Universidad Católica Argentina
Facultad de Ingeniería

Matemática Discreta
Ingeniería Informática

Telma Caputti

Buenos Aires-Argentina
2008

Matemática Discreta
Ingeniería Informática

Telma Caputti

.

IMPRESO EN LA ARGENTINA

A los Doctores Enzo Gentile y Miguel Marcos Herrera.

Tabla de Contenidos

Capítulo 1

Números Naturales

1.1 Principio de inducción

1.1.1 Conjuntos Inductivos

Sea R el conjunto de los números reales.

Definición

Un subconjunto $S \subseteq R$ es <u>*inductivo*</u> si satisface las siguientes propiedades

$$\begin{array}{llll} a) & 1 & \in & S \\ b) & si\ j \in S & \Rightarrow (j+1) & \in S \end{array}$$

Conjuntos inductivos

a) R

b) $R_{>0}$

c) N

Conjuntos no inductivos

a) $\emptyset \subset R$ ya que no satisface (a)

b) $S = [1, 2]$ ya que no satisface (b)

Definición

Dado I un conjunto inductivo de números reales.
Si $I \subset N \Rightarrow I = N$.
Es decir, el conjunto de los números naturales es el <u>*menor*</u> conjunto inductivo de R en el sentido de la inclusión, es decir,
Si S es un subconjunto inductivo de R entonces $N \subset S$.

Ejemplo I

$\forall\, n \in N \Rightarrow D[(x-a)^n] = n(x-a)^{n-1}$

En efecto

a) Si $n = 1$ la propiedad es válida pues $D[(x-a)] = 1$

b) Hagamos la siguiente hipótesis inductiva

Supongamos válida la propiedad para $n = k \in N$, es decir,

$$D[(x-a)^k] = k(x-a)^{k-1}$$

c) y probemos la tesis inductiva, es decir, su validez para $n = k+1$

$$D[(x-a)^{k+1}] = (k+1)(x-a)^k$$

En efecto

$$\begin{aligned} D[(x-a)^{k+1}] &= D[(x-a)^k(x-a)] \\ &= D[(x-a)^k](x-a) + (x-a)^k D[x-a] \\ &= k(x-a)^{k-1}(x-a) + (x-a)^k \\ &= (k+1)(x-a)^{k+1-1} \\ &= (k+1)(x-a)^k \end{aligned}$$

Ejemplo II

$$[\cos\alpha + i\sin\alpha]^n = \cos n\alpha + i\sin n\alpha \;\forall\, n \in N$$

En efecto
a) Si n=1 entonces la propiedad se verifica trivialmente

b) Hagamos la siguiente hipótesis inductiva

Supongamos válida la propiedad para $n = k \in N$, es decir

$$[\cos\alpha + i\sin\alpha]^k = \cos k\alpha + i\sin k\alpha$$

c) y probemos la tesis inductiva, es decir, su validez para $n = k+1$

$$[\cos\alpha + i\sin\alpha]^{k+1} = \cos(k+1)\alpha + i\sin(k+1)\alpha$$

En efcto

$$\begin{array}{rcl} [\cos\alpha + i\sin\alpha]^{k+1} & = & [\cos\alpha + i\sin\alpha]^k[\cos\alpha + i\sin\alpha] \\ & = & [\cos k\alpha + i\sin k\alpha][\cos\alpha + i\sin\alpha] \\ & = & \cos k\alpha[\cos\alpha - \sin k\alpha\sin\alpha) \\ & + & i\sin k\alpha\cos\alpha + \cos k\alpha\sin\alpha) \\ & = & \cos(k+1)\alpha + i\sin(k+1)\alpha \end{array}$$

Ejemplo III

$$10^{n+1} + 10^n + 1 \ es\ divisible\ por\ 3\ \forall n \in N$$

En efecto

a) Si $n = 1$ el resultado es 111 que es múltiplo de 3

b) Hagamos la siguiente hipótesis inductiva
Supongamos cierta la propiedad para $n = k$ es decir

$$10^{k+1} + 10^k + 1 \ es\ divisible\ por 3$$

y probemos la tesis inductiva, es decir, su validez para $n = k + 1$

$$10^{k+2} + 10^{k+1} + 1 \ es\ divisible\ por 3$$

En efecto,

$$10^{k+2} + 10^{k+1} + 1 = 10(10^{k+1} + 10^k + 1) - 10 + 1$$

es mútiplo de 3 ya que es suma de múltiplos de 3.

Ejemplo IV

$$\sum_{i=1}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)\ \forall n \in N$$

En efecto

a) Si $n = 1$ resulta $1 = \frac{1}{6}(2)(3)$

b) Hagamos la siguiente hipótesis inductiva

Supongamos válida la propiedad para $n = k$, es decir,

$$\sum_{i=1}^{k} i^2 = \frac{1}{6}k(k+1)(2k+1)$$

y comprobemos la tesis inductiva, es decir, su validez para $n = k + 1$

$$\sum_{i=1}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2k+3)$$

En efecto

$$\begin{array}{rcc}
\sum_{i=1}^{k+1} i^2 & = & \sum_{i=1}^{k} i^2 + (k+1)^2 \\
 & = & \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \\
 & = & \frac{1}{6}(k+1)[k(2k+1) + 6(k+1)] \\
 & = & \frac{1}{6}(k+1)(2k^2 + 7k + 6) \\
 & = & \frac{1}{6}(k+1)2(k+2)(k+\frac{3}{2}) \\
 & = & \frac{1}{6}(k+1)(k+2)(2k+3)
\end{array}$$

calculando las raíces de la ecuación cuadrática $2k^2 + 7k + 6$.

1.2 Principios de Inducción y Buena Ordenación

1.2.1 Conjuntos con primer elemento

Definición

Sea J un subconjunto de R.
$j_0 \in J$ es <u>*primer elemento*</u> de J (o elemento minimal en J) si cualquiera sea $j \in J$ se satisface $j_0 \leq j$.

Ejemplos de conjuntos con primer elemento

Los siguientes conjuntos de números reales tienen primer elemento

a) N

b) $[0, 1)$

c)$\{3, 4, 5, 1/4, 1/2, -1/8\}$

Ejemplos de conjuntos sin primer elemento

Los siguientes conjuntos de números reales no tienen primer elemento

a) Z

b) $\emptyset$

c) $(0, 1]$

1.2.2 Conjuntos Bien Ordenados

Definición

Un subconjunto S de números reales está *bien ordenado* si *todo* subconjunto no vacío de S tiene primer elemento.

Ejemplos de conjuntos bien ordenados

a) $\emptyset$

b) Todo subconjunto de números reales de la forma $\{a_1, a_2, \ldots, a_n\}$

1.2.3 Unión e intersección de Conjuntos Bien Ordenados

Teorema

Sean S_1 y S_2 subconjuntos de R bien ordenados.
Entonces

a) $S_1 \cup S_2$ está bien ordenada

b) $S_1 \cap S_2$ está bien ordenada

Demostración

Probamos sólo que la unión de conjuntos bien ordenados está bien ordenada.
En efecto
Por cierto, si $S_1 = \emptyset$ ó $S_2 = \emptyset$ no hay nada que probar.
Supongamos entonces que $S_1 \neq \emptyset$ y $S_2 \neq \emptyset$.

Sea

$$T \neq \emptyset \ : \ T \subset S_1 \cup S_2 \neq \emptyset$$

Por cierto

$$T = (S_1 \cap T) \cup (S_2 \cap T$$

Observemos que si $S_1 \cap T = \emptyset$ entonces $T \subset S_2$ con lo cual tiene primer elemento.
Análogamente sucede si $S_2 \cap T = \emptyset$.
Sean, entonces, ambos $S_1 \cap T \neq \emptyset$ y $S_2 \cap T \neq \emptyset$ y sean
s_1 el primer elemento de $S_1 \subset T$ y s_2 el primer elemento de $S_2 \subset T$.

Luego, $s = \min\{s_1, s_2\}$ es primer elemento de T

Teorema

N está bien ordenado.

<u>*Demostración*</u>

Sea S el conjunto de todos los números naturales j con la siguiente propiedad

j no pertenece a ningún subconjunto de N sin primer elemento

Es claro que $1 \in S$ pues 1 es primer elemento de cualquier subconjunto de números naturales que lo contenga.
Sea $k \in S$, es decir, que todo conjunto de números naturales que contiene a k tiene primer elemento.

Probemos que $(k+1) \in S$

Sea Y un subconjunto de números naturales que contiene a $(k+1)$. Si $k \in Y$ entonces Y tiene primer elemento.
Ahora, supongamos que $k \notin Y$ y formemos el conjunto $Y \cup \{k\} = \tilde{Y}$
Dado que $it\tilde{Y}$ contiene a k tiene primer elemento.
Llamemos y_0 a ese número con lo cual $y_0 \leq k$ y, además, $y_0 \leq y \ \forall \ n \in Y$.
Ahora bien, si $y_0 = k$ entonces $(k+1)$ es primer elemento de Y pues $k \notin Y$ y $(k+1) \in Y$.

Si $y_0 \neq k$ entonces $y_0 \in Y$ siendo su primer elemento. Por lo tanto, hemos probado que si Y es un subconjunto de N que contiene a $(k+1)$ entonces Y tiene primer elemento. Esto, equivale a decir que $(k+1) \in S$. Por lo tanto, S es inductivo.
Según el Principio de Inducción resulta $S = N$ lo cual se traduce en que

Todo número natural pertenece sólo a conjuntos de números naturales con primer elemento.

Por lo tanto, todo subconjunto de números naturales que contiene por lo menos un número natural tiene primer elemento.

Recí procamente, supuesto válido el Principio de Buena Ordenación en N es posible deducir el Principio de Inducción.

Queda propuesto como ejercicio para el lector la deducción del Principio de Inducción a partir del Principio de Buena Ordenación.

Cardinal de Partes de un Conjunto

Teorema
Sea X un subconjunto de n elementos, es decir $Card\ X = n$.
Entonces, la familia de partes de X ($P(X)$ tiene cardinal 2^n.
Demostración
Si $n = 0$ es X el conjunto vací o y como el único subconjunto del conjunto vací ó es él mismo, por lo tanto, $CardP(X) = 2^0 = 1$.

Supongamos válido el Teorema cuando $n = k$ y veamos que se verifica para $n = k + 1$.
Sea, entonces, $Card(X) = k + 1$ y sea $x \in X$. Consideremos una partición de X de las siguientes dos formas:

La primera agrupa a todos los subconjuntos de X que contienen a x y la segunda agrupa a todos los subconjuntos de X que no contienen a x.
Si denotamos por

$$X_1, X_2, ..., X_j$$

todos los subconjuntos de X que no contienen a x logramos

$$X_1 \cup \{x\}, X_2 \cup \{x\}, ..., X_j \cup \{x\}$$

que es una colección de conjuntos que sí contienen a x. Por lo tanto, el número de subconjuntos de X que contienen a x es igual al número de subconjuntos de X que no lo contienen.

Si $Y = X - \{x\}$ resulta $CardP(X) = 2CardP(Y) = 2 \cdot 2^k = 2^{k+1}$ pues $P(Y)$ contiene todos los subconjunto de X que no contienen a x.
Por lo tanto, la propiedad enunciada es válida para $n = k + 1$.

1.2.4 Ejercicios

Ejercicio 1

Sea $a \in R$
$\forall\ n \in N$ definimos la potencia a^n como sigue:

$$\begin{array}{rcl} a^1 & = & a \\ a^{k+1} & = & a^k a \end{array}$$

Por lo tanto, el conjunto S de números naturales para los cuales está definido a^n es inductivo y así $S = N$.

Probar

$\forall\ n, m \in N$

a) $(a.b)^n = a^n.b^n$

b) $a^n.a^m = a^{n+m}$

c) $(a/b)^n = a^n/b^n$ si $b \neq 0$

d) $(a^n)^m = a^{n.m}$

Ejercicio 2

$\forall\ n \in N$ definimos $n!$ como sigue

$$\begin{array}{ccc} 0! & = & 1 \\ 1! & = & 1 \\ (n+1)! & = & (n+1)n! \end{array}$$

Probar

$n! \geq 2^{n-1} \quad \forall\ n \in N$

Ejercicio 3

Sea $a \in R - \{1\}$. Probar inductivamente que

$$\sum_{k=0}^{n} a^k = \frac{a^{n+1}-1}{a-1}\ \forall n \geq 0$$

Ejercicio 4

Probar, inductivamente, las siguientes relaciones

a) $\sum_{k=1}^{n}(2k-1) = n^2$

b) $\sum_{k=1}^{n} kk! = (n+1)! - 1$

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

d) $\sum_{k=1}^{n} k^3 = [\frac{n(n+1)}{2}]^2$

Ejercicio 5

Dado k entero tal que $0 \leq k \leq n$ definimos el coeficiente binomial

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{k!(n-k)!}$$

Probar, inductivamente, las siguientes relaciones

a) $\forall\ n \in N$ y todo k tal que $0 \leq k \leq n$ es

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \left(\begin{array}{c} n \\ n-k \end{array} \right)$$

b) La ley del triángulo de Tartaglia
$\forall\ n \in N$ y todo k tal que $1 \leq k \leq n$ es

$$\left(\begin{array}{c} n+1 \\ k \end{array} \right) = \left(\begin{array}{c} n \\ k-1 \end{array} \right) + \left(\begin{array}{c} n \\ k \end{array} \right)$$

e ilustrar para $n = 7$.

c) El Teorema binomial
Dados a y b n'umeros reales y $n \in N$ es válida la siguiente relación

$$(a+b)^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a^k b^{n-k}$$

d) Deducir de la parte (c) que

$$\sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) = 2^n$$

y

$$\sum_{k=0}^{n} (-1)^k \left(\begin{array}{c} n \\ k \end{array} \right) = 0$$

Ejercicio 6

Probar

a) $n! + (n+1)! = (n+2)n!\ \forall\ n \in N$

b) $(n+1)! - n! = n(n!)\ \forall\ n \in N$

c) $n(n-1)(n-2)! = n!\ \forall\ n \geq 2$

Ejercicio 7

Probar que cualquiera sea n natural, dados a y b reales es válido

$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-k-1}$$

Deducir que si n y p son números naturales, entonces

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

Ejercicio 8

Probar que si un conjunto de números naturales H satisface las siguientes propiedades

$$\begin{array}{ccc} k_0 & \in & H \\ Si\ n \in H\ y\ n \geq k_0 & \Rightarrow & (n+1) \in H \end{array}$$

entonces H contiene al conjunto de todos los números naturales $n \geq k_0$.

Ejercicio 9

Probar, inductivamente, cada una de las siguientes desigualdades

a) $2^n \geq 2n+1\ \forall\ n \in N$

b) $2^n \geq n^2\ \forall\ n \geq 4$

c) $\frac{\prod_{k=1}^{n}(2k-1)}{\prod_{k=1}^{n} 2k} \leq \frac{1}{\sqrt{n+1}}\ \forall\ n \geq 1$

Ejercicio 10

Probar que $\forall\ a \in R\backslash\{1\}$ y $\forall\ n \in N$

$$\prod_{k=1}^{n}[1 + a^{2^{k-1}}] = \frac{1-a^{2^n}}{1-a}$$

a) ¿Cuánto vale el producto si $a = 1$?.

Ejercicio 11

Sean $a_1, a_2, ..., a_n$ números reales, todos del mismo signo, y todos mayores que -1. Probar, por inducción, que

$$(1 + a_1)(1 + a_2) \cdots (1 + a_n) \geq 1 + a_1 + a_2 + \cdots + a_n$$

a) Deducir que si $a \in R$ y $a > -1$ entonces

$$(1 + a)^n \geq 1 + na$$

b) Probar que si $n > 1$ entonces la igualdad es válida si y sólo si $a = 0$.

Ejercicio 12

Diseñe e implemente por computadora algoritmos sencillos para cada una de las sumatorias del Ejercicio 5.

Ejercicio 13

Sea b un número entero positivo. Probar, inductivamente, que cualquiera sea el entero $n \geq 0$ existen enteros no negativos q y r tales que

$$n = qb + r \quad \text{con} \quad 0 \leq r < b$$

1.2.5 Forma alternativa del Principio de Inducción

Sean n un entero positivo y $P(n)$ una proposición matemática.
a) si $P(1)$ es verdadera y,
b) si $P(k{+}1)$ es verdadera para k entero positivo siempre que $P(1), P(2), ..., P(k)$ son verdaderas entonces $P(n)$ es verdadera para todo $n$entero positivo.

Demostración

Consideramos el conjunto

$$F = \{t \in Z^+ : P(t) \ \textit{es falsa}\}$$

y veamos que F es el conjunto vacío.
En efecto, si $F \neq \emptyset$ según el Principio de Buena Ordenación el conjunto F tiene primer elemento s. Dado que $P(1)$ es verdadera es $s \neq 1$ con lo cual es $s > 1$ y, en consecuencia, es $(s - 1) \in Z^+$.
Como $(s - 1) \notin F$ resulta $P(s - 1)$ verdadera. Luego, por la hipótesis (b) es $P(s{-}1{+}1) = P(s)$ verdadero lo cual contradice que $s \in F$. Por lo tanto, $F = \emptyset$.

Ejemplo I

Consideremos un grafo no dirigido $G = \{N, A\}$ con N nodos y A arcos.
Un grafo no dirigido G es un <u>*árbol*</u> si G es conexo y no tiene ciclos.
La forma alternativa del Principio de Inducción nos permite probar la siguiente propiedad
<u>*Teorema*</u>
Si $G = \{N, A\}$ es un árbol entonces

$$Card(N) = Card(A) + 1$$

<u>*Demostración*</u>
Hacemos esta demostración por inducción en $Card(A)$
Si $Card(A) = 0$ entonces el árbol consta de un solo nodo aislado, es decir, $Card(N) = 1 = Card(A) + 1$.
Supongamos válida la propiedad para cualquier árbol que contenga a lo sumo k arcos con $k \geq 0$ y consideremos un árbol $G = \{N, A\}$ con $Card(A) = k + 1$ a partir del cual podemos obtener dos sub-árboles, a saber

$$\begin{array}{rcl} G_1 & = & \{N_1, A_1\} \\ G_2 & = & \{N_2, A_2\} \end{array}$$

donde

$$\begin{array}{rcl} Card(N) & = & Card(N_1) + Card(N_2) \\ Card(A_1) & = & Card(A) - Card(A_2) - 1 \end{array}$$

Como $Card(A_1)$ y $Card(A_2)$ son no negativos y menores o iguales que k, entonces, según el Principio de Inducción, se verifican

$$Card(A_i) + 1 = Card(N_i) \quad i = 1, 2$$

En consecuencia,

$$\begin{array}{rcl} Card(N) & = & Card(N_1) + Card(N_2) \\ & = & Card(A_1) + 1 + Card(A_2) + 1 \\ & = & (Card(A_1) + Card(A_2) + 1) + 1 \\ & = & Card(A) + 1 \end{array}$$

con lo cual obtenemos lo propuesto vía la forma alternativa del Principio de Inducción.

Observación

A cada n entero positivo le asociamos la proposición $P(n)$.
Si para cada m es $P(k)$ verdadera para todo $k < m$ implica que $P(m)$ es verdadera, entonces, podemos afirmar que $P(n)$ es verdaera para todo entero positivo n.
En efecto, sea S el conjunto de n enteros positivos para los cuales es $P(n)$ falsa.

A menos que el conjunto S sea vacío tendrá mínimo elemento m. Por la elección de m es $P(k)$ verdadera para todo $k < m$ de ahí que $P(m)$ deba ser cierta, obteniendo así una contradicción. La única solución es admitir que S sea vacío.

1.2.6 Otros Ejercicios

Ejercicio 1

Mostrar, inductivamente, la validez de las siguientes relaciones

a) $1 + 3 + 5 + ... + (2n - 1) = n^2$

b) $1.3 + 2.4 + 3.5 + ... + n(n + 2) = \frac{1}{6}n(n + 1)(2n + 7)$

c) $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$

d) $\sum_{i=1}^{n} 2^{i-1} = \sum_{i=0}^{n-1} = 2^n - 1$

e) $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4} = (\sum_{i=1}^{n} i)^2$

f) $n - 2 < \frac{n^2-n}{12}$ para $n > 10$

g) $\sum_{k=1}^{n} k(k!) = (n + 1)! - 1$

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

i) $\frac{1}{2n} \leq \frac{1.3.5....(2n-1)}{2.4.6....(2n)} \leq \frac{1}{sqrtn+1}$

j) $3^n + 7^n - 2$ es divisible por 8 para todo $n \geq 1$

k) Dados $a_1, ..., a_{2^n}$ números reales positivos se verifica la siguiente desigualdad

$$[a_1.a_2...a_{2^n}]^{\frac{1}{2^n}} \leq \frac{1}{2^n}[a_1 + a_2 + ... + a_{2^n}]$$

Ejercicio 2

Sea para n entero positivo $P(n)$ el número aproximado de bacterias en un cultivo después de n horas. Si

$$\begin{array}{lcc} P(1) & = & 1000 \\ P(2) & = & 2000 \\ P(n) & = & P(n-1) + P(n-2) \ \ \forall\ n > 2 \end{array}$$

mostrar que

$$P(n) = \frac{1000}{\sqrt{5}}\{(\frac{1+\sqrt{5}}{2})^{n+1} - (\frac{1-\sqrt{5}}{2})^{n+1}\}$$

Ejercicio 3

Sea para n entero positivo $P(n)$ la siguiente propoisición

$$\sum_{i=1}^{n} = \frac{(n+0,5)^2}{2}$$

a) Mostrar que la validez de $P(k)$ implica la validez de $P(k+1)$ para cualquier k entero positivo.
b)¿Es verdadera $P(n)$ para todo entero positivo?.

Ejercicio 4

Dadas n rectas en el plano, suponiendo que no hay dos rectas que sean paralelas y que tampoco hay tres que se corten en el mismo punto, probar, inductivamente que dividen el plano cartesiano en

$$\frac{n^2+n+2}{2}$$

regiones.
Manejo de sumatorias y de productorias

1.3 Sumatorias

1.3.1 Definición

Dada la sucesión $a_1, a_2, ..., a_n$ de números reales, emplearemos la notación $\sum_{R(j)} a_j$ para denotar la sumatoria de elementos a_j donde j es un entero positivo que satisface la condición $R(j)$. En repetidas oportunidades, el significado preciso de esta notación es el siguiente

$$\begin{aligned} \textstyle\sum_{R(j)} a_j &= (\lim_{n\to\infty} \textstyle\sum_{\substack{0 \leq j \leq n \\ R(j)}} a_j + \\ &+ (\lim_{n\to\infty} \textstyle\sum_{\substack{-n \leq j \leq 0 \\ R(j)}} a_j) \end{aligned}$$

siempre y cuando ambos límites existan con valor finito.

1.3.2 Propiedades

a)

$$[\sum_{R(i)} a_i][\sum_{S(j)} b_j] = \sum_{R(i)}[\sum_{S(j)} a_i b_j]$$

b) Cambio de índices variables

$$\sum_{R(i)} a_i = \sum_{R(j)} a_j = \sum_{R_{p(j)}} a_{p(j)}$$

En este caso, la función $p(j)$ dependiendo de j representa una permutación del rango de valores, es decir, para cada entero i que satisfaga la relación $R(i)$ debe haber otro entero j tal que $p(j) = i$ y recíprocamente.
Por ejemplo,

$$\sum_{j=1}^{n} a_j = \sum_{j=2}^{n+1} a_{j-1}$$

c) Intercambio del orden de sumación

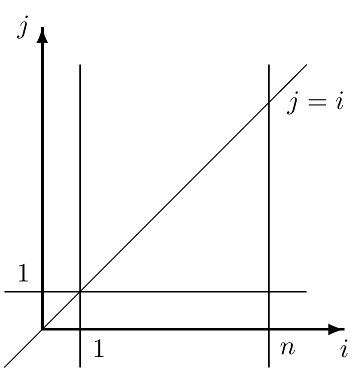
$$\sum_{R(i)} \sum_{S(j)} a_{ij} = \sum_{S(j)} \sum_{R(i)} a_{ij}$$

Por ejemplo,

$$\begin{aligned} \textstyle\sum_{R(i)} \sum_{j=1}^{n} a_{ij} &= \textstyle\sum_{R(i)} [a_{i1} + a_{i2} + \cdots + a_{in}] \\ \textstyle\sum_{j=1}^{n} \sum_{R(i)} a_{ij} &= \textstyle\sum_{R(i)} a_{i1} + \cdots + \sum_{R(i)} a_{in} \end{aligned}$$

Por ejemplo,

$$\begin{aligned} \textstyle\sum_{i=1}^{n} \sum_{j=1}^{i} a_{ij} &= \textstyle\sum_{i=1}^{n} \{a_{i1} + a_{i2} + \cdots + a_{ii}\} \\ &= \textstyle\sum_{i=1}^{n} a_{i1} + \cdots + \sum_{i=1}^{n} a_{ii} \\ &= \{a_{11} + \cdots + a_{n1}\} + \cdots + \{a_{1i} + \cdots + a_{ni}\} \end{aligned}$$



Cuando $1 \leq i \leq n$ es $1 \leq j \leq i$
y cuando $j \leq i \leq n$ es $1 \leq j \leq n$
con lo que la doble sumatoria
se transforma en $\sum_{j=1}^{n} \sum_{i=j}^{n} a_{ij}$.

1.3.3 Ejemplos

Ejemplo I

$$^{M}\sum_{j=0}^{n} a_j = \sum_{\substack{j=0 \\ j=\text{par}}}^{n} a_j + ^{M}\sum_{\substack{j=1 \\ j=\text{impar}}}^{n+1} a_j = \sum_{k=0}^{n/2} a_{2k} + \sum_{k=0}^{n/2} a_{2k+1}$$

Ejemplo II

$$S_1 = \sum_{i=0}^{n}\sum_{j=0}^{i} a_i a_j = \sum_{j=0}^{n}\sum_{i=j}^{n} a_i a_j = \sum_{i=0}^{n}\sum_{j=i}^{n} a_i a_j = S_2$$

Intercambiando i con j y reordenando $a_j a_i = a_i a_j$ queda:

$$\begin{aligned} 2S_1 &= S_1 + S_2 = \\ &= \textstyle\sum_{i=0}^{n}(\sum_{j=0}^{i} a_i a_j + \sum_{j=i}^{n} a_i a_j) = \\ &= \textstyle\sum_{i=0}^{n}(\sum_{j=0}^{n} a_i a_j + a_i a_i) = \\ &= \textstyle\sum_{i=0}^{n}\sum_{j=0}^{n} a_i a_j + \sum_{i=0}^{n} a_i^2 = \\ &= \textstyle(\sum_{i=0}^{n} a_i)(\sum_{j=0}^{n} a_j) + \sum_{i=0}^{n} a_i^2 = \\ &= \textstyle(\sum_{i=0}^{n} a_i)^2 + \sum_{i=0}^{n} a_i^2 \end{aligned}$$

Por lo tanto

$$\sum_{i=0}^{n}\sum_{j=0}^{i} a_i a_j = \frac{1}{2}[(\sum_{i=0}^{n} a_i)^2 + \sum_{i=0}^{n} a_i^2]$$

Ejemplo III

$$\begin{aligned} \textstyle\sum_{j=0}^{n} ax^j &= \textstyle a + \sum_{j=1}^{n} ax^j = a + x\sum_{j=1}^{n} ax^{j-1} = \\ &= \textstyle a + x\sum_{j=0}^{n-1} ax^j = a + x\sum_{j=0}^{n} ax^j - ax^{n+1} \end{aligned}$$

de donde

$$(1-x)\sum_{j=0}^{n} ax^j = a - ax^{n+1}$$

$$\sum_{j=0}^{n} ax^j = a\frac{1-x^{n+1}}{1-x} \quad \forall \;\; x \neq 1$$

Ejemplo IV

$$\begin{aligned}\sum_{j=0}^{n}(a+bj) &= \sum_{n-j=0}^{n}(a+b(n-j)) = \sum_{j=0}^{n}(2a+bn-a-bj)\\ &= \sum_{j=0}^{n}(2a+bn) - \sum_{j=0}^{n}(a+bj)\\ &= (n+1)(2a+bn) - \sum_{j=0}^{n}(a+bj)\end{aligned}$$

con lo cual

$$\sum_{j=0}^{n}(a+bj) = \frac{1}{2}(n+1)(2a+bn) = a(n+1) + \frac{b}{2}n(n+1)$$

Sólo recordamos que estas propiedades también son válidas para productorias.

1.3.4 Ejercicios

Ejercicio 1

Teniendo en cuenta el Ejemplo 3, ¿Qué sucede si $x = 1$; cuánto vale la sumatoria?.

Ejercicio 2

¿Cuánto vale la suma siguiente?

$$1 + \frac{1}{7} + \frac{1}{49} + \frac{1}{343} + \cdots + \frac{1}{7^n} + \cdots$$

Ejercicio 3

Teniendo en cuenta el Ejemplo 4 y suponiendo $m \leq n$ evaluar $\sum_{j=m}^{n} j$.

Ejercicio 4

Verificar que $\sum_{j=0}^{n} jx^j = \frac{nx^{n+2}-(n+1)x^{n+1}+x}{(x-1)^2}$ si $x \neq 1$ sin emplear el Principio de Inducción.

Ejercicio 5

Evaluar $\sum_{j=m}^{n}(a_j - a_{j-1})$ con $(1 < m \leq n)$ para los elementos de la sucesión $a_1, a_2, \ldots, a_j, a_{j+1}, \ldots$.

Ejercicio 6

Probar que

$$\prod_{j=1}^{n}(1-a_j) \geq 1 - \sum_{j=1}^{n} a_j$$

con $0 < a_j < 1$.

Ejercicio 7

Hallar una fórmula sencilla para

$$\prod_{j=2}^{n}(1-\frac{1}{j^2})$$

Ejercicio 8

Considerar la llamada matriz de Vandermonde dada por

$$\left\| \begin{array}{cccc} x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & & & \\ x_1^n & x_2^n & \cdots & x_n^n \end{array} \right\|$$

y mostrar que su determinante es

$$\prod_{j=1}^{n} x_j \prod_{1 \leq i < j \leq n} (x_j - x_i)$$

Ejercicio 9

Considerar la siguiente matriz, llamada matriz combinatoria

$$\left\| \begin{array}{cccc} x+y & y & \cdots & y \\ y & x+y & \cdots & y \\ \vdots & & & \\ y & y & \cdots & x+y \end{array} \right\|$$

donde los coeficientes $a_{ij} = x + \delta_{ij}$ y con

$$\delta_{ij} = \left\{ \begin{array}{l} 1 \,\mathrm{si}\, i = j \\ 0 \,\mathrm{si}\, i \neq j \end{array} \right.$$

y mostrar que su determinante es $x^{n-1}(x+ny)$.

