightarrow x \notin A \cup B \\ &\Leftrightarrow x \notin A \text{ y } x \notin B \\ &\Leftrightarrow x \in A^c \text{ y } x \in B^c \\ &\Leftrightarrow x \in A^c \cap B^c \end{aligned}$$

y como las implicaciones son dobles, se demuestra que $(A \cup B)^c \subset A^c \cap B^c$ leyendo hacia abajo y hacia arriba se lee que $A^c \cap B^c \subset (A \cup B)^c$. □

Ejemplo 4 (Distributividad)**.** *Por demostrar, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, utilizando las propiedades anteriores. Se prosigue mediante dobles implicaciones*[4]*.*

Demostración. Sea $x \in A \cup (B \cap C)$.

$$\begin{aligned} x \in A \cup (B \cap C) &\Leftrightarrow x \in A \text{ o bien } x \in (B \cap C) \\ &\Leftrightarrow x \in A \text{ o bien } x \in B \text{ y } x \in C \end{aligned}$$

Ahora se tienen dos casos, o que $x \in A$ o que $x \in B$ y $x \in C$.

1. Caso $x \in A$

$$\begin{aligned} x \in A &\Rightarrow x \in A \cup B \text{ y } x \in A \cup C \\ &\Leftrightarrow (A \cup B) \cap (A \cup C) \end{aligned}$$

2. Caso $x \in B$ y $x \in C$

$$\begin{aligned} x \in B \text{ y } x \in C &\Leftrightarrow x \in A \cup B \text{ y } x \in A \cup C \\ &\Leftrightarrow (A \cup B) \cap (A \cup C) \end{aligned}$$

Por lo tanto, $x \in (A \cup B) \cap (A \cup C)$. Ahora faltaría tomar $x \in (A \cup B) \cap (A \cup C)$ y probar que también $x \in A \cup (B \cap C)$, pero como las implicaciones son casi todas dobles (en ambos sentidos), es cosa de seguir la prueba hacia atrás, con pocas modificaciones. □

Como en este ejemplo, no es raro que las pruebas de doble contención mutua se den por dobles implicaciones, por lo que probar un caso implica probar el otro también.

[4] Decir que $a \Leftrightarrow b$ equivale a decir que $a \Rightarrow b$ y que $a \Leftarrow b$ por lo que a se sigue de b y b se sigue de a.

Ejemplo 5 (Diferencia simétrica)**.** *Se llama diferencia simétrica a la unión de dos conjuntos menos la intersección. Generalmente se escribe como*

$$A \circ B = A \cup B - A \cap B.$$

Otra forma de escribirlo es $(A - B) \cup (B - A)$*. Ahora se demostrará que estas dos formas son equivalentes.*

Demostración. Como costumbre, se toma un elemento en un conjunto y se prueba que está en el otro. Sea $x \in A \cup B - A \cap B$. Se procede como sigue.

$$\begin{aligned} x \in A \cup B - A \cap B &\Leftrightarrow x \in A \cup B \ \text{ y } \ x \notin A \cap B \\ &\Leftrightarrow (x \in A \ \text{ o } \ x \in B) \ \text{ y } \ (x \notin A \text{ y } x \notin B) \\ &\Leftrightarrow (x \in A \ \text{ y } \ x \notin B) \ \text{ o } \ (x \in B \ \text{ y } \ x \notin A) \end{aligned}$$

y como esa es la definición de diferencia de conjuntos

$$\begin{aligned} &\Leftrightarrow x \in A - B \ \text{ o } \ x \in B - A \\ &\Leftrightarrow x \in (A - B) \cup (B - A) \end{aligned}$$

que es lo que se quería demostrar. □

Dos conjuntos A y B se dicen *disjuntos* si su intersección es el conjunto vacío. En ese caso, se tiene que la cardinalidad de la unión es la suma de las cardinalidades:

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

Definición 5. *El* producto cartesiano *de dos conjuntos* A *y* B *es* $A \times B = \{(a, b) | a \in A \text{ y } b \in B\}$*. El conjunto de los matrimonios es un producto cartesiano de los Esposos×Esposas.*

Ejemplo 6. *El producto cartesiano* $\mathbb{N} \times \mathbb{N} = \mathbb{N}^2$ *se compone de todas las parejas de números enteros positivos.*

Ejemplo 7. *El producto cartesiano* $\mathbb{R} \times \mathbb{R}$ *es el llamado plano cartesiano, formado por todas las parejas de puntos con coordenadas reales* (x, y)*. Es más comunmente descrito como* $\mathbb{R}^2$*.*

Definición 6. *Sea* A *un conjunto. La colección de todos los subconjuntos de* A *se llama el* conjunto potencia *de* A *y lo denotaremos*[5] *por* $2^A = \{X | X \subset A\}$*. Esta es una operación importante para modelar el paralelismo.*

Ejemplo 8. *Si* $A = \{a, b, c\}$*, entonces*

$$2^A = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

por lo que $|2^A| = 8$*.*

[5] En algunos textos lo escriben como $\mathcal{P}(A)$.

En vista de lo anterior, se puede conjeturar que para todo conjunto A se cumple

$$|2^A| = 2^{|A|} \tag{1.2}$$

y dejaremos su prueba para la sección 3. En el ejemplo, $|A| = 3$ y $2^3 = 8$.

Por otra parte, no es difícil probar que si dos conjuntos A y B son disjuntos, entonces

$$|2^{A\cup B}| = 2^{|A|+|B|} \tag{1.3}$$

pues por (1.2), que se probará en la página 33, se tiene que $|2^{A\cup B}| = 2^{|A\cup B|}$, así que basta probar que $|A \cup B| = |A| + |B|$.

Demostración. Sean $A = \{a_1, a_2, \ldots, a_m\}$ y $B = \{b_1, b_2, \ldots, b_n\}$ dos conjuntos disjuntos, es decir no hay ninguna $a_i \in B$ ni $b_i \in A$. Siendo así,

$$A \cup B = \{a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n\}$$

por lo que $|A \cup B| = m + n$, de donde $|A \cup B| = |A| + |B|$. □

Ejemplo 9. *Sean el conjunto $A = \{a, b\}$ y calculemos $A \times 2^A$, el producto cartesiano de A con su conjunto potencia. Primeramente,*

$$2^A = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$

así que $A \times 2^A$ se construye con todas las posibles parejas de un elemento de A con uno de sus subconjuntos.

$$A \times 2^A = \{(a, \emptyset), (a, \{a\}), (a, \{b\}), (a, \{a, b\}), (b, \emptyset), (b, \{a\}), (b, \{b\}), (b, \{a, b\})\}$$

Así como la notación $\Sigma_{i=1}^n x_i$ sirve para condensar la suma de n valores, si tenemos una colección de conjuntos $A_1, A_2, \ldots, A_n$ se puede indicar su unión como $\bigcup_{i=1}^n A_i$. De manera similar para la intersección.

Capítulo 2

Relaciones y Funciones

Al estudiar los fenómenos de la naturalez, se ha comprendido la importancia de la causa y su efecto. La manera como en matemáticas se formaliza esta observación es asociando elementos de un conjunto (los causales) con otro (efectos) mediante alguna relación o regla fija. Interesa estudiar las propiedades de las diversas formas de establecer vínculos entre un conjunto y otro, pues las propiedades generales se aplicarán a los casos particulares que interesan.

2.1. Relaciones

Las relaciones por sí mismas no se emplean en la Teoría de la Computación, sólo se presentan como el concepto del que surgen las funciones, al agregar cierta restricción.

Definición 7. *Una* relación *es un subconjunto del producto cartesiano entre dos conjuntos*[1].

De esta forma, se hacen asociaciones entre parejas de elementos de conjuntos distintos. Por ejemplo, sean $A = \{a, b, c\}$ y $B = \{1, 2, 3\}$. Debe ser claro que el conjunto $R = \{(a, 3), (b, 1), (b, 2), (c, 3)\}$ es una relación pues $R \subset A \times B$.

Definición 8. *Al conjunto A se le llama* dominio *y a B* rango *(o codominio).*

En el caso de las relaciones no hay restricciones en la manera de definirlas. Puede definirse la relación inversa si se intercambian dominio y rango, $R^{-1} \subset B \times A$.

Ejemplo 10. *Un ejemplo clásico es el de las relaciones familiares. Ser* padre de *o* prima de *son relaciones.*

[1]Las relaciones no tiene por qué restringirse a dos conjuntos. Por ejemplo, se puede definir una relación entre 3 conjuntos, como x prepara comida para y y z. Incluso entre n elementos: $R \subset A_1 \times A_2 \times A_3 \cdots \times A_n$, por lo que un elemento de la relación tiene la forma $(x_1, x_2, x_3, \ldots, x_n)$. En el caso de este texto solo interesan las relaciones entre 2 conjuntos.

Si f es la regla que asocia elementos del conjunto A con elementos del conjunto B, se acostumbra escribir $f : A \to B$. Si $a \in A$ y $b \in B$ están relacionados, se puede escribir $f(a) = b$ y en algunas ocasiones afb.