1.3.5 Techos y Pisos

Sea x un número real. Definimos parte entera de x y la denotamos por $[x]$ como el único número entero que satisface

$$[x] \leq x < [x] + 1$$

Por razones de trabajo computacional, denotamos por $\lfloor x \rfloor$ al número entero *más grande* que satisface

$$\lfloor x \rfloor \leq x$$

y lo llamamos el piso de x y,
denotamos por $\lceil x \rceil$ al número entero *más chico* que satisface

$$\lceil x \rceil > x$$

y lo llamamos el techo de x.

Ejemplos

a)

$$\begin{aligned} \lfloor \sqrt{2} \rfloor &= 1 \\ \lceil \sqrt{2} \rceil &= 2 \end{aligned}$$

b)

$$\begin{aligned} \lfloor 0.5 \rfloor &= 0 \\ \lceil -0.5 \rceil &= 0 \\ \lfloor -0.5 \rfloor &= -1 \end{aligned}$$

1.3.6 Propiedades

a) $\lceil x \rceil = \lfloor x \rfloor$ sí y sólo sí x es entero

b) $\lceil x \rceil = \lfloor x \rfloor + 1$ sí y sólo sí x no es entero

c) $\lfloor -x \rfloor = -\lceil x \rceil$

d) $x - 1 < \lfloor x \rfloor \leq x < \lceil x \rceil \leq x + 1$

e) $x \equiv x \pmod{0}$; $x \equiv 0$ (mód y) $\Leftrightarrow y|x$

Si x e y son números reales cualesquiera, definimos la siguiente relación binaria

$$x \equiv x - y\lfloor x/y \rfloor \ (m\acute{o}d y) \ si \ y \neq 0$$

que, también, denotamos por $x$mód $y = x - y\lfloor x/y \rfloor$ si $y \neq 0$ interpretando x mód y como el resto de dividir a x por y. De este modo, la parte fraccionaria o mantisa de x está dada por la cantidad x mod 1 con lo cual x se expresa como $x = \lfloor x \rfloor + x \ mod \ 1$

1.3.7 Ejercicios

Ejercicio 1

Si n y m son números enteros calcular

a) $\lfloor \frac{m+n}{2} \rfloor + \lfloor \frac{n-m+1}{2} \rfloor$

b) $\lceil \frac{m+n}{2} \rceil + \lceil \frac{n-m+1}{2} \rceil$

c) Rehacer los cálculos de (a) y de (b) cuando $m = 0$

Ejercicio 2

Verificar las siguientes igualdades

a) $\sum_{k=1}^{n} \lfloor \frac{k}{2} \rfloor = \lfloor \frac{n^2}{4} \rfloor$

b) Evaluar, análogamente, $\sum_{k=1}^{n} \lceil \frac{k}{2} \rceil$

Ejercicio 3

Probar que cualquiera sea $x \in \Re$ para todo entero positivo n vale

$$\lfloor xrfloor + \lfloor x + \frac{1}{n} \rfloor + \cdots + \lfloor x + \frac{n-1}{n} \rfloor = \lfloor nx \rfloor$$

1.4 Coeficientes Binomiales

Recordemos, rápidamente, que la permutación de n objetos está dada por el factorial de n, que denotamos por

$$n! = n(n-1)\ldots 1 = \prod_{k=1}^{n} k$$

y, también, que las combinaciones de n objetos tomados de a k están dados por

$$\begin{aligned} C_{n,k} = \begin{pmatrix} n \\ k \end{pmatrix} &= \tfrac{n!}{k!(n-k)!} = \tfrac{n(n-1)\ldots(n-k+1)}{k!} \\ &= \prod_{j=1}^{k} [\tfrac{n+1-j}{j}] \ \text{ para } \ 0 \leq k \leq n \end{aligned}$$

1.4.1 Propiedades

Representacion por factoriales

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \quad 0 \leq k \leq n$$

Simetría

$$\binom{n}{k} = \binom{n}{n-k} \quad \forall\ n \geq 0\ ,\ k\ entero$$

puesto que si k es negativo o si $k > n$ el coeficiente binomial está definido como cero.

Movimientos Posibles

a) $\binom{n}{k} = \binom{n}{n-k} = \frac{n(n-1)!}{k(k-1)!(n-k)!} = \frac{n}{k}\binom{n-1}{k-1} \quad k \neq 0$

b) $k\binom{n}{k} = n\binom{n-1}{k-1}$

c) $\frac{1}{n}\binom{n}{k} = \frac{1}{k}\binom{n-1}{k-1}$

d) $\binom{n}{k} = \frac{n}{n-k}\binom{n-1}{k} \quad k \neq n$

ó equivalentemente

e) $(n-k)\binom{n}{k} = n\binom{n-1}{k}$

Suma de coeficientes binomiales

a)
$$\begin{aligned}
\binom{n}{k} &= \binom{n-1}{k} + \binom{n-1}{k-1} \\
&= \frac{(n-1)!}{k!(n-k-1)!} + \frac{k(n-1)!}{k(k-1)!(n-k)!} \\
&= \frac{(n-1)!}{k!(n-k-1)!}\left(1 + \frac{k}{(n-k)}\right) \\
&= \frac{(n-1)!}{k!(n-k-1)!}\frac{n}{n-k} \\
&= \binom{n}{k}
\end{aligned}$$

b)
$$\begin{aligned}
n\binom{n-1}{k} + n\binom{n-1}{k-1} &= (n-k)\binom{n}{k} + k\binom{n}{k} \\
&= n\binom{n}{k}
\end{aligned}$$

Sumatoria de coeficientes binomiales

a) $\sum_{k=0}^{m}\binom{n+k}{k}=\binom{n+m+1}{m}$

Aplicando repetidas veces la relación (a) de la propiedad anterior a partir del último término de la sumatoria puesto que, por ejemplo,

$$\begin{aligned}\binom{n+m}{m} &= \binom{n+m-1}{m}+\binom{n+m-1}{m-1}\\ \binom{n+m-1}{m-1} &= \binom{n+m-2}{m-1}+\binom{n+m-2}{m-2}\end{aligned}$$

y así sucesivamente.
Probémoslo por inducción en m
Si $m=1$ entonces
$\sum_{k=0}^{m}\binom{n+k}{k}=\binom{n}{0}+\binom{n+1}{1}=1+(n+1)=n+2$

y si $m=1$ entonces $\binom{n+2}{1}=n+2$.
Supongamos válida la relación para m y veamos que vale para $(m+1)$

$$\begin{aligned}\sum_{k=0}^{m+1}\binom{n+k}{k} &= \sum_{k=0}^{m}\binom{n+k}{k}+\binom{n+m+1}{m+1}\\ &= \binom{n+m+1}{m}+\binom{n+m+1}{m+1}\\ &= \binom{n+m+2}{m+1}\end{aligned}$$

Ejemplo

$$\begin{aligned}\sum_{k=0}^{m}\binom{k}{n} &= \sum_{k=-n}^{m-n}\binom{k+n}{n}\\ &= \sum_{-n\leq k<0}+\sum_{k=0}^{m-n}\binom{k+n}{n}\\ &= \sum_{k=0}^{m-n}\binom{n+k}{k}\\ &= 0+\sum_{k=0}^{m-n}\binom{k+n}{n}\\ &= \binom{n+m-n+1}{m-n}+\binom{m+1}{n+1} \quad \textit{con} \quad m\geq n\end{aligned}$$

Cuando $n=1$, esta relación proporciona

$$\binom{0}{1}+\binom{1}{1}+\cdots+\binom{m}{1}=0+1+\cdots+m=\binom{m+1}{2}=\frac{(m+1)m}{2}$$

que no es más que la suma de una progresión aritmética.

Si, por ejemplo, queremos calcular $\sum_{k=0}^{n} k^2$ basta observar que

$$k^2 = 2\binom{k}{2} + \binom{k}{1}$$

con lo cual es

$$\begin{aligned}
\sum_{k=0}^{n} k^2 &= \sum_{k=0}^{n}[2\binom{k}{2} + \binom{k}{1}] \\
&= 2\binom{n+1}{3} + \binom{n+1}{2} \\
&= 2\frac{(n+1)n(n-1)}{6} + \frac{n(n+1)}{2} \\
&= n(n+1)[\frac{n-1}{3} + \frac{1}{2}] \\
&= \frac{1}{6}n(n+1)(2n+1)
\end{aligned}$$

También la sumatoria $\sum_{k=0}^{n} k^3$ puede obtenerse de manera similar.

Indice Superior Negativo

La identidad básica dada por

$$\binom{-n}{k} = (-1)^k \binom{n+k-1}{k}$$

con k entero no negativo resulta inmediatamente de la definición dada por $C_{(n,k)}$ en términos de la productoria de k factores reemplazando n por $(-n)$. Como ejemplo del empleo de esta relación probemos la siguiente fórmula

$$\begin{aligned}
\sum_{k=0}^{m} \binom{n}{k}(-1)^k &= \binom{n}{0} - \binom{n}{1} + \cdots + (-1)^m \binom{n}{m} \\
&= (-1)^m \binom{n-1}{m} \quad m \geq 0 \textit{ entero}
\end{aligned}$$

En efecto, calculemos, apoyándonos en la identidad básica, la relación

$$\begin{aligned}
\sum_{k=0}^{m} \binom{n}{k}(-1)^k &= \sum_{k=0}^{m} \binom{-n+k-1}{k} \\
&= \binom{-n+m}{m} \\
&= (-1)^m \binom{n-1}{m}
\end{aligned}$$

Producto de coeficientes binomiales

$$\begin{aligned}\binom{n}{m}\binom{m}{k} &= \tfrac{n!}{m!(n-m)!}\tfrac{m!}{k!(m-k)!} \\ &= \tfrac{n!(n-k)!}{k!(n-m)!(m-k)!} \\ &= \binom{n}{k}\tfrac{(n-k)!}{(n-m)!(m-k)!} \\ &= \binom{n}{k}\binom{n-k}{m-k} \quad \forall\ n \geq m \geq k \geq 0\end{aligned}$$

Ejemplo de Aplicación

Determinar los valores de $a_0, a_1, a_2, \ldots$ tales que $n! = a_0 + a_1 n + a_2 n(n-1)(n-2) + \cdots \quad \forall\ n \geq 0$. Esta expresión, por cierto, es equivalente a

$$n! = \sum_k \binom{n}{k} k! a_k$$

Para calcular los coeficientes a_k, nos apoyamos en la siguiente identidad (la cual queda como ejercicio para el lector)

$$\sum_k \binom{r}{k}\binom{s+k}{n}(-1)^k = (-1)^r \binom{s}{n-r} \quad \forall\, n\ entero,\ r \geq 0\ entero$$

que, en el caso particular, de ser $s = 0$, se reduce a

$$\sum_k \binom{r}{k}\binom{k}{n}(-1)^k = (-1)^r \binom{0}{n-r} = (-1)^r \delta_{nr}$$

$\forall\ \ n\ entero\ ,\ \forall\ r \geq 0\ entero$

donde

$$\delta_{nr} = \begin{cases} 1 & \text{si } n = r \\ 0 & \text{si } n \neq r \end{cases}$$

Esta fórmula es importante ya que $\forall\ \ n \neq r$ vale cero, lo que nos permite escribir

$$\begin{aligned}\textstyle\sum_n n! \binom{m}{n}(-1)^n &= \textstyle\sum_n \sum_k \binom{n}{k} k! a_k \binom{m}{n}(-1)^n \\ &= \textstyle\sum_k k! a_k \sum_n \binom{n}{k}\binom{m}{n}(-1)^n \\ &= \textstyle\sum_k k! a_k \sum_n \binom{m}{n}\binom{n}{k}(-1)^n \\ &= \textstyle\sum_k k! a_k (-1)^m \delta_{km} = (-1)^m m! a_m\end{aligned}$$

por lo tanto

$$\begin{aligned} a_m &= \textstyle\sum_{n\geq 0} (-1)^{m+n} \frac{n!}{m!}\binom{m}{n} \\ &= \textstyle\sum_{n=0}^{m} \frac{(-1)^{m+n}}{(m-n)!} = \sum_{n=0}^{m} \frac{(-1)^n}{n!}\end{aligned}$$

Esto implica

$$\sum_k \binom{r}{k} (-1)^k [c_o \binom{k}{0} + c_1 \binom{k}{1} + \cdots + c_r \binom{k}{r}] = (-1)^r c_r$$

con lo cual con una elección conveniente de los coeficientes c_r podemos representar cualquier polinomio en k como una suma de coeficientes binomiales con índice superior k. Entonces, obtenemos

$$\sum_k \binom{r}{k} (-1)^k [\sum_{j=0}^{r} b_j k^j] = (-1)^r n! b_r \, ; \, r \geq 0 \ \ entero$$

y damos respuesta a un ejercicio propuesto.

1.4.2 Ejercicios

Ejercicio 1

Probar que cualquier polinomio $\sum_{k=0}^{m} a_k x^k$ puede expresarse como $\sum_{k=0}^{m} b_k \binom{x}{k}$ para $b_0, b_1, \ldots, b_m$ coeficientes convenientemente elegidos.

Ejercicio 2

Si p es primo, probar

a) $\binom{n}{p} \equiv \lfloor \frac{n}{p} \rfloor (m\acute{o}d\ p)$

b) $\binom{p}{k} \equiv 0 (m\acute{o}d\ p)$ para $k = 1, 2, \ldots, (p-1)$

c) $\binom{p-1}{k} \equiv (-1)^k (m\acute{o}d\ p)$ para $k = 0, 1, \ldots, (p-1)$

Ejercicio 3

Evaluar $\sum_{k=0}^{n} k^4$

Ejercicio 4

Un caso particular de la fórmula del binomio de Newton está dado por

$$\sum_{k=0}^{n} \binom{n}{k} x^k = (1+x)^n \quad n \geq 0 \ \ entero\ y\ |x| < 1$$

Entonces, empleando este caso particular y usando que $(1+x)^r(1+x)^s = (1+x)^{r+s}$ probar la siguiente identidad básica

$$\sum_k \binom{r}{k}\binom{s}{n-k} = \binom{r+s}{n} \quad n \ \ entero$$

Ejercicio 5

Probar, inductivamente, la siguiente relaci'on

$$\sum_k \binom{r}{k}\binom{s+K}{n}(-1)^k = (-1)^r\binom{s}{n-r}$$

con n entero y $r \geq 0$ entero.

Ejercicio 6

Dados k y n enteros positivos, mostrar que

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

1.5 Conversión de Coef.Binomiales en Potencias

Este tema es importante en la teoría de interpolación, dentro del análisis numérico, dado que son particularmente necesarios los llamados factoriales ó facultades (también llamados números de Stirling de primera clase).
Elfactorial de diferencia $h = 1$ y grado n es un producto de factores de progresión aritmética se define por

$$n!\binom{x}{n} := [x]^n := x(x-1)\ldots(x-n+1)$$

Su diferencia primera está dada por

$$\begin{aligned}\Delta[x]^n &= [x+1]^n - [x]^n \\ &= x(x-1)(x-2)\ldots(x-n+2)[(x+1)-(x-n+1)]\end{aligned}$$

es decir

$$\Delta[x]^n = n[x]^{n-1}$$

Es claro que las diferencias sucesivas responden a la misma expresión,y por lo tanto, inferimos

$$\frac{\Delta[x]^n}{n!} = \frac{[x]^{n-1}}{(n-1)!}$$

o sea

$$\frac{[x+1]^n}{n!} = \frac{[x]^n}{n!} + \frac{[x]^{n-1}}{(n-1)!}$$

que por cierto permite tabular rápidamente $[x+1]^n/n!$ para valores naturales de x y armar en forma análoga un triángulo de Tartaglia. Dado un polinomio

$$P_{n(x)} = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$$

simplificamos en forma sensible el cálculo de sus diferencias sucesivas expresándolo como suma de factoriales

$$P_{n(x)} = \alpha + \beta[x] + \gamma[x]^2 + \cdots + \nu[x]^n$$

donde

a) α es el resto de dividir por x, es decir, $P_{n(x)} = \alpha + xP_{n-1(x)}$

b) β es el resto de dividir $P_{n-1(x)}$ por $(x-1)$, es decir, $P_{n-1(x)} = \beta + (x-1)P_{n-2(x)}$

c) γ es el resto de dividir $P_{n-2(x)}$ por $(x-2)$, es decir, $P_{n-2(x)} = \gamma + (x-2)P_{n-3(x)}$

y así sucesivamente.
Entonces, obtenemos las siguientes diferencias sucesivas

$$\begin{array}{rcl} \Delta P_{n(x)} & = & \beta + 2!\gamma[x] + \cdots + n\nu[x]^{n-1} \\ \Delta^2 P_{n(x)} & = & 2!\gamma + \cdots + n(n-1)\nu[x]^{n-2} \\ & \cdots & \\ \Delta^n P_{n(x)} & = & n!\nu \end{array}$$

En particular, si los puntos son $x = 0, 1, 2, \ldots, n$ calculamos los coeficientes $\alpha, \beta, \gamma, \delta, \ldots, \nu$ como sigue

$$\begin{array}{rcl} \alpha & = & y_0 \\ \beta & = & \Delta^1 y_0 = y_1 - y_0 \\ 2!\gamma & = & \Delta^2 y_0 = y_2 - 2y_1 + y_0 \\ & \cdots & \\ n!\nu & = & \Delta^n y_0 \end{array}$$

De este modo, obtenemos la siguiente conocida fórmula de Newton-Gregory (1670)

$$P_n(x) = y_0 + \frac{x}{1!}\Delta y_0 + \frac{x(x-1)}{2!}\Delta^2 y_0 + \cdots + \frac{x(x-1)\ldots(x-n+1)}{n!}\Delta^n y_0$$

1.5.1 Ejemplo 1

Consideremos el polinomio

$$P_4(x) = x^4 - 12x^3 + 30x^2 - 20x + 7$$

Mediante la aplicación de la regla de Ruffini obtenemos

$$\alpha = 7 \quad \beta = -1 \quad \gamma = 1 \quad \delta = -6$$

con lo cual expresamos

$$P_4(x) = 7 - [x] + [x]^2 - 6[x]^3 + [x]^4$$

mientras que sus diferencias sucesivas son

$$\begin{array}{rcc} \Delta P_4(x) & = & -1 + 2[x] - 18[x]^2 + 4[x]^3 \\ \Delta^2 P_4(x) & = & 2 - 36[x] + 12[x]^2 \\ \Delta^3 P_4(x) & = & -36 + 24[x] \\ \Delta^4 P_4(x) & = & 24 \\ \Delta^5 P_4(x) & = & 0 \end{array}$$

1.5.2 Ejemplo 2

Consideremos el polinomio

$$P_5(x) = x^5 - 10x^4 + 35x^3 - 50x^2 + 24x$$

Mediante la aplicación sucesiva de la regla de Ruffini obtenemos

$$\alpha = 0 \quad \beta = 0 \quad \gamma = 0 \quad \delta = 0 \quad \epsilon = 0$$

Por lo tanto,

$$P_5(x) = [x]^5 = 5! \begin{pmatrix} x \\ 5 \end{pmatrix}$$

Luego

$$\begin{pmatrix} x \\ 5 \end{pmatrix} = \frac{1}{5!}\{x^5 - 10x^4 + 35x^3 - 50x^2 + 24x\}$$

1.5.3 Ejemplo 3

Consideremos los puntos $x = 0, 1, 2, 3, 4, 5$ y calculemos vía la función $f(x) = x^5$ las ordenadas correspondientes: $y_0 = 0$, $y_1 = 1$, $y_2 = 32$, $y_3 = 243$, $y_4 = 1024$,

$y_5 = 5^5 = 3125$. Entonces, de acuerdo a lo considerado, obtenemos

$$
\begin{array}{rcc}
\alpha = y_0 & = & 0 \\
\beta = \Delta^1 y_0 & = & y_1 - y_0 = 1 \\
2!\gamma = \Delta^2 y_0 & = & y_2 - 2y_1 + y_0 = 32 - 2 = 30 \\
3!\delta = \Delta^3 y_0 & = & y_3 - 3y_2 + 3y_1 - y_0 = 243 - 96 + 3 = 150 \\
4!\epsilon = \Delta^4 y_0 & = & y_4 - \begin{pmatrix} 4 \\ 1 \end{pmatrix} y_3 \\
 & + & \begin{pmatrix} 4 \\ 2 \end{pmatrix} y_2 - \begin{pmatrix} 4 \\ 3 \end{pmatrix} y_1 + \begin{pmatrix} 4 \\ 4 \end{pmatrix} y_0 \\
 & = & 1024 - 4(243) + 6(32) - 4(1) \\
 & = & 1024 - 972 + 192 - 4 \\
 & = & 240 \\
5!\nu = \Delta^5 y_0 & = & y_5 - \begin{pmatrix} 5 \\ 1 \end{pmatrix} y_4 + \\
 & + & \begin{pmatrix} 5 \\ 2 \end{pmatrix} y_3 - \begin{pmatrix} 5 \\ 3 \end{pmatrix} y_2 + \\
 & + & \begin{pmatrix} 5 \\ 4 \end{pmatrix} y_1 - \begin{pmatrix} 5 \\ 5 \end{pmatrix} y_0 \\
 & = & 3125 - 5(1024) + 10(243) - 10(32) + 5 \\
 & = & 3124 - 5120 + 2430 - 320 + 5 \\
 & = & 120
\end{array}
$$

Por lo tanto

$$
\begin{array}{rcc}
x^5 & = & y_0 + \begin{pmatrix} x \\ 1 \end{pmatrix} \Delta^1 y_0 + \begin{pmatrix} x \\ 2 \end{pmatrix} \Delta^2 y_0 + \\
 & + & \begin{pmatrix} x \\ 3 \end{pmatrix} \Delta^3 y_0 + \begin{pmatrix} x \\ 4 \end{pmatrix} \Delta^4 y_0 + \\
 & + & \begin{pmatrix} x \\ 5 \end{pmatrix} \Delta^5 y_0 \\
x^5 & = & 0 + \begin{pmatrix} x \\ 1 \end{pmatrix} 1! + \begin{pmatrix} x \\ 2 \end{pmatrix} 2!(15) + \\
 & + & \begin{pmatrix} x \\ 3 \end{pmatrix} 3!(25) + \begin{pmatrix} x \\ 4 \end{pmatrix} 4!(10) + \\
 & + & \begin{pmatrix} x \\ 5 \end{pmatrix} 5! \\
x^5 & = & \begin{pmatrix} x \\ 5 \end{pmatrix} 5! + 10 \begin{pmatrix} x \\ 4 \end{pmatrix} 4! + \\
 & + & 25 \begin{pmatrix} x \\ 3 \end{pmatrix} 3! + 15 \begin{pmatrix} x \\ 2 \end{pmatrix} 2! + \\
 & + & \begin{pmatrix} x \\ 1 \end{pmatrix} 1! \\
 & = & [x]^5 + 10[x]^4 + 25[x]^3 + 15[x]^2 + [x]
\end{array}
$$

Este ejemplo nos muestra que

$$\begin{aligned} x^n &= \textstyle\sum_{k=0}^{n} \left\{ \begin{matrix} n \\ k \end{matrix} \right\} \left(\begin{matrix} x \\ k \end{matrix} \right) k! \\ &= \textstyle\sum_{k=0}^{n} \left\{ \begin{matrix} n \\ k \end{matrix} \right\} [x]^k \end{aligned}$$

donde los coeficienmtes $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ se denominan números de Stirling de segunda especie que están tabulados y además son fácilmente calculables mediante diferencias sucesivas de la potencia x^n considerada, es decir,

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} \equiv \frac{\Delta^k y_0}{k!}$$

En el Ejemplo 2 logramos la conversión de un coeficiente binomial en potencia según hemos visto. En general, vale la relación siguiente

$$n! \left(\begin{matrix} x \\ n \end{matrix} \right) = [x]^n = \sum_{k=0}^{n} (-1)^{n-k} \left[\begin{matrix} n \\ k \end{matrix} \right] x^k$$

donde los coeficientes $\left[\begin{matrix} n \\ k \end{matrix} \right]$ son llamados números de Stirling de primera especie, los cuales están tabulados.
Algunos casos especiales son los siguientes

a) $\left(\begin{matrix} 0 \\ n \end{matrix} \right) = \left[\begin{matrix} 0 \\ n \end{matrix} \right] = \left\{ \begin{matrix} 0 \\ n \end{matrix} \right\}$

b) $\left(\begin{matrix} n \\ n \end{matrix} \right) = \left[\begin{matrix} n \\ n \end{matrix} \right] = \left\{ \begin{matrix} n \\ n \end{matrix} \right\} = 1$

c) $\left(\begin{matrix} n \\ 2 \end{matrix} \right) = \left[\begin{matrix} n \\ n-1 \end{matrix} \right] = \left\{ \begin{matrix} n \\ n-1 \end{matrix} \right\}$

d) $\left[\begin{matrix} n \\ 0 \end{matrix} \right] = \left\{ \begin{matrix} n \\ 0 \end{matrix} \right\} = 0$

e) $\left[\begin{matrix} n \\ 1 \end{matrix} \right] = (n-1)!$

f) $\left\{ \begin{matrix} n \\ 1 \end{matrix} \right\} = 1$

g) $\left\{ \begin{matrix} n \\ 2 \end{matrix} \right\} = 2^{n-1} - 1$

1.6 Relaciones de Recurrencia

1.6.1 Ejemplos

Ejemplo I

Una persona coloca u$s 1000 al 12% anual.
Si A_n denota el monto al cabo de n años establecemos la relación entre A_n y A_{n-1}
Por cierto

$$A_n = A_{n-1} + 0.12A_{n-1} = 1.12A_{n-1} \quad \forall\, n \geq 1$$

siendo el monto inicial $A_0 = 1000$. La relación de recurrencia es, entonces, $A_n = 1.12A_{n-1}$ que conduce a

$$A_n = 1.12A_{n-1} = (1.12)^2 A_{n-2} = \cdots = (1.12)^n A_0$$

Ejemplo II

La sucesión de Fibonacci es otro ejemplo de recurrencia.
Por ejemplo,
¿Cuántas parejas de conejos habrá después de un año si al comienzo sólo hay una pareja y sabemos que cada una produce, al mes una nueva pareja, la cual se torna reproductiva al mes?
Supongamos que no se producen muertes, y sea f_i el número de parejas de conejos al cabo del i-ésimo mes, con lo cual, $f_0 = 1$. Al finalizar el primer mes hay sólo una pareja ya que comienza a ser productiva después de un mes, con lo cual, es $f_1 = 1$.
Las condiciones $f_0 = 1$ y $f_1 = 1$ son las condiciones iniciales para la sucesión de Fibonacci. El crecimiento en las parejas de conejos $(f_n - f_{n-1})$ del mes $(n-1)$ al mes n se debe a que cada pareja viva en el mes $(n-2)$ produce una pareja adicional. Esto es

$$\begin{array}{rcl} f_n - f_{n-1} & = & f_{n-2} \\ f_n & = & f_{n-1} + f_{n-2} \end{array}$$

Por lo tanto, la relación de recurrencia

$$\begin{array}{rcl} f_0 & = & 1 \\ f_1 & = & 1 \\ f_n & = & f_{n-1} + f_{n-2} \quad \forall \;\; n \geq 2 \end{array}$$

define la sucesión de Fibonacci.

Ejemplo III

<u>*Torre de Hanoi*</u>
Consideremos un juego de ingenio, llamado la Torre de Hanoi, según el cual tres

espigas salen de una tabla y existen n discos con orificios centrales para ensartar con la condición de que si un disco es insertado en una espiga sólo podrá situarse sobre él un disco de menor diámetro. Si todos los discos estuvieran insertados en una espiga y sólo se puede mover un disco a la vez. El problema consiste en transferir los discos a otra espiga con los requerimientos anteriores.
Si c_n denota el número de movimientos con los cuales puede resolverse el problema de los n discos queremos hallar una relación de recurrencia y una condición inicial para la sucesión numérica $c_1, c_2, \ldots, c_n, \ldots$

a) Supongamos que tenemos n discos en la espiga 1. Entonces, en c_{n-1} movimientos, pueden moverse los $(n-1)$ discos superiores a la espiga 2. Durante estos movimientos el disco inferior de la espiga 1 permanece fijo. A continuación se pasa a la espiga 3 el disco que quedó en la 1. Finalmente, en c_{n-1} movimientos, pueden pasarse a la espiga 3 los $(n-1)$ discos que están en la espiga 2.

b) Por lo tanto, la relación de recurrencia buscada es

$$c_n = 2c_{n-1} + 1$$

con la condición inicial $c_1 = 1$.

Ejemplo IV

Desarreglos
En una reunión social n personas dejan sus abrigos en el guardarropas. Al retirarse, los abrigos se devuelven al azar y, desafortunadamente, ninguna persona recibe el abrigo correcto.
Sea D_n el número de maneras en las cuales n personas pueden recibir sus n abrigos equivocados o desarreglados. Veamos que la sucesión $D_1, D_2, \ldots, D_{n-1}, \ldots$ satisfacen la siguiente relación de recurrencia

$$D_n = (n-1)(D_{n-1} + D_{n-2})$$

Es claro que D_n es el número de permutaciones

$$m_1, \ldots, m_n \;\; de \; 1, \ldots, n$$

donde $m_i \neq i$ para $i = 1, 2, \ldots, n$.
Tales permutaciones se llaman desarreglos.
Supongamos que hay C desarreglos de $1, \ldots, n$ de la forma

$$2, m_2, \ldots, m_n$$

En general, hay C desarreglos de $1, \ldots, n$ de la forma

$$k, m_2, \ldots, m_n$$

donde k es un entero fijo tal que $2 \leq k \leq n$. Dado que para el primer término existen $(n-1)$ posibilidades, es

$$D_n = (n-1)C$$

Dividamos los desarreglos de 1 a n $2, m_2, \ldots, m_n$ de la siguiente forma

$$\begin{aligned} 2, 1, m_3, \ldots, m_n \\ 2, m_2, m_3, \ldots, m_n \text{ con } m_2 \neq 1 \end{aligned}$$

En la primera relación hay $(n-2)$ números $m_3, \ldots, m_n$ fuera de posición con lo cual hay D_{n-2} de ellos. En la segunda relación hay $(n-1)$ números $m_2, \ldots, m_n$ fuera de posición con lo cual hay D_{n-1} de ellos. Por lo tanto,

$$C = D_{n-1} + D_{n-2}$$

Por lo tanto, obtenemos la fórmula de recurrencia propuesta.