Ejemplo 11. *La relación entre pares de números enteros (m, n) se define por m divide a n, o $m|n$, lo que significa que el cociente n/m deja residuo cero, como en $6/3 = 2$.*

Dependiendo de su naturaleza, las relaciones pueden tener ciertas propiedades importantes. Una relación R puede ser

- *Reflexiva*, cuando todo elemento está relacionado consigo mismo, es decir, $(x, x) \in R$. Las relaciones $=$ y $\subset$ son reflexivas pues un elemento siempre es igual a sí mismo y todo conjunto es subconjunto de sí mismo.
- *Simétrica*, cuando $(x, y) \in R$ implica que $(y, x) \in R$. Ser hermano de es una relación simétrica, pero ser hijo de no lo es.
- *Transitiva*, si dados $(x, y) \in R$ y $(y, z) \in R$ se tiene que $(x, z) \in R$. Ser pariente de es una relación de transitiva, así como la contención de conjuntos.

Por comodidad, si $x \in A$ está relacionado con $y \in B$ bajo la relación R entonces se acostumbra escribir $R(x) = y$, además de la habitual $(x, y) \in R$ y se dice que R va de A a B, $R : A \to B$.

En el caso de las relaciones familiares, la relación *ser primo de* es una relación simétrica pero no reflexiva pues una persona no es primo de sí misma. Por el mismo motivo, tampoco transitiva.

Adicionalmente pueden definirse la antisimetría, la irreflexividad y otras propiedades, pero las que interesan para los objetivos de este texto son las mencionadas.

Definición 9. *Se dice que una relación R sobre un conjunto X es* de equivalencia *cuando es reflexiva, simétrica y transitiva. R separa a X en subconjuntos disjuntos dos a dos llamados* clases de equivalencia*, de tal manera que en una misma clase, todos los elementos están relacionados. Las clases de equivalente son una* partición *de X.*

La igualdad numérica es un ejemplo de relación de equivalencia. A continuación otros ejemplos menos elementales.

Ejemplo 12. *El conjunto de los rectángulos con la relación «tiene la misma área que» es una relación de equivalencia.*

Ejemplo 13. *Los ángulos que regresan el mismo valor real para cierta función trigonométrica fija.*

Ejemplo 14. *Congruencia modulo m. Dados dos valores a y b enteros y m, se dice que a es congruente con b módulo m ($a \equiv b \mod m$) si*

$$a - b = k \times m$$

para algún entero k. La congruencia módulo m es una relación de equivalencia.

2.2. Funciones

Este tipo especial de relaciones es muy útil cuando se trata de determinar si dos conjuntos tienen la misma cardinalidad, lo que en teoría de lenguajes formales es muy importante. Para ello es necesario definir algunos conceptos.

Definición 10. *Se dice que una relación $f : A \to B$ es una* función *si ocurre que $f(x) = y$ y $f(x) = z$ implica necesariamente que $y = z$, es decir, un mismo elemento en el dominio no está asociado a dos distintos del rango.*

La función $f : \mathbb{R} \to \mathbb{R}$ definida como $f(x) = x$ o (x, x) es llamda *función identidad* y es un ejemplo de función pues cada valor de $\mathbb{R}$ está asociado con sigo mismo y con ninguno más. En la notación $f(x)$, a x se le conoce como argumento.

Ejemplo 15. *La relación $\{(a, 1), (a, 2), (b, 3)\}$ no es una función porque al elemento a le corresponden tanto el 1 como el 2. Por lo mismo, la raíz cuadrada $\sqrt{} : \mathbb{R} \to \mathbb{R}$ no es una función si consideramos que $2 \times 2 = (-2) \times (-2)$, es decir, tanto el 2 como el -2 están asociados con el 4. Pero si restringimos el dominio considerando sólo la rama positiva $f(x) = +\sqrt{x}$ sí se trata de una función.*

En la sección 1 de conjuntos, faltó presentar el axioma de elección, pero era necesario antes haber definido las funciones. Y ahora es posible.

2.3. Axioma de elección

Este axioma dice que dada una colección de conjuntos, cada uno con al menos un objeto, se puede tomar exactamente un objeto de cada conjunto y ponerlos en un nuevo conjunto, aún si hay una cantidad infinita de conjuntos, y no hay una regla que indique qué objetos tomar. Formalmente, se define primero una función de elección.

Definición 11. *f es una* función de elección *si dado un conjunto no vacío A, f regresa uno (y sólo uno) de sus elementos, es decir, $f(A) \in A$.*

El *axioma de elección* dice que para cada colección de conjuntos no vacíos X existe una función de elección cuyo dominio es X.

Ejemplo 16. *Sea el conjunto X definido como*

$$X = \{\{1, 3, 4\}, \{2, 4\}, \{5, 6, 8\}\}$$

una colección de conjuntos. Una posible función de elección definida sobre X es

$$\begin{aligned} f(\{1, 3, 4\}) &= 3 \\ f(\{2, 4\}) &= 2 \\ f(\{5, 6, 8\}) &= 8 \end{aligned}$$

pues de cada conjunto se ha seleccionado un elemento.

Es un axioma controversial pues Kurt Gödel y Paul Cohen probaron, en 1931, que el axioma es independiente de la teoría de conjuntos, en el sentido de que tanto el axioma como su negación pueden resultar ciertos. La decisión de usarlo obedece más bien a la idea de que es conveniente pues algunas demostraciones son posibles de manera más simple.

Negar el axioma de elección equivale a aceptar cosas extrañas, como la existencia de dos conjuntos cuya cardinalidad es incomparable, en el sentido de que no se sabe cuál es mayor.

2.4. Funciones inversas y biyectivas

Definición 12. *Una función se dice automorfismo cuando el dominio es el mismo conjunto que el rango.*

Definición 13. *Si $f : A \to B$ es una función, su* imagen inversa *es la relación de $f^{-1} : B \to A$ definida como*

$$f^{-1}(y) = \{x | f(x) = y\}.$$

★

La imagen inversa no necesariamente es una función, pues puede darse el caso de una función donde $f(x) = f(y) = z$, con $x \neq y$ por lo que la imagen inversa es $f^{-1}(z) = x$ y $f^{-1}(z) = y$, asociando x y y al mismo elemento z, lo que no cumple con la definición de función.

Los conceptos siguientes, de inyectividad, sobreyectividad y biyectividad son importantes al momento de comparar la cardinalidad de conjuntos.

Definición 14. *Sea $f : A \to B$ una función. Se dice que f es* inyectiva *si a cada elemento del dominio A le corresponde un valor distinto del rango B, es decir, que si dados $a \in A$ y $b \in B$, ocurre que $f(a) = f(b)$ entonces necesariamente $a = b$. De manera más corta, se dice que f es 1 a 1.*

★

Proposición 5. *Si una función es inyectiva, entonces el rango tiene al menos tantos elementos como el dominio, es decir, $|A| \leq |B|$.*

Ejemplo 17. *La función $f : \mathbb{N} \to \mathbb{N}$ definida como $f(n) = 2n$ es una biyección del conjunto de los naturales al conjunto de los pares, pues para cada natural en el dominio corresponde un par y para cada par en el rango corresponde un único número natural que es su mitad. Es claro que tiene inversa.*

En vista del ejemplo anterior, hay tantos enteros como números pares, aunque el sentido común indique lo contrario.

Por su definición misma, la imagen inversa de una función inyectiva siempre es otra función.

Definición 15. *Se dice que $f : A \to B$ es* sobreyectiva *(o simplemente sobre) si cada elemento b del rango le corresponde al menos uno en el dominio, es decir, existe $a \in A$ tal que $f(a) = b$. Simbólicamente:*

$$\forall b \in B \exists a \in A : f(a) = b$$

Proposición 6. *Si una función es sobreyectiva, entonces el dominio tiene al menos tantos elementos como el rango, es decir,* $|A| \geq |B|$.

Ejemplo 18. *La función que a cada palabra le asocia su letra inicial es sobreyectiva en el conjunto del abecedario, pues hay al menos una palabra que comienza con cada letra.*

Para la Teoría de la Computación, es importante el siguiente resultado.

Proposición 7. *Sea* X *un conjunto. Entonces se cumple que hay más elementos en el conjunto potencia* 2^X *que en* X*, es decir,* $|X| < |2^X|$.

Demostración. Si a cada elememto $x \in X$ se le asocia el conjunto $\{x\}$, entonces se tiene una función inyectiva de X a 2^X, con lo que se garantiza que $|X| \leq |2^X|$, por la proposición 5. Lo que falta probar es que $|X| \neq |2^X|$. Se mostrará que no existe una función sobreyectiva de X a 2^X, suponiendo su existencia y llegando a contradicciones.

Sea $f : X \to 2^X$ cualquier función sobreyectiva y sea el subconjunto $A \subset X$ construido como

$$A = \{x | x \in X \text{ y } x \notin f(x)\} \tag{2.1}$$

es decir, si $x_1 \in X$ es un elemento de A, entonces $f(x_1) \in 2^X$ (o $f(x_1) \subset X$) es un subconjunto de X que no contiene a x_1.

Es claro que A, al ser un subconjunto de X, pertence a 2^X, es decir, es un elemento del dominio, así que, como se supone que f es sobreyectiva, debe existir un valor $\hat{x} \in X$ tal que $f(\hat{x}) = A$. Sólo puede ocurrir una de dos cosas, o $\hat{x} \in f(\hat{x})$ o $\hat{x} \notin f(\hat{x})$.