Ejemplo V

<u>*Función de Ackermann*</u>
La función de Ackermann puede definirse por las siguientes relaciones de recurrencia como sigue

$$A_{(m,0)} = A_{(m-1,1)}$$

y $\forall \; n \geq 1 \; y \; \forall \; m \geq 1$ es

$$A_{(m,n)} = A_{(m-1, A(m,n-1))}$$

y las condiciones iniciales

$$A_{(0,n)} = n + 1 \;\; forall \;\; n \geq 0$$

1.6.2 Ejercicios

Ejercicio 1

Si D_n denota el número de desarreglos de n objetos verificar que

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

Ejercicio 2

A partir de la sucesión de Fibonacci probar

a) ${f^2}_{n+2} - {f^2}_{n+1} = f_n f_{n+3} \;\; \forall \;\; n \geq 0$

b) ${f^2}_{n+1} = f_n f_{n+2} + (-1)^{n+1} \;\; \forall \;\; n \geq 0$

Ejercicio 3

Probar, inductivamente, que

a)$A_{(1,n)} = n + 2 \;\; \forall \;\; n \geq 0$

b) $A_{(2,n)} = 3 + 2n \;\; \forall \;\; n \geq 0$

c) Determinar, inductivamente, el valor de $A_{(3,n)}$ inductivamente.

Ejemplo VI

Intentemos resolver una relación de recurrencia referida a una sucesión $a_0, a_1, a_2, \ldots, a_n, \ldots$ para determinar el n-ésimo término a_n. Por ejemplo,

Dada la siguiente relación de recurrencia

$$S_n = 2S_{n-1}$$

con la condición inicial $S_0 = 1$ resolvámosla por iteración.
En efecto

$$S_n = 2S_{n-1} = 2^2 S_{n-2} = \cdots = 2^n S_0 = 2^n$$

Ejemplo VII

Hallar una expresión explícita para C_n el número de movimientos en el juego de la torre de Hanoi con n discos.
La relación de recurrencia obtenida fue

$$\begin{array}{rcl} c_n & = & 2c_{n-1} \\ c_1 & = & 1 \end{array}$$

Resolviéndola por iteración obtenemos

$$\begin{array}{rcc}
c_n & = & 2c_{n-1}+1 = 2(2c_{n-2}+1)+1 \\
& = & 2^2c_{n-2}+3 = 2^3c_{n-3}+2^2+2+1 \\
& = & 2^4c_{n-4}+2^3+2^2+2+1 \\
& \dots & \\
& = & 2^{n-1}c_1+2^{n-2}+2^{n-3}+\cdots+2+1 \\
& = & 2^{n-1}+2^{n-2}+2^{n-3}+\cdots+2+1 \\
& = & 2^n\{\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^{n-1}}+\frac{1}{2^n}+1\}-2^n \\
& = & 2^n-1
\end{array}$$

Sumando la progresión geométrica de razón $\frac{1}{2}$.

1.6.3 Definición

Llamamos relación de recurrencia homogénea lineal de orden k y con coeficientes constantes a una relación de la forma

$$a_n = c_1a_{n-1}+c_2a_{n-2}+\cdots+c_ka_{n-k}$$

Si a esta relación de recurrencia se le agregan k condiciones iniciales

$$a_0 = C_0, a_1 = C_1, \dots, a_{k-1} = C_{k-1}$$

definimos unívocamente la sucesión $a_0, a_1, \dots$

Ejemplos

La relación de recurrencia dada por $A_n = (1.12)A_{n-1}$ y la sucesión de Fibonacci $f_n = f_{n-1}+f_{n-2}$ son, ambas, relaciones de recurrencia homogéneas lineales con coeficientes constantes, la primera de orden 1 y la segunda de orden 2.
Por cierto, una solución iterativa de $A_n = (1.12)A_{n-1}$ es $A_n = ct^n$.
Si queremos hallar una solución de la forma t^n para la sucesión de Fibonacci necesitamos

$$t^n = t^{n-1}+t^{n-2}$$

ó

$$t^n - t^{n-1} - t^{n-2} = 0$$

ó

$$t^2 - t - 1 = 0$$

ecuación cuadrática que admite como soluciones $t = \frac{1\pm\sqrt{5}}{2}$, con lo cual, una solución estará dada por

$$U_n = bS_n + dT_n = b(\frac{1+\sqrt{5}}{2})^n + d(\frac{1-\sqrt{5}}{2})^n$$

Ahora bien, para que se satisfagan las condiciones iniciales $f_0 = f_1 = 1$ debemos tener $U_0 = U_1 = 1$, es decir,

$$\begin{array}{rcl} U_0 & = & bS_0 + dT_0 = b + d = 1 \\ U_1 & = & bS_1 + dT_1 = \frac{b}{2}(1+\sqrt{5}) + \frac{d}{2}(1-\sqrt{5}) = 1 \end{array}$$

La solución de estas ecuaciones en b y en d :

$$d = \frac{\sqrt{5}-1}{2\sqrt{5}} \quad y \quad b = \frac{\sqrt{5}+1}{2\sqrt{5}}$$

Por lo tanto, $U_n = f_n = \frac{1}{\sqrt{5}}(\frac{\sqrt{5}+1}{2})^{n+1} - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^{n+1}$.

1.6.4 Teorema

Dada la relación de recurrencia homogénea lineal de segundo orden con coeficientes constantes

$$a_n = c_1 a_{n-1} + c_2 a_{n-2}$$

a) Si S_n y T_n son soluciones de esta relación de recurrencia entonces $U_n = bS_n + dT_n$ también es solución.

b) Si r es raíz de $t^2 - c_1 t - c_2 = 0$ entonces r^n es solución de la relación dada.

c) Sea a_n una solución de esta relación de recurrencia que satisface $a_0 = C_0$ y $a_1 = C_1$ y si $r_1 \neq r_2$ son raíces de la ecuación cuadrática $t^2 - c_1 t - c_2 = 0$ existen constantes b y d tales que $a_n = b{r_1}^n + d{r_2}^n \;\; \forall \;\; n \geq 0$.

Demostración

Dado que S_n y T_n son soluciones de la relación de recurrencia, satisfacen

$$\begin{array}{rcl} S_n & = & c_1 S_{n-1} + c_2 S_{n-2} \\ T_n & = & c_1 T_{n-1} + c_2 T_{n-2} \end{array}$$

con lo cual

$$\begin{array}{rcl} U_n & = & bS_n + dT_n \\ & = & c_1(bS_{n-1} + dT_{n-1}) + c_2(bS_{n-2} + dT_{n-2}) \\ & = & c_1 U_{n-1} + c_2 U_{n-2} \end{array}$$

resulta ser solución de la relación de recurrencia.

a) Si r es raíz de $r^2 = c_1 r + c_2$ resulta

$$\begin{aligned} c_1 r^{n-1} + c_2 r^{n-2} &= r^{n-2}\{c_1 r + c_2\} \\ &= r^{n-2} \cdot r^2 = r^n \end{aligned}$$

con lo cual, r^n resuelve la relación de recurrencia dada.

b) Definiendo $U_n = b{r_1}^n + d{r_2}^n$ que satisface la relación de recurrencia dada para que satisfaga las condiciones iniciales debe cumplirse

$$\begin{aligned} U_0 &= b + d = C_0 \\ U_1 &= br_1 + dr_2 = C_1 \end{aligned}$$

con lo cual

$$r_1 U_0 - U_1 = d(r_1 - r_2) = r_1 C_0 - C_1$$

Dado que $r_1 \neq r_2$ podemos obtener $d = \frac{r_1 C_0 - C_1}{r_1 - r_2}$ y, en consecuencia, obtenemos el valor de b.

1.6.5 Teorema

Dada la relación de recurrencia homogénea lineal de segundo orden con coeficientes constantes

$$a_n = c_1 a_{n-1} + c_2 a_{n-2}$$

Sea a_n una solución que satisface $a_0 = C_0$ y $a_1 = C_1$. Si las raíces r_1 y r_2 de la ecuación cuadrática $t^2 = c_1 t + c_2$ son coincidentes entonces existen constantes b y d tales que $a_n = br^n + dnr^n \quad \forall \quad n \geq 0$.

Demostración

De acuerdo con la demostración del Teorema anterior r^n es una solución de la relación de recurrencia dada. Como $r = r_1 = r_2$ es raíz doble de la ecuación $r^2 = c_1 r + c_2$ debe satisfacerse y, por cierto,

$$t^2 - c_1 t - c_2 = (t - r)^2$$

con lo cual $c_1 = 2r$ y $c_2 = -r^2$.
Ahora bien,

$$\begin{aligned} c_1(n-1)r^{n-1} + c_2(n-2)r^{n-2} &= 2r(n-1)r^{n-1} - r^2(n-2)r^{n-2} \\ &= r^n\{2(n-1) - (n-2)\} = nr^n \end{aligned}$$

luego, nr^n es solución de la relación de recurrencia dada y según el Teorema anterior, es $U_n = br^n + dnr^n$.
Para encontrar las constantes b y d tales que $U_0 = c_0$ y $U_1 = c_1$ procedemos como antes

$$\begin{array}{rcccl} U_0 & = & b + dn & = & C_0 \\ U_1 & = & br + dnr & = & C_1 \end{array}$$

de donde $rC_0 = C_1$ con $(b, d) = (c_0 - dn, d) = (c_0, 0) + d(-n, 1)$.
En general, si r es una raíz de multiplicidad m de

$$t^k - c_1 t^{k-1} - c_2 t^{k-2} - \cdots - c_k = 0$$

que corresponde a una relación de recurrencia homogénea lineal de orden k con coeficientes constantes puede probarse que

$$r^n, nr^n, \ldots, n^{m-1} r^n$$

son soluciones de

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

1.6.6 Ejemplo I

Raíces complejas conjugadas

Dada la siguiente relación de recurrencia

$$\begin{array}{rcl} a_n & = & 2a_{n-1} - 2a_{n-2} \;\; \forall \;\; n \geq 2 \\ a_0 & = & a_1 = 1 \end{array}$$

al intentar la solución $a_n = cr^n$ con r y c no nulas obtenemos como ecuación característica $r^2 - 2r + 2 = 0$ cuyas raíces son $1 \underline{+} i$.
Entonces, la solución general está dada por $c_1(1 + i)^n + c_2(1 - i)^n$ con c_1, c_2 constantes complejas. En virtud del Teorema de De Moivre escribimos

$$\begin{array}{rcl} (1 + i)^n & = & (\sqrt{2})^n [\cos \frac{n}{4} + i \sin \frac{n}{4}] \\ (1 - i)^n & = & (\sqrt{2})^n [\cos \frac{n}{4} - i \sin \frac{n}{4}] \end{array}$$

que proporcionan

$$a_n = k_1 (\sqrt{2})^n \cos \frac{n}{4} + k_2 (\sqrt{2})^n \sin \frac{n}{4}$$

con $k_1 = c_1 + c_2$ y $k_2 = (c_1 - c_2)i$.

1.6.7 Ejemplo II

Raíces reales repetidas

La siguiente relación de recurrencia

$$\begin{array}{rcl} a_{n+2} & = & 4a_{n+1} - 4a_n \ \ \forall \ \ n \geq 0 \\ a_0 & = & a_1 = 3 \end{array}$$

admite como ecuación característica $r^2 - 4r + 4 = (r-2)^2 = 0$ con raíz doble $r = 2$. Dado que no obtenemos soluciones linealmente independientes, intentamos, $a_n = n2^n$ que proporciona

$$\begin{array}{rcl} 4a_{n+1} - 4a_n & = & 4(n+1)2^{n+1} - 4n2^n \\ & = & 2(n+1)2^{n+2} - n2^{n+2} \\ & = & (2n+2-n)2^{n+2} \\ & = & (n+2)2^{n+2} \\ & = & a_{n+2} \end{array}$$

de modo que $a_n = n2^n$ es una solución linealmente independiente. Así, la solución general es

$$a_n = c_1 2^n + c_2 n 2^n$$

que con $a_0 = 1$ y $a_1 = 3$ proporcionan

$$a_n = 2^n + \frac{n}{2}2^n \ \ \forall n \geq 0$$

Observación
En general, si

$$c_n a_n + c_{n-1}a_{n-1} + ... + c_{n-k}a_{n-k} = 0$$

con $c_{n-k} \neq 0$ y $c_n \neq 0$ admite a r como raíz de multiplicidad m con $2 \leq m \leq k$ la solución general tiene la forma

$$A_0 r^n + A_1 n r^n + ... + A_{m-1} n^{m-1} r^n$$

con $A_0, A_1, ..., A_{m-1}$ constantes arbitrarias.

1.6.8 Ejemplo III

Relaciones de recurrencia no homogéneas

Consideremos, por ejemplo, la siguiente relación de recurrencia no homogénea

$$a_n - a_{n-1} = f(n) \ \ \forall n \geq 1$$

Para tal relación, tenemos

$$\begin{array}{lcccc} a_1 & = & a_0 + f(1) & & \\ a_2 & = & a_1 + f(2) & = & a_0 + f(1) + f(2) \\ a_3 & = & a_2 + f(3) & = & a_0 + f(1) + f(2) + f(3) \\ & \cdots & & & \end{array}$$

$$a_n = a_0 + \sum_{i=1}^{n} f(i)$$

Por ejemplo, la relación de recurrencia

$$\begin{array}{rcl} a_n - a_{n-1} & = & 3n^2 \quad \forall n \geq 1 \\ a_0 & = & 7 \end{array}$$

Aquí, $f(n) = 3n^2$, de modo tal que la solución general es

$$a_n = a_0 + \sum_{i=1}^{n} f(i) = 7 + 3\sum_{i=1}^{n} i^2 = 7 + \frac{3}{6}n(n+1)(2n+1)$$

Observación

En general, en virtud del método de coeficientes indeterminados, podemos recordar que si $f(n) = kr^n$ con k constante y $n \geq 0$ entonces la solución particular de la relación de recurrencia está dada por $a_n^p = Ar^n$ si r^n no resuelve la relación homogénea asociada y cuando lo es es $a_n^p = Bnr^n$.

Resumiendo, para el caso de una relación de recurrencia de orden dos si $f(n) = kr^n$ tenemos

a) $a_n^p = Ar^n$ si r^n no resuelve la relación de recurrencia homogénea

b) $a_n^p = Bnr^n$ si $a_n^h = c_1 r^n + c_2 r_1^n$ con $r_1 \neq r$

c) $a_n^p = Cn^2 r^n$ si $a_n^h = (c_1 + c_2 n) r^n$

1.6.9 Ejemplo IV

Consideremos un problema de análisis de algoritmos. Para $n \geq 1$ sea C un conjunto de números reales con $Card(C) = 2^n$.

¿Cuántas comparaciones deben efectuarse entre pares de números de C para determinar los elementos máximo y mínimo de C?.

Si a_n denota el número de comparaciones necesarias, por cierto, es $a_1 = 1$.

Cuando $n = 2$ es $Card(C) = 4$ y

$$C = \{x_1, x_2, y_1, y_2\} = C_1 \cup C_2$$

donde $C_1 = \{x_1, x_2\}$ y $C_2 = \{y_1, y_2\}$

Dado que $a_1 = 1$ basta una comparación para determinar los elementos máximo y mínimo en C_1 y de $C)_2$ (también los máximos) conoceremos los elementos máximo y mínimo de C.

Para determinar los elementos máximo y mínimo de C_1 y de C_2 son necesarias a_n compraciones y para comparar los elementos máximos y mínimos de C_1 y de C_2 se necesita una comparación más. En consecuencia, es

$$a_{n+1} = 2a_n + 2 \quad \forall n \geq 1$$

Aquí, $a_n^h = C2^n$ y $a_n^p = A$ es una constante. Al sustituir a_n^p en la relación, hallamos $A = 2A + 2$, es decir, $a = -2$. Luego, es $a_n = C2^n - 2$ que con $a_1 = 1$ proporciona $C = \frac{3}{2}$.
Por lo tanto, es $a_n = \frac{3}{2}(2^n) - 2$.
<u>*Observación*</u>
A modo de conclusión, dada una relación de recurrencia lineal no homogénea con cor=eficientes constantes de la forma

$$c_n a_n + ... + a_{n-k} a_{n-k} = f(n)$$

donde c_{n-k} y c_n son no nulos denotamos por a_n^h la solución de la relación homogénea asociada.

a) Si $f(n)$ es un múltiplo de una de la ssiguientes formas y <u>no</u> es solución de la relación homogénea asociada, entonces a_n^p tiene el siguiente aspecto
a)

$f(n)$	a_n^p
C *constante*	A *constante*
n	$A_0 + A_1 n$
n^2	$A_0 + A_1 n + A_2 n^2$
$n^t \ t \in Z^+$	$A_0 + A_1 n + ... + A_{t-1} n^{t-1} + A_t n^t$
$r^n \ r \in R$	Ar^n
$\sin n\alpha$	$A \sin n\alpha + B \cos n\alpha$
$\cos n\alpha$	$A \sin n\alpha + B \cos n\alpha$
$n^t r^n$	$r^n (A_0 + A_1 n + ... + A_t n^t)$
$r^n \sin n\alpha$	$Ar^n \sin n\alpha + Br^n \cos n\alpha$
$r^n \cos n\alpha$	$Ar^n \sin n\alpha + Br^n \cos n\alpha$

b) Si $f(n)$ es una combinación lineal de términos de esta tablilla entonces a_n^p también lo será.

c) Si $f(n)$ contiene sumandos tales como cr^n ó $(c_1 + c_2 n)R^n$ y r es solución de la ecuación caraterística, entonces, denotando por $f_1(n)$ a uno de estos sumandos, multiplicamos la solución particular a_n^p correspondiente a $f_1(n)$ por la menor potencia n^s para la cual ningún sumando de $n^s f_1(n)$ resuelve la relación homogénea asociada. Entonces, $n^s a_{n_1}^p$ es la parte correspondiente de a_n^p.

1.7 Ejercicios

Ejercicio 1

Resolver las siguientes relaciones de recurrencia

a) $$\begin{array}{rcl} a_{n+1} & = & a_n + (2n+3) \ \ \forall\, n \geq 0 \\ a_0 & = & 1 \end{array}$$

b) $$\begin{array}{rcl} a_{n+1} & = & a_n + (3n^2 - n) \ \ \forall n \ \geq 0 \\ a_0 & = & 3 \end{array}$$

c) $$\begin{array}{rcl} a_{n+1} & = & 2a_n + 2^n \ \ \forall\, n \geq 0 \\ a_0 & = & 1 \end{array}$$

1.7.1 Ejercicio 2

Resolver las siguientes relaciones de recurrencia

a) $$\begin{array}{rcl} a_{n+2} + 3a_{n+1} + 2a_n & = & 3^n \ \ \forall\, n \geq 0 \\ a_0 & = & 0 \\ a_1 & = & 1 \end{array}$$

b) $$\begin{array}{rcl} a_{n+2} + 4a_{n+1} + 4a_n & = & 7 \ \ \forall\, n \geq 0 \\ a_0 & = & 0 \\ a_1 & = & 2 \end{array}$$

c) $$\begin{array}{rcl} a_{n+2} + 4a_{n+1} + 4a_n & = & n^2 \ \ \forall\, n \geq 0 \\ a_0 & = & 0 \\ a_1 & = & 2 \end{array}$$

1.7.2 Ejercicio 3

Resolver la relación de recurrencia

$$d_n = 4(d_{n-1} - d_{n-2})$$

con las condiciones iniciales $d_0 = d_1 = 1$.

Ejercicio 4

De acuerdo con el Teorema anterior, $S_n = r^n$ es una solución siendo r solución de $t^2 = 4t - 4$ ó $(t-2)^2 = 0$, es decir, raíz doble $t = 2$. Por lo tanto, $S_n = 2^n$ es solución y, además, $T_n = n2^n$ es solución, con lo cual, la solución general es

$$U_n = aS_n + bT_n = a2^n + bn2^n = 2^n(a + bn)$$

Para satisfacer las condiciones iniciales deben cumplirse

$$\begin{array}{rcccl} U_0 & = & a & = & 1 \ \ \textit{es decir} \ \ a = 1 \\ U_1 & = & 2(b+1) & = & 1 \ \ \textit{es decir} \ \ b = -\frac{1}{2} \end{array}$$

Ejercicio 5

Resolver las siguientes relaciones de recurrencia

a) $$\begin{array}{rcl} \sqrt{a_n} & = & \sqrt{a_{n-1}} + 2\sqrt{a_{n-2}} \\ a_0 & = & a_1 = 1 \end{array}$$

b) $$\begin{array}{rcl} a_n & = & \frac{\sqrt{a_{n-1}}}{a^2{}_{n-2}} \\ a_0 & = & 1 \\ a_1 & = & 2 \end{array}$$

c) $$\begin{array}{rcl} a_n & = & -2na_{n-1} + 3n(n-1)a_{n-2} \\ a_0 & = & 1 \\ a_1 & = & 2 \end{array}$$

Ejercicio 6

La relación

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \mathcal{F}(n)$$

se llama relación no homogénea lineal de segundo orden con coeficientes constantes. Sea $\mathcal{G}(n)$ una solución particular de la relación *no* homogénea.
Probar que cualquier solución U_n de la relación de recurrencia no homogénea es de la forma

$$U_n = V_n + \mathcal{G}(n)$$

donde V_n es solución de la relación de recurrencia homogénea.

1.7.3 Método de funciones generadoras

Intentemos resolver la relación de recurrencia

$$\begin{array}{rcl} a_n - a_{n-1} & = & n \ \ \forall\, n \geq 1 \\ a_0 & = & 1 \end{array}$$

mediante la técnica de la función generadora de Taylor, es decir,
Multiplicando, miembro a miembro, la relación de recurrencia, por x^n y sumando entre 1 e infinito, obtenemos

$$\sum_{n=1}^{\infty} a_n x^n - 3\sum_{n=1}^{\infty} a_{n-1}x^n = \sum_{n=1}^{\infty} nx^n$$

En esta identidad, deseamos conocer los elementos de la sucesión $\{a_n\}_{n\geq 1}$. Para esto, llamamos a $f(x) = \sum_{n=0}^{\infty} a_n x^n$ la función generadora de la sucesión de números reales $\{a_n\}_{n\geq 1}$.

Re-escribimos la identidad anterior como sigue

$$\begin{array}{rcl} (f(x)-a_0)-3x\sum_{n=1}a_{n-1}x^{n-1} & = & \sum_{n=1}^{\infty}nx^n \\ & = & \sum_{n=0}^{\infty}nx^n \\ (f(x)-a_0)-3x\sum_{n=0}^{\infty}a_nx^n & = & f(x)-a_0-3xf(x) \\ & = & \sum_{n=0}^{\infty}x^n \end{array}$$

Ahora bien, cuál es la función generadora para la sucesión $\{n\}_{n\geq 0}$?.

$$\begin{array}{rcl} \sum_{n=0}^{\infty} & = & \frac{1}{1-x} \quad si \quad |x|<1 \\ \sum_{n=1}^{\infty}nx^{n-1} & = & \frac{d}{dx}(\frac{1}{1-x})=\frac{1}{(1-x)^2} \\ & = & \sum_{n=0}^{\infty}(n+1)x^n \end{array}$$

y, también,

$$x\sum_{n=1}^{\infty}nx^{n-1}=\sum_{n=1}^{\infty}nx^n$$

con lo cual obtenemos

$$\begin{array}{rcl} (f(x)-1)-3xf(x) & = & \frac{x}{(1-x)^2} \\ f(x)(1-3x)-1 & = & \frac{x}{(1-x)^2} \\ f(x)(1-3x) & = & \frac{x}{(1-x)^2}+1 \\ & = & \frac{x^2-x+1}{(1-x)^2} \\ f(x) & = & \frac{1}{1-3x}+\frac{x}{(1-x)^2)(1-3x)} \\ & = & \frac{1}{1-3x}+\frac{A}{1-x}+\frac{B}{(1-x)^2}+\frac{C}{1-3x} \end{array}$$

que descompuesta en fracciones simples proporciona el siguiente sistema de ecuaciones

$$\begin{array}{rcl} A+B+C & = & 0 \\ 4A+3B+2C & = & -1 \\ 3A+C & = & 0 \end{array}$$

con soluciones

$$\begin{array}{rcl} A & = & -\frac{1}{4} \\ B & = & -\frac{1}{2} \\ C & = & \frac{3}{4} \end{array}$$

Por lo tanto,

$$\begin{array}{rcl} f(x) & = & \frac{1}{1-3x}-\frac{1}{4}\frac{1}{1-x}-\frac{1}{2}\frac{1}{(1-x)^2}+\frac{3}{4}\frac{1}{1-3x} \\ & = & \frac{7}{4}\sum_{n=0}^{\infty}3^nx^n-\frac{1}{4}\sum_{n=0}^{\infty}x^n-\frac{1}{2}\sum_{n=0}^{\infty}(n+1)x^n \\ & & \sum_{n=0}^{\infty}[\frac{7}{4}3^n-\frac{1}{4}-\frac{n+1}{2}]x^n \end{array}$$

Por lo tanto, la sucesión $\{a_n\}_{n\geq 0}$ buscada está dada por

$$a_n=\frac{7}{4}3^n-\frac{1}{4}-\frac{n+1}{2}$$

Capítulo 2

Números Enteros

2.1 Propiedades de los Números Enteros

Sabemos por resultados del Algebra que sobre el conjunto de números enteros $\mathcal{Z}$ están definidas dos operaciones: suma y producto, con las siguientes propiedades Para la $(+)$

a) conmutativa

b) asociativa

c) distributiva

d) existe elemento neutro 0

e) existe inverso aditivo

Para el producto $(\cdot)$

a) conmutativa

b) asociativa

c) distributiva respecto del producto

d) existe elemento neutro 1

e) es válida la ley de simplificación del producto, es decir,

$$Si \;\; c \neq 0 \; y \; ac = bc \; entonces \; a = b$$

También, sabemos de la unicidad del elemento neutro y del inverso aditivo. Una consecuencia de la ley de simplificación es

$$Si \;\; a \cdot b = 0 \; entonces \; a = 0 \;\; ó \;\; b = 0$$

2.1.1 Ley de Simplificación (divisores del cero)

La ley de simplificación para el producto equivale a afirmar que el producto de dos factores no nulos es distinto de cero.

Demostración

Supongamos que $a \neq 0$. Entonces , $a \cdot b = 0 = a \cdot 0$ por la ley de la simplificación es $b = 0$.
Inversamente , si $a \neq 0$ y $ab = ac$ entonces $ab - ac = a(b - c) = 0$ con lo cual $b - c = 0$, es decir, $b = c$.

Los elementos no nulos a y b cuyo producto $ab = 0$ se denomina divisores del cero ó divisores nulos con lo cual la ley de simplificación de producto, equivale a afirmar que $\mathcal{Z}$ es un dominio de integridad sin divisores nulos.

2.1.2 Aplicación

Como aplicación de este teorema consideremos el conjunto de todos los números de la forma $a + b\sqrt{3}$ con a y b enteros.

Es fácil verificar que la suma y el producto de números de esta forma la conservan , en efecto

$$\begin{aligned} (a + b\sqrt{3}) + (c + d\sqrt{3}) &= (a + c) + (b + d)\sqrt{3} \\ (a + b\sqrt{3}) \cdot (c + d\sqrt{3}) &= (ac + 3bd) + (ad + bc)\sqrt{3} \end{aligned}$$

Con estas operaciones se satisfacen las propiedades distributivas , asociativa y conmutativa. Además, $0 = 0 + 0\sqrt{3}$ y $1 = 1 + 0\sqrt{3}$ .Por otra parte, la ecuación $(a + b\sqrt{3}) + x = 0$ tiene solución $x = -a - b\sqrt{3}$.
Finalmente veamos que es válida la ley de simplificación de productos admitiendo que la ecuación $x^2 = 3y^2$ no admite soluciones enteras no nulas x e y pues

$$x^2 = 3y^2 \Leftrightarrow x^2 - 3y^2 = 0 \Leftrightarrow (x - \sqrt{3}y)(x + \sqrt{3}y) = 0$$

de aquí $x + y\sqrt{3} = 0$ *sólo sí* $x = y = 0$.

Supongamos que en el conjunto de números considerado hubiese divisores de cero, como $(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3} = 0$ de acuerdo con la observación anterior sería

$$\begin{cases} ac + 3bd &= 0 \\ ad + bc &= 0 \end{cases}$$

Multiplicando la primera por d y la sgunda por c y restando , obtenemos $b(3d^2 - c^2) = 0$.
Dado que la ley de simplificación vale para números enteros es $b = 0$; $\vee$; $3d^2 - c^2 = 0$, si $3d^2 = c^2$ debe ser $d = c = 0$ por lo dicho y si $b = 0$ las ecuaciones anteriores dan $ac = ad = 0$, es decir, $a = 0$ ó $c = d = 0$. En cualquier caso, uno de los supuestos divisores del cero, $a+b\sqrt{3}$ ó $c+d\sqrt{3}$ resulta también igual a cero.

Anillos

2.1.3 Definición

Dado un conjunto A no vacío en el cual se definen dos operaciones binarias, por ejemplo, suma y producto decimos que $(A, +, \cdot)$ es un anillo si para todo $a \in A$ y para todo $b \in A$ y para todo $c \in A$ se verifican las siguientes condiciones

a) $a + b = b + a$

b) $a + (b + c) = (a + b) + c$

c) existe $z \in A$ tal que $a + z = z + a = a$ para todo $a \in A$

d) para todo $a \in A$ existe $a^{'} \in A$ tal que $a + a^{'} = a^{'} + a = z$

e) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

f) $a(b + c) = a \cdot b + a \cdot c$

Observaciones

a) Si $ab = ba$ para todo $a \in A$ y para todo $b \in A$ entonces A es un anillo conmutativo.

b) Si existe $u \in A$ tal que $au = ua$ para todo $a \in A$ entonces u se denomina *identidad* multiplicativa. Entonces, A se llama anillo con identidad.

c) Se dice que A no tiene divisores propios de cero si para todo $a \in A$ y para todo $b \in A$ entonces $ab = z$ implica $a = z$ ó $b = z$

En qualquier anillo, son únicos la identidad, el elemento neutro y el inverso multiplicativo.

2.1.4 Teorema

Sea $(A, +, \cdot)$ un anillo conmutativo con identidad. Entonces, A es un dominio entero si y sólo sí para $a, b, c \in A$ con $a \neq z$ entonces $ab = ac$ implica $b = c$.
De este modo, un anillo conmutativo con identidad que satisfaga la ley de cancelación del producto es un dominio entero.

2.1.5 Teorema

Un dominio entero finito $(D, +, \cdot)$ es un campo.

demostración

dado que D es finito, enumeramos los elementos de D por $d_1, ..., d_n$.
Para $d \in D$ con $d \neq z$ es $dD = \{dd_1, ..., dd_n\} \subseteq D$ pues es cerrado bajo la multiplicación.
Ahora bien, como $Card(D) = n$ y $dD \subseteq D$ si pudiésemos probar que dD contiene n elementos tendríamos $dD = D$.
Si $Card(D) < n$ entonces $dd_i = dd_j$ para $1 \leq i < j \leq n$ pero como D es un dominio entero y $d \neq z$ resulta $d_i = d_j$ contradicción pues supusimos que $d_i \neq d_j$. Luego, $dD = D$ y para algún $1 \leq k \leq n$ es $dd_k = u$ el elemento unidad de D. Entonces, $dd_k = u$ y así, es d la unidad de D y como d se seleccionó arbitrariamente, concluimos que $(D, +, \cdot)$ es un campo.

Dominios de Integridad Ordenados

2.1.6 Definición

La relación natural $a < b$ vale si $b - a$ es un entero positivo.

De esta forma, consideramos
a) La suma de dos enteros positivos es positiva.

b) El producto de dos enteros positivos es positivo.

c) Ley de tricotomía

Para cualquier a entero es válida una y sólo una de las siguientes alternativas : $a = 0, \ ; \ ; a > 0, \ ; \ ; -a > 0$

En consecuencia, todo dominio de integridad que contenga elementos positivos con las tres propiedades enunciadas se dice *ordenado*.

2.1.7 Propiedades

a) En todo dominio de integridad ordenado, $\forall \;\; a \neq 0$ es $a^2 > 0$.

b) La unidad $1 = 1^2$ es siempre positiva.

c) En un dominio ordenado, $a < b$ significa $b - a > 0$. Además, $a \leq b$ significa; o bien $a < b$ o bien $a = b$.
En consecuencia , es válida la ley transitiva

Si $a < b$ y $b < c$ entonces $a < c$ pues $b - a \;\; > 0$ y $c - b \;\; > 0$ y así $(b - a) + (c - b) = c - a \; > 0$ lo cual significa $a < c$.

d) Si $a < b$ entonces $a + c < b + c$

e) Si $a < b$ y $0 < c$ entonces $ac < bc$

f) Entre dos elementos cuales quiera a y b es válida una y sólo una de las siguientes relaciones $a < b$ ó $a = b$ ó $a > b$.

2.1.8 Valor Absoluto en un Dominio

En un dominio ordenado definiremos valor absoluto de un número a, como sigue

$$|a| = \begin{cases} +a & \text{si } a \geq 0 \\ -a & \text{si } a < 0 \end{cases}$$

Es fácil demostrar que

a) $|ab| = |a| \cdot |b|$

b) $|a + b| \leq |a| + |b|$

Observamos que, por definición, es

a) $-|a| \leq a \leq |a|$

b) $-|b| \leq b \leq |b|$

con lo cual

$-(|a| + |b|) \leq a + b \leq |a| + |b|$

2.1.9 Ejercicios

Ejercicio 1

Probar que en todo dominio de integridad los únicos elementos idempotentes, es decir , que $xx = x$ son cero y uno.

Ejercicio 2

¿ Cuáles de los siguientes conjuntos de números son dominios de integridad ?.

a) Todos los enteros positivos

b) Todos los enteros impares

c) Todos los números de la forma $a + b\sqrt{2}$ con a y b enteros

Ejercicio 3

Probar en un dominio ordenado las siguientes reglas

a) Si $a < 0$ es $ax > ay$ si y sólo sí $x < y$

b) $a < b$ implica $a^2 < b^2$

Ejercicio 4

Probar que la ecuación $x^2 + 1 = 0$ no puede tener soluciones en un dominio ordenado.

Ejercicio 5

Probar en un dominio ordenado que

$$||a| - |b|| \leq |a - b|$$

2.2 Divisibilidad de enteros

Una ecuación $ax = b$ con coeficientes a y b enteros no siempre tiene solución entera. Cuando una tal solución existe, decimos que b es divisible por a.

2.2.1 Definición

a/b "a divide a b" cada vez que existe un entero d tal que $b = ad$.

La relación a/b es reflexiva y transitiva por cierto, pues

a) a/b ya que $a = 1 \cdot a$

b) a/b y b/c implica a/c equivale a decir : $b = d_1 a \ \wedge \ c = d_2 b$ con d_1 y d_2 enteros.

De esto resulta : $c = d_2 b = (d_2 d_1)a$, es decir, a/c.

2.2.2 Divisores Enteros de 1

Teorema

Los únicos divisores de 1 son ± 1.

Esto significa que si dos enteros a y b son tales que $ab = 1$ han de ser $a = \pm 1$ y $b = \pm 1$.
Demostración

En efecto, $ab = 1$ dá $|ab| = |a||b| = 1$.
Dado que $a \neq 0$ y $b \neq 0$ son $|a|$ y $|b|$ enteros positivos. Es fácil ver que no hay enteros positivos entre 0 y 1; en consecuencia, por la ley de tricotomía, deben ser $|a| \geq 1$ y $|b| \geq 1$. Luego, $|a||b| \neq 1$ (≥ 1). Entonces, $|a| = 1$ y $|b| = 1$ y , por lo tanto , $a = \pm 1$; $b = \pm 1$.

Dado que $a = a1 = (-a)(-1)$, todo entero a divisible por a, $-a$, 1, -1.
Los números a y $(-a)$, por dividirse mutuamente, se llaman asociados.

2.2.3 Enteros Asociados

Definición

Dos enteros a y b se llaman asociados si se verifican las relaciones siguientes

$$a/b \ \ y \ \ b/a$$

Los asociados de 1 se llaman unidades

Observemos que si a y b son asociados entonces $a = bd_1$ y $b = ad_2$ con lo cual, es $a = ad_1 d_2$ de donde $d_1 d_2 = 1$ es decir d_1 es un divisor de 1 y, por lo tanto, debe ser $d_1 = \pm 1$. Por lo tanto, $b = \pm a$ así que los únicos asociados de a son $\pm a$.

Por lo tanto, dos enteros a y b son asociados si y solo sí $|a| = |b|$.

2.2.4 Números Primos

Definición

Un entero p es primo si $p \neq 0$ y $p \neq \pm 1$ es divisible por ± 1 y $\pm p$.

2.2.5 Algoritmo de la división o de Euclides

Dados dos números enteros a y b, $b > 0$ existen dos enteros q y r tales que

$$a = bq + r \quad 0 \leq r < b$$

Demostración

Es fácil ver que existen algunos múltiplos enteros de b que no exceden a a, por ejemplo, como $b > 0$ es $b \geq 1$ puesto que entre 0 y 1 no existen enteros. Así, $-|a|b \leq -|a| \leq a$.
Por lo tanto, el conjunto de las diferencias $a-bx$ contiene por lo menos un entero no negativo, a saber, el $a - (-|a|)b$. Luego, por el Principio de Buena Ordenación existe un mínimo no negativo para $(a - bx)$ al que llamamos $a - bq = r$. Por construcción, $r \geq 0$ mientras que si $r \geq b$ entonces, $r - b = a - b(q + 1) \geq 0$ sería menor que $(a - bq)$ que contradice la elección de q. Por tanto, $0 \leq r < b$ y

$$a = bq + (a - bq) = bq + r$$

Colorario

Dados dos enteros a y b quedan unívocamente determinados el cociente q y el resto r tales que $a = bq + r$ con $0 \leq r < b$.

Es inmediato pues suponiendo que sea

$$\begin{array}{ccll} a = bq + r & = & bq' + r' & con \quad 0 \leq r < b \\ 0 & \leq & & r' < b \end{array}$$

tendríamos $r - r' = b(q' - q)$ es decir, $(r - r')$ es múltiplo de b ó sea $b/(r - r')$ y, además, $|r - r'| < |b|$. En consecuencia, $r - r'$ debe ser cero, es decir, $r = r'$ con lo cual $bq' = bq$, ó va $q' = q$.

2.2.6 Ejercicio

Si a/b probar que $|a| \leq |b|$ cuando $b \neq 0$

2.2.7 Definición

Un conjunto S de números enteros es cerrado para la suma y la diferencia cuando $a+b$ y $(a-b)$ pertenecen a S para cualesquiera sean los números enteros a y b en S.

Un ejemplo importante de conjuntos de números enteros cerrado para la suma y la diferencia es

El conjunto de todos los múltiplos xm de un entero fijo m. Estos son los únicos conjuntos de números enteros con esta propiedad.

Elemento Mínimo de un Conjunto

2.2.8 Teorema

Todo conjunto no vacío de enteros, cerrado para la suma y la diferencia, contiene sólo el 0 ó contiene un número positivo mínimo del cual todos los demás son múltiplos.

Demostración

Sea S tal conjunto. Supongamos que existe un elemento $a \neq 0$ en S.
Por propiedad de cerrado S contiene la diferencia $a-a=0$ y, también contiene a $0-a=-a$. Por lo tanto, S contiene al menos un número positivo a ó $(-a)$. El Principio de Buena Ordenación asegura que S tiene mínimo elemento positivo b.
El conjunto S debe contener todos los múltiplos de b

Inductivamente, podemos asegurar, que contiene a $b \cdot 1$ y que si contiene a $b \cdot k$ también contiene a $bk + b \cdot 1 = b(k+1)$.
Los múltiplos negativos tales como $-bn = 0 - bn$ también pertenecen a S pues éste es cerrado para la diferencia.
Ahora bien, observemos que S no puede contener enteros que no sean múltiplos de b pues si existiera $a \neq \dot{b}$ también pertenecería a S el resto de la división por b, es decir, $r = a - bq$.
Como $0 \leq r < b$ siendo b el mínimo entero positivo en S entonces debe ser $r=0$ y $a = bq$.

2.2.9 Máximo Común Divisor

Definición

Un número entero d se llama máximo común divisor de dos enteros a y b cada vez que verifique d/a; d/b y si $c/a \wedge c/b$ implica c/d.

Teorema

Dos enteros cualesquiera $a \neq 0$ y $b \neq 0$ tienen m.c.d. positivo $(a,\ b)$ el cual puede expresarse como

$$(a,\ b) = sa + tb$$

donde s y t son números enteros.

Demostración

Para cada dos números de esta forma tenemos

$$(s_1a + b_1b) \pm (s_2a + b_2b) = (s_1 \pm s_2)a + (b_1 \pm b_2)b$$

Por lo tanto, el conjunto S de todos los enteros de la forma $sa + tb$ es cerrado para la suma y la diferencia. En consecuencia, por el Teorema anterior, tal conjunto estará constituido por todos los múltiplos de un número entero positivo $d = sa + tb$.
Es claro que si c es factor común de a y de b entonces es factor común de d. Además, los enteros $a = 1a + 0b$ y $b = 0a + 1b$ pertenecen a S; en consecuencia, serán múltiplos de mínimo número d del conjunto. Es decir, d es un divisor común al cual dividen todos los demás divisores de a y de b comunes a ambos; luego $d = (a,\ b)$.
Análogamente, definimos mínimo común múltiplo.

Mínimo Común Múltiplo

Definición

Dos enteros cualesquiera a y b tienen m.c.m. $[a,\ b]$ el cual es divisor de todos los múltiplos comunes siendo él, a su vez, un múltiplo común.

Para hallar el m.c.d. entre a y b enteros, empleamos el algoritmo de Euclides, a saber

Sean a y b enteros positivos (si fuese alguno negativo no se altera el m.c.d. pues $(a,\ b) = (-a,\ b)$).

El algoritmo de la división dá

$$a = bq_1 + r_1 \quad 0 \leq r_1 < b$$

Cualquier entero que divide a a y a b divide al resto r_1 y, recíprocamente, todo divisor común de b y de r_1 es divisor de a. Es decir, que los divisores comunes del par $a,\ b$ son los mismos que los del par $b,\ r_1$ con lo cual $(a,\ b) = (b,\ r_1)$.
Iterando este procedimiento obtenemos

$$\begin{array}{rcll}
b & = & r_1 q_2 + r_2 & 0 < r_2 < r_1 \\
r_1 & = & r_2 q_3 + r_3 & 0 < r_3 < r_2 \\
& \vdots & & \vdots \\
r_{n-2} & = & r_{n-1} q_n + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} & = & r_n q_{n-1} &
\end{array}$$

Dado que el resto disminuye permanentemente, habrá finalmente resto cero con lo cual el m.c.d. buscado es

$$(a,\ b) = (b,\ r_1) = (r_1,\ r_2) = \cdots = (r_{n-1},\ r_n)$$

pero podemos observar que r_n / r_{n-1} con lo cual $(r_n,\ r_{n-1}) = r_n$.
Por lo tanto, el m.c.d. dados dos enteros a y b es el último resto distinto de cero obtenido a partir del Algoritmo de Euclides.

El mismo algoritmo puede emplearse para representar explícitamente al m.c.d. como combinación lineal $sa + tb$.
En efecto,

$$\begin{array}{rcccc}
r_1 & = & a - bq_1 & = & a + (-q_1)b \\
r_2 & = & b - q_2 r_1 & = & (-q_2)a + (1 + q_1 q_2)b
\end{array}$$

Luego, r_n también puede obtenerse como combinación lineal de a y de b.

2.3 Propiedades de los Números Primos

2.3.1 Teorema I

Si p es primo, p/ab implica p/a ó p/b.

Demostración

Por definición, un número primo p tiene únicos factores ± 1 y $\pm p$.
Si la conclusión p/a es falsa entonces los únicos divisores comunes entre p y a son ± 1, por lo tanto, un m.c.d. $(a,\ p) = 1$ y así

$$\begin{array}{rcl}
1 & = & sa + tp \\
b & = & sab + tpb
\end{array}$$

Ambos términos de la derecha son divisibles por p, luego p/b.
Si $(a,\ b) = 1$ entonces a y b son *primos* entre sí, es decir que no tienen divisores comunes salvo ± 1

2.3.2 Teorema II

Si $(a,\ c) = 1$ y c/ab entonces c/b.

2.3.3 Teorema III

Si $(a,\ c) = 1$ y a/m y c/m entonces ac/m.

Demostración

En efecto, $m = ad$ y, además, c/m.
Luego, por el Teorema inmediatamente anterior al ser $(a,\ c) = 1$ resulta que c/d; en consecuencia, $m = ad = a(cd')$, por lo tanto ac/m.

2.3.4 Ejercicios

Ejercicio 1

Probar que $(0,\ a) = |a| \quad \forall\, a \in \mathcal{Z}$

Ejercicio 2

Probar que b/c y $|c| < b$ implica $c = 0$.

Ejercicio 3

Mostrar que el algoritmo de la división vale también para b negativo siempre y cuando $0 \leq r < |b|$.

Ejercicio 4

Mostrar, inductivamente, que en el Algoritmo de Euclides cada resto es $r_k = s_k a + t_k b$ con $s_k,\ t_k$ enteros.

Ejercicio 5

¿Cuáles de los siguientes conjuntos de enteros son cerrados para la suma y para la diferencia

a) Todos los enteros m tales que $(m,\ 7) = 1$.

b) Todos los enteros m tales que $6/m$ y $24/m^2$.

c) Todos los enteros m tales que alguna potencia de m es divisible por 64.

Ejercicio 6

a) Probar que si $(a,\ m) = (b,\ m) = 1$ entonces $(ab,\ m) = 1$.

b) Probar que si $(a,\ c) = d$, a/b y c/b entonces ac/bd.

c) Probar que $[a,\ b] = ac/d$.

2.3.5 Teorema fundamental de la Aritmética

Todo entero *no* nulo tiene *única* descomposición en producto de (± 1) por factores primos positivos salvo el orden en el cual estos factores se consideren.

Demostración

Sea $\mathcal{P}(a)$ la proposición que dice
"a puede descomponerse en producto de factores primos" tal como lo enunciamos.
Si $a = 1$ ó si a es primo, por cierto, $\mathcal{P}(a)$ es verdadera.

Si a admite un divisor positivo $b \neq 1$ y $b \neq a$ con lo cual $a = bc$, $b < a$, $c < a$ podemos, de acuerdo con el segundo principio de inducción (Ejercicio 6 sobre Principio de Inducción), suponer que $\mathcal{P}(b)$ y $\mathcal{P}(c)$ son verdaderos con lo cual b y c pueden expresarse como producto de factores primos, a saber

$$b = p_1 p_2 \cdots p_r \quad y \quad c = q_1 q_2 \cdots q_s$$

de modo que

$$a = bc = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$$

que es la forma requerida.

Para mostrar la unicidad de la descomposición, consideremos dos posibles descomposiciones en producto de factores primos de un entero a, a saber

$$a = (\pm 1)p_1p_2\cdots p_m = (\pm 1)q_1q_2\cdots q_n$$

Como todos los primos $p_1, p_2, \cdots, p_m$ son positivos al igual que los primos $q_1, q_2, \cdots, q_n$ resulta que el p_1 es un divisor de $a = \pm q_1q_2\cdots q_n$.
Por lo tanto, por un Teorema anterior, podemos asegurar que p_1 divide por lo menos a un factor q_j de este producto.

Como $(p_1,\ q_j) = 1$ y p_1/q_j deben ser $p_1 = q_j$, por lo tanto,

$$p_2p_3\ldots p_m = {q'}_2{q'}_3\cdots{q'}_m$$

donde las " ' " denotan el reordenamiento al haber eliminado a q_j.
Este procedimiento puede iterarse hasta lograr $m = n$.

Si en una descomposición aparece un número primo p varias veces escribimos

$$a = \pm {p_1}^{n1}{p_2}^{n2}\cdots{p_m}^{nm}(0 < p_1 < p_2 < \cdots < p_m)$$

2.4 Congruencias

2.4.1 Definición

Decimos que $a \equiv b \pmod{m}$ cada vez que $m/(b-a)$

2.4.2 Teorema I

Es condición necesaria y suficiente para que dos enteros a y b sean congruentes módulo m que tengan el mismo resto al dividirlos por m.

Demostración

Como $a \equiv b \pmod{m} \Leftrightarrow a \equiv b \pmod{-m}$ basta probar el Teorema para $m > 0$.
Supongamos que $a \equiv b \pmod{m}$, entonces, $a - b = cm$ y, además, $b = mq + r$ con $0 \leq r < m$. Entonces,

$$a = b + cm = (qm + r) + cm = (q + c)m + r$$

por lo tanto, r es el resto de dividir a a por m es decir, el resto de dividir por m es el mismo.
Reciprocamente, si el resto es el mismo, con lo cual $a = qm + r$ y $b = q'm + r$,

en cuyo caso,

$$a - b = (q - q')m$$

es decir que $m/(a-b)$, así que $a \equiv b \pmod{m}$.

2.4.3 Propiedades

La relación congruencia es reflexiva, simétrica y transitiva, es decir, es una relación de equivalencia.

a) Reflexiva: $a \equiv a \pmod{m}$ pues $m/(a-a)$.

b) Simétrica: $a \equiv b \pmod{m}$ implica $b \equiv a \pmod{m}$.

Si $a \equiv b \pmod{m}$ entonces $m/(b-a)$ es decir, $a - b = md$. Obviamente, $b - a = (-d)m$.

c) Transitiva: $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$ entonces $a \equiv c \pmod{m}$. En efecto

$$\left.\begin{array}{rcl} b-a & = & dm \\ c-b & = & d'm \end{array}\right\} c - a = c - b + b - a = d'm - dm = (d' - d)m$$

2.4.4 Teorema II

Si $a \equiv b \pmod{m}$ entonces $\forall\ x \in \mathcal{Z}$ vale

$$\begin{array}{rcl} a + x & \equiv & b + x \pmod{m} \\ -a & \equiv & -b \pmod{m} \end{array}$$

Entonces

$$a \cdot x \equiv b \cdot x \pmod{m}$$

Demostración

a) $a + x \equiv b + x \pmod{m} \Leftrightarrow m/(b + x - a - x)$, es decir, $m/(b-a)$.

b) $ax \equiv bx \pmod{m} \Leftrightarrow m/(bx - ax)$, es decir,

$$\begin{array}{rcccc} bx - ax & = & (b-a)x & = & dm \\ bx - ax & = & (d'm)x & = & dm \\ & = & (d'x)m & = & dm \\ & & \Rightarrow & d = d'x & \end{array}$$

c) $$\begin{array}{rcl} (-a) \equiv (-b) \pmod{m} & \Leftrightarrow & (-b+a) = dm \\ & \Leftrightarrow & -(b-a) = dm \end{array}$$

<u>*Observación*</u>

$2 \cdot 7 \equiv 2 \cdot 1 \pmod{12}$ pero $7 \not\equiv 1 \pmod{12}$ es decir, que no puedo simplificar.

2.4.5 Teorema III

Si c es primo con m entonces

$$ca \equiv cb \pmod{m} \Rightarrow a \equiv b \pmod{m}$$

Demostración

$ca \equiv cb \pmod{m} \Leftrightarrow m/c(b-a)$ lo cual implica, al ser, $(m,\ c) = 1$ que $m/(b-a)$ es decir, $a \equiv b \pmod{m}$.

2.4.6 Teorema IV

Si $(m,\ c) = 1$ entonces la congruencia $cx \equiv b \pmod{m}$ tiene una solución entera x. Dos soluciones cualesquiera x_1 y x_2 son congruentes módulo m.

Demostración

Como $(m,\ c) = 1$ resulta $1 = sc + tm$ con s y t enteros $b = bsc + btm$ donde btm es múltiplo de m, así que $b \equiv (bs)c \pmod{m}$. Esto dice que $x = bs$ es solución de $b \equiv cx \pmod{m}$. Por otra parte, dos soluciones cualesquiera x_1 y x_2 de esta congruencia proporcionan $cx_1 \equiv cx_2 \pmod{m}$ pues la relación de congruencia es simétrica y transitiva. Como $(m,\ c) = 1$, puedo simplificar, como en el Teorema anterior, y resulta $x_1 \equiv x_2 \pmod{m}$.

2.4.7 Colorario

Si p es primo y $c \not\equiv 0 \pmod{p}$ entonces $cx \equiv b \pmod{p}$ tiene única solución módulo p.

Demostración

La demostración es consecuencia de la siguiente propiedad

Todo dominio de integridad finito es un campo
La hipótesis de ser D finito permite enumerar los elementos $b_1, ..., b_n$ en D.
Para probar que es un campo bastará probar que

$$\forall\ a \in D \quad a \neq 0 \quad existe \quad a^{-1} \in D : a \cdot a^{-1} = a^{-1} \cdot a = 1$$

Calculemos los productos
$ab_1, ..., ab_n \in D$ todos diferentes pues si $ab_i = ab_j$ entonces $b_i = b_j$ en contra de lo supuesto. Como $ab_1, ..., ab_n$ son los mismos elementos de D $(aD \subseteq D)$ entonces, uno de ellos debe ser la unidad, por ejemplo, $ab_1 = 1$ implica b_1 es el inverso de a. Por cierto, si $ax \equiv 1 (modp)$ con p primo y $a \neq 0$ es lo mismo que $ax = 1$ en Z_p.

2.4.8 Teorema V

Si los módulos m_1 y m_2 son tales que $(m_1,\ m_2) = 1$ entonces las congruencias

$$\begin{array}{l} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{array}$$

tienen una solución común, x.
Dos soluciones cualesquiera son congruentes módulo $(m_1\ m_2)$.

Demostración

La primera congruencia tiene solución a b_1; la solución más general es $x = b_1 + ym_1$ para cualquier entero y.
Esta debe verificar la segunda congruencia, es decir,

$$b_1 + ym_1 \equiv b_2 \pmod{m_2}$$

ó

$$ym_1 \equiv (b_2 - b_1) \pmod{m_2}$$

Como $(m_1,\ m_2) = 1$ podemos resolver esta congruencia por el método del Teorema anterior.
Ahora, supongamos que x y x' son soluciones del sistema

$$\left\{ \begin{array}{lcl} x & \equiv & b_1 \pmod{m_1} \\ x & \equiv & b_2 \pmod{m_2} \end{array} \right.$$

Por lo tanto,

$$\begin{array}{lcl} x' - x & \equiv & 0 \pmod{m_1} \\ x' - x & \equiv & 0 \pmod{m_2} \end{array}$$

Al ser $(m_1,\ m_2) = 1$ la diferencia $(x' - x)$ es divisible por $(m_1\ m_2)$ así que $x \equiv x' \pmod{m_1 m_2}$.

2.4.9 Ejercicios

Ejercicio 1

Resolver las siguientes congruencias

a) $3x \equiv 2 \pmod{5}$

b) $243x + 17 = 101 \pmod{725}$

c) $6x + 3 \equiv 4 \pmod{10}$

Ejercicio 2

Probar que $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ implican $a+c \equiv b+d \pmod{m}$ y $ac \equiv bd \pmod{m}$.

Ejercicio 3

Probar que $ax \equiv b \pmod{m}$ tiene solución si y sólo sí $(a,\ m)/b$

Ejercicio 4

Mostrar que $x^2 \equiv 35 \pmod{100}$ no tiene solución

Ejercicio 5

Mostrar que si x es impar no divisible por 3 entonces $x^2 \equiv 1 \pmod{24}$

Ejercicio 6

Resolver las congruencias simultáneas

a) $x \equiv 2 \pmod{5}$ y $3x \equiv 1 \pmod{8}$

b) $3x \equiv 2 \pmod{5}$ y $2x \equiv 1 \pmod{3}$

2.4.10 Introducción a $\mathcal{Z}_n$

Los enteros pares son congruentes con $0 \pmod{2}$ mientras que los enteros impares son congruentes con $1 \pmod{2}$
Estos restos pueden sumarse y multiplicarse de modo tradicional cuidando de

reemplazar el resultado por el resto de dividir por 2.
Esto nos da la siguiente tabla

$$\begin{array}{rclcr} 0+0 & = & 1+1 & =0 & 0+1=1 \\ 0\cdot 0 & = & 0\cdot 1 & =0 & 1\cdot 1=1 \end{array}$$

Esto muestra que $1+1 \equiv 0 \pmod 2$ en particular.
Hasta ahora hemos visto que la realción de congruencia es de equivalencia y, además, que si

$$a \equiv b \pmod m \text{ y } c \equiv d \pmod m \text{ entonces} a+c \equiv b+d \pmod m \text{ y } ac \equiv bd \pmod m$$

Esto dice que cada entero es "igual" a uno de los n posibles restos $0, 1, 2, \dots, (n-1)$. Podemos establecer, a modo de ejemplo, tablas para la suma y para el producto en el caso $n = 5$ a saber

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\bullet$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

2.4.11 Teoremas relativos a $\mathcal{Z}_n$

2.4.12 Teorema I

En el sistema $\mathcal{Z}_n$ de enteros mód lo n son válidas la suma y el producto con sus propiedades enunciadas al hablar de dominios de integridad pero no es válida la ley de simplificación para el producto.

A título de ejemplo, observemos que al ser $a(b+c) = ab + ac$ para enteros cuales quiera debe ser $a(b+c) \equiv (ab+ac) \pmod n$.
En cuanto a la ley de simplificación para el producto, si fuese válida equivaldría a asegurar la no existencia de divisores de "0" en $\mathcal{Z}_n$ con lo cual $ab = 0$ deberá implicar $a = 0$ ó $b = 0$. En $\mathcal{Z}_n$ esto se traduce diciendo

Si $ab = 0 \pmod n$ entonces $a \equiv 0 \pmod n$ ó $b \equiv 0 \pmod n$

pero esto a su vez implica que :

> Si n/ab entonces n/a ó n/b lo cual es *verdadero si* n es *primo.* Si n *no* fuera primo entonces admitirá una descomposición $n = ab$ con lo cual n/ab *sin necesidad* de que n/a ó n/b.

Por lo tanto, *no* vale la ley de simplificación para el producto.

2.4.13 Teorema II

La ley de simplificación para el producto en $\mathcal{Z}_n$ es válida si y solo sí n es primo

2.4.14 Clases Residuales

La congruencia módulo n es una relación de equivalencia tal como hemos visto y, en consecuencia, produce en Z una partición en n clases de equivalencia, a saber

$$[0] = \{..., -2n, -n, 0, n, 2n, ...\} = \{0 + nx : x \in itZ\}$$

$$[1] = \{..., -2n + 1, -n + 1, 1, n + 1, 2n + 1, ...\} = \{1 + nx : x \in Z\}$$

$$\cdots$$

$$[n - 1] = \{..., -n - 1, -1, n - 1, 2n - 1, 3n - 1, ...\} = \{(n - 1) + nx : x \in Z\}$$

Esencialmente, estamos reemplazando la congruencia por la igualdad, es decir, que todos los enteros que dan el mismo resto al dividirlos por n pueden agruparse. Cada uno de estos grupos se llama clase residual
Por ejemplo, para $n = 5$ hay cinco clases residuales correspondientes a los posibles restos : $0, 1, 2, 3, 4$. Algunos de éstos son

$$[1] = \{\cdots, -14, -9, -4, 1, 6, 11, 16, \cdots\}$$

$$[2] = \{\cdots, -13, -8, -3, 2, 7, 12, 17, \cdots\}$$

Para cada módulo n, la clase residual r_n dada por un resto r con $0 \leq r < n$ está formada por todos los enteros a que dan el mismo resto r en su división por n.
Cada entero pertenece a una y sólo una clase residual y dos enteros pertenecientes a una misma clase son congruentes entre sí $\pmod n$.
Hay n clases residuales módulo n.
Supongamos que dos restos r y s en $\mathcal{Z}_n$ dan un resto t, es decir, $r + s \equiv t \pmod n$ el mismo resultado lo obtendríamos de la siguiente manera

Si $a \in r_n$ y $b \in s_n$ entonces $(a + b) \in t_n$ pues si $a \equiv r \pmod n$ y si $b \equiv s \pmod n$ entonces $a + b \equiv r + s \pmod n$.

Si $a \in a_n$ y $b \in b_n$ entonces :

$$\begin{aligned} (a + b) &= a_n + b_n \\ (ab)n &= a_n \cdot b_n \end{aligned}$$

Por ejemplo, $6 \in 1_5$ y $-13 \in 2_5$ proporcionan $6 + (-13) = -7 \in 3_5$.

2.4.15 Teorema III

$\mathcal{Z}_n$ es un campo si y sólo sí n es primo
Sea n primo y supongamos que $0 < a < n$. Entonces, $(a, n) = 1$ con lo cual existenenteros s, t tales que $as + tn = 1$.
Así, $as \equiv 1$ $(mod\ n)$ ó $[a][s] = [1]$ y $[a]$ es la unidad de $\mathcal{Z}_n$ y así es un campo.
Recíprocamente, si n <u>no</u> es primo entonces $n = n_1 n_2$ con $1 < n_1, n_2 < n$. Luego, $[n_1] \neq [0]$ y $[n_2] \neq [0]$ mientras que $[n_1[n_2 = [n_1 n_2] = [0]$ y $\mathcal{Z}_n$ no es un dominio entero, por lo tanto, <u>no</u> puede ser un campo.

2.4.16 Teorema IV

En $\mathcal{Z}_n$, es $[a]$ una unidad si y sólo sí $(a, n) = 1$

Demostración

Si $(a, n) = 1$ entonces por el Teorema anterior obtenemos el resultado. Recíprocamente, sea $[a] \in \mathcal{Z}_n$ y sea $[a]^{-1} = [s]$. Entonces, $[as] = [a][s] = [1]$ lo cual implica que $as \equiv\ (mod\ n)$, es decir, $as = 1 + tn$ con $t \in \mathcal{Z}$ pero, $1 = as + n(-t)$ con lo cual es $(a, n) = 1$.