1. Si $\hat{x} \in f(\hat{x}) = A$ entonces, por la definición (2.1), debe ocurrir que $\hat{x} \notin f(\hat{x})$!
2. Si $\hat{x} \notin f(\hat{x}) = A$ entonces, por la definición (2.1), debe ocurrir que $\hat{x} \in f(\hat{x})$!

En ambos casos se llega a una contradicción, por lo que tal función f no puede ser sobreyectiva. Como f es cualquier función sobreyectiva, entonces no puede haber tal función, por lo que $|X| < |2^X|$. El diagrama de la figura 2.1 esquematiza lo anterior.

□

De la proposición anterior se desprende que siempre es posible construir conjuntos más grandes, por lo que no existe el mayor de los conjuntos. Sólo obsérvese que $|A| < |2^A| < |2^{2^A}| < \cdots$, construyendo cada vez conjuntos mayores.

Definición 16. *Si al mismo tiempo una función es inyectiva y sobreyectiva, entonces se dice que es* biyectiva.

Ejemplo 19. *La función* $f : [0, 1] \longrightarrow [2, 4]$ *dada por*

$$f(x) = 2x + 2$$

es una biyección. En los extremos, $f(0) = 2$ *y* $f(1) = 4$*. Conforme* x *va de 0 a 1, la función pasa de 2 a 4, de manera continua y lineal.*

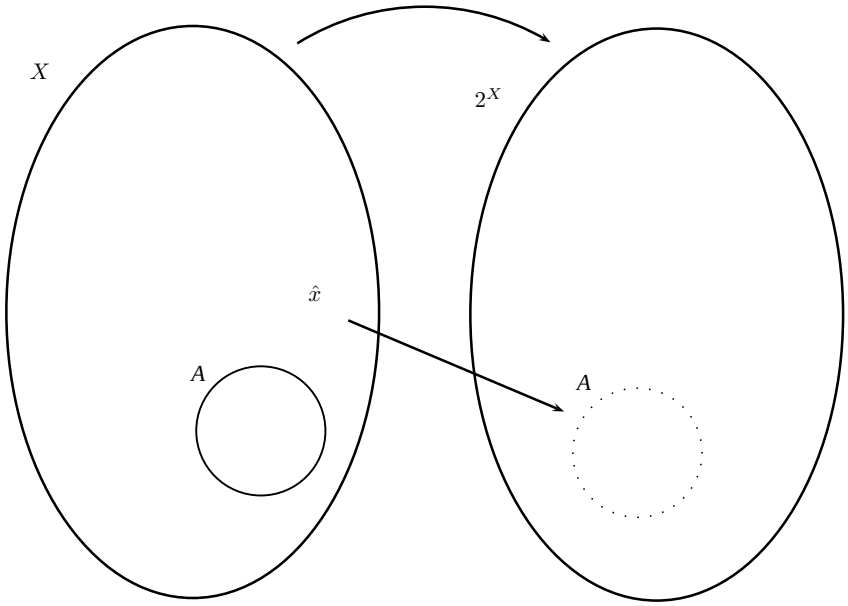


Figura 2.1: La función $f : X \to 2^X$ y el conjunto A. ¿$\hat{x}$ pertenece a A o no?

Para las funciones biyectivas, dominio y rango tienen la misma cardinalidad, $|A| = |B|$, lo que es útil para demostrar equivalencias entre lenguajes y conjuntos en general. Toda función biyectiva tiene función inversa. La función identidad es biyectiva. ★

Ejemplo 20. *La fución* $f : \mathbb{N} \longrightarrow \mathbb{R}$ *definida como*

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

es biyectiva y permite comprobar que hay tantos elementos en $(0, 1)$ *como en* $\mathbb{R}$*. Esta es conocida como la función logística.*

Ejemplo 21. *Sea* $f : 2^X \to \mathbb{N}$ *definida como* $f(A) = |A|$*, la función que a cada subconjunto de* X *le asigna su cardinalidad. La función no es inyectiva pues todos los subconjuntos con la misma cardinalidad tiene la misma imagen en el rango. Por otra parte, si el conjunto* X *es finito, el número natural* $|X| + 1$ *no tiene asignado ningún subconjunto pues el mayor tiene* $|X|$ *elementos, por lo que tampoco es sobreyectiva con el rango definido como todo* $\mathbb{N}$*.*

El siguiente es otro resultado importante para la Teoría de la Computación.

Proposición 8. *No hay un conjunto infinito más pequeño que* $\mathbb{N}$*, es decir, si* X *es un conjunto infinito, entonces* $|\mathbb{N}| \leq |X|$*.*

Demostración. Para probar esta aseveración, basta mostrar una función inyectiva de los naturales a cualquier conjunto infinito. La construcción de tal función se basa en el axioma de elección, presentado en la página 17.

Sea $g : 2^X \to X$ una función de elección con dominio en la colección de subconjuntos no vacíos de X, es decir, si $A \subset X$ y $A \neq \emptyset$, entonces $g(A) \in A$ y evidentemente, $g(A) \in X$. De esta forma, $g : 2^X \to X$ y $g(X) \in X$.

De esta definición se desprende que si $x \in X$, entonces $g\left(X - \{x\}\right)$ no puede ser x pues se requiere que g seleccione un elemento que pertenezca al conjunto que es su argumento.

Ahora, se define una función $f : \mathbb{N} \to X$ inductivamente:

$$\begin{aligned} f(1) &= g(X) \\ f(x_n) &= g(X - \{f(0), f(1), \ldots, f(x_{n-1})\}), \text{ para } n > 1. \end{aligned}$$

De esta manera, $f(2) = g(\, X - \{f(1)\}\,)$. Es importante observar que $f(x_n)$ está bien definido pues X es un conjunto infinito y $X - \{f(0), f(1), \ldots, f(x_{n-1})\}$ no es vacío, de hecho sigue siendo infinito.

$f(x_n)$ debe ser distinto de $f(0), f(1), \ldots, f(x_{n-1})$, ya que se han eliminado de X y no pueden ser elegidos por g. Como cada $f(x_i)$ se asocia a un valor distinto en X, entonces f es inyectiva, por lo que $|\mathbb{N}| \leq |X|$ para todo conjunto infinito X. □

La anterior proposición garantiza que con los números naturales se pueden contar desde el más pequeño de los conjuntos infinitos. Al haber conjuntos mayores (proposición 7), como, $2^{\mathbb{N}}$, también existen conjuntos que NO se pueden contar, llamados *no-numerables* o *incontables*, lo que queda garantizado por la proposición 7. La conclusión es que el conjunto potencia de cualquier conjunto infinito no se puede contar. A continuación otro ejemplo en un tema conocido.

Ejemplo 22. *Sea $\mathcal{F} = \{f | f : \mathbb{R} \to \mathbb{R}\}$ el conjunto de todas las funciones reales de variable real. Podemos definir una función*[2] *$f : \mathcal{F} \to \mathcal{F}$ tal que si $g \in \mathcal{F}$ entonces $f(g)$ sea la derivada de g, $f(g) = \frac{dg}{dx} = g'$.*

$\mathcal{F}$ no es inyectiva. Basta mostrar dos funciones que tengan la misma derivada: $f(x) = 2$ y $g(x) = 3$. En estos dos casos, la derivada es 0.

$\mathcal{F}$ no es sobreyectiva pues para la función $h(x) = e^{x^2}$ no existe imagen inversa, es decir, no hay función cuya derivada sea h.

2.5. Hipótesis del continuo

Un hecho interesante es el conocido como la hipótesis del continuo. Como ya se vio, $|\mathbb{N}| < |2^{\mathbb{N}}|$. Es posible especular sobre la existencia de un conjunto $A \subset 2^{\mathbb{N}}$ tal que

$$|\mathbb{N}| < |A| < |2^{\mathbb{N}}| \tag{2.2}$$

[2] En matemáticas, una función cuyo argumento es una función es llamada operador o funcional.

es decir, que siempre sea posible encontrar una cardinalidad intermedia en medio de conjuntos infinitos. En particular, si existe un subconjunto de los números reales con cardinalidad menor que la de $\mathbb{R}$ y mayor que la de $\mathbb{N}$.

Esta, que pareciera una pregunta un tanto inocente es más complicada de lo que se cree. Fue formulada en 1900 por el gran matemático Hilbert, como una de sus 23 problemas más importantes de las matemáticas. Varios de los 23 fueron resueltos, particularmente la hipótesis del continuo, pero su solución resultó más extraña.

Por una parte, en 1940 Kurt Gödel demostró que la hipótesis no podía ser refutada en los axiomas ZFC[3], así que la agregó como un axioma más.

Por otra parte, en 1963, Paul Cohen demostró que la hipótesis no podía ser demostrada en el sistema ZFC, por lo que hacía a esa teoría axiomática inconsistente.

Así, la hipótesis del continuo no puede ser demostrada ni refutada. Si se usa o no, en cada caso se llega a un sistemas axiomáticos distintos, ambos consistentes.