2.4.17 Ejemplo

Hallar en $\mathcal{Z}_{72}$ el valor de $[25]^{-1}$

Dado que $(25, 72) = 1$ el Algoritmo de Euclides proporciona

$$\begin{array}{rcrl} 72 & = & 2(25) + 22 & 0 < 22 < 25 \\ 25 & = & 1(22) + 3 & 0 < 3 < 22 \\ 22 & = & 7(3) + 1 & 0 < 1 < 3 \end{array}$$

Luego,

$$\begin{array}{rcc} 1 = 22 - 7(3) & = & 22 - 7(25 - 22) = (-7)(25) + 8(22) \\ (-7)(25) + 8[72 - 2(25)] & = & 8(72) - 23(25) \end{array}$$

lo cual implica que

$$1 \equiv (-23)(25)(mod\ 72) = (-23 + 72)(25)(mod\ 72)$$

entonces, es

$$[1] = [49][25]$$

y así, es $[25]^{-1} = [49]$ en $\mathcal{Z}_{72}$. De este modo, es $[25]$ la unidad en $\ddagger_{72}$.
Pero, hay alguna manera de saber cuántas unidades tiene $\mathcal{Z}_{72}$?.

Según el Teorema anterior, si $1 \leq a < 72$ entonces existe $[a]^{-1}$ si y sólo sí $(a, 72) = 1$. En consecuencia, el número de unidades en $\mathcal{Z}_{72}$ es el número de enteros a con $1 \leq a < 72$ y $(a, 72) = 1$.
Luego,

$$\Phi(72) = \Phi(2^3 3^2) = (72)[1 - \frac{1}{2}][1 - \frac{1}{3} = 72.\frac{1}{2}\frac{2}{3} = 24$$

En general, para cualquier $n \in \mathcal{Z}^+$ con $n > 1$ hay $\Phi(n)$ unidades y $n - 1 - \Phi(n)$ divisores propios de cero en $\mathcal{Z}_n^+$.

Observación

2.4.18 Ejercicios

Ejercicio 1

Si $x \in 4_8$ e $y \in 4_8$ determinar el conjunto de sumas $x + y$ y de productos $x \cdot y$.

Ejercicio 2

Calcular en $\mathcal{Z}_7$ los siguientes productos

a) $(3 \cdot 4) \cdot 5$

b) $3 \cdot (4 \cdot 5)$

c) $3 \cdot (4 + 5)$

d) $3 \cdot 4 + 3 \cdot 5$

2.5 Sistemas de numeración

Por cierto que $327 = 3(10)^2 + 2(10) + 7$.
En general, para un número natural k, el último dígito r (última cifra en su expresión decimal) es el resto obtenido cuando k se divide por 10, con lo cual $k = 10q + r$ con $0 \leq r < q$.

a) Si $q = 0$ entonces $k = r$.

b) Si $q > 0$ entonces k tendrá como expresión una sucesión de dígitos que representen al entero q seguidos del dígito r.

Por otra parte, es claro que todo entero positivo k puede expresarse unívocamente como

$$k = 10^t r_t + 10^{t-1} r_{t-1} + \cdots + 10^2 r_2 + 10 r_1 + r_0$$

donde todos los restos $r_0, r_1, \ldots, r_t$ están comprendidos entre 0 y 9. De esta manera, la expresión decimal para k es la sucesión de cifras

$$r_t r_{t-1} \cdots r_1 r_0$$

Esto permite sospechar que el estudio de congruencias permitirá que cualquier entero $n > 1$ podrá proporcionar una base de numeración puesto que, por ejemplo, los primos enteros son

Decimal	*Base dos*
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000
9	1001

En realidad, obtenemos dos sistemas de números enteros equivalentes pues, por ejemplo, al paralelismo entre la notación decimal y la diádica es una correspondencia biunívoca entre $\mathcal{Z}_{10}$ y $\mathcal{Z}_2$. La suma de dos enteros decimales y de dos enteros diádicos correspondientes dan resultados que se corresponden con esta coordinación. En efecto, $2 + 5 = 7 \leftrightarrow 10 + 101 = 111$. A esta correspondencia se la denomina isomorfismo

2.5.1 Isomorfismo

definición

Dados dos dominios de de integridad D y D' un *isomorfismo* entre D y D' es una correspondencia biunívoca entre sus elementos a, b en D las siguientes condiciones

$$\begin{aligned} (a+b)' &= a' + b' \\ (a \cdot b)' &= a' \cdot b' \end{aligned}$$

2.5.2 Ejemplos

a) En cualquier dominio de integridad la identidad es un isomorfismo.

b) Recordemos el conjunto de números de la forma $a+b\sqrt{3}$ con a y b en un dominio de integridad. Este conjunto es isomorfo consigo mismo de modo no trivial : $a+b\sqrt{3} \quad \leftrightarrow \quad a-b\sqrt{3}$.

Esta correspondencia es un *isomorfismo* ya que, $\forall \quad a = m+n\sqrt{3}$ y $b = m_1+n_1\sqrt{3}$ tenemos

$$\begin{array}{rcl} a+b & = & (m+m_1)+(n+m_1)\sqrt{3} \\ (a+b)' & = & (m+m_1)-(n+n_1)\sqrt{3} \\ a'+b' & = & (m-n\sqrt{3})+(m_1-n_1\sqrt{3}) \\ & = & (m+m_1)-(n+n_1)\sqrt{3} \end{array}$$

Además,

$$\begin{array}{rcl} ab & = & (mm_1+3nn_1)+(mn_1+nm_1)\sqrt{3} \\ (ab)' & = & (mm_1+3nn_1)-(mn_1+nm_1)\sqrt{3} \\ a'\cdot b' & = & (m-n\sqrt{3})\cdot(m_1-n_1\sqrt{3}) \\ & = & (mm_1+3nn_1)-(mn_1+nm_1)\sqrt{3} \end{array}$$

Por lo tanto,

$$\begin{array}{rcl} (a+b)' & = & a'+b' \\ (a\cdot b)' & = & a'\cdot b' \end{array}$$

Por cierto, que un isomorfismo conserva diferencias, obviamente. Por definición, $a-b$ es la solución de la ecuación $a = b+x$ con lo cual $b+(a-b) = a$, por lo tanto, $a' = b'+(a-b)'$ es decir, que $(a-b)'$ es la única solución de la ecuación $b' = x+a'$, es decir, que $(a-b)' = a'-b'$.
Obviamente, $0' = 0$ y $1' = 1$.

2.5.3 Ejercicios

Ejercicio 1

Efectuar, en el sistema dádico las siguientes operaciones

$$101+1011 \quad ; \quad (111)(101) \quad ; \quad 11(1100+110)$$

Ejercicio 2

a) ¿Es válida en base 7 la igualdad $101^2 = 10201$?

b) ¿En qué base lo es?

c) Lo mismo para $(101)(102) = 10302$

Ejercicio 3

a) Los cinco primeros múltiplos 18, 27, 36, 45 y 54 de 9 son tales que $2/(18 + 27 + 36 + 45 + 54)$

b) ¿Es cierto en general? En caso afirmativo probarlo y, en caso negativo, dar un contra-ejemplo.

Ejercicio 4

a) Dar una regla para calcular raíz cuadrada en cualquier sistema de numeración.

b) Ilustrar calculando la parte entera de $\sqrt{20000}$ en base 7, es decir, $\sqrt{4802}$ en base decimal.

Ejercicio 5

Un tendero tiene *sólo* cinco pesas de 1, 3, 9, 27 y 81 libras. Puede colocar las pesas en ambos platillos de la balanza. ¿Cómo pesará hasta 121 libras?.

Una última curiosidad

2.5.4 Teorema de Fermat (1640)

Si a es entero y p es primo entonces $a^p \equiv a(mod\ p)$.

Demostración

Obviamente, si $a \equiv 0 \pmod{p}$, es decir, p/a ó sea a es múltiplo de p entonces también es $a^p \equiv 0 \pmod{p}$
Supongamos, entonces, que a *no* es múltiplo de p, es decir, que $a \not\equiv 0 \pmod{p}$.
A partir de los restos de dividir por p, es decir, 0, 1, 2, ..., $(p-1)$ consideremos los números: $0, a, 2a, \ldots, (p-1)a \pmod{p}$.
Por cierto estos p números son distintos puesto que sabemos que

"Si $ax \equiv by(mod\ p)$ y si $a \equiv b(mod\ p)$ y si $(a,\ p) = 1$ entonces $x \equiv y(mod\ p$"

Como

$$\begin{array}{ccc} 0\ mod\ p & = & 0 - p\lfloor \frac{0}{p} \rfloor = 0 \\ a\ mod\ p & = & a - p\lfloor \frac{a}{p} \rfloor \\ 2a\ mod\ p & = & 2a - p\lfloor \frac{2a}{p} \rfloor \\ & \cdots & \\ (p-1)\ mod\ p & = & (p-1)a - p\lfloor \frac{(p-1)a}{p} \rfloor \end{array}$$

Estos p números: $0, a, 2a, \ldots, (p-1)a$ son distintos, no negativos y menores que p (son restos de dividir por p) entonces el primero de estos números es *cero* y los restantes son los enteros $1, 2, ..., (p-1)$ en algún orden, es decir, resultan ser los enteros $0, 1, 2, \ldots, p-1$, por lo tanto,

$$a(2a)\ldots((p-1)a) \equiv 1 \cdot 2 \cdot \ldots (p-1) \pmod{p}$$

luego

$$a^p(1 \cdot 2 \cdot \ldots (p-1)) \equiv a(1 \cdot 2 \cdot \ldots (p-1)) \pmod{p}$$

donde cada uno de los factores $1, 2, \ldots, (p-1)$ es primo con p.

2.6 Información Complementaria

2.6.1 Principio de inclusión y exclusión

Consideremos un conjunto S con $Card(S) = n$ y condiciones C_i con $i = 1, 2, ...m$ que cumplen algunos elementos de S. El número de elementos de S que no satisface ninguna de la condiciones C_i está dado por

$$\begin{array}{ccc} \overline{N} & = & N - \sum_{i=1}^{m} N_{i=1} N(C_i) + \\ + & & \sum_{1 \leq i < j \leq m} N(C_i C_j) - \\ - & & \sum_{1 \leq i < j < k \leq m} N(C_i C_j C_k) + \\ \cdots & & (-1)^m N(C_1 C_2, ..., C_m) \end{array}$$

Podemos probar este resultado por inducción en m pero emplearemos un argumento combinatorio.
Veamos que para cada $x \in S$ tal x contribuye igual cero o con uno en cada miembro de esta relación. En efecto, si x no cumple ninguna condición entonces x se cuenta una vez en $\overline{N}$ y otra en N pero en ningún otro término, en consecuencia, x aporta uno a cada sumando de la relación anterior.
La otra posibilidad es que x satisfaga r de las m condiciones C_i. En este caso x no aportará nada a $\overline{N}$ pero se encuentra en el miembro derecho de la relación anterior

a) se encuentra una vez en N

b) se encuentra r veces en $\sum_{i=1}^{m} N(C_i)$

c) se encuentra $\binom{r}{2}$ en $\sum_{1\leq i<j\leq m} N(C_i C_j)$

d) se encuentra $\binom{r}{3}$ en $\sum_{1\leq i<j<k\leq m} N(C_i C_j C_k)$

e) se encuentra $\binom{r}{r}$ en $\sum N(C_1 ... C_m)$

donde la sumatoria se toma sobre todas las selecciones de tamaño r de la m condiciones.
Luego, según el teorema del Binomio, x se cuenta

$$(1+(-1))^r = \sum_{j=0}^{r} \binom{r}{j} = 0$$

veces.
Establecemos, ahora, la siguiente notación

$$S_m = \sum N(C_{i_1}, ..., C_{i_k}) \quad 1 \leq k \leq m$$

donde la sumatoia se toma sobre todas las selecciones de tamaño k de la lista de m condiciones. Por lo tanto, S_k tiene $\binom{m}{k}$ sumandos.

2.6.2 Ejemplo I

Veamos cómo emplear el principio de inclusión y de exclusión en un problema de enumeración, a saber

Determinar el número de enteros positivos n con $1 \leq n \leq 100$ y n no es divisible ni por 2, ni por 3, ni por 5.
Aquí, $S = \{1, 2, ..., 100\}$ y $N = 100$.
Para cada $n \in S$ se verifica

a) la condición C_1 si n es divisible por 2

b) la condición C_2 si n es divisible por 3

c) la condición C_3 si n es divisible por 5

La respuesta a este problema es $N(\overline{C_1}, \overline{C_2}, \overline{C_3})$.

Para $r \in R$ denotamos por $\lfloor r \rfloor$ a

$$\lfloor r \rfloor = \begin{cases} r & \text{si } r \text{ es entero} \\ \textit{el mayor entero menor que } r \textit{ no entero} & \end{cases}$$

En nuestro problema tenemos

$$\begin{array}{rcl} N(C_1) & = & \lfloor 50 \rfloor \\ N(C_2) & = & \lfloor \frac{100}{3} \rfloor \\ N(C_3) & = & \lfloor \frac{100}{5} \rfloor \\ N(C_1 C_2) & = & \lfloor \frac{100}{6} \rfloor = 16 \\ N(C_1 C_3) & = & \lfloor \frac{100}{10} \rfloor = 10 \\ N(C_2 C_3) & = & \lfloor \frac{100}{15} \rfloor = 6 \\ N(C_1 C_2 C_3) & = & \lfloor \frac{100}{30} \rfloor = 3 \end{array}$$

Por lo tanto, según el principio de inclusión y de exclusión, obtenemos

$$N(\overline{C_1}, \overline{C_2}, \overline{C_3}) = 100 - (50 + 33 + 20) + (16 + 10 + 6) - 3 = 26$$

Es decir, los primeros 26 números primos.

2.6.3 Ejemplo II

Para $n \in Z^+$ sea $\Phi(n)$ el número de enteros positivos m con $1 \leq m < n$ y $(m, n) = 1$. Esta función, importante en el Algebra abstracta, llamada función Φ de Euler proporciona, a título de ejemplo

$$\begin{array}{rcl} \Phi(2) & = & 1 \\ \Phi(3) & = & 2 \\ \Phi(4) & = & 2 \\ & \cdots & \\ \Phi(p) & = & p-1 \end{array}$$

Queremos deducir una fórmula para $\Phi(n)$ que esté relacionada con n de modo tal que no sea necesario hacer comparaciones en cada caso con m y $1 \leq m < n$. Sea $n \geq 2$. Escribamos

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_t^{\alpha_t}$$

con $p_1, ..., p_t$ números primos distintos y $\alpha_1, ..., \alpha_t \geq 1$.
Por ejemplo, tomemos, para fijar ideas $t = 4$. Con $C = \{1, 2, ..., n\}$ y $Card(C) = n$ para cada $i = 1, 2, 3, 4$ decimos que

$k \in C$ satisface la condición C_i si p_i / k

Para $1 \leq k < n$ con $(k, n) = 1$ si p_i no divide a k con $i = 1, 2, 3, 4$ resulta

$$\Phi(n) = N(\overline{C_1 C_2}, \overline{C_3}, \overline{C_4})$$

a) Para $i = 1, 2, 3, 4$ es $N(C_i) = n/p_i$

b) Para $1 \leq i < j \leq 4$ es $(C_i C_j) = n/(p_i p_j)$

c) Para $1 \leq i < j < k \leq 4$ es $N(C_i C_j C_k) = n/(p_i p_j p_k)$
y es

d) $N(C_1 C_2 C_3 C_4) = n/(p_1 p_2 p_3 p_4)$

Luego,

$$\begin{array}{rcc} \Phi(n) & = & C_0 - C_1 + C_2 - C_3 + C_4 \\ & = & n - [\frac{n}{p_1} + ... + \frac{n}{p_4}] + [\frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + ... + \frac{n}{p_3 p_4}] \\ & - & [\frac{n}{p_1 p_2 p_3} + ... + \frac{n}{p_2 p_3 p_4}] + \frac{n}{p_1 p_2 p_3 p_4} \end{array}$$

Operando, obtenemos

$$\Phi(n) = \frac{n}{p_1 p_2 p_3 p_4}[(p_1 - 1)(p_2 - 1)(p_3 - 1)(p_4 - 1)] = n \prod_{i=1}^{4}(1 - \frac{1}{p_i})$$

En general, es $\Phi(n) = n \prod_{p/n}(1 - \frac{1}{p})$ donde la productoria se toma sobre todos los primos p que dividen a n

2.6.4 Ejercicios

Ejercicio 1

Determinar el número de enteros positivos n $1 \leq n \leq 2000$ tales que

a) No son divisibles por $2, 3$ ó 5

b) No son divisibles por $2, 3, 5$ ó 7

c) No son divisibles por $2, 3,$ ó 5 y por 7

Ejercicio 2

Hallar los números reales x tales que

a) $7\lfloor x \rfloor = \lfloor 7x \rfloor$

b) $\lfloor 7x \rfloor = 7$

c) $\lfloor x + 7 \rfloor = x + 7$

d) $\lfloor x + 7 \rfloor = lfloorx \rfloor + 7$

Ejercicio 3

Calcular $\Phi(n)$ cuando $n = 51, 420, 12300$

Ejercicio 5

Para $n \in Z^+$ determinar

a) $\Phi(2^n)$

b) $\Phi(2^n p)$ con p primo impar.

Capítulo 3

Generadoras y Representaciones Asintóticas

3.1 Funciones Generadoras

3.1.1 Definición

En muchas oportunidades, numéricamente hablando, es necesario obtener información acerca de una sucesión de números reales $\{a_n\}n \geq 0$. En estos casos, suele obtenerse tal información por medio de una función G, la cual se llama generadora para la sucesión $a_0, a_1, a_2, \ldots, a_n, \ldots$ y que está dada por la serie de potencias

$$G(z) = \sum_{n \geq 0} a_n z^n$$

donde z es un parámetro, generalmente, real.

3.1.2 Operaciones

Combinaciones Lineales

Si G_1 es la función generadora para la sucesión $a_0, a_1, \ldots, a_n, \ldots$ y si G_2 es la función generadora para la sucesión $b_0, b_1, \ldots, b_n, \ldots$ entonces $\alpha G_1(z) + \beta G_2(z)$ es la función generadora para la sucesión $[\alpha a_n + \beta b_n]_{n \geq 0}$.
Formalmente, escribimos

$$\begin{aligned} \alpha G_1(z) + \beta G_2(z) &= \alpha \textstyle\sum_{k \geq 0} a_k z^k + \beta \sum_{k \geq 0} b_k z^k \\ &= \textstyle\sum_{k \geq 0} [\alpha a_k + \beta b_k] z^k \end{aligned}$$

Producto por potencias de z

Si $G(z)$ es la función generadora para la sucesión $\{a_n]\}_{n\geq 0}$ entonces $z^n G(z)z$ es la función generadora para la sucesión $0,\ldots,0,a_1,a_2,\ldots$.
Formalmente, escribimos

$$z^n \sum_{k\geq 0} a_k z^k = \sum_{k\geq 0} a_{k-n} z^k$$

simplemente llamando $n+k=k$.

Producto por potencias negativas de z

Análogamente, si $[GZ) - a_0 - a_1 z - \cdots - a_{n-1} z^{n-1}]z^{-n}$ es la función generadora para la sucesión $a_n, a_{n+1}, \ldots$ entonces, lo escribimos

$$z^{-n} \sum_{k\geq 0} a_k z^k = \sum_{k\geq 0} a_{k+n} z^k$$

simplemente llamando $k-n=k$.

Ejemplos

a) Si $G(z)$ es la función generadora para la sucesión constante $1,1,1,\ldots,1,\ldots$ entonces $zG(z)$ genera la sucesión $0,1,1,\ldots$ con lo cual $(1-z)G(z) = 1$. Esto proporciona una fórmula importante, como es la de la suma de una serie geométrica de razón z con $|z|<1$, a saber

$$\frac{1}{1-z} = \sum_{k\geq 0} z^k \quad \text{si } |z|<1$$

b) La sucesión de Fibonacci $0,1,1,2,3,5,8,13,\ldots$ está definida, como hemos visto, por

$$F_0 = 0; F_1 = 1; F_{n+2} = F_{n+1} + F_n \quad \forall\, n \geq 0$$

Para tal sucesión consideremos la función generadora

$$G(z) = \sum_{n\geq 0} F_n z^n$$

a partir de la cual, formalmente, escribimos

$$zG(z) = \sum_{n\geq 0} F_n z^{n+1}$$

$$z^2 G(z) = \sum_{n\geq 0} F_n z^{n+2}$$

de modo que

$$\begin{array}{rl}(1-z-z^2)G(z) & = \sum_{m=0}^{\infty} F_m z^m - \sum_{m=1}^{\infty} F_{m-1} z^m - \sum_{m=2}^{\infty} F_{m-2} z^m \\ & = F_0 + F_1 z + \sum_{m=2}^{\infty} F_m z^m - F_0 z - \\ & \quad - \sum_{m=2}^{\infty} F_{m-1} z^m - \sum_{m=2}^{\infty} F_{m-2} z^m \\ & F_0 + (F_1 - F_0) z + \sum_{m=2}^{\infty} [F_m - F_{m-1} - F_{m-2}] z^m \\ & 0 + z + \sum_{m=2}^{\infty} F_{m-2} [F_m - (F_{m-1} + F_{m-2})] z^m \\ & = z\end{array}$$

puesto que por definición la sucesión de Fibonacci verifica $F_m = F_{m-1} + F_{m-2} \ \forall\, m \geq 2$.
Esto nos permite escribir, formalmente

$$G(z) = \frac{z}{1-z-z^2} = \frac{-z}{z^2+z-1}$$

Como el denominador es una ecuación cuadrática en z con raíces $z_{1,2} = (1/2)(-1\underline{+}\sqrt{5})$ podemos, utilizando fracciones simples, escribir

$$\begin{array}{rl}\frac{-z}{z^2+z-1} & = \frac{A}{z+\tilde{\phi}} + \frac{B}{z+\phi} \\ & = \frac{A(z+\phi)+B(z+\tilde{\phi})}{(z+\tilde{\phi})(z+\phi)} \\ & = \frac{(A+B)z+A\phi+B\tilde{\phi}}{(z+\tilde{\phi})(z+\phi)}\end{array}$$

donde $\begin{array}{rl}\phi & = (1+\sqrt{5})/2 \\ \tilde{\phi} & = 1-\phi = (1-\sqrt{5})/2\end{array}$ que proporciona el siguiente sistema de ecuaciones

$$\left\{\begin{array}{l} A+B=-1 \\ A\phi + B\tilde{\phi} = 0 \end{array}\right.$$

Con soluciones $A = \tilde{\phi}/\sqrt{5}$ y $B = \phi/\sqrt{5}$.
Por lo tanto, la función generadora $G(z)$ se expresa por

$$\begin{array}{rl}G(z) & = (\tilde{\phi}/\sqrt{5})\frac{1}{z+\tilde{\phi}} - (\phi/\sqrt{5})\frac{1}{z+\phi} = \\ & = \frac{1}{5}[\frac{1}{1+z\tilde{\phi}^{-1}} - \frac{1}{1+z\phi^{-1}}] = \\ & = \frac{1}{5}[\frac{1}{1-z\phi} - \frac{1}{1-z\tilde{\phi}}]\end{array}$$

teniendo en cuenta que $\tilde{\phi}^{-1} = -\phi$ y que $\phi^{-1} = -\tilde{\phi}$ como es fácil verificar. De este modo, a condición de ser $|\phi z| < 1$ y $|\tilde{\phi} z| < 1$ la función generadora $G(z)$ se expresa como diferencias de dos series geométricas, a saber

$$G(z) = \frac{1}{5}\sum_{k=0}^{\infty} (\phi z)^k - \frac{1}{5}\sum_{k=0}^{\infty} (\tilde{\phi} z)^k$$

Es claro que el coeficiente z debe coincidir con F_n, con lo cual está dado por

$$F_n = \frac{1}{5}[\phi^n - \tilde{\phi}^n]$$

Ahora bien, como $\tilde{\phi} \cong -0.61803\cdots$ con valor absoluto inferior a uno resulta que $\lim_{n\to\infty} \tilde{\phi}^n = 0$ y que $F_n \cong \phi^n/\sqrt{5}$ para n suficientemente grande.
También, a partir de la expresión $G(z)$, resulta por simple cálculo

$$\begin{aligned} G(z)^2 &= \tfrac{1}{5}[\tfrac{1}{(1-\phi z)^2} + \tfrac{1}{(1-\tilde{\phi} z)^2} - \tfrac{2}{(1-\phi z)-(1-\tilde{\phi} z)}] \\ &= \tfrac{1}{5}[\tfrac{1}{(1-\phi z)^2} + \tfrac{1}{(1-\tilde{\phi} z)^2} - \tfrac{2}{1-\underbrace{(\phi+\tilde{\phi})}_{1} z + \underbrace{\phi\tilde{\phi}}_{-1}\; z^2}] \\ &= \tfrac{1}{5}[\tfrac{1}{(1-\phi z)^2} + \tfrac{1}{(1-\tilde{\phi} z)^2} - \tfrac{2}{1-z-z^2}] \end{aligned}$$

con lo cual el coeficiente de z^n, en esta expresión, está dado por

$$\begin{aligned} \textstyle\sum_{k=0}^{n} F_k F_{n-k} &= \tfrac{1}{5}(n+1)(F_n + 2F_{n-1}) - 2F_{n+1} \\ &= \tfrac{n-1}{5} F_n + \tfrac{2n}{5} F_{n-1} \end{aligned}$$

y el lector debe verificar que:

$$\begin{aligned} \forall \;\; n \text{ entero es} \quad \phi^n &= F_n \phi + F_{n-1} \\ y \quad \tilde{\phi}^n &= F_n \tilde{\phi} + F_{n-1} \end{aligned}$$

Producto de Cauchy

Si $G_1(z)$ es la función generadora para la sucesión $a_0, a_1, \ldots, a_n, \ldots$ y $G_2(z)$ es la función generadora para la sucesión $b_0, b_1, \ldots, b_n, \ldots$ entonces el producto formal $G_1(z)G_2(z)$ es la función generadora de la sucesión $s_0, s_1, \ldots, s_n, \ldots$ donde los elementos S_n están dados por el producto de Cauchy, es decir,

$$s_n = \sum_{k=0}^{n} a_k b_{n-k}$$

También si $b_n \equiv 1 \;\; \forall \; n$ puede verificarse

$$\frac{1}{1-z} G(z) = a_0 + (a_0 + a_1)z + (a_0 + a_1 + a_2)z + \cdots$$

Conviene aclarar que, en este punto, si multiplicáramos formalmente tres funciones generadoras de la sucesión $s_0, s_1, \ldots$ el término general s_n estará dado por

$$s_n = \sum_{\substack{i,j,k>0 \\ i+j+k=n}} a_i b_j c_k$$

La regla general para el producto de cualquier número de funciones generadoras, siempre y cuando esto sea posible, es

$$\prod_{j\geq 0} (\sum_{k\geq 0} a_{jk} z^k) = \sum_{n\geq 0} z^n (\sum_{\substack{k_0, k_1, \ldots \geq 0 \\ k_0+k_1+\cdots=n}} a_{0_{k_0}} a_{1_{k_1}} \cdots$$

Relaciones de congruencias y raíces n-ésimas de la unidad

Es claro qye $G_{(cz)}$ es la función generadora para la sucesión $a_0, ca_1, c^2a_2, \ldots$.
En particular, la función $G(z) = (1 - cz)^{-1}$ es generadora de la sucesión $1, c, c^2, c^3, \ldots$
Un tratamiento es el siguiente

$$\begin{aligned} \tfrac{1}{2}[G(z) + G_{(-z)}] &= \textstyle\sum_{k=0}^{\infty} a_{2k} z^{2k} \\ \tfrac{1}{2}[G(z) - G_{(-z)}] &= \textstyle\sum_{k=0}^{\infty} a_{2k+1} z^{2k+1} \end{aligned}$$

Recordemos el tema de raíces mésimas de la unidad.
Consideramos $w = e^{2\pi k/m}$ $k = 0, 1, \ldots, m-1$.
Entonces

$$\sum_{s \equiv k \pmod{m}} a_s z^s = \frac{1}{m} \sum_{j=0}^{m-1} w^{-jk} G_{(w^j z)}$$

con $k = 0, 1, \ldots, m-1$.
Por ejemplo, si $m = 3$ y $k = 1$ obtenemos

$$w = \cos \frac{2}{3}\pi + i \sin \frac{2}{3}\pi$$

y así

$$a_1 z + a_4 z^4 + a_7 z^7 + \cdots = \frac{1}{3}[G(z) + w^{-1} G_{(wz)} + w^{-2} G_{(w^2 z)}]$$

Derivación e Integración término a término

Si $G(z) = \sum_{k=0}^{\infty} a_k z^k$ entonces, formalmente, escribimos

$$\begin{aligned} D[G(z)] &= \textstyle\sum_{k=1}^{\infty} k a_k z^{k-1} \\ &= \textstyle\sum_{k=0}^{\infty} (k+1) a_{k+1} z^k \end{aligned}$$

con lo cual la función generadora de la sucesión $\{na_n\}$ es $zD[G(z)]$ y si, bajo ciertas condiciones de convergencia, pudiésemos integrar término a término, es decir

$$\begin{aligned} \textstyle\int_0^z G(t)dt &= \textstyle\int_0^z \sum_{k=0}^{\infty} a_k t^k dt = \sum_{k=0}^{\infty} a_k \int_0^z t^k dt \\ &= \textstyle\sum_{k=0}^{\infty} \frac{a_k}{k+1} z^{k+1} \\ &= \textstyle\sum_{k=0}^{\infty} \frac{1}{k} a_{k-1} z^k \end{aligned}$$

En particular, si derivamos e integramos $\frac{1}{1-z}$ obtenemos

$$\begin{aligned} \tfrac{1}{(1-z)^2} &= 1 + 2z + 3z^2 + \cdots = \textstyle\sum_{k=0}^{\infty} (k+1) z^k \\ \ln \tfrac{1}{1-z} &= z + \tfrac{1}{2} z^2 + \tfrac{1}{3} z^3 + \cdots = \textstyle\sum_{k=1}^{\infty} \frac{1}{k} z^k \end{aligned}$$

Luego, obtenemos

$$\frac{1}{1-z}\ln\frac{1}{1-z} = z + \frac{3}{2}z^2 + \frac{11}{6}z^3 + \cdots = \sum_{k=1}^{\infty} H_k z^k$$

que es la función generadora para los números armónicos $H_n := 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} = \sum_{k=1}^{n}\frac{1}{k}$; $n \geq 0$ que estudiaremos más adelante.

3.1.3 Desarrollo de Series de Potencias

Siempre y cuando sea posible determinar el desarrollo en serie de potencias de una función, implícitamente, determinamos la función generadora para una sucesión particular.

Ejemplos

a) La serie binomial

$$(1+z)^r = 1 + rz + \frac{r(r-1)}{2!}z^2 + \cdots = \sum_{k=0}^{\infty}\binom{r}{k}z^k$$

b) Para valores negativos de r obtenemos, como caso particular,

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

de acuerdo con la identidad básica entre coeficientes binomiales de índice superior negativo

c) La serie exponencial

$$e^z = \sum_{k=0}^{\infty}\frac{z^k}{k!}$$

d) En general, obtenemos la siguiente expresión relacionada con los números de Stirling de segunda especie

$$(e^z-1)^n = n!\sum_{k=0}^{\infty}\left\{ \begin{matrix} k \\ n \end{matrix} \right\}\frac{z^k}{k!}$$

e) La serie logarítmica

$$\ln(1+z) = \sum_{k=1}^{\infty}\frac{(-1)^{k+1}}{k}z^k$$

se convierte en

$$-\ln(1-z) = \ln(\frac{1}{1-z}) = \sum_{k=1}^{\infty} \frac{z^k}{k}$$

por simple sustitución en la expresión anterior. También, empleando números de Stirling de primer especie, obtenemos

$$[\ln(\frac{1}{1-z})]^n = n! \sum_{k=1}^{\infty} \begin{bmatrix} k \\ n \end{bmatrix} \frac{z^k}{k!}$$

3.1.4 Ejercicios

Ejercicio 1

a) Hallar todos los valores de n para los cuales $F_n = n$

b) Hallar todos los calores de n para los cuales $F_n = n^2$

Ejercicio 2

Probar que si n *no* es primo, entonces tampoco F_n es primo con una excepción. Establecer tal excepción

Ejercicio 3

¿Puede calcularse F_{-n} a partir de F_n? Intente calcular F_{-1} y F_{-2}

Ejercicio 4

¿Cuál es la función generadora para la sucesión $2, 5, 13, 35, \ldots (2^n + 3^n)$?

Ejercicio 5

Considerar la relación

$$\frac{1}{1-z} \ln \frac{1}{1-z} = \sum_{k=1}^{\infty} H_k z^k$$

que no es más que una función generadora para la sucesión de números armónicos $\{H_n\}$.
Entonces

a) Diferenciar esta función generadora y comparar con la función generadora para $\sum_{k=1}^{n} H_k$

b) ¿Qué relación puede deducir?

Ejercicio 6

Probar, inductivamente, la expresión de $(e^z - 1)^n$ como

$$n! \sum_{k=0}^{\infty} \left\{ \begin{matrix} k \\ n \end{matrix} \right\} \frac{z^k}{k!}$$

Ejercicio 7

a) Encontrar la función generadora para

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

b) Diferenciar tal función generadora y expresar los coeficientes en términos de números armónicos

3.2 Números armónicos

3.2.1 Propiedades

Comparación entre números armónicos

Consideremos $m > 0$ y para este m el número armónico H_{2^m} y el $H_{2^{m+1}}$.
Es claro que

$$H_{2^{m+1}} = H_{2^m} + \frac{1}{2^m+1} + \frac{1}{2^m+2} + \cdots + \frac{1}{2^{m+1}}$$

donde aparecen 2^m factores
Por otra parte

$$\begin{array}{lcl} H_{2^{m+1}} & > & H_{2^m} + \frac{1}{2^m+1} + \cdots + \frac{1}{2^{m+1}} \\ H_{2^{m+1}} & > & H_{2^m} + \frac{2^m}{2^{m+1}} \\ H_{2^{m+1}} & > & H_{2^m} + \frac{1}{2} \end{array}$$

es decir, que cada vez que incrementemos m en uno el miembro derecho aumenta según $1/2$

Estimación y constante de Euler

Existe una estimación bien conocida del tamaño aproximado de H_n dada por la siguiente expresión

$$H_n = \ln n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} - \varepsilon$$

donde $0 < \varepsilon < \frac{1}{252n^6}$ y $\gamma = 0.5772156649\ldots$ es la constante de Euler.
En realidad, el comportamiento de H_n es logarítmico

3.2.2 Relaciones útiles entre números armónicos

Es válida la siguiente relación

$$\sum_{k=1}^{n} H_k = (n+1)H_n - n$$

En efecto

$$\sum_{k=1}^{n} H_k = \sum_{k=1}^{n}\sum_{j=1}^{k} \frac{1}{j} = \sum_{j=1}^{n}\sum_{k=j}^{n} \frac{1}{j} = \sum_{j=1}^{n} \frac{n+1-j}{j}$$

Esta fórmula es un caso particular de

$$\sum_{k=1}^{n} \binom{k}{m} H_k$$

El truco reside en sumar por partes que es una técnica muy útil para determinar $\sum_k a_k b_k$ cuando las cantidades $\sum a_k$ y $(b_{k+1} - b_k)$ tienen expresiones simples como veremos en un próximo ejercicio.
Observemos que

$$\binom{k}{m} = \binom{k+1}{m+1} - \binom{k}{m+1}$$

que es de fácil verificación y, por lo tanto,

$$\binom{k}{m} H_k = \binom{k+1}{m+1} \underbrace{(H_{k+1} - \frac{1}{k+1})}_{H_k} - \binom{k}{m+1} H_k$$

y así

$$
\begin{aligned}
\textstyle\sum_{k=1}^{n}\binom{k}{m}H_k &= [\binom{2}{m+1}H_2- \\
&-\binom{1}{m+1}H_1]+\cdots+ \\
&+[\binom{n+1}{m+1}H_{n+1}-\binom{n}{m+1}H_n]- \\
&-\textstyle\sum_{k=1}^{n}\binom{k+1}{m+1}\frac{1}{k+1} \\
\textstyle\sum_{k=1}^{n}\binom{k}{m}H_k &= \binom{n+1}{m+1}H_{n+1}-\binom{1}{m+1}H_1- \\
&-[\textstyle\sum_{k=0}^{n}\binom{k}{m}]\frac{1}{m+1}+ \\
&+\frac{1}{m+1}\binom{0}{m} \\
&= \binom{n+1}{m+1}H_{n+1}-\binom{1}{m+1}H_1- \\
&-\frac{1}{m+1}\binom{n+1}{m+1}+\frac{1}{m+1}\binom{0}{m}
\end{aligned}
$$

según la relación (a) de sumatorias de coeficientes binomiales. Por lo tanto

$$\sum_{k=1}^{n}\binom{k}{m}H_k=\binom{n+1}{m+1}(H_{n+1}-\frac{1}{m+1})$$

3.2.3 Ejercicios

Ejercicio 1

Sea $T_{m,n}=H_m+H_n-H_{mn}$ para m,n positivos. Entonces, cuando m o n crecen T_{mn} decrece.
Calcular el máximo y el mínimo de $T_{m,n}$

Ejercicio 2

¿Qué valores tienen H_0, H_1 y H_2?

Ejercicio 3

Probar que $H_n=\left[\begin{matrix} n+1 \\ 2 \end{matrix}\right]/n!$, es decir, que los números armónicos están directamente relacionados con los números de Stirling de primer especie.

Ejercicio 4

Compare la siguiente relación

$$\sum_{k=1}^{n} H_k = (n+1)H_n - n$$

con $\sum_{k=1}^{n} \ln k$ y estime la diferencia de una función de n

Ejercicio 5

Regla de sumación por partes

Probar la siguiente relación

$$\sum_{k=1}^{n} (a_{k+1} - a_k)b_k = a_n b_n - a_1 b_1 - \sum_{k=1}^{<n} a_{k+1}(b_{k+1} - b_k)$$

Ejercicio 6

Evaluar, sumando por partes

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

3.3 Números de Bernoulli

Los números de Bernoulli son números especiales que permiten deducir la aproximación general para los H_n.
En efecto, consideremos la $\int_1^n f(x)dx$ siendo $f(x)$ una función diferenciable. Por conveniencia, emplearemos la siguiente notación

$$\{x\} = x \equiv x - \lfloor x \rfloor (\text{mód } 1)$$

Consideremos la siguiente integral (a resolver por partes)

$$\begin{aligned} \textstyle\int_1^n [\{x\} - \frac{1}{2}] f(x)' dx &= (x - k - (1/2)) f(x)|_k^{k+1} - \textstyle\int_k^{k+1} f(x)dx \\ &= \tfrac{1}{2}[f(k+1) - f(k)] - \textstyle\int_k^{k+1} f(x)dx \end{aligned}$$

y sumando ambos miembros de esta igualdad en $k = 1, \ldots, n$, obtenemos

$$\int_1^n (\{x\} - \frac{1}{2}) f(x)dx = \sum_{k=1}^{<n} f(k) + \frac{1}{2}(f(n) - f(1)) + \int_1^n f(x)dx$$

es decir

$$\sum_{k=1}^{<n} f(k) = \int_1^n f(x)dx - \frac{1}{2}(f(n) - f(1)) + \int_1^n B_1(\{x\})f(x)'dx$$

siendo $B_1(\{x\}) = x - (1/2)$.
Por cierto, debemos volver a integrar por partes, pero antes, digamos que los números de Bernoulli son los coeficientes del desarrollo en serie de potencias de

$$\frac{x}{e^x - 1} = B_0 + B_1 x + \frac{B_2 x^2}{2!} + \cdots = \sum_{k=0}^{\infty} \frac{B_k x^k}{k!}$$

Estos números, introducidos por Bernoulli en 1713, se encuentran tabulados, pero algunos de sus valores son

$$B_0 = 1; B_1 = -1/2; B_2 = 1/6; B_3 = 0; B_4 = -1/30$$

Dado que

$$\frac{x}{e^x - 1} + \frac{x}{2} = \frac{x}{2}\frac{e^x + 1}{e^x - 1} = -\frac{x}{2}\frac{e^{-x} + 1}{e^{-x} - 1}$$

es una función impar, resultan

$$B_3 = B_5 = B_7 = B_9 = \ldots = 0$$

Multiplicando ambos miembros de la expresión

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}$$

por $e^x - 1$, obtenemos, igualando los coeficientes de las potencias de x, la fórmula

$$\sum_k \begin{pmatrix} n \\ k \end{pmatrix} B_k = B_m + \delta_{n1}$$

Esto es fácil de verificar y queda propuesto como ejercicio para el lector.

3.3.1 Polinomios de Bernoulli

En efecto, al realizar el producto de Cauchy de dos series de potencias cuyos coeficientes involucran coeficientes binomiales, es decir, el producto de

$$\sum_{n=0}^{\infty} \frac{a_n}{n!} z^n \quad \text{por} \quad \sum_{n=0}^{\infty} \frac{b_n}{n!} z^n$$

obtenemos la serie de potencias

$$\sum_{n=0}^{\infty} c_n z^n$$

donde los coeficientes binomiales contribuyeron a

$$c_n = \sum_k \binom{n}{k} a_k b_{n-k}$$

A partir de esto, definimos los polinomios de Bernoulli dados por

$$B_m(x) = \sum_k \binom{m}{k} B_k x^{m-k}$$

Por cierto, si $m = 1$ entonces $B_1(x) = B_0 x + B_1 = x - (1/2)$ y si $m > 1$ tenemos $B_m(1) = B_m(0) = B_m$, es decir, que $B_m(\{x\})$ no tiene discontinuidades en puntos de abscisa entera x.
La relevancia de los polinomios de Bernoulli y de los números de Bernoulli puede observarse a partir de

$$\begin{aligned} B_m(x)' = \textstyle\sum_k \binom{m}{k} (m-k) B_k x^{m-k-1} \quad &= m \textstyle\sum_k \binom{m-1}{k} B_k x^{m-k-1} \\ &= m B_{m-1}(x) \end{aligned}$$

y, por lo tanto, cuando $m \geq 1$, podemos integrar por partes, obtenemos

$$\begin{aligned} \tfrac{1}{m!} \textstyle\int_1^n B_m(\{x\}) f^{(m)}(x) dx \quad &= \tfrac{1}{(m+1)!} [B_{m+1}(1) f^{(m)}(n) - B_{m+1}(0) f^{(m)}(1)] \\ &\quad - \tfrac{1}{(m+1)!} \textstyle\int_1^n B_{m+1}(\{x\}) f^{(m+1)}(x) dx \end{aligned}$$

Esto nos permite continuar la aproximación de la expresión

$$\begin{aligned} \textstyle\sum_{1 \leq k \leq n} f(k) \quad &= \textstyle\int_1^n f(x)dx - \tfrac{1}{2}(f(n) - f(1)) + \tfrac{B_2}{2!}(f(n)' - f(1)') + \cdots \\ &\quad \cdots + \tfrac{(-1)^m}{m} B_m((f(n)^{(m-1)} - f(1)^{(m-1)})) + R_m \\ &= \textstyle\int_1^n f(x)dx + \sum_{k=1}^m \tfrac{B_k}{k!} [f(n)^{(k-1)} - f(1)^{(k-1)}] + R_m \end{aligned}$$

Es fácil verificar que, cuando m es par es

$$|B_{m(\{x\})}| \leq |B_m|$$

y que

$$|\frac{B_{m(\{x\})}}{m!}| < \frac{4}{(2\pi)^m}$$

con lo cual obtenemos una acotación para el resto R_m. A partir de ahora, apliquemos esta fórmula general de Euler a casos particulares, a saber

a) Sea $f(x) = \frac{1}{x}$
Es sabido que sus derivadas sucesivas tienen por expresión $f^{(m)}(x) = (-1)^m \frac{m!}{x^{m+1}}$.

Por lo tanto, la fórmula general de Euler nos proporciona

$$H_{n-1} = \ln n + \sum_{k=1}^{m} \frac{B_k}{k}(-1)^{k-1}[\frac{1}{n^k} - 1] + R_{mn}$$

Luego, obtenemos

$$\gamma = \lim_{n\to\infty}(H_{n-1} - \ln n) = \sum_{k=1}^{m} \frac{B_k}{k}(-1)^k + \lim_{n\to\infty} R_{mn}$$

por lo tanto

$$\lim_{n\to\infty} R_{mn} = -\int_1^\infty B_{m(\{x\})}\frac{dx}{x^{m+1}}$$

existe, lo cual asegura que la constante de Euler existe.
Reuniendo estas últimas expresiones obtenemos la aproximación general para números armónicos dada por

$$\begin{aligned} H_{n-1} &= \ln n + \gamma + \textstyle\sum_{k=1}^m \frac{(-1)^{k-1}B_k}{kn^k} + \int_n^\infty \frac{B_{m(\{x\})}\,dx}{x^{m+1}} \\ &= \ln n + \gamma + \textstyle\sum_{k=1}^m \frac{(-1)^{k-1}B_k}{kn^k} + \mathcal{O}(\frac{1}{n^m}) \end{aligned}$$

donde $\mathcal{O}(\frac{1}{n^m})$ es una *cota* que obtendremos más adelante.

b) En particular, agregando $\frac{1}{n}$ en ambos miebros de esta igualdad, obtenemos

$$H_n = \ln n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} - \epsilon$$

con

$$0 < \epsilon < \frac{B_k}{6n^6} = \frac{1}{252n^6}$$

c) Sea, ahora, $f(x) = \ln x$.
Aplicando la fórmula general de Euler, obtenemos

$$\begin{aligned} \ln(n-1)! &= n\ln n - n + 1 - \tfrac{1}{2}\ln n + \\ &+ \textstyle\sum_{1<k\le m} \frac{B_k(-1)^k}{k(k-1)}(\frac{1}{n^{k-1}} - 1) + R_{mn} \end{aligned}$$

Al igual que antes

$$\begin{aligned} \lim_{n\to\infty}[\ln n! - n\ln n + n - \tfrac{1}{2}\ln n] &= 1 + \textstyle\sum_{1<k\le m} \frac{B_k(-1)^{k+1}}{k(k-1)} + \\ &+ \lim_{n\to\infty} R_{mn} \end{aligned}$$

existe.
A tal límite se lo denomina *constante de Stirling* σ. En general, obtenemos

$$\begin{aligned} \ln n! &= (n+\tfrac{1}{2})\ln n - n + \sigma + \textstyle\sum_{1<k\le m} \frac{B_k(-1)^{k+1}}{k(k-1)n^{k-1}} + \\ &+ \mathcal{O}(\frac{1}{n^m}) \end{aligned}$$

En particular, si $m = 5$, obtenemos

$$\ln n! = (n + \frac{1}{2}) \ln n - n + \sigma + \frac{1}{12n} - \frac{1}{360n^3} + \mathcal{O}(\frac{1}{n^5})$$

es decir,

$$n! = e^{\sigma} \sqrt{n} (\frac{n}{e})^n \exp \left[\frac{1}{12n} - \frac{1}{360n^3} + \mathcal{O}(\frac{1}{n^5})\right]$$

Dado que puede probarse que $e^{\sigma} = \sqrt{2\pi}$ escribimos, en particular,

$$n! = \sqrt{2\pi n} (\frac{n}{e})^n [1 + \frac{1}{12n} + \frac{1}{288n^2} - \frac{139}{51840n^3} - \frac{571}{2488326n^4} + \mathcal{O}(\frac{1}{n^5})]$$

3.4 Representaciones Asintóticas

3.4.1 Definición

Dadas las funciones f y g definidas sobre los números naturales escribimos

$$f(n) = \mathcal{O}(g(n))$$

y decimos que $f(n)$ es de orden a lo sumo $g(n)$ si existe una constante positiva c tal que

$$|f(n)| \leq c|g(n)| \ \forall \ n \ \text{natural suficientemente grande}$$

3.4.2 Ejemplos

Ejemplo I

Por cierto,

$$n^2 + n + 3 \leq 3n^2 + 3n^2 + 3n^2 = 9n^2$$

con lo cual con $c = 9$ escribimos

$$n^2 + n + 3 = \mathcal{O}(n^2)$$

Ejemplo II

Consideremos el polinomio

$$P(n) = 3n^3 + 6n^2 + 4n + 2$$

Por cierto

$$\begin{array}{ll} |P(n)| & \leq 3n^3 + 6n^2 + 4n + 2 \\ & 6n^3 + 6n^3 + 6n^3 + 6n^3 \\ & 24n^3 \end{array}$$

Por lo tanto

$$3n^3 + 6n^2 + 4n + 2 = \mathcal{O}(n^3)$$

3.4.3 Teorema

Sea P un polinomio en n de grado k con expresión

$$a_k n^k + a_{k-1} n^{k-1} + \cdots + a_1 n + a_0$$

Entonces

$$P(n) = \mathcal{O}(n^k)$$

Demostración

Definimos

$$c = \max |a_k|, |a_{k-1}|, \ldots, |a_1|, |a_0|$$

Entonces

$$\begin{aligned} |P(n)| & \leq |a_k| n^k + |a_{k-1}| n^{k-1} + \cdots + |a_1| n + |a_0| \\ & \leq cn^k + cn^{k-1} + \cdots + cn + c \\ & \leq cn^k + cn^k + \cdots + cn^k + cn^k \\ & \leq (k+1) cn^k \end{aligned}$$

Por lo tanto, es

$$P(n) = \mathcal{O}(n^k)$$

3.4.4 Definición

Si un algoritmo necesita $f(n)$ unidades de tiempo para procesar datos de tamaño n y $f(n) = \mathcal{O}(g(n))$ decimos que el tiempo requerido por el algoritmo es $\mathcal{O}(g(n))$.

Operaciones

Algunas operaciones simples pueden explicitarse mediante la notación $\mathcal{O}$ de Euler, a saber

a) $f(n) = \mathcal{O}(f(n))$

b) $c\mathcal{O}(f(n)) = \mathcal{O}(f(n))$ si c es una constante

c) $\mathcal{O}(f(n)) + \mathcal{O}(f(n)) = \mathcal{O}(f(n))$

d) $\mathcal{O}(\mathcal{O}(f(n))) = \mathcal{O}(f(n))$

e) $\mathcal{O}(f(n))\mathcal{O}(g(n)) = \mathcal{O}(f(n)g(n))$

f) $\mathcal{O}(f(n)g(n)) = f(n)\mathcal{O}(g(n))$

3.4.5 Ejemplos

Ejemplo 1

a) Si la función $g(x)$ está dada por una serie infinita, es decir,

$$g(x) = \sum_{k\geq 0} a_k x^k \quad \text{tal que} \quad |x| \leq r$$

que converge absolutamente, es decir, que $\sum_{k\geq 0} |a_k||x^k|$ existe.
En este caso, podemos escribir

$$g(x) = \sum_{k\geq 0} a_k x^k + \mathcal{O}(x^{m+1}) \ \ , |x| \leq r$$

Son ejemplos de esta situación las siguientes relaciones

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} = \sum_{k=0}^{m} \frac{x^k}{k!} + \mathcal{O}(x^{m+1}) \ ; \ |x| \leq r$$

$$\ln(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k = \sum_{k=0}^{m} \frac{(-1)^{k+1}}{k} x^k + \mathcal{O}(x^{m+1}) \ ; \ |x| \leq r < 1$$

$$(1+x)^{\alpha} = \sum_{k=0}^{\infty} \begin{pmatrix} \alpha \\ k \end{pmatrix} x^k = \sum_{k=0}^{m} \begin{pmatrix} \alpha \\ k \end{pmatrix} x^k + \mathcal{O}(x^{m+1}) \ ; \ |x| \leq r < 1$$

b) Es sabido que $\lim_{n\to\infty} \sqrt[n]{n}$.
Entonces, podemos escribir

$$\sqrt[n]{n} = e^{\frac{1}{n}\ln n} = 1 + \frac{1}{n}\ln n + \mathcal{O}((\frac{1}{n}\ln n)^2)$$

Por lo tanto

$$n(\sqrt[n]{n} - 1) = \ln n + \mathcal{O}(\frac{1}{n}(\ln n)^2)$$

es decir, que para n suficientemente grande es

$$n(\sqrt[n]{n} - 1) \approx \ln n$$

pues $\lim_{n\to\infty} \frac{1}{n}(\ln n)^2 = 0$

3.4.6 Ejercicios

Ejercicio 1

¿Cuál es el límite $\lim_{n\to\infty} \mathcal{O}(n^{-1/3})$?

Ejercicio 2

Mutiplicar la cantidad: $[\ln n + \gamma + \mathcal{O}(1/n)]$ por $(n + \mathcal{O}(\sqrt{n}))$ expresando el resultado en términos de la $\mathcal{O}$ de Euler.

Ejercicio 3

Dar una expresión asintótica para $n(\sqrt[n]{a} - 1)$ si $a > 0$ en términos de $\mathcal{O}(1/n^3)$

Ejercicio 4

Probar que $\forall\ m \geq 0$ fijo es $e^{\mathcal{O}(x^m)} = 1 + \mathcal{O}(x^m)$ si $|x| \leq r$.

Ejercicio 5

Supongamos $a > 1$ y que $f(n) = \mathcal{O}(\log n)$. ¿Es cierto que $f(n) = \mathcal{O}(\log n)$?

Ejercicio 6

Verificar que si

$$f(n) = \mathcal{O}(h(n)) \ \text{ y } \ g(n) = \mathcal{O}(h(n))$$

entonces

$$f(n) + g(n) = \mathcal{O}(h(n))$$

y

$$cf(n) = \mathcal{O}(h(n)) \quad \text{cualquiera sea } c$$

Ejercicio 7

a) Mostrar que $n! = \mathcal{O}(n^n)$

b) Mostrar que $2^n = \mathcal{O}(n!)$

Ejercicio 8

Definimos $f(n) = \mathcal{O}(g(n))$ si existen constantes positivas c_1 y c_2 tales que

$$c_1|g(n)| \leq |f(n)| \leq c_2|g(n)|$$

para n a partir de un n_0 en adelante. Entonces, probar

a) $2n - 1 = \mathcal{O}(n)$

b) $3n^2 - 1 = \mathcal{O}(n^2)$

c) $\frac{12n^2-4n-1}{n-1} = \mathcal{O}(n)$

Capítulo 4

Algebras de Boole y Circuitos Combinatorios

4.1 Algebras de Boole

4.1.1 Definición

Un álgebra booleana B consiste en un conjunto $S = \{0, 1\}$ en el cual se han definido dos operaciones binarias "+" y "·" y un operador de complementación "′" que satisfacen las siguientes propiedados

a) Ley asociativa (tanto para + como para ·).
b) Ley conmutativa (tanto para + como para ·).
c)Ley distributiva

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \forall\ x, y, z \in S$$
$$x + (y \cdot z) = (x + y) \cdot (x + z) \quad \forall\ x, y, z \in S$$

d) Ley de identidad: $x + 0 = 1 \quad ; \quad x \cdot 1 = x \quad \forall\ x \in S$
e) Ley de complementación: $x + x' = 1\ ;\ \ x \cdot x' = 0\ \ ;\forall\ x \in S$
Denotaremos un álgebra booleana por $B = (S, +, \cdot, ', 0, 1)$.

4.1.2 Ejemplos

Ejemplo I

Es evidente que dado U el conjunto universal, la familia de partes de U, es decir $\mathcal{P}(U)$ con $\cap$ (unión), $\cup$ (intersección), c (complementación), $\emptyset = 0$, $U = 1$ es un álgebra booleana.

Ejemplo II

Sea B el conjunto de todos los enteros positivos divisores de 30, es decir, $B = \{2, 3, 5, 6, 10, 15, 30\}$
Para cualquier par de enteros x e y en B definimos

a) $x + y = m.c.m\{x, y\}$ (el mínimo común múltiplo entre x e y

b) $x \cdot y = m.c.d\{x, y\}$ (el máximo común divisor entre x e y

c) $x^{'} = 30/x$

Entonces, con el 1 como el elemento 0 y el 30 como el elemento 1 obtenemos $(B, +, \cdot, ', 0, 1)$ un álgebra booleana.
En efecto, sólo veamos una de las leyes distributivas para esta álgebra
Intentamos ver que

$$m.c.d(x, m.c.m\{y, z\}) = m.c.m(m.c.d\{x, y\}, m.c.d\{x, z\})$$

Para esto basta escribir

$$\begin{array}{rcccc} x & = & 2^{k_1}3^{k_2}5^{k_3} & & \\ y & = & 2^{m_1}3^{m_2}5^{m_3} & & \\ z & = & 2^{n_1}3^{n_2}5^{n_3} & & \\ 0 & \leq & k_i, m_i, n_i & \leq & 1 \\ i & = & 1, 2, 3 & & \end{array}$$

Entonces, $m.c.m\{y, z\} = 2^{s_1}3^{s_2}5^{s_3}$ donde $s_i = \max\{m_i, n_i\}$ con $i = 1, 2, 3$ con lo cual es $m.c.d\{x, m.c.m\{y, z\}) = 2^{t_1}3^{t_2}5^{t_3}$ donde $t_i = \min\{k_i, s_i\}$ con $i = 1, 2, 3$

Por otra parte, $m.c.d\{x, y\} = 2^{u_1}3^{u_2}5^{u_3}$ donde $u_i = \min\{k_i, m_i\}$ con $i = 1, 2, 3$ y $m.c.d\{x, z\} = 2^{v_1}3^{v_2}5^{v_3}$ donde $v_i = \min\{k_i, u_i\}$ con $i = 1, 2, 3$
Luego,

$$\begin{array}{rcc} m.c.m(m.c.d\{x, y\}, m.c.d\{x, z\}) & = & 2^{w_1}3^{w_2}5^{w_3} \\ w_i & = & \max\{u_i, v_i\} \quad i = 1, 2, 3 \end{array}$$

Así,

$$\begin{array}{rcc} w_i & = & \max|[u_i, v_i\} = \max\{\min\{k_i, m_i\}, \min\{k_i.n_i\} \\ t_i & = & \min\{k_i, \max\{m_i, n_i\} \end{array}$$

Para verificar este resultado necesitamos que $w_i = t_i$ para $i = 1, 2, 3$. Si $k_i = 0$ resulta $w_i = 0 = t_i$ y si $k_i = 1$ entonces $w_i = \max\{m_i, n_i\} = t_i$
Cabe observar que el número 30 puede reemplazarse por cualquier entero positivo $m = p_1p_2p_3$ con p_i primos distintos entre sí.

4.1.3 Ejercicios

Ejercicio 1

Probar que el elemento x', llamado complemento de x, es único en toda álgebra booleana.

Ejercicio 2

Probar en un álgebra booleana las siguientes propiedades

a) Leyes de idempotencia: $x + x = x \ ; \ x \cdot x = x \ \forall \ x \in S$.

b) Ley de acotación: $x + 1 = x \ ; \ x \cdot 0 = 0 \ \forall \ x \in S$.

c) Leyes de Absorción: $x + x \cdot y = x \ ; \ x \cdot (x + y) = x \ \forall \ x, y \in S$.

d) Ley de involución: $(x')' = x \ \forall \ x \in S$.

e) Leyes de De Morgan

$$\begin{array}{l} (x + y)' = x' \cdot y' \quad \forall \ x, y \in S \\ (x \cdot y)' = x' + y' \quad \forall \ x, y \in S \end{array}$$

f) $0^{'} = 1$ y $1^{'} = 0$

g) $xy^{'} = 0$ si $xy = x$ y $x + y^{'} = 1$ si $x + y + = x$

h) Leyes asociativas: $x(yz) = (xy)z$ y $x + (y + z) = (x + y) + z$

i) Leyes de cancelación:

i_1) $xy = xz$ y $x^{'}y = x^{'}z$ implican $y = z$

i_2) $x + y = x + z$ y $x^{'} + y = x^{'} + z$ implican $y = z$

Verificación de estas leyes

a) Probemos la condición i

$y = y \cdot 1 = (x + x^{'})y = xy + x^{"}y = xz + x^{'}z + (x + x^{'})z = 1 \cdot z = z$

La segunda parte de la condición i es la condición dual

b) Probemos la condición ii

$$\begin{array}{rcl} x+(x(yz) & = & x+(xy)z \\ x^{'}+x(yz) & = & x^{'}+(xy)z = x^{'}+x(yz) \end{array}$$

Por idempotencia y por absorción tenemos

$$x+x(yz) = (x+x)(x+yz) = x(x+yz) = x$$

Además,

$$x+x(yz) = (x+xy)(x+z) = x(x+z) = x$$

Entonces,

$$x^{'}+x(yz) = (x+x^{'})(x^{'}+yz) = 1(x^{'}+yz) = x^{'}+yz$$

mientras que

$$\begin{array}{rcccl} x^{'}+(xy)z & = & (x^{'}+xy)(x^{'}+z) & = & [(x^{'}+x)(x^{'}+y)](x^{'}+z) \\ & = & 1(x^{'}+y)(x^{'}+z) & = & (x^{'}+y)(x^{'}+z) = x^{'}+yz \end{array}$$

Luego, en virtud de la ley de cancelación obtenemos el resultado

La segunda parte de la condición ii es la condición dual

c) Probemos la ley de unicidad de inversos:

$x+y=1$ y $xy=0$ implican $y=x^{'}$
En efecto,
$x^{'} = x^{'}+0 = x^{'}+xy = (x+x^{'})(x^{'}+y) = 1(x^{'}+y) = (x^{'}+y)(x+y) = y+xx^{'} = y+0 = y$

d) La ley de involución es corolario de esta propiedad puesto que x y x" son complementos (inversos) de $x^{'}$
las condiciones $x+x^{'}=1$ y $(x^{'})^{'}+x^{'}=1$ implican $x=(x^{'})^{'}$

e) Probemos una de las leyes de De Morgan

Observemos que quedará probada si probamos que $x^{'}+y^{'}$ es el complemento de xy. En efecto,

$$\begin{array}{rcccl} (xy)+x^{'}+y^{'} & = & (xy+x^{'})+y^{'} & = & (x+x^{'})(x^{'}+y)+y^{'} \\ 1(x^{'}+y)+y^{'} & = & x^{'}+y+y^{'} & = & x^{'}+(y+y^{'}) \\ & = & x^{'}+1 & & \end{array}$$

Además,

$$xy(x^{'}+y^{'}) = (xy)x^{'}+(xy)y^{'} = (xx^{'})y+x(yy^{'}) = 0.y+0.x = 0$$

Por lo tanto, $x^{'} + y^{'}$ es el complemento de (xy) y por la unicidad del complemento es $x^{'}y^{'} = (x+y)^{'}$

f) Probemos la condición g

$$\begin{array}{ccccc} x & = & x.1 & = & x(y+y^{'}) \\ & = & xy+xy^{'} & = & x+xy^{'} \end{array}$$

implican $xy^{'} = 0$
Además,

$$\begin{array}{ccccc} 1^{'} & = & 0 & = & (x+y^{'})^{'} \\ & = & x^{'}(y^{'})^{'} & = & x^{'}.y \\ & = & (x+y^{'}).y & = & (x^{'}y^{'}).y \\ & = & x^{'}(y^{'}y^{'}) & = & 0 \\ & = & x^{'}.0 & = & 0 \end{array}$$

g) Probemos la ley de acotación

$$\begin{array}{ccccc} x.0 & = x(xx^{'}) & = & (x.x)x^{'} & \\ & = & x.x^{'} & = & 0 \\ x+1 & = & x+(x+x^{'}) & = & (x+x)+x^{'} \\ & = & x+x^{'} & = & x+x^{'} \\ & = & x+x^{'} & = & 1 \end{array}$$

h) Finalmente, probemos la ley de absorción

$$\begin{array}{ccccc} x(x+y) & = & x.x+x.y & = & x+xy \\ & = & x & & \\ x+x.y & = & x.1+x.y & = & x(y+1) \\ & = & x.1 & = & x \end{array}$$

Ejercicio 3

Dado $S = \{1,2,3,6\}$ definimos

$x + y =$ mcm $\{x, y\}$ (mínimo común múltiplo)

$x \cdot y =$ mcd $\{x, y\}$ (máximo común divisor)

x' = 6/x

cualesquiera sean x e y en S.