2.6. Composición de Funciones

Sean $f : A \to B$ y $g : B \to C$ dos funciones. Se define la *composición de funciones* $(g \circ f) : A \to C$ como

$$(g \circ f) = g(f(x)). \tag{2.3}$$

Realmente la composición de funciones no es algo nuevo ya que la función $3x + 1$ es la composición de las funciones $f(x) = 3x$ y $g(x) = x + 1$, pues $(g \circ f) = g(f(x)) = 3x + 1$.

Si los dominios y rangos son el mismo, una función puede componerse consigo misma, lo que se denota por $f \circ f = f(f(x)) = f^2(x)$. Esto no debe confundirse con el cuadrado de la función $[f(x)]^2$. Por ejemplo, si $f(x) = \cos(x)+3$, entonces

$$\begin{aligned} f^2(x) &= \cos\left(\cos(x) + 3\right) + 3 \\ \text{mientras que} \quad [f(x)]^2 &= \left(\cos(x) + 3\right)^2. \end{aligned}$$

A partir del concepto de composición, se define el de potencia de una función, de manera recursiva.

$$\begin{aligned} f^0(x) &= x \text{ la función identidad} \\ f \circ f^n &= f^n \circ f = f^{n+1} \end{aligned}$$

Cuando se calcula f^n se dice que se está iterando la función, lo que es muy común tanto en matemáticas como en computación, pues la f puede representar un programa o algoritmo.

[3]El sistema de Zermelo-Fraenkel-Choice.

2.7. Funciones computables

Un programa puede verse como una función que recibe una entrada y produce una salida. Tanto entrada como salida pueden codificarse como cadenas de bits, por lo que cada programa se interperta como una función de $\mathbb{N}$ en $\mathbb{N}$.

¿Cuántas funciones hay? ¿Cuántos programas se pueden programar? Estas dos preguntas son de gran importancia en el mundo de la computación pues si son la misma cantidad, entonces es posible hacer un programa para cada función que se pueda definir, independientemente de si son 1 a 1, sobre, biyectivas o con cualquier estructura especial.

Considérese cualquier lenguaje de programación. Está basado en una cantidad finita de palabras reservadas y operadores. Con esos elementos, se pueden comenzar a enumerar los programas desde el más pequeño construible, aumentando la cantidad de bytes uno por uno de ser posible. Esto nos da una numeración para los posibles programas, por lo que son tantos programas como números naturales. Cad programa resuelve un único problema, aunque claramente la relación *(programa, problema)* no es inyectiva.

Por otra parte, contar las funciones posibles de $\mathbb{N}$ en $\mathbb{N}$ requiere algo más de esfuerzo. Una función no tiene restricciones de dominio y rango, por lo que se puede comenzar con las funciones que van de $\mathbb{N}$ en $\{0,1\}$. Con ese dominio y rango se definen las *funciones características*. Sea $A \subset \mathbb{N}$ y su función característica $f_A : \mathbb{N} \to \{0,1\}$ como

$$f_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases}$$

que caracteríza a los elementos del conjunto A marcándolos con 1. ¿Cuántas funciones características hay? Tantas como subconjuntos se pueden definir para los números naturales, por lo que hay al menos tantas funciones como $|2^{\mathbb{N}}|$. Y eso que sólo se está contando esa familia de funciones.

Por la proposición 7, eso significa que hay más funciones que programas. ★ Este resultado es de gran importancia pues indica que hay una infinidad de problemas que no tiene solución computable, o sea que hay problemas para los que no hay programas que los resuelvan. Se acaba así la intención de que la computadora resuelva todo. Todo lo anterior es la prueba de la contundente

Proposición 9. *Hay más problemas que posibles programas de computadora.*

Pero, ¿cuáles son esos problemas para los que no hay solución? ¿aparecen en la vida cotidiana? Son muchas las preguntas que falta responder y son de gran importancia tanto teórica como práctica.

2.7.1. Incompletitud de las matemáticas

Un problema de tamaño mayúsculo para los matemáticos surgió cuando Kurt Gödel, en 1930, demostró su primer teorema de incompletitud, que dice lo siguiente.

Proposición 10. *En cualquier formalización consistente de las matemáticas que sea lo bastante fuerte para definir el concepto de números naturales, se puede construir una afirmación que ni se puede demostrar ni se puede refutar dentro de ese sistema.*

Poco tiempo después, se probó el segundo teorema, que dice que ningún sistema completo puede usarse para demostrarse a sí mismo, importantísimo resultado de la lógica matemática. La triste conclusión es que las computadoras no se pueden utilizar para programar demostradores automáticos de teoremas pues siempre habrá alguna sentencia cuya veracidad no se puede probar.

Estas limitaciones son las que se estudian en la Teoría de la Computación, buscando siempre hasta dónde es posible hacer con una computadora y qué tan eficientemente. Estos temas son conocidos como *computabilidad y complejidad.*

Capítulo 3

Inducción Matemática

Antes de entrar al tema central, vale la pena detenerse en un error común al estudiar matemáticas.

3.1. La falsa prueba de los casos particulares

Un error frecuente que cometen aquellos que no han estudiado suficiente matemáticas es de pretender comprobar algunos casos particulares de una propiedad y con eso darla por cierta.

Ejemplo 23. *Obsérvese los siguientes cálculos.*

$$1^3 + 2^3 = 9 = 3^2 = (1+2)^2$$
$$1^3 + 2^3 + 3^3 = 36 = 6^2 = (1+2+3)^2$$

A partir de esto podemos suponer que la suma de los cubos es el cuadrado de la suma, al menos para enteros positivos. Con notación matemática:

$$\sum_{i=1}^{n} i^3 = \left(\sum_{i=1}^{n} i \right)^2$$

¿Será cierto o mera coincidencia?

Ejemplo 24. *Sea $p(n) = x^2 - x + 41$. Si evaluamos este polinomio en $n = 0$ obtenemos 41, que es un número primo. Lo mismo ocurre para*

$$p(1) = 41 \quad \textit{primo}$$
$$p(2) = 43 \quad \textit{primo}$$
$$p(3) = 47 \quad \textit{primo}$$
$$p(4) = 53 \quad \textit{primo}$$
$$p(5) = 61 \quad \textit{primo}$$

y surge la sospecha de que p produce números primos. Si se evalúa $p(10)$ *se obtiene 131 y para* $n = 20$ *es 421, también primos. ¡Un polinomio que produce puros números primos! ¿Coincidencia o verdad?*

No es raro que al encontrar ciertos algunos casos particulares, la gente crea que la regla se cumplirá siempre. En el primer ejemplo, sí se cumple que la suma de cubos es igual al cuadrado de la suma. En el segundo ejemplo, se trata de algo falso. Si el polinomio se evalúa en $n = 41$, se obtiene $1681 = 41^2$ que evidentemente no es primo.

Como es impensable tratar de probar todos los posibles casos (debido a la infinitud de los números naturales), se requiere otra estrategia para garantizar que la propiedad de interés se cumple siempre. Una de tales estrategias es la prueba por inducción matemática, que a continuación se presenta.

3.2. Inducción matemática

Es clásico el juego de colocar las piezas de un dominó de tal manera que todas caigan con tirar sólo una. Muchos de videos impresionantes se pueden localizar. ¿Qué garantiza que todas las piezas caerán?

Tirar una pieza no es suficiente, la siguiente debe estar suficientemente cerca. Y la siguiente. Una pieza aislada no tirará a todas. Es necesario tener 1-la garantía de que cualquier pieza podrá tirar a la siguiente.

Cuando ya se está seguro de que cualquier pieza puede tirar la siguiente, sólo se garantiza que habrá una reacción en cadena, pero todavía falta algo: 2-tirar la primera. Estas dos ideas son la manera como trabaja la inducción matemática. Ahora es necesario formalizarla.

La inducción matemática es una técnica de demostración para propiedades que se cumplen para los números naturales, aunque hay una extensión para números reales. La idea es comprobar que si una propiedad se cumple en un caso cualquiera, digamos n, entonces también cumple en el caso siguiente $n+1$. Una vez probado eso (que cualquier dominó tirará al siguiente), lo único para ver que se cumple en todos los casos es comprobar si ocurre en el primer caso, $n = 1$ (tirar el primer dominó). Este es conocido como *caso base*.

La suposición de que la propiedad se cumple para un caso cualquiera n se llama *hipótesis de inducción* y es la premisa en la que se basará nuestra deducción, no se sabe si es cierta, sólo se le supone verdadera. Lo que se hace es probar una regla y generalizarla de manera conveniente[1].