Probar que $(S, +, \cdot, ', 1, 6)$ es un álgebra booleana.

Ejercicio 4

Dado n un entero positivo considerar S como el conjunto de todos los divisores de n incluidos 1 y n. Definir S, $x+y$, $x \cdot y$ como en el ejercicio anterior con $x' = n/x$. ¿Qué condiciones debe satisfacer n para que $(S, +, \cdot, ', 1, n)$ sea un álgebra booleana?

4.1.4 Orden Parcial

Consideremos, ahora, $(P(U), \cup, \cap, c, \emptyset, U)$ donde $U = \{1, 2, 3\}$ con un orden parcial dado por la inclusión de subconjuntos.
Además, consideramos $(S, +, \cdot, ', 1, 30)$ donde $S = \{1, 2, 3, 5, 6, 10, 15, 30\}$ con las operaciones + y $\cdot$ dadas por

$$\begin{aligned} x + y &= m.c.m\{x, y\} \\ x \cdot y &= m.c.d\{x, y\} \\ x' &= 30/x \end{aligned}$$

Aquí, el elemento <u>*cero*</u> es el divisor 1 y el elmento <u>*uno*</u> es el divisor 30
De esta manera, la relación R definida en S por xRy si x divide a y es un orden parcial
:a pregunta es: ¿Es posible ordenar parcialmente cualquier álgebra finita?.

Definición

Si x e y pertenecen al álgebra booleana entonces $x \leq y$ si $xy = x$
esta relación, así definida, es un orden parcial
En efecto,
Para todo $x \in B$ es $x.x = x$ entonces $x \leq x$ con lo cual la relación es reflexiva.
Ahora, sean x e y en B con $x \leq y$ e $y \leq x$
De este modo son $xy = x$ y $yx = y$ con lo cual es $x = y$ con lo cual la relación es anti-simétrica.
Finalmente, veamos que es transitiva
Si $x \leq y$ e $y \leq z$ entonces $x \leq z$. En efecto,
$xy = x$ e $yz = y$ implican $x = xy = x(yz) = (xy)z = xz$, es decir, $x = xz$ luego es $x \leq z$
El álgebra formada por los divisores de 30 tiene un orden parcial dado por
$x \leq y$ si $xy = x$ pero, como definimos $xy = m.c.d\{x, y\}$ entonces si $m.c.d\{x, y\}+$ $xy = x$ implica x/y.

4.1.5 Definición

Sea $B = \{0, 1\}$ con la suma y el producto conocidos.
x es una variable booleana si sólo toma los valores de B con lo cual, obviamente, es $x + x = x$ y $x.x = x$

4.1.6 Definición

Si $n \in Z^+$ sea $B^n = \{b_1, b_2 ..., , b_n\}$ tal que $b_i \in \{0,1\}$ para todo $i = 1, ..., m$
Una función $f : B^n \to B$ se llama función booleana o de conmutación de n variables

Ejemplo

Sea $f : B^3 \to B$ donde $f(x, y, z) + xy + z$ siendo x, y, z variables booleanas. Esta función booleana se evalúa de la siguiente forma

x	y	z	xy	$f(x,y,z) = xy + z$
0	0	0	0	0
0	0	1	0	1
0	1	0	0	0
0	1	1	0	1
1	0	0	0	0
1	0	1	0	1
1	1	0	1	1
1	1	1	1	1

4.1.7 Definición

Para cualquier $n \in Z^+$ si f es una función booleana enlas n variables $x_1, x_2, ..., x_n$ se denominan

a) $literal$ a cada término x_i ó a su complemento $x_i^{'}$ para $i = 1, 2, ..., n$

b) $conjunción\ fundamental$ a un término de la forma $y_1 \wedge y_2 \wedge .... \wedge y_n$ cada $y_i = x_i$ ó $x_i^{'}$

c) $forma\ normal\ disyuntiva$ (f.n.d) a una representación de f como una suma (disyunción) de conjunciones fundamentales

Ejemplo I

hallar la F.n.d para $f : B^3 \to B$ dada por

$$f(x, y, z) = xy + \overline{x}z = (x \wedge y) \vee (\overline{x} \wedge z)$$

La siguiente tabla contiene cuatro unos que indican las conjunciones fundamentales necesarias para la f.n.d con lo cual es

$$f(x, y, z) = \overline{xy}z + \overline{x}yz + xy\overline{z} + xyz$$

En realidad, podemos lograrla así

$$\begin{aligned} f(x,y,z) &= xy+\overline{x}y = xy(z+\overline{z})+\overline{x}(y+\overline{y})z \\ &= xyz+xy\overline{z}+\overline{x}yz+\overline{x}\overline{y}z \end{aligned}$$

x	y	z	xy	$\overline{x}z$	f
0	0	0	0	0	0
0	0	1	0	1	1
0	1	0	0	0	0
0	1	1	0	1	1
1	0	0	0	0	0
1	0	1	0	0	0
1	1	0	1	0	1
1	1	1	1	0	1

4.1.8 Ejercicio 1

Hallar la f.n.d para la función dada por

$$f(w,x,y,z)=wx\overline{y}+wy\overline{z}+xy$$

Por cierto, podemos expresar má s compactamente la f.n.d de ubn función booleana no nula.
Por ejemplo, $f=\sum m(1,3,6,7)$ donde m indica los términos (termin) de la sfilas $2,4,7,8$ de la tabla del Ejemplo I anterior con las combinaciones binarias de $1,3,6$ y 7 respectivamente.

4.1.9 Definición

Llamamos f.n.c (forma normal conjuntiva) a la conjunción de disyunciones fundamentales

Ejemplo II

Dada la siguiente función booleana $g: B^4 \to B$

$$g(w,x,y,z)=(w+x+y)(x+\overline{y}+z)(x+\overline{y}+z)(w+\overline{y})$$

hallar la f.n.c correspondiente

a)

$$\begin{aligned} w+x+y &= w+x+y+0 = w+x+y+(z\overline{z}) \\ &= (w+x+y+z)(w+x+y+\overline{z}) \end{aligned}$$

b)

$$(x+\overline{y}+z) = w\overline{w}+x+\overline{y}+z = (w+x+\overline{y}+z)(\overline{w}+x+\overline{y}+z)$$

c)

$$\begin{array}{lcc}
w+\overline{y} & = & w+x\overline{x}+\overline{y} \\
 & = & (w+x+\overline{y})(w+\overline{x}+\overline{y}) \\
 & = & (w+x+\overline{y}+z\overline{z})(w+\overline{x}+\overline{y}+z\overline{z}) \\
 & = & (w+x+\overline{y}+z)(w+x+\overline{y}\overline{z})\cdot \\
 & \cdot & (w+\overline{x}+\overline{y}+z)(w+\overline{x}+\overline{y}+\overline{z}) \\
 & = & (w+x+y+z)(w+x+y+\overline{z})\cdot \\
\&\cdot & (w+x+\overline{y}+z)(\overline{w}+x+\overline{y}+z)\cdot & \\
 & \cdot & (w+x+\overline{y}+\overline{z})(w+\overline{x}+\overline{y}+z)\cdot \\
 & \cdot & (w+\overline{x}+\overline{y}+\overline{z})
\end{array}$$

Para cada disyunción fundamental $d_1+d_2+d_3+d_4$ asociamos el número binario $b)1b_2b_3b_4$ donde

$$\begin{array}{lcl}
b_1 & = & 0 \;\; si \;\; d_1 = w \\
b_1 & = & 1 \;\; si \;\; d_1 = \overline{w} \\
 & \ldots & \\
b_4 & = & 0 \;\; si \;\; d_4 = z \\
b_4 & = & 1 \;\; si \;\; d_4 = \overline{z}
\end{array}$$

Luego, obtenemos g como *producto de termax*, es decir,

$$g = \prod M(0,1,2,3,6,7,10)$$

Ejercicio

Dada $f : B^3 \to B$ por la siguiente tabla

x	y	z	f
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

Hallar, explícitamente, la f.n.c como $f = \prod M(0,2,6)$

Ejemplo III

Hallar la red de compuertas para la función booleana

$$f(w,x,y,z) = \sum m(4,5,7,8,9,11)$$

Determinemos f en f.n.d. escribiendo cada número termin en notación binaria y hallamos, después, conjunción fundamental correspondiente, a saber

$$\begin{array}{rclc} 5 & = & 0101 & \overline{w}x\overline{y}z \\ 7 & = & 0111 & \overline{w}xyz \\ 8 & = & 1000 & w\overline{xyz} \\ 9 & = & 1001 & w\overline{xy}z \\ 11 & = & 1011 & w\overline{x}y\overline{z} \\ 4 & = & 0100 & \overline{w}x\overline{yz} \end{array}$$

Entonces

$$f(w,x,y,z) = \overline{w}xz + \overline{w}x\overline{y} + w\overline{xy} + w\overline{x}z$$

llamada suma minimal de productos.

Ejercicio

Deducir la expresión de f dada en el Ejemplo III.

4.1.10 Diagramas de Karnaugh

Dado que es necesario maximizar la velocidad se pretende representar una función booleana como suma minimal de productos. Para esto, para funciones que contengan más de 6 variables booleanas se emplea un método gráfico denominado *diagrama de Karnaugh* (1953) basado en la f.n.d. de una función booleana.
En el Ejemplo III anterior

$$\overline{w}x\overline{y}z + \overline{w}xyz \Rightarrow \overline{w}xz$$

Esto significa que si dos conjunciones fundamentales difieren exactamente en un literal entonces pueden combinarse en un término producto sin ese literal.

Ejemplo IV

Sea $g : B^4 \to B$ dada por

$$g(w,x,y,z) = wx\overline{yz} + wx\overline{y}z + wxyz + wxy\overline{z}$$

donde cada conjunción fundamental difiere de su predecesora exactamente en una literal.
En efecto, puede simplicarse así

$$g(w,x,y,z) = wx\overline{y}(\overline{z}+z_{+}wxy(z+\overline{z}) = wx\overline{y}+wxy = wx(\overline{y}+y) = wx$$

La clave de este proceso de reducción reside en reconocer pares, cuartetas,..., 2^n-adas de conjunciones fundamentales donde dos términos adyacentes cualesquiera difieren exactamente en una literal.

Ejemplo V

Dadas $f(w,x) = wx$ y $g(w,x) = w+x$

	x	0	1	0	1
w					
0					1
1			1	1	1
			wx		$w+x$

es el diagrama de Karnaugh correspondiente donde $w+x$ representa la f.n.d. siguiente

$$w\overline{x}+\overline{w}x+wx = x(\overline{w}+w)+w\overline{x} = x+w\overline{x}$$

difieren en una sola literal, entonces, $w\overline{x}+wx = w(x+\overline{x}) = w$. También, $\overline{w}x+wx = x(w+\overline{w}) = x$

Ejemplo V

Sean w, x e y tres variables booleanas y la función $f(w,x,y) = xy$ con valores dados en el siguiente diagrama de Karnaugh

	xy	00	01	11	10
w					
0		1			1
1		1		1	

Si $f(w,x,y) = \sum m(0,2,4,7)$ entonces

$$\begin{array}{rcl} 0 & = & 000(\overline{wxy}) \\ 2 & = & 010(\overline{w}x\overline{y}) \\ 4 & = & 010(w\overline{xy}) \\ 7 & = & 111(wxy) \end{array}$$

Según la tabla anterior el 1 para wxy no es adyacente a ningún otro 1, es decir, está aislado, por lo tanto, wxy estará en la suma minimal de productos.

El 1 para $\overline{w}x\overline{y}$ no estä aislado pues es adyacente al 1 para $\overline{wxy}$ entonces

$$\overline{w}x\overline{y} + \overline{wxy} = \overline{wx}$$

El 1 para $\overline{wxy}$ y el 1 para $w\overline{xy}$ dan

$$\overline{w}(\overline{xy}) + w(\overline{xy}) = \overline{xy}$$

Por lo tanto, $f(w, x, y) = wxy + \overline{wy} + \overline{xy}$

4.1.11 Ejercicios

Ejercicio 1

Dadas la siguiente tabla

xy	00	01	11	10
w				
0	1			1
1	1			1

y $f(w, x, y) = \sum m(0, 2, 4, 6)$ verificar que $f(w, x, y) = \overline{y}$

Ejercicio 2

Dadas la siguiente tabla

xy	00	01	11	10
w				
0		1	1	1
1		1	1	1

y $f(w, x, y) = \sum M(1, 2, 3, 5, 6, 7)$ verificar $f(w, x, y) = x + y$

Ejercicio 3

Hallar la suma minimal de productos para $f(w, x, y, z) = \sum m(0, 1, 2, 3, 8, 9, 10)$ a partir de la siguiente tabla

yz	00	01	11	10
wx				
00	1	1	1	1
01				
11				
10	1	1		1

y verificar que

$$f(w,x,y,z) = \overline{xz} + \overline{wx} + \overline{xy}$$

4.2 Circuitos

Los circuitos electrónicos pueden ser combinatorios o secuenciales. En un circuito combinatorio, los datos de salida están unívocamente determinados para toda combinación de datos de entrada. Los circuitos combinatorios no tienen memoria en el siguiente sentido: los datos de entrada anteriores y el estado del sistema no afectan los datos de salida. En caso contrario, llamaremos al circuito secuencial.
Los circuitos combinatorios se construyen usando dispositivos de estado sólido llamados compuertas, que son capaces de producir cambios de voltaje (valores de 0 o 1 para un bit dado). Existen compuertas elementales: AND, OR y NOT.

4.2.1 Definiciones

Compuerta AND

Una compuerta AND acepta $x_1, \ldots, x_n$ como datos de entrada siendo $x_1, \ldots, x_n$ bits y produce un dato de salida denotado por $x_1 \wedge \ldots \wedge x_n$ y dado por

$$x_1 \wedge \ldots \wedge x_n = \begin{cases} 1 & \text{si todas las entradas son 1} \\ 0 & \text{en cualquier otro caso} \end{cases}$$

Tal compuerta tiene asociada una tabla de verdad que no es más que la correspondiente a la conjunción de dos proposiciones, donde Verdadero es 1 y Falso es 0.

Compuerta OR

Una compuerta OR acepta a $x_1, \ldots, x_n$ como entradas y produce un dato de salida denotado por
$x_1 \vee \ldots \vee x_n$ y dado por

$$x_1 \vee \ldots \vee x_n = \begin{cases} 1 & \text{si alguna entrada es 1} \\ 0 & \text{si todas las entradas son cero} \end{cases}$$

Por cierto, esta compuerta corresponde a la disyunción de dos proposiciones

Compuerta NOT

Esta compuerta corresponde al conectivo lógico negación. Generalmente, se lo denomina inversor.

Expresión booleana

Una expresión booleana con los símbolos $x_1, \ldots, x_n$ está definida recursivamente por

$$0, 0, x_1, \ldots, x_n$$

Ejemplos

a) $X(x_1) = \overline{x_1}$

b) $X(x_1, x_2) = x_1 \vee x_2$

c) $X(x_1, x_2) = x_1 \wedge x_2$

d) $X(x_1, x_2, x_3) = \overline{(x_1 \wedge x_2) \vee x_3}$
En este caso, si $x_1 = 1; x_2 = 0; x_3 = 0$ la expresión booleana se convierte en

$$X(x_1, x_2, x_3) = X(1, 0, 0) = \overline{(1 \wedge 0) \vee 0} = \overline{0} = 1$$

d) La siguiente expresión booleana: $[x_1 \vee (\overline{x_2} \vee x_3)] \vee x_2$ es un circuito combinatorio.

4.2.2 Ejercicios

Ejercicio 1

Justificar cuál o cuáles de las siguientes expresiones es booleana

a) $x_1 \wedge (x_2 \wedge x_3)$

b) $(x_1 \wedge x_2) \vee \overline{x_3}$

c) $(x_1 \wedge \overline{x_2}) \vee x_3$

d) $(x_1 \wedge \overline{x_2}) \wedge (x_1 \vee \overline{x_3})$

Ejercicio 2

Llamamos circuito de conmutación a un circuito formado por interruptores, cada uno de los cuales puede estar abierto o cerrado, con B valiendo 0 ó 1 respectivamente. Decimos que la salida del circuito es 1 si la corriente circula entre los extremos inicial y final; en caso contrario decimos que la salida es cero. La tabla de conmutación presenta las salidas de los circuitos para todos los valores de operación de los interruptores.
En un caso particular, la tabla de conmutación está dada por

A	B	C	Salida del circuito
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	1
0	0	1	1
0	0	0	1

Si tenemos dos interruptores A y B tales que la salida del circuito sea 1 cuando tanto A como B estén cerrados, configuracion un circuito en serie configurado por $A \wedge B$. En cambio, cuando tengamos dos interruptores A y B tales que la salida del circuito sea 1 estando uno de los dos interruptores cerrado, tendremos una configuración llamada circuito en paralelo denotada por $A \vee B$. En este caso particular, es fácil comprobar que la configuración responde a

$$(A \wedge B) \vee \overline{A} \wedge (B \wedge C)$$

A partir de estas observaciones, representar las siguientes expresiones como circuitos de conmutación y construir la tabla correspondiente

a) $(A \vee \overline{B}) \wedge A$

b) $A \wedge (\overline{B} \vee C)$

c) $(\overline{A} \wedge B) \vee (C \wedge A)$

d) $\{A \vee [(B \wedge \overline{C}) \vee (\overline{B} \wedge C)]\} \wedge (\overline{A} \wedge B \wedge C)$

Ejercicio 3

Analizar la validez de la siguiente afirmación

Toda expresión booleana representa un circuito de conmutación En caso de que sea válida, probar su validez; en caso contrario, dar un contraejemplo.

4.2.3 Síntesis de circuitos

Denotaremos el "OR exclusivo" de lógica proposicional por $\oplus$. Dada una expresión booleana $X(x_1, \ldots, x_n)$ llamamos *función booleana* a una función de la forma

$$f(x_1, \ldots, x_n) = X(x_1, \ldots, x_n)$$

Por ejemplo, $f(x_1, \ldots, x_n) = x_1 \wedge (\overline{x_2} \vee x_3)$ es una función booleana.

4.2.4 Definición

Un minitérmino en los símbolos $x_1, \ldots, x_n$ es un a expresión booleana de la forma

$$y_1 \wedge y_2 \wedge \ldots \wedge y_n$$

donde cada $y_i = x_i$ ó bien cada $y_i = \overline{x_i}$.

4.2.5 Definición

Si f es una función booleana no idénticamente nula tal que cada elemento $(a_1, \ldots, a_n)$ toma el valor 1 tomando

$$m_i = y_1 \wedge \ldots \wedge y_n$$

donde cada $y_i = x_i$ si $a_i = 1$ ó bien $y_i = \overline{x_i}$ si $a_i = 0$ resulta

$$f(x_1, \ldots, x_2) = m_1 \vee m_2 \vee \ldots \vee m_k$$

Esta representación de la función booleana se denomina forma normal disyuntiva de la función f.

Por ejemplo, la forma normal disyuntiva para el "OR exclusivo" está dada por

$$x_1 \oplus x_2 = (x_1 \wedge \overline{x_2}) \vee (\overline{x_1} \wedge x_2)$$

Lo cual es fácil de comprobar.

4.2.6 Ejercicios

Ejercicio 1

Determinar la forma normal disyuntiva de cada una de las siguientes funciones y trazar el circuito combinatorio correspondiente a)

x	y	$f(x,y)$
1	1	1
1	0	0
0	1	1
0	0	1

b)

x	y	$f(x,y)$
1	1	0
1	0	1
0	1	0
0	0	1

c)

x	y	z	$f(x,y)$
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	1

d)

x	y	z	$f(x,y,z)$
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	1
0	1	0	1
0	0	1	0
0	0	0	0

Ejercicio 2

Establecer la forma normal disyuntiva de cada una de las siguientes funciones:

1. $f(x,y) = x \ \vee \ x \wedge y$
2. $f(x,y) = (x \vee y) \wedge (\overline{x} \vee \overline{y})$
3. $f(x,y,z) = x \vee y \wedge (x \vee \overline{z})$

4. $f(x,y,z) = [y \wedge z \ \vee \ x\ can\ \overline{z}] \wedge \overline{[x \wedge \overline{y} \vee z]}$

Capítulo 5

Grafos y Algoritmos

5.1 Teoría de Grafos

5.1.1 Defінción

Un grafo es un conjunto de dos o más puntos $N_i, i \in I$ llamados nodos o vértices del grafo diferentes entre sí tales que ciertos pares de estos puntos están unidos por una o más líneas $A_{ij}, j \in J$ llamadas arcos, ramas o *ejes del grafo* relacionados por una matriz de incidencia nodo/arco de orden $I \times J$ cuyos coeficientes están dados por

a) $[+1]$ si el arco j proviene del nodo i

b) $[-1]$ si el arco j llega al nodo i

c) $[0]$ en cualquier otro caso

5.1.2 Definición

Un arco o rama orientada tiene al nodo i como punto inicial y al nodo j como punto terminal.

5.1.3 Definición

Un camino que une los nodos i y j es un conjunto ordenado de arcos o ramas $A_{ip}, A_{pq}, \ldots, A_{tu}, A_{uj}$ tal que cada nodo de este conjunto ordenado es un punto final de dos y sólo dos ramas en tal conjunto. Los nodos N_i y N_j se llaman puntos extremales de tal camino y cuando $N_i \equiv N_j$ el camino se denomina un ciclo.

5.1.4 Definición

Un nodo N_j se llama fuente si todo arco que lo tiene como punto inicial está orientado de modo tal que el flujo sobre esa rama se mueve desde N_J hacia otro nodo.

5.1.5 Definición

Análogamente, un nodo N_J se llama vertedero si toda rama que lo tiene como punto terminal está orientado de modo tal que el flujo proviene de otros nodos llegando a N_j.

5.1.6 Definición

Una cadena es una secuencia de nodos y de arcos de la forma N_1, A_{12}, N_2, A_{23}, $\ldots$, $N_{k-1}, A_{k-1,k}, N_k$.

5.1.7 Definición

Una árbol es un grafo que no tiene ciclos y, además, es conexo. Por lo tanto, entre dos nodos cualesquiera del árbol existe una única cadena que une dichos nodos.

5.1.8 Definición

Para cada arco A_{ij} existe un número positivo d_{ij} llamado capacidad de flujo a través del arco.

5.1.9 Definición

Una red es un grafo tal que el flujo puede tomar lugar en las ramas de tal grafo. Esta red puede ser orientada o no dependiendo de la orientación de las ramas.

5.1.10 Definición

Considerando una red y de ésta un subconjunto X de nodos y otro subconjunto X^c (complemento del anterior) se denomina corte en una red y se denota por $c(X, X^c)$ al conjunto de todos los arcos A_{ij} que satisfacen

o bien $N_i \in X$ y $N_j \in X^c$
o bien $N_j \in X$ y $N_i \in X^c$

Es decir, un corte en una red es un conjunto de arcos de modo tal que la supresión de algún arco de tal conjunto desconectará la red.

5.1.11 Definición

En una red $N_1, A_{12}, N_2, \ldots, N_{k-1}, A_{k-1,k}, N_k$ con N_1 fuente y N_k vertedero el monto máximo del flujo que puede pasar a través de la red está limitado por el arco de capacidad mínima entre todos los arcos de la cadena. Este arco de mínima capacidad se denomina cuello de botella de la red. Además, la suma de las capacidades de los arcos de un corte es mayor o igual que el flujo máximo v cada vez que el corte separe N_S de N_t. El valor de un corte es $\sum_{i,j} d_{ij}$ tal que $N_i \in X$ y $N_j \in X^c$.

5.1.12 Teorema

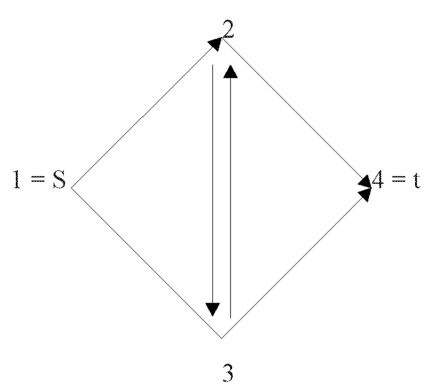
El teorema central en la teoría de flujos en redes es el de flujo máximo-corte mínimo enunciado por Ford-Fulkerson, que establece

> "En cualquier red el valor máximo del flujo de la fuente al vertedero es igual a la capacidad del mínimo corte que separe la fuente del vertedero."

5.1.13 Ejemplos

Ejemplo I

Conviniendo que 1 es la fuente (source) y que 4 es el vertedero (sink) observamos

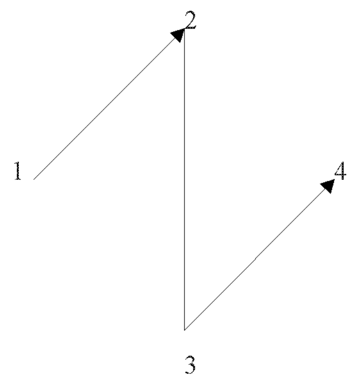


a) La secuencia $N_1, A_{12}, N_2, A_{24}, N_4$ es una cadena

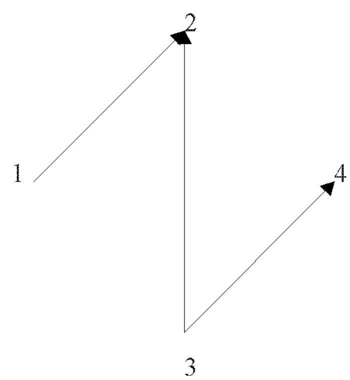
b) La secuencia $N_1, A_{13}, N_3, A_{32}, N_2, A_{24}, N_4$ es una camino

c) La secuencia $N_2, A_{23}, N_3, A_{32}, N_3$ es un ciclo

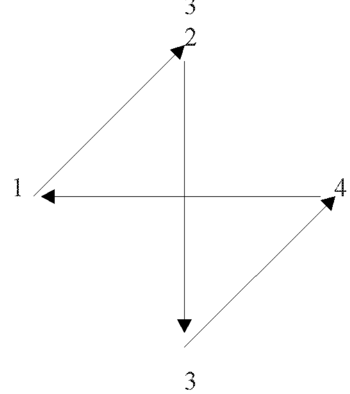
Ejemplo II



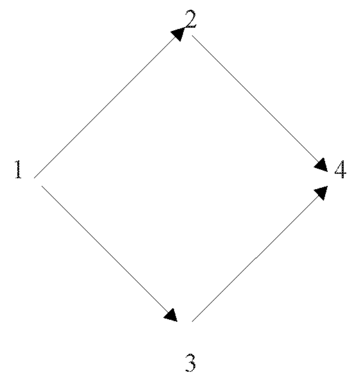
i.



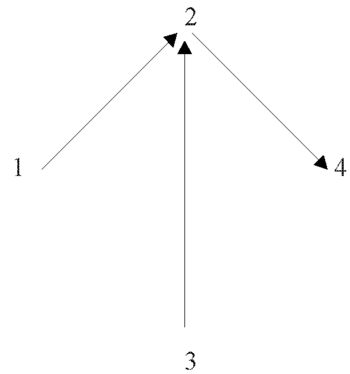
ii.



iii.



iv.



v.

En (i) la secuencia $N_1, A_{12}, N_2, A_{23}, N_3, A_{34}, N_4$ es un camino.

a) La secuencia $N_4, A_{34}, N_3, A_{32}, N_2, A_{12}, N_1$ es una cadena

b) La secuencia $N_4, A_{41}, N_1, A_{12}, N_2, A_{23}, N_3, A_{34}, N_4$ es un circuito o camino cerrado o ciclo

c) La secuencia $N_4, A_{24}, N_2, A_{12}, N_1, A_{13}, N_3, A_{34}, N_4$ es un ciclo o cadena cerrada

d) Las secuencias $N_1, A_{12}, N_2, A_{24}, N_4$ y N_3, A_{32}, N_2 son árboles

Observación

a) Todo camino es una cadena pero no al revés

Ejemplo III

Desde el punto de vista de las aplicaciones, ejemplos típicos de redes acíclicas son: la adopción de un plan de inversiones para una empresa, la construcción de edificios y la inserción de un producto en el mercado donde interesa conocer la duración del programa a realizar. En este tipo de problemas, el conjunto de tareas a realizar constituye un programa representable mediante un grafo llamado grafo de ordenamiento donde los arcos representan las operaciones a realizar y asociado con cada arco hay un número que representa la duración de la tarea y donde los nodos representan acontecimientos. Este grafo de ordenamiento es un grafo orientado donde no puede retrocederse a ningún nodo, con lo cual no hay circuitos ni ciclos, es decir, es una típica red acíclica

5.2 Modelos Matemáticos y Algoritmos

Ya estamos en condiciones de formular el modelo matemático asociado con la red que involucre la optimización de alguna función del flujo a través de la red sujeta a ciertas restricciones de capacidad en los arcos de red y a ciertas restricciones de conservación del flujo en todo nodo de la red a excepción del la fuente y del vertedero en la siguiente forma

5.2.1 Definición

Un conjunto de enteros no negativos $x_{ij} \geq 0$ se llaman flujo en una red si se satisfacen las siguientes condiciones

a) $0 \leq x_{ij} \leq d_{ij}$ para todo i y para todo j (esto da la restricción de la capacidad de cada arco A_{ij})

b) $\sum_i x_{ij} - \sum_k x_{jk} =$

$$\begin{cases} -v & \text{si} \quad j = s \ \text{(fuente)} \\ 0 & \text{si} \quad j \neq s,t \ \text{(el nodo no es fuente ni vertedero)} \\ +v & \text{si} \quad j = t \ \text{vertedero} \end{cases} \quad \text{donde v es el flujo}$$

La segunda relación indica que el flujo se conserva en todo nodo a excepción de la fuente y el vertedero. Por lo tanto, la variación del índice j es $2, 3, \ldots, (n-1)$

5.2.2 Maximización del Flujo

Para formular el modelo del problema que maximiza el flujo a través de la red es natural considerar como función objetivo

$$v = \sum_{j=2}^{n-1} x_{Sj}$$

En el caso de una red con n nodos y m arcos sujeta a las siguientes condiciones

$$\begin{array}{l} 0 \leq x_{ij} \leq d_{ij} \quad \forall\, i,\ \forall\, j \\ \sum_i x_{ij} - \sum_k x_{jk} = 0 \qquad j = 2, 3, \ldots, (m-1) \end{array}$$

Introduciendo a v como variable el problema de flujo máximo a través de una red tiene el siguiente aspecto matricial

maximizar $z = cx$ sujeta a $Ax = 0, \tilde{A}x \leq d, x \geq 0$ donde
a) $c \in \mathcal{R}^{1\times(m+1)}$ siendo la primera componente de este vector fila uno y los m restantes nulos

b)$x \in \mathcal{R}^{(m+1)\times 1}$ siendo la primera componente de este vector columna v y la m restantes los valores de x_{ij} en cada uno de los m arcos

c)$A \in \mathcal{R}^{n\times(m+1)}$ es la matriz de incidencia nodo/arco

d) $\tilde{A} \in \mathcal{R}^{n\times(m+1)}$ es una matriz particionada de la forma $\tilde{A} = [0, I_m]$ que proporciona la restricción de capacidad en cada arco

e)$d \in \mathcal{R}^{m\times 1)}$
Aquí , la matriz A se caracteriza por tener en cada columna dos enteros no nulos: $(+1)$ y (-1) y portener una propiedad no del todo aparente: la de ser totalmente unimodular pues todo subdeterminante tiene valor 1 o cero. Esta propiedad garantiza la solución óptima entera si todas las componentes del vector d son enteras

5.2.3 Minimización del Costo

El modelo matemático correspondiente al problema de minimizar el costo del flujo a través de una red con n nodos y m arcos se propone como sigue

a) Minimizar $z = cx$ sujeta a $Ax = b$ (restricciones de conservación de flujo en cada nodo de la red a excepción de la fuente y del vertedero) tal que $0 \leq x \leq \mu$ (restricciones de capacidad en cada arco de la red)

La matriz A de incidencia nodo/arco tiene en sus filas los nodos y en sus columnas los arcos. Si existen dos arcos desde el nodo i al nodo j entonces uno de ellos puede reemplazarse por dos arcos (i, k) y (k, j) donde k es un nuevo nodo con lo cual para cada arco (es decir, para cada columna) e_j tenemos

a) $F(j) = i$ con $A_{ij} = 1$

b) $F(j) = k$ con $A_{kj} = -1$

es decir, que en cada columna ej en la fila i-ésima aparece (+1) mientras que en la fila k-ésima aparece (-1)
De ahora en adelante, emplearemos la siguiente notación

a) $e_j = (F(j), T(j))$

b) $\mathcal{A} = \{e_1, e_2, \ldots, e_n\}$ conjunto de arcos

c) $\mathcal{N} = \{1, 2, \ldots, m\}$ conjunto de nodos

d) $\mathcal{G} = \{\mathcal{A}, \mathcal{N}\}$ un grafo

Además, diremos que $\mathcal{G}$ es un *grafo* propio si $n \geq 2$ y $m \geq 1$

5.3 Subgrafos

5.3.1 Definición

Decimos que $\tilde{\mathcal{G}} = \{\tilde{\mathcal{A}}, \tilde{\mathcal{N}}\}$ es un *subgrafo* de $\mathcal{G}$ si $\tilde{\mathcal{A}} \subset \mathcal{A}$ y si $\tilde{\mathcal{N}} \subset \mathcal{N}$
Además, si $\tilde{\mathcal{N}} = \mathcal{N}$ decimos que $\tilde{\mathcal{G}}$ genera $\mathcal{G}$ o bien que $\tilde{\mathcal{G}}$ es el subgrafo generado por $\mathcal{G}$

5.3.2 Definición

Una sucesión finita $P = \{S_1, e_{j_1}, S_2, e_{j_2}, S_n, e_{j_n}, S_{n+1}\}$ teniendo al menos un arco se dice *camino* si sus elementos impares son nodos distintos del grafo y si sus elementos pares son arcos de $\mathcal{G}$, y si para cada arco e_{ji} pertenece a (S_i, S_{i+1}) o bien a (S_{i+1}, S_i)
Observemos que esta definición corresponde a la noción de cadena

5.3.3 Orientación

Para cualquier cualquier camino o ciclo P de longitud n (número de arcos que lo componen) se define orientación de la sucesión $O_i(P)$ de n elementos por

$$\begin{array}{lll} O_i(P) = +1 & \text{si} & e_{ji} = (S_i, S_{i+1}) \\ O_i(P) = -1 & \text{si} & e_{ji} = (S_{i+1}, S_i) \end{array}$$

5.3.4 Proposición

Dado un camino o un ciclo P en un grafo propio $\mathcal{G}$ con matriz de incidencia nodo/arco A de columnas $A(j)$ correspondientes al arco e_j vale la siguiente igualdad

$$\sum_{i=1}^{n} O_i(P)A(ji) = e^{S_1} - e^{S_{n+1}}$$

Demostración

a) Si $e_{j_i} = (S_i, S_{i+1})$ entonces $O_i(P)A(j_i) = e^{S_i} - e^{S_{i+1}}$

b) Si $e_{j_i} = (S_{i+1}, S_i)$ entonces $O_i(P)A(j_i) = (-1)(e^{S_{i+1}} - e^{S_i}) = e^{S_i} - e^{S_{i+1}}$
Por lo tanto, en cualquier caso es

$$O_i(P)A(j_i) = e^{S_i} - e^{S_{i+1}}$$

con lo que, sumando en $i = 1, 2, \ldots, n$ obtenemos lo propuesto
Observemos que si P es un ciclo entonces $S_1 = S_{n+1}$ con lo que $\sum_{i=1}^{n} O_i(P)A(j_i) = 0$. Esto dice que las columnas $A(j_i)$ de la matriz de incidencia nodo/arco incluidas en un ciclo son linealmente dependientes

5.3.5 Árbol

Un árbol $\mathcal{T} = \{\tilde{\mathcal{A}}, \tilde{\mathcal{N}}\}$ es un grafo arco-conexo sin ciclos

5.3.6 Proposición

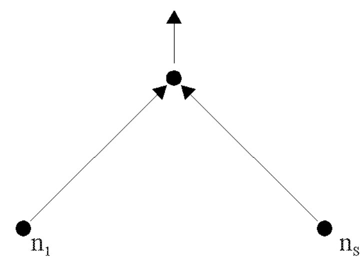
Sea A la matriz de incidencia nodo/arco para un grafo propio $\mathcal{G}$. Entonces, dado un árbol $\mathcal{T}$ subgrafo de $\mathcal{G}$ con al menos dos nodos ($n \geq 2$), las columnas $A(j)$ de la matriz A correspondiente a los arcos $e_j \in \mathcal{A}$ son linealmente independientes

Demostración

Si $n = 2$ entonces existe un solo arco e_j con lo cual existe una sola columna $A(j)$ no nula la cual, por cierto, es linealmente independiente
Si $n > 2$ entonces sea m el número entero más grande tal que todos los subgrafos de $\mathcal{G}$ que son árboles con $k = 2, 3, \ldots, n$ nodos tienen las columnas $A(j)$ de la matriz A correspondientes a sus arcos linealmente independientes

Por lo tanto, de acuerdo con la definición de m existe algún arbol con $(m+1)$ nodos cuyas columnas $A(j)$ en A son linealmente dependientes, vale decir, existe un árbol $\tilde{\mathcal{T}} = \{\tilde{\mathcal{A}}, \tilde{\mathcal{N}}\}$ con $\mathcal{N}$ conteniendo $(m+1)$ nodos y con las columnas (arcos) en $\tilde{\mathcal{A}}$ linealmente dependientes. Por lo tanto, existe una combinación lineal de dichas columnas con escalares no nulos que verifica

$$\sum_{e_{ji} \in \tilde{\mathcal{A}}} \alpha_i A(j_i) = 0 \text{ con } \alpha_i \neq 0 \text{ para algún } i$$



Dado que $\tilde{\mathcal{T}}$ es un árbol existe por lo menos un nodo i donde incide un solo arco de modo que sacando el nodo n_1 y el arco e_{n_1} obtenemos otro árbol $\bar{\mathcal{T}} = \{\bar{\mathcal{A}}, \bar{\mathcal{N}}\}$ donde $\bar{\mathcal{A}} = \tilde{\mathcal{A}} - e_{n_1}$ y donde $\bar{\mathcal{N}}$ tiene m nodos. Por lo tanto, de acuerdo con la definición de m, tenemos

$$\sum_{e_{ji} \in \bar{\mathcal{A}}} \alpha_i A(j_i) + \alpha_{n_1} A(j_{n_1}) = 0$$

y al ser $\bar{\mathcal{T}}$ un árbol con m nodos, todos los coeficientes α_i tal que $e_{ji} \in \bar{\mathcal{A}}$ son nulos, con lo que $\alpha_{n_1} = 0$.

5.3.7 Proposición

Todo grafo $\mathcal{G} = \{\mathcal{A}, \mathcal{N}\}$ arco-conexo con $\mathcal{N} \neq \emptyset$ tiene un subgrafo que es un árbol generado por $\mathcal{G}$. Este árbol $\mathcal{T}$ tiene n nodos y $(n-1)$ arcos

5.3.8 Observación

Observemos que, dada la estructura de la matriz A la suma de sus filas es cero, luego el rango$(A) = (n-1)$, con lo cual existen sólo $(n-1)$ columnas linealmente independientes. Esto permite reformular el problema propuesto agregando una variable artificial a con un nivel cero y una columna e_l con $1 \leq l \leq n$ a fin de obtener una matriz básica con rango máximo

5.3.9 Proposición

Sea A la matriz de incidencia nodo/arco para un grafo propio arco-conexo $\mathcal{G}$ con n nodos y sea $\mathcal{T} = \{\tilde{\mathcal{A}}, \mathcal{N}\}$ el árbol generado por $\mathcal{G}$. Entonces

$$\omega = \{A(j) : e_j \in \tilde{\mathcal{A}}\} \cup \{e_l\}$$

genera el espacio n-dimensional. Aquí l se llamará *nodo raíz.*

Demostración

Es necesario ver que ω genera e_i con $i = 1, 2, \ldots, n$ para $i \neq l$. Sea p un nodo distinto de l; por ser $\mathcal{T}$ un árbol generado por $\mathcal{G}$ existe un único camino o cadena que una p con l, con lo cual, de acuerdo con lo demostrado en una Proposición anterior, se verifica

$$\sum O_i(P)A(j_i) = e_p - e_l$$

donde $A(j_i)$ son las columnas correspondientes a los arcos del árbol. Por lo tanto,

$$e_p = e_l + \sum_i O_i(P)A(j_i)$$

y así generan el espacio euclídeo n-dimensional $\mathcal{E}^n$

5.3.10 Observación

Observamos que esta proposición asegura que la construcción de la matriz B básica para la matriz $[A, e_l]$ se logra a partir de ω teniendo siempre la matriz básica B al vector e_l puesto que al ser base de $\mathcal{E}^n$ tiene n columnas linealmente independientes, y como rango$(A) = n - 1$ debe contener a la columna e_l. Es decir que toda base B corresponde a un árbol generador con raíz de n nodos

5.3.11 Proposición

Observamos que toda base B definida sobre un grafo propio $\mathcal{G}$ es triangular inferior. En efecto, sea A la matriz de incidencia nodo/arco para el grafo propio $\mathcal{G}$ con nodo raíz l que, además, es conexo, y sea B una base cualquiera obtenida de $[A, e_l]$. Entonces, B es triangular inferior

Demostración

Sea $\mathcal{T} = \{\mathcal{A}, \mathcal{N}\}$ un árbol generador con raíz asociado con B y sea n el número de nodos de tal árbol. Como $\mathcal{G}$ es un grafo propio es $n \geq 2$ y puede asegurarse que al menos tiene dos puntos finales. Sea, entonces, N_1 un nodo final de $\mathcal{T}$ distinto de la raíz y sea e_{j_1} el arco de $\mathcal{T}$ incidente en N_1. Luego, la fila N_1, correspondiente al nodo de la matrix B tiene un elemento no nulo e igual a (± 1). Ahora bien, permutando filas y columnas de la matriz, logramos que la primera fila corresponda al nodo N_1 y la *primera columna* corresponda al arco e_{j_1} con lo cual la matriz B tiene el siguiente aspecto

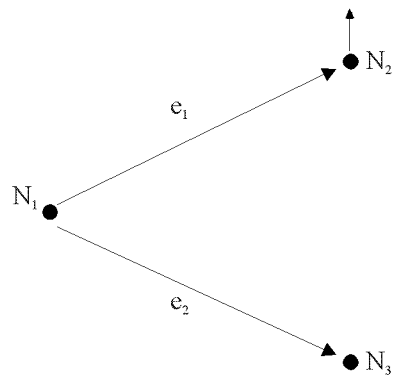
$$\left\| \begin{array}{cccc} \pm 1 & \vdots & & \}N_1 \\ \cdots & & \cdots & \\ \underbrace{\pm e_s}_{e_{j_1}} & \vdots & B^1 & \end{array} \right\|$$

Ahora, consideramos el árbol $\mathcal{T}^1 = \{\mathcal{N} - \{N_1\}, \mathcal{A} - \{e_{j_1}\}\}$ el cual tiene $(n-1)$ arcos
Si $n-1 = 1$ entonces B^1 es de 1×1 y así B es triangular. En caso contrario, si $n-1 > 1$ entonces $\mathcal{T}^1$ tiene al menos dos puntos finales, sea N_2 uno de estos dos puntos finales en $\mathcal{T}^1$ distinto del nodo raíz y sea e_{j_2} el arco en $\mathcal{T}^1$ incidente en N_2. Entonces, la fila n_2 de B^1 tiene un elemento no nulo con valor $\pm 1)$. De esta manera, repitiendo el procedimiento anterior permutando filas y columnas de B^1, hasta que la primera fila de B^1 corresponda al nodo N_2 y la primera columna de B_1 corresponda a e_{j_2}. Por lo tanto, la matriz B tiene el siguiente aspecto

$$\left\| \begin{array}{cccccc} \pm 1 & \vdots & & \vdots & & \}N_1 \\ \cdots & & \cdots & & \cdots & \\ \pm e_s & \vdots & \pm 1 & \vdots & & \}N_2 \\ \cdots & & \cdots & & \cdots & \\ \underbrace{\qquad}_{e_{j_1}} & \vdots & \underbrace{\pm e_t}_{e_{j_2}} & \vdots & B^2 & \end{array} \right\|$$

Por lo tanto, repitiendo el procedimiento n veces la matriz B es triangular inferior

5.3.12 Ejemplo III



Sea el siguiente árbol generador con raíz en el nodo N_2

$$N_2, e_1, N_1, e_2, N_3$$

correspondiente a la siguiente matriz básica

$$\begin{array}{c} \left\| \begin{array}{ccc} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 0 \end{array} \right\| \end{array} \begin{array}{l} N_1 \\ N_2 \\ N_3 \end{array}$$

Para triangular esta matriz tomamos F_3 correspondiente al nodo N_3 distinto del nodo raíz N_2 y procedemos como sigue

$$\begin{array}{cccccccccccccc} & & & & & & & & & e_4 & e_1 & & \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & -1 & 0 & 0 & N_3 \\ -1 & 0 & 1 & 0 & -1 & 1 & -1 & 0 & 0 & 1 & 1 & 0 & N_1 \\ 0 & \leftarrow -1 & 0 & -1 & 0 & 0 & 0 & -1 & 1 & 0 & 1 & 1 & N_2 \end{array}$$

5.4 Consideraciones sobre optimización del flujo

Observemos que conocida una matriz básica B y su inversa B^{-1} podemos calcular

$$\begin{aligned} z &= c_B x_B + c_N x_N \\ b &= B x_B + N x_N \\ x_B &= B^{-1} b - B^{-1} N x_N \\ z &= c_B B^{-1} b + (c_N - c_B B^{-1} N) x_N \end{aligned}$$

y a partir de estas expresiones debemos determinar las variables no básicas x_N candidatas a cambiar el flujo en la red. Para esto, es necesario analizar el signo de las componentes no básicas

$$c_N - c_B B^{-1} N = c_N - \pi N$$

donde $\pi = c_B B^{-1}$ es el vector de variables duales o nodos potenciales

Calculando las variables duales π soluciones del sistema de ecuaciones $c_B = \pi B$ con B una matriz triangular inferior y $\mathcal{T}_B$ un árbol básico con nodo raíz l obtenemos

$$\begin{aligned} &\pi_l = 0 \\ &\pi_{F(j)} - \pi_{T(j)} = e_j \end{aligned}$$

para $e_j = (F(j), T(j)) \in \mathcal{T}_B$
Por lo tanto, para los arcos no básicos se verificará

$$\pi_{F(j)} - \pi_{T(j)} - c_j \geq 0$$

con lo cual podemos caracterizar conjuntos de arcos candidatos a cambiar el flujo sobre arcos no básicos, por ejemplo, el e_k que generará un ciclo en $\mathcal{T}_B$ como sigue

$$\begin{aligned} &\tau_1 = \{e_j : x_j = 0 \text{ y } \pi_{F(j)} - \pi_{T(j)} - c_j > 0\} \\ &\tau_2 = \{e_j : x_j = u_j \text{ y } \pi_{F(j)} - \pi_{T(j)} - c_j < 0\} \end{aligned}$$

Si consideramos el arco e_k con columna $A(k) = e^{F(k)} - e^{T(k)}$ que genera un ciclo en $\mathcal{T}_B$ existe un único camino P en $\mathcal{T}_B$ que une $F(k)$ con $T(k)$ y podemos escribir

$$\sum_{i=1}^{n} O_i(P)A(j_i) = e^{F(k)} - e^{T(k)}$$

Entonces,

$$c_B B^{-1} A(k) = c_B Y$$

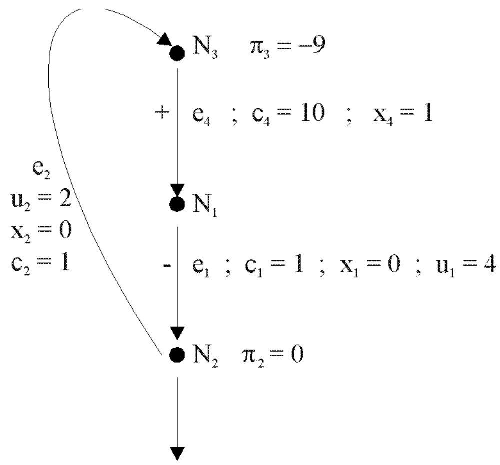
es simplemente

$$\sum_{i=1}^{n} e_{j_i} O_i(P)$$

Para determinar el vector que sale de la base, para cada arco $e_k \in \tau_1 \cup \tau_2$ definimos $\delta = 1$ si $e_k \in \tau_1$ y $\delta = -1$ si $e_k \in \tau_2$ según el flujo x_{jk} sobre el arco e_k aumente o disminuya. De esta manera, el criterio de salida de la base está dado por

$$\begin{aligned} \Delta_1 &= \min_{O_i(P)=\delta=1}\{x_{ji}, +\infty\} \\ \Delta_2 &= \min_{-O_i(P)=\delta=1}\{u_{ji} - x_{ji}, +\infty\} \\ \Delta &= \min\{\Delta_1, \Delta_2, u_k\} \end{aligned}$$

Si recordamos el ejemplo de la triangulación inferior el árbol básico estaba dado por



Nodo	*Arco*	*Costo*	π	*Variable*	*Capacidad*
N_3	$e_4(+)$	$c_4 + 10$	$\Pi_3 = -9$	$x_4 = 1$	
N_1	$e_1(-)$	$c_1 = 1$	$\Pi_1 = 1$	$x_1 = 0$	$u_1 = 4$
N_2	*Raíz*		$\Pi_2 = 0$		
	e_2	$c_2 = 1$		$x_2 = 0; e_2$	$u_2 = 2$

siendo nuestro propósito formar un ciclo insertando el arco e_2. En este caso, para tal arco se verifica

$$\Pi_2 - \Pi_3 - c_2 = 0 - (-9) - 1 = 8$$

con lo cual

$$e_k = e_2 \in \tau_1$$

con lo que $\delta = 1$. Luego, $\Delta_1 = 1; \Delta_2 = 2; \Delta = 1$
Para cambiar el flujo en todo otro arco $e_j \in P$ hacemos

$$\tilde{x}_{ji} = x_{ji} - \Delta\delta O_i(P) \ \ ; \ \ \tilde{x}_{jk} = x_{jk} + \Delta\delta$$

es decir,

$$\begin{array}{l} \tilde{x}_2 = 0 + 1 = 1 \ \ ; \ \ \tilde{x}_1 = 0 - O_1(P) = 1 \\ \tilde{x}_4 = 1 - O_2(P) = 0 \end{array}$$

con lo que reemplazamos x_4 por x_2
Al cambiar el flujo, cambió el árbol básico y también cambiaron las variables duales, es decir, a partir de

$$\tau_3 = \{e_{ji} : x_{ji} = 0 \ \text{ donde } \ O_i(P) = \delta\}$$

y

$$\tau_4 = \{e_{ji} : x_{ji} = u_{ji} \ \text{ donde } \ -O_i(P) = \delta\}$$

seleccionamos cualquier $e_m \in \tau_3 \cup \tau_4$ para reemplazar en $\mathcal{T}_B$ e_k por e_m (en nuestro caso $e_4 \in \tau_3$), recalculamos las variables duales y volvemos al paso uno. El proceso termina cuando $\tau_1 \cup \tau_2 = \emptyset$ pues se alcanzó el óptimo

5.4.1 Ejemplo IV

Minimizar

$$x_1 + x_2 + 3x_3 + 10x_4$$

sujeta a las siguientes restricciones

$$\begin{array}{rcrcrcrcrcr} x_1 & & & + & x_3 & + & x_4 & & & = & 5 \\ -x_1 & + & x_2 & & & & & + & x_5 & = & 0 \\ & - & x_2 & - & x_3 & - & x_4 & & & = & -5 \end{array}$$
$$0 \le x_1 \le 4 \ ; \ 0 \le x_2 \le 2 \ ; \ 0 \le x_3 \le 4 \ ; \ 0 \le x_4 \le 10 \ ; \ 0 \le x_5 \le 1$$

Etapa 0 -Inicialización

$$\begin{array}{ll} x_B = [x_1\, x_4\, x_5] & = [0\,1\,0] \\ x_n = [x_2\, x_3] & = [0\,4] \end{array}$$

Entonces

$$B = \left\| \begin{array}{ccc} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 0 \end{array} \right\| ; B^{-1} = \left\| \begin{array}{ccc} 1 & 0 & 1 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \end{array} \right\| ; N = \left\| \begin{array}{cc} 0 & 1 \\ 1 & 0 \\ -1 & -1 \end{array} \right\|$$

Etapa 0 - Costos en la Iteración 1

Con $[x_1\, x_2\, x_3\, x_4\, x_5] = [0\,0\,4\,1\,0]$

$$c_n - c_B B^{-1} N = [1\,3] - [1\,10\,0] \left\| \begin{array}{ccc} 1 & 0 & 1 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \end{array} \right\| \left\| \begin{array}{cc} 0 & 1 \\ 1 & 0 \\ -1 & -1 \end{array} \right\| = [-8\ -7]$$

Entonces, $\tau_1 = \{1\}; \tau_2 = \emptyset; k = 1; \delta = 1$

Etapa 2 - Test del Cociente

$$y = B^{-1} N(1) = \left\| \begin{array}{ccc} 1 & 0 & 1 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \end{array} \right\| \left\| \begin{array}{c} 0 \\ 1 \\ -1 \end{array} \right\| = \left\| \begin{array}{c} -1 \\ +1 \\ 0 \end{array} \right\|$$

Con lo cual

$$\Delta_1 = 1 \ ; \ \Delta_2 = 4 \ ; \ \Delta = \min\{1, 4, 2\} = 1$$

Etapa 3 - Actualización del Flujo

$$x_N = x_2 = 0 + 1 = 1$$
$$x_B = [x_1\, x_4\, x_5] = [0\,1\,0] - [-1\,1\,0] = [1\,0\,0]$$

Etapa 4 - Cambio de base

Ahora $\tau_3 = \{2\}$; $\tau_4 = \emptyset$, entonces $N(1)$ reemplaza a $B(2)$, de ahí que

$$B = \begin{Vmatrix} 1 & 0 & 0 \\ -1 & 1 & 1 \\ 0 & -1 & 0 \end{Vmatrix} \quad ; \quad B^{-1} = \begin{Vmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \end{Vmatrix}$$

$$x_B = [x_1\, x_2\, x_3] \qquad ; \qquad x_N = [x_3\, x_4]$$

5.4.2 Iteración 2

Etapa 1 - Costos en la Iteración 2

Con $[x_1\, x_2\, x_3\, x_4\, x_5] = [1\,1\,4\,0\,0]$

$$c_N - c_B B^{-1} N = [3\,10] - [1\,10] \begin{Vmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 1 \end{Vmatrix} \begin{Vmatrix} 1 & 1 \\ 0 & 0 \\ -1 & -1 \end{Vmatrix} = [1\,8]$$

Entonces, $\tau_1 = \emptyset; \tau_2 = \{1\}; k = 1; \delta = -1$.

Etapa 2 - Test del Cociente

$$y = B^{-1}N(1) = \begin{Vmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 1 \end{Vmatrix} \begin{Vmatrix} 1 \\ 0 \\ -1 \end{Vmatrix} = \begin{Vmatrix} 1 \\ 1 \\ 0 \end{Vmatrix}$$

con lo cual

$$\Delta_1 = \infty \; ; \; \Delta_2 = \min\{3, 1\} \; ; \; \Delta = \min\{\infty, 1, 4\} = 1$$

Etapa 3 - Actualización del Flujo

$$x_N = x_3 = 4 + 1(-1) = 3$$
$$x_B = [x_1\, x_2\, x_3] = [1\,1\,0] - 1(-1)[1\,1\,0] = [2\,2\,0]$$

Etapa 4 - Cambio de Base

Ahora, $\tau_3 = \emptyset$; $\tau_4 = \{2\}$. Entonces $N(1)$ reemplaza a $B(2)$, de ahí que

$$= \begin{Vmatrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 0 \end{Vmatrix} \quad ; \quad B^{-1} = \begin{Vmatrix} 1 & 0 & 1 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \end{Vmatrix}$$

$$x_B = [x_1\, x_3\, x_5] \quad ; \quad x_N = [x_2\, x_4]$$

5.4.3 Iteración 3

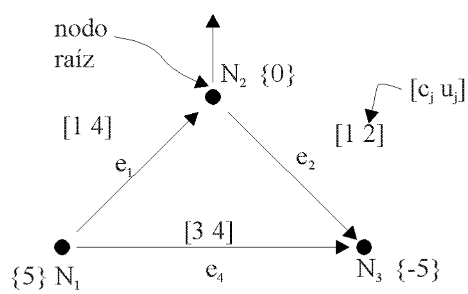
Etapa 1 - Costos en la Iteración 3

Con $[x_1\, x_2\, x_3\, x_4\, x_5] = [2\,2\,3\,0\,0]$

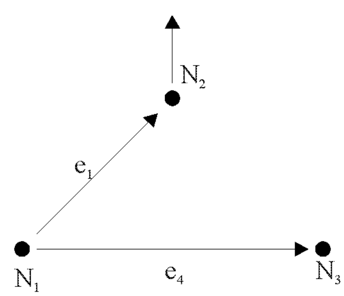
$$c_N - c_B B^{-1} N = [1\,10] - [1\,3\,0] \begin{Vmatrix} 1 & 0 & 1 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \end{Vmatrix} \begin{Vmatrix} 1 & 1 \\ 1 & 0 \\ -1 & -1 \end{Vmatrix} = [1\,7]$$

Entonces, $\tau_1 \cup \tau_2 = \emptyset$ y se ha alcanzado el óptimo

El grafo asociado con el Ejemplo IV tiene los siguientes árboles generados con raíces y las siguientes bases trianguladas son



a) Árbol básico para la iteración 1 es

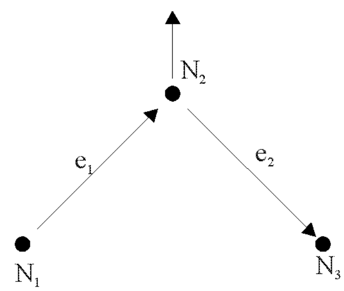


$$N_2, e_1, N_1, e_2, N_3$$

y la matriz básica asociada triangulada inferiormente dada por

$$\begin{array}{c} \begin{array}{ccc} e_4 & e_1 & \end{array} \\ \left\| \begin{array}{ccc} -1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & -1 & 1 \end{array} \right\| \begin{array}{c} N_3 \\ N_1 \\ N_2 \end{array} \end{array}$$

(b) Árbol básico para la Iteración 2 es

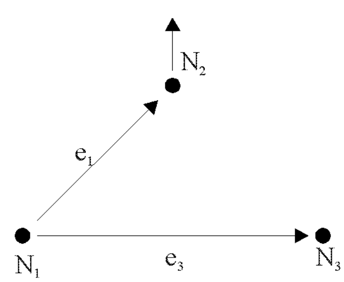


$$N_1, e_1, N_2, e_2, n_3$$

y la matriz básica asociada triangulada inferiormente dada por

$$\begin{array}{c} \begin{array}{ccc} e_1 & e_2 & \