Ejemplo 25. *Aunque es claro que* $2^n < 3^n$*, se puede utilizar inducción para probarlo.*

Demostración. El caso base es para $n = 1$: $2^1 = 2 < 3 = 3^1$. Supóngase que $2^n < 3^n$ para tratar de demostrar que $2^{n+1} < 3^{n+1}$. Se tiene que se cumplen las

[1] $(\forall P)[P(0) \wedge (\forall k \in \mathbb{N})(P(k) \Rightarrow P(k+1))] \Rightarrow (\forall n \in \mathbb{N})[P(n)]$ es la inducción con simbología lógica. Más simplemente, una vez que se prueba $P(1)$, basta probar que para toda n, $P(n) \Rightarrow P(n+1)$. Se trata de lógica de segundo orden, pues el cuantificador afecta predicados, no variables.

desigualdades

$$2 < 3$$
$$2^n < 3^n$$

pues son el caso base y la hipótesis de inducción. Si se multiplican término a término se obtiene

$$2 \cdot 2^n < 3 \cdot 3^n$$

que es lo que se quería demostrar. □

Ejemplo 26. *Probar que todo número natural de la forma $n^3 - n$ es múltiplo de 3, es decir, es igual a $3k$, para algún k entero.*

Demostración. El caso base es $n = 1$ y se cumple pues

$$1^3 - 1 = 1 - 1 = 0 = k * 0.$$

Ahora, la hipótesis de inducció que se supone cierta es que $n^3 - n = 3k$ para algún k. Lo que hay que demostrar es que

$$(n+1)^3 - (n+1) = 3k$$

para algún otro valor k. El uso de la misma variable k no debe causar confusión, se trata de el valor que corresponda para cada caso. Procediendo:

$$\begin{aligned}(n+1)^3 - (n+1) &= n^3 + 3n^2 + 3n + 1 - n - 1 \\ &= n^3 + 3n^2 + 2n \\ &= n^3 + 3n^2 + 2n + n - n \quad \text{(sumando un cero)} \\ &= n^3 - n + 3n^2 + 3n \\ &= 3k + 3n^2 + 3n \quad \text{(por hipótesis de inducción)} \\ &= 3(k + n^2 + n)\end{aligned}$$

que también es un múltiplo de 3. □

Este problema tiene una solución más simple, pues

$$\begin{aligned}n^3 - n &= (n^2 - 1)n \\ &= (n+1)(n-1)n\end{aligned}$$

que son 3 números consecutivos, desde $n-1$ a $n+1$, por lo que necesariamente debe haber algún múltiplo de 3.

Como puede observarse, no importa el orden en que se prueba. Que la hipótesis de inducción $P(n)$ implica que $P(n+1)$ es válida y el caso base, son dos cosas independientes. Se acostumbra probar el caso base primero pues si no se cumple ya no tiene caso intentar el paso inductivo.

Ejemplo 27 (Desigualdad de Bernoulli)**.** *Para todo número real $x \geq -1$ y cualquier entero $n \geq 1$ se cumple*

$$(1+x)^n \geq 1 + nx \tag{3.1}$$

Demostración. El caso base, para $n = 0$ es directo: $(1+x)^0 = 1 \geq 1 + ox$. Como hipótesis de inducción, se supone que $(1+x)^n \geq 1 + nx$. Lo que hay que demostrar es que

$$(1+x)^{n+1} \geq 1 + (n+1)x \tag{3.2}$$

por lo que se procede de la siguiente manera.

$$\begin{aligned} 1 + x &= 1 + x \\ (1+x)(1+x)^n &\geq (1+x)(1+nx) \\ (1+x)^{n+1} &\geq 1 + nx + x + nx^2 \\ (1+x)^{n+1} &\geq 1 + (n+1)x + nx^2 \end{aligned}$$

y como $nx^2 \geq 0$, entonces $(1+x)^{n+1} \geq 1 + (n+1)x$. □

La desigualdad de Bernoulli es de gran utilidad en muchas demostraciones matemáticas[2]. En ocasiones, la n se acostumbra cambiar por otra letra al enunciar la hipótesis de inducción, típicamente k, como en el caso siguiente.

Ejemplo 28. *El ejemplo más habitual de inducción es la regla para calcular la suma de los números enteros hasta n, que dice*

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \tag{3.3}$$

y que probó Euler de una manera muy ingeniosa a la edad de 7 años, aunque no con inducción. Aplicando inducción la prueba es como sigue.

Demostración. Primero se comprueba para el caso base, $n = 1$ y se cumple pues

$$1 = \frac{1(2)}{2}$$

así que se procede a plantear la hipótesis de inducción. Esta supone que la regla es cierta para un número arbitrario k, es decir,

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2} \tag{3.4}$$

y solo queda demostrar que es cierta para $k+1$. ¿Qué significa exactamente que sea cierta para $k+1$? Significa que la ecuación (3.3) aplicada a $k+1$ debe decir

$$1 + 2 + 3 + \cdots + k + (k+1) = \frac{(k+1)(k+2)}{2} \tag{3.5}$$

[2]Consulte el lector interesado el teorema del binomio y aplíquelo a $(1+x)^n$.

y que se debe llegar a este hecho a partir de la hipótesis de inductiva para k, ecuación (3.4). Para probarlo, basta hacer uso de la hipótesis, sumarle $(k+1)$ y calcular el resultado.

$$1+2+3+\cdots+k+(k+1)=\frac{k(k+1)}{2}+(k+1) \tag{3.6}$$

Ahora se procede a transformar el resultado en el segundo término de la ecuación (3.5), basta para ello álgebra de secundaria.

$$\frac{k(k+1)}{2}+(k+1)=\frac{k(k+1)}{2}+\frac{2(k+1)}{2} \tag{3.7}$$

$$=\frac{k(k+1)+2(k+1)}{2} \tag{3.8}$$

$$=\frac{(k+2)(k+1)}{2} \tag{3.9}$$

Está última expresión es igual al segundo término de la ecuación (3.5), que es lo que se quería demostrar. □

Es importante recalcar que en esta técnica de demostración, la hipótesis inductiva se supone cierta para un valor k arbitrario (el que sea), de ahí que, junto con el caso base, se llegue a que la propiedad se cumple para todas los casos a partir del base.

Como en el ejemplo anterior, es común que las demostraciones por inducción se reduzcan a álgebra sencilla, pero lo escencial es plantear la ecuación que hay que demostrar. En el ejemplo previo, la ecuación (3.5).

Ejemplo 29. *Otro ejemplo algebráico. La suma de los primeros n enteros impares positivos es n^2, es decir,*

$$1+3+5+7+\cdots+(2n-1)=n^2 \tag{3.10}$$

o, de manera más compacta, $\sum_{i=1}^{n}(2i-1)=n^2$.

Demostración. Primero, se comprueba el caso base:

$$1=1^2$$

y siendo cierto, se plantea la hipótesis de inducción: suponemos cierto lo que queremos demostrar para cierto valor k.

$$1+3+5+7+\cdots+(2k-1)=k^2 \tag{3.11}$$

Ahora, comprobamos que la regla se cumple para el siguiente caso, es decir, al sumar el impar que sigue de $2k-1$, que es $2k+1$. Es simple verlo pues

$$k^2+2k+1=(k+1)^2 \tag{3.12}$$

es uno de los productos notables más conocidos desde la secundaria. Así, se comprueba que la regla (3.10) se cumple. □

Ejemplo 30. *Ahora la suma de los pares:*

$$2 + 4 + 6 + \cdots + 2n = n(n + 1) \tag{3.13}$$

Demostración. Caso base para $n = 1$: $2 = 1(2)$ se cumple. Como hipótesis de inducción, sea cierta la ecuación (3.13) para cualquier n. Lo que hay que demostrar es que

$$2 + 4 + 6 + \cdots + 2n + 2(n + 1) = (n + 1)(n + 2).$$

Haciendo un poco de álgebra en la suma:

$$\begin{aligned} 2 + 4 + 6 + \cdots + 2n + 2(n + 1) &= n(n + 1) + 2(n + 1) \\ \text{y factorizando el término } (n + 1) &: \\ &= (n + 2)(n + 1) \end{aligned}$$

que es lo que se quería demostrar. □

Ejemplo 31. *Probar que* $\frac{n^n}{3^n} < n!$*, para* $n \geq 1$*.*

Demostración. Para el caso base la desigualdad se cumple trivialmente pues

$$\frac{1}{3} < 1.$$

Por hipótesis de inducción, se supone que la propiedad se cumple y lo que hay que demostrar es que

$$\frac{(n + 1)^{n+1}}{3^{n+1}} < (n + 1)!$$

y hay varias formas de construir la desigualdad. Como

$$\lim_{n\to\infty} (1 + \frac{1}{n})^n = e < 3 \tag{3.14}$$

entonces se tiene que $(1+\frac{1}{n})^n < 3$. De esto se obtiene $\left(\frac{n+1}{n}\right)^n < 3$ y por lo tanto

$$\frac{(n + 1)^n}{3} < n^n$$

reorganizando los factores. Multiplicando a ambos lados de la desigualdad por $\frac{n+1}{3^n}$ se obtiene

$$\frac{(n + 1)(n + 1)^n}{3^n 3} < \frac{n^n}{3^n}(n + 1)$$

Realizando las operaciones se obtiene

$$\frac{(n + 1)^{n+1}}{3^{n+1}} < \frac{n^n}{3^n}(n + 1) < n!(n + 1) = (n + 1)!$$

que es lo que se quería demostrar. □

De los ejemplos anteriores, se ve que para realizar la demostración se requiere siempre de la hipótesis de inducción, a veces de un poco de álgebra o de conocimientos matemáticos de todo tipo (como en el límite (3.14) en el ejemplo previo.)

Ejemplo 32. *Por demostrar:* $n! < \frac{n^n}{2^n}$ *para toda* $n \geq 6$.

Demostración. Caso bas: $n = 6$

$$6! = 720 < \frac{6^6}{2^6} = \frac{46654}{64} = 729$$

Como hipótesis de inducción, se supone cierto que $n! < \frac{n^n}{2^n}$ y se intentará demostrar que

$$(n+1)! < \frac{(n+1)^{n+1}}{2^{n+1}}.$$

Obsérvese que para $n \geq 6$ se cumple que

$$(n+1)! = n!(n+1) < (n+1)\frac{n^n}{2^n} \tag{3.15}$$

por hipótesis de inducción. Por otra parte, se sabe que

$$\frac{(n+1)^n}{n^n} = \left(\frac{n+1}{n}\right)^n = \left(1+\frac{1}{n}\right)^n \geq 1 + n\frac{1}{n} = 2 \tag{3.16}$$

aplicando la desigualdad de Bernoulli (3.1) (ejemplo 27). Esto puede verse como $\frac{n^n}{(n+1)^n} \leq 2$.

Utilizando las ecuaciones (3.15) y (3.16) se tiene que

$$\begin{aligned}(n+1)! &< (n+1)\frac{n^n}{2^n} && (3.17)\\ &= (n+1)\frac{n^n}{2^n}\frac{(n+1)^n}{(n+1)^n} && (3.18)\\ &\leq \frac{(n+1)^{n+1}}{2^n}\frac{1}{2} && (3.19)\\ &= \frac{(n+1)^{n+1}}{2^{n+1}} && (3.20)\end{aligned}$$

que es lo que se quería demostrar. □

Ejemplo 33. *Probar por inducción que*

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3}\cdots\frac{1}{n\cdot(n+1)} = \frac{n}{n+1}. \tag{3.21}$$

Demostración. El caso base es para $n = 1$, que es claro por $\frac{1}{1\cdot 2} = \frac{1}{2}$. Como hipótesis de inducción, se supone que (3.21) es cierto y se tiene que demostrar que

$$\sum_{k=1}^{n+1} \frac{1}{k(k+1)} = \frac{n+1}{n+2}$$

por lo que se parte de la sumatoria $\sum_{k=1}^{n+1} \frac{1}{k(k+1)}$, se separa el último sumando, se aplica la hipótesis de inducción y se realizan las operaciones.

$$\begin{aligned}
\sum_{k=1}^{n+1} \frac{1}{k(k+1)} &= \sum_{k=1}^{n} \frac{1}{k(k+1)} + \frac{1}{(n+1)(n+2)} \\
&= \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} \\
&= \frac{n}{n+1}\frac{n+2}{n+2} + \frac{1}{(n+1)(n+2)} \\
&= \frac{n(n+2)+1}{(n+1)(n+2)} \\
&= \frac{n^2+2n+2+1}{(n+1)(n+2)} \\
&= \frac{(n+1)^2}{(n+1)(n+2)} \\
&= \frac{n+1}{n+2}
\end{aligned}$$

que es lo que se quería demostrar. □

Ahora un ejemplo con propiedades entre conjuntos.

Ejemplo 34 (Ley de D'Morgan generalizada)**.** *Se puede generalizar a partir del ejemplo 3 (pág. 12). Se cumple que:*

$$(A_1 \cup A_2 \cup \cdots \cup A_n)^c = A_1^c \cap A_2^c \cap \cdots \cap a_n^c$$

o equivalentemente, $\left(\bigcup_{k=1}^{n} A_k\right)^c = \bigcap_{k=2}^{n} A_k^c$*, para* $n > 1$.

Demostración. El caso base es para $n = 2$, que se demuestra en el ejemplo 3. Como hipótesis inductiva, supóngase cierto para n

$$\left(\bigcup_{k=1}^{n} A_k\right)^c = \bigcap_{k=1}^{n} A_k^c \tag{3.22}$$

y lo que se quiere demostrar es que es válido para $n+1$:

$$\left(\bigcup_{k=1}^{n+1} A_k\right)^c = \bigcap_{k=1}^{n+1} A_k^c. \tag{3.23}$$

Calculando:

$$\left(\bigcup_{k=1}^{n+1} A_k\right)^c = \left(\bigcup_{k=1}^{n} A_k \cup A_{n+1}\right)^c \tag{3.24}$$

$$= \left(\bigcup_{k=1}^{n} A_k\right)^c \cap A_{n+1}^c \tag{3.25}$$

$$= \bigcap_{k=1}^{n} A_k^c \cap A_{n+1}^c \tag{3.26}$$

$$= \bigcap_{k=1}^{n+1} A_k^c \tag{3.27}$$

que es lo que se quería demostrar. Lo que se hizo paso a paso fue: (3.24)-separar A_{n+1} de la unión, (3.25)-aplicar el caso base y luego (3.26)-la hipótesis de inducción. Al final sólo (3.27)-se agregó $A_n + 1$ a la intersección. ν *v u* □

Ejemplo 35. *En el ejemplo (8) se dio por hecho que la cardinalidad del conjunto potencia es igual a elevar 2 a la cardinalidad del conjunto, lo que se puede probar por inducción. Sea A un conjunto no vacío. Se quiere demostrar que* $|2^A| = 2^{|A|}$. *Esto se hace por inducción sobre la cardinalidad de A.*

Demostración. La afirmación es evidente para un conjunto con un elemento, $|A| = 1$, pues $2^A = \{\emptyset, A\}$ y

$$|2^A| = |\{\emptyset, A\}| = 2$$

que es 2^1. Este es el caso base.

Por hipótesis de inducción, sea cierto que $|2^A| = 2^{|A|}$ para $|A| = n$. A partir de esta hipótesis hay que probar que se cumple para un conjunto con un elemento más.

Sea A un conjunto con $n+1$ elementos, $A = B \cup \{x\}$, donde B es un conjunto con n elementos que no contiene a x. Entonces,

$$\begin{aligned} 2^A &= 2^{B \cup \{x\}} \\ &= 2^B \cup \{T \cup \{x\} \text{ tal que } T \in 2^B\} \end{aligned}$$

por lo tanto, al ser 2^B y $\{T \cup \{x\} \text{ tal que } T \in 2^B\}$ conjuntos disjuntos, se tiene que

$$\begin{aligned} |2^A| &= \left|2^B \cup \{T \cup \{x\} \text{ tal que } T \in 2^B\}\right| \\ &= \left|2^B\right| + \left|\{T \cup \{x\} \text{ tal que } T \in 2^B\}\right| \end{aligned}$$

y por hipótesis de inducción,

$$\begin{aligned} &= 2^n + 2^n = 2 \cdot 2^n \\ &= 2^{n+1} \end{aligned}$$

que es lo que se quería demostrar. □

Ejemplo 36. *Las Torres de Hannoi un ejemplo frecuente en los cursos de estructuras de datos o matemáticas discretas, pues se presta para introducir conceptos como pilas, recursividad o ecuaciones de recurrencia. Consisten en 3 torres, además de un conjunto de n discos de diámetro que se insertan en las torres. En la posición inicial del juego, todos los discos están en la priemra torre y el objetivo es pasarlas todas hasta la tercera torre, con la mínima cantidad posible de movimientos, respetando dos reglas:*

1. *Se mueve un disco cada vez.*
2. *No se puede colocar un disco sobre otro de menor diámetro.*

Debe ser claro que para mover un único disco, se requiere un sólo movimiento. Para dos discos se requieren 3. Incluso podemos pensar en el caso de cero discos: 0 discos requieren 0 movimientos para terminar el juego. Es de gran importancia la consideración de casos particulares tan simples como los 3 anteriores, pues su comprensión permite percibir patrones generales que pueden ser complicados a partir de casos grandes.

De esta forma, si llamamos T_i a la cantidad de movimientos para pasar i discos de la primera a la tercera torre, ya sabemos que $T_0 = 0$, $T_1 = 1$ y que $T_2 = 3$.

El caso $n = 3$ no es tan complicado, ya que primero se pasan los dos discos menores a la torre central, con T_2 movimientos, luego el disco mayor a la tercera y finalmente los dos discos en la torre del centro se pasan a la tercera, de nuevo con T_2 movimientos. Es decir, en total $T_2 + 1 + T_2$ movimientos.

Esto da una idea excelente para saber cuántos movimientos se requieren en el caso de n discos: se pasan $n-1$ discos a la torre central, con T_{n-1} movimientos, luego el disco mayor a la tercera torre y finalmente los $n - 1$ discos se mueven de nuevo, ahora a la torre final. De esta forma, se tiene que

$$T_n = 2T_{n-1} + 1 \tag{3.28}$$

que es una regla que nos relaciona la cantidad de movimientos necesarios para mover n discos, a partir de que sabemos la cantidad de movimientos para $n - 1$. La ecuación (3.28) es una ecuación de recurrencia. El problema no se ha resuelto, pues no sabemos cuántos movimientos se requieren para $n = 8$, por ejemplo, pues necesitamos una fórmula que nos permita conocer T_n sin requerir de los valores anteriores.

La ecuación (3.28) junto con el hecho de que $T_0 = 0$ (caso base), permiten conocer cualquier valor de T_n. El caso de T_3 es

$$\begin{aligned} T_3 &= 2T_2 + 1 \\ &= 2 \times 3 + 1 \\ &= 7 \end{aligned}$$

pues $T_2 = 3$, como ya se había calculado. En resumen, si para $n = 0, 1, 2, 3$ tenemos que T_n vale 0, 1, 3 y 7, por lo que por inspección parece ser que la regla es

$$T_n = 2^n - 1 \tag{3.29}$$

cosa que probaremos por inducción para no tener dudas.

Demostración. El caso base ya se comprobó desde el inicio del análisis del problema, al contar los movimientos necesarios para mover 0, 1 y 2 discos. Como sea, es claro que $T_1 = 2^1 - 1 = 1$, o bien, $T_0 = 2^0 - 1 = 0$. El caso base se cumple.

Como hipótesis de inducción suponemos que la regla es cierta para cierto valor k, es decir,

$$T_k = 2^k - 1 \tag{3.30}$$

Como conocimiento que suponemos cierto tenemos dos ecuaciones, la regla de recurrencia (3.28) y la hipótesis de inducción (3.30). Usando estos dos hechos es sencillo terminar la prueba, calculando T_{k+1} a partir de T_k.

$$\begin{aligned} T_{k+1} &= 2T_k + 1 \\ &= 2(2^k - 1) + 1 \\ &= (2 \cdot 2^k - 2) + 1 \\ &= 2^{k+1} - 1 \end{aligned}$$

Así, hemos probado que nuestra regla supuesta (3.29) es correcta y ahora tenemos una fórmula cerrada, no de recurrencia, para conocer la cantidad mínima de movimientos T_n para resolver las Torres de Hannoi. □

3.2.1. Inducción más fuerte

En algunos casos, es común que demostrar la hipótesis inductiva directa es difícil y resulta mejor plantear una hipótesis distinta, más fuerte. Es el caso de los dos ejemplos siguientes.

Ejemplo 37. *Probar que*

$$\frac{1}{2} \times \frac{3}{4} \times \cdots \times \frac{2n-1}{2n} \leq \frac{1}{\sqrt{3n}}.$$

En este caso, si se plantea la hipótesis de inducción directa, se llega a caminos sin salida algebraica sencilla, lo que obliga a plantear una hipótesis mas fuerte (en el sentido de una mejor cota), que incluya a la original.

Sea $A_n = \frac{1}{2} \times \frac{3}{4} \times \cdots \times \frac{2n-1}{2n}$. *La hipótesis más fuerte que se plantea es*

$$A_n \leq \frac{1}{\sqrt{3n+1}} \tag{3.31}$$

que es más fuerte que la original porque $\sqrt{3n+1} \leq \sqrt{3n}$.

Demostración. El caso base es $n = 1$ que se cumple pues

$$A_1 = \frac{1}{2} = \frac{1}{\sqrt{3 \times 1 + 1}}$$

La hipótesis de inducción es entonces la ecuación (3.31) y lo que se desea demostrar es que

$$A_{n+1} \leq \frac{1}{\sqrt{3n+4}}$$

Como

$$A_{n+1} = A_n \times \frac{2n+1}{2n+2}$$

por lo que, aplicando la hipótesis de inducción, es posible escribir

$$A_{n+1} \leq \frac{2n+1}{2n+2} \times \frac{1}{\sqrt{3n+1}}$$

y elevando el segundo término al cuadrado, con algo de manipulación algebraica se obtiene

$$\begin{aligned}\left(\frac{2n+1}{2n+2} \times \frac{1}{\sqrt{3n+1}}\right)^2 &= \frac{(2n+1)^2}{(2n+2)^2(3n+1)} \\ &= \frac{(2n+1)^2}{(2n+1)^2(3n+4)+n} \\ &< \frac{(2n+1)^2}{(2n+1)^2(3n+4)} \\ &= \frac{1}{3n+4}\end{aligned}$$

que es lo que se buscaba probar. □

El siguiente es otro caso donde no se plantear la hipótesis inducción obvia causa problemas y es preferible utilizar una hipótesis mas fuerte, al parecer más compleja, pero que facilita las cosas. Es un caso en el que llegar a la solución puede ser un poco más laborioso.

Ejemplo 38. *Demostrar que* $\sqrt{2\sqrt{3\sqrt{\cdots\sqrt{n}}}} < 3$. *El hecho de que*

$$\sqrt{2\sqrt{3\sqrt{\cdots\sqrt{n}}}} < \sqrt{2\sqrt{3\sqrt{\cdots\sqrt{n\sqrt{n+1}}}}}$$

no ayuda, así que es necesario cambiar la hipótesis de inducción a una más fuerte.

Demostración. La hipótesis de inducción que se plantea es la siguiente. Con $n \geq 2$ fija, se asume que para $2 \leq k \leq n$ se cumple

$$\sqrt{k\sqrt{(k+1)\sqrt{\cdots\sqrt{n}}}} < k+1 \tag{3.32}$$

El caso base es ahora cuando $k = n$, que se cumple pues $\sqrt{n} < n < n+1$. Si la hipótesis de inducción (3.32) es cierta, entonces hay que probar que

$$\sqrt{(k-1)\sqrt{k\sqrt{\cdots\sqrt{n}}}} < k$$

lo que ya no es difícil. Tomando el lado izquierdo de la ecuación y elevando al cuadrado se tiene:

$$\begin{aligned}\left(\sqrt{(k-1)\sqrt{k\sqrt{\cdots\sqrt{n}}}}\right)^2 &= (k-1)\sqrt{k\sqrt{(k+1)\sqrt{\cdots\sqrt{n}}}} \\ &< (k-1)(k+1) \\ &< k^2 - 1 < k^2\end{aligned}$$

por lo que se llega al resultado esperado. □

Otra manera de aplicar inducción matemática, con algo de manipulación algebraica, es verlo como la necesidad de controlar el tamaño de

$$a_n = 2^{1/2}3^{1/4}4^{1/8}\cdots n^{1/2^{n-1}}$$

tomando logaritmos (para facilitar el trabajo[3]*) y demostrando que* $\log(a_n) < \log(3)$*. Una vez más como en otras demostraciones por inducción de desigualdades, es más sencillo demostrar algo más fuerte. En este caso, es mejor demostrar que*

$$\log(a_n) = \frac{\log 2}{2} + \frac{\log 3}{4} + \cdots + \frac{\log n}{2^{n-1}} < \log 3 - \frac{\log n}{2^{n-2}}.$$

Los detalles restantes de la prueba se dejan al lector diligente.

El ejemplo anterior está diseñado para mostrar al alumno que es necesario adaptar la forma de inducción. En ocasiones no es fácil dar con una forma que facilite las manipulaciones algebraicas subsecuentes. Por fortuna, estos casos aparecen poco en Teoría de la Computación.

3.3. Inducción como herramienta constructiva

La indución se utiliza también para definir cosas. Una definición inductiva es una receta para definir entidades matemáticas, usualmente conjuntos, que describe la manera como se agregan elementos, siempre partiendo de uno o más casos base. En estos casos, se dice que se hace una construcción inductiva.

Ejemplo 39. *Se pueden definir los números pares de manera inductiva como sigue.*

1. Caso base *0 es un número par.*

[3] Puede trabajarse con el produto a_n, pero es un poco más laborioso.

2. *$n+1$ es un número par si n no es un número par.*

El ejemplo anterior supone el orden bien conocido de los números naturales y no otro, donde se entiende que $n+1$ es el sucesor de n. Si la definición anterior resultara un tanto forzada, el ejemplo que sigue es bastante conocido en computación.

Otra área donde es común emplear inducción es en teoría de grafos, tan empleada en estructuras de datos. Recuérdese que un grafo $G = (E, V)$ es un conjunto E de vértices conectados con las aristas T. Dos definiciones útiles:

Definición 17. *Un gráfo se dice conectado o conexo si para cada par de nodos de G siempre hay una ruta o camino usando sus aristas.*

Definición 18. *Un gráfo se dice acíclico si cada par de nodos tiene una ruta única que los une.*

Ejemplo 40. *Un árbol binario es una estructura de datos de gran utilidad (y con muchas variantes), que se define eficientemente de manera inductiva.*

1. Caso base *El conjunto vacío es un árbol binario.*
2. *Un árbol binario tiene un nodo llamado raíz, ligado a otros dos árboles binarios, llamados hijo izquierdo e hijo derecho.*

Ejemplo 41. *Un árbol (no necesariamente binario) se puede definir de varias maneras. Van tres de ejemplo:*

- *Un árbol es un grafo acíclico conexo.*
- *Un nodo sólo es un árbol. Un árbol se forma uniendo dos árboles con una arista.*
- *El conjunto vacío es un árbol. Un árbol es un nodo conectado a un conjunto finito de árboles.*

Cada definición lleva a una prueba distinta de ciertas propiedades sobre árboles. El siguiente ejemplo trata sobre un concepto empleado como ejemplo para programadores novatos pero es de gran utuilidad en muchas áreas científicas.

Ejemplo 42. *Los números de Fibonacci, son bien conocidos en computación, que se pueden definir inductivamente como sigue.*

$$F_0 = 0 \tag{3.33}$$

$$F_1 = 1 \tag{3.34}$$

$$F_{n+1} = F_n + F_{n-1} \tag{3.35}$$

De esta manera, los números de Fibonacci son 0, 1, 1, 2, 3, 5, 8, 13, y así, cada nuevo número se forma sumando los dos anteriores. La ecuación (3.35) se emplea en muchas pruebas donde los números de Fibonacci aparecen. Cumplen con gran cantidad de propiedades interesantes, que pueden demostrarse por inducción, como las que siguen.

Ejemplo 43. *Los números de Fibonacci cumplen con*

$$\sum_{i=0}^{n} F_i = F_{n+2} - 1 \tag{3.36}$$

Demostración. Caso base: para $n = 0$ se cumple pues

$$F_0 = 0 = F_2 - 1 = 1 - 1 = 0$$

y falta plantear la hipótesis inductiva y probarla para el siguiente caso.

Hipótesis de inducción: supongamos que se cumple que

$$\sum_{i=0}^{n} F_i = F_{n+2} - 1 \tag{3.37}$$

y veamos si es válido para el caso $n + 1$. Lo que hay que demostrar es que

$$\sum_{i=0}^{n+1} F_i = F_{n+3} - 1$$

y partiendo de esta sumatoria:

$$\begin{aligned} \sum_{i=0}^{n} F_i + F_{n+1} &= F_{n+2} - 1 + F_{n+1} && \text{por (3.37)} \\ &= F_{n+2} + F_{n+1} - 1 \end{aligned}$$

y finalmente, por (3.35)

$$= F_{n+3} - 1$$

que es lo que se quería demostrar. □

Ejemplo 44. *Probar que* $\sum_{i=1}^{n} F_i^2 = F_n F_{n+1}$.

Demostración. Caso base $n = 1$: $F_1^2 = 1 = F_1 F_2 = 1 \cdot 1 = 1$.

Como hipótesis de inducción, supóngase que

$$\sum_{i=1}^{n} F_i^2 = F_n F_{n+1} \tag{3.38}$$

para cualquier $n \geq 1$. Lo que hay que probar es que

$$\sum_{i=1}^{n+1} F_i^2 = F_{n+1} F_{n+2}$$

así que se procede de la sumatoria:

$$\begin{aligned}
\sum_{i=1}^{n+1} F_i^2 &= \sum_{i=1}^{n} F_{n+1}^2 + F_{n+1}^2 && \text{separando } F_{n+1}^2 \\
&= F_n F_{n+1} + F_{n+1}^2 && \text{por (3.38)} \\
&= F_{n+1}(F_n + F_{n+1}) && \text{factorizando} \\
&= F_{n+1} F_{n+2} && \text{por (3.35)}
\end{aligned}$$

que es lo que se quería demostrar. □

El siguiente ejemplo es un poco más elaborado. Se sugiere que el lector haga algunos intentos propios antes de leer la demostración.

Ejemplo 45. *Probar que* $F_{n+1}F_{n+2} - F_n F_{n+3} = (-1)^n$.

Demostración. El caso base funciona para $n = 0$ pues

$$F_1 F_2 - F_0 F_3 = 1 \cdot 1 - \cdot 2 = 1 = (-1)^0$$

y si asumimos que lo que queremos probar es cierto, lo que se requiere probar es que $F_{n+2}F_{n+3} - F_{n+1}F_{n+4} = (-1)^{n+1}$. A calcular, desarrollando los términos con subíndice $n+2$ a $n+4$, reagrupando y haciendo algo de álgebra:

$$\begin{aligned}
F_{n+2}F_{n+3} - F_{n+1}F_{n+4} &= \\
&= (F_n + F_{n+1})(F_{n+1} + F_{n+2}) - F_{n+1}(F_{n+3} + F_{n+2}) \\
&= F_n F_{n+1} + F_n F_{n+2} + F_{n+1}^2 + F_{n+2}F_{n+1} - F_{n+1}(2F_{n+2} + F_{n+1}) \\
&= F_n(F_{n+1} + F_{n+2}) + F_{n+1}^2 + F_{n+2}F_{n+1} - 2F_{n+1}F_{n+2} - F_{n+1}^2 \\
&= F_n F_{n+3} - F_{n+1}F_{n+2} \\
&= -(F_{n+1}F_{n+2} - F_n F_n + 3) \\
&= -(-1)^n = (-1)^{n+1}
\end{aligned}$$

□

Es importante para los estudiantes encontrar la manera como estas demostraciones ocurren. Entender cómo se justifica pasar de una línea a otra.

La inducción matemática es ampliamente utilizada en las ciencias de la computación, pues todas las entidades con las que una computadora trabaja son numerables. De ahí la importancia que reviste. A veces empleada para demostrar propiedades y a veces para construir conceptos que se requiere formalizar.

3.4. Inducción estructural

Un tipo especial de inducción se aplica cuando se trata de un problema que involucra estructuras definidas de manera inductiva. La *inducción estructural* se usa para probar que cierta proposición $P(x)$ se cumple para toda estructura definida recursivamente. Este tipo de estructuras siempre preservan un orden parcial bien definido.

En las pruebas por inducción estructural, el caso base se establece para las estructuras mínimas posibles. Luego, suponiéndo la propiedad cierta, hay que probar que se cumple para las subestructuras inmediatas de la estructura S, también se cumplen para S.

Ejemplo 46. *En todo árbol T, la cantidad de aristas $|E|$ es igual a la cantidad de vértices $|V|$ menos 1. Considérese la segunda de las definiciones.*

Demostración. Caso base: Si T consta de un vértice, entonces tiene cero aristas, así que

$$|E| = |V| - 1 = 0$$

Como hipótesis de inducción, se supone que si un árbol tiene k vértices, entonces posee $k-1$ aristas, con $k \leq n$.

Considérese ahora un árbol $T = (E_T, V_T)$ con $n+1$ vértices. Sea e una arista arbitraria y sea $G = (V, T)$ la gráfica que resulta de eliminar e de T, es decir, $G = (E - \{e\}, V_T)$.

El grafo G consta de dos componenetes conexas $G_1 = (E_1, V_1)$ y $G_2 = (E_2, V_2)$, que tienen de 1 a n nodos máximo, por lo que cumplen la hipótesis de inducción. Así, se tiene que

$$\begin{aligned} |V| &= |V_1| + |V_2| \\ |E| &= |E_1| + |E_2| \\ &= |V_1| - 1 + |V_2| - 1 \quad \text{(por hipótesis de inducción)} \\ &= |V| - 2 \end{aligned}$$

y como $|E_T| = |E| + 1$ por la arista eliminada e, se tiene

$$|E_T| = |V| - 2 + 1 = |V| - 1$$

que es lo que se quería demostrar. □

Ejercicios

Conjuntos

1.1 Defina el conjunto de las letras mayúsculas y minúsculas de dos maneras distintas.

1.2 Probar que los números impares son tantos como las potencias de 10.

1.3 Calcule $\left|2^{\{a,b,c\}}\right|$.

1.4 Demuestre los casos faltantes de las proposiciones 3 y 4.

1.5 Demostrar que $(A \cup B)^c = A^c \cap B^c$.

1.6 Demostrar que si $A - B = B - A$ entonces $A = B$.

1.7 Demostrar que si dos conjuntos A y B son disjuntos, entonces $|2^{A \cup B}| = 2^{|A|+|B|}$.

1.8 ¿Por qué no puede definirse una función de elección sobre un conjunto potencia?

Funciones

2.1 Compruebe que la congruencia módulo m es una relación de equivalencia.

2.2 Pruebe que la norma vectorial euclideana es sobreyectiva.

2.3 Demuestre que hay tantos pares como números naturales.

2.4 Analice la posible biyectividad de la función que asocia a cada polinmio el conjunto de sus raíces.

2.5 ¿Es biyectiva la función que asocia cada programa con su salida?

Inducción matemática

3.1 Pruebe que $0 + 2 + 4 + 6 + \cdots + 2n = n(n + 1)$

3.2 Pruebe que $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

3.3 Pruebe que $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2$. De esto hay una prueba geométrica interesante.

3.4 Pruebe que $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$.

3.5 Pruebe que $\sum_{i=1}^{n} \frac{1}{2^i} = 1 - \frac{1}{2^n}$.

3.6 Pruebe que $\sum_{i=2}^{n} \frac{1}{i^2} < 2$.

En el caso de los números de Fibonacci, constantemente se emplea la ecuación (3.35).

3.7 Pruebe que $\sum_{i=0}^{n} F_i = F_{n+2} - 1$.

3.8 Pruebe que $\sum_{i=0}^{n} F_i^2 = F_n F_{n+1}$.

3.9 Pruebe que $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.

3.10 $2^n < n!$.

3.11 $n! < n^n$.

3.12 Un árbol con n vértices tiene $n - 1$ aristas.

3.13 Todo número natural se puede escribir como la suma de potencias de 2.

3.14 La gráfica completa K_n tiene $n(n - 1)/2$ aristas.

3.15 Todo grafo conexo $G = (V, E)$ con $|V| \geq 2$, tiene al menos dos vértices tales que al quitarlos, G sigue estando conectada.

3.16 Una gráfica planar con n vértices, e aristas y f caras cumple con $n-e+f = 2$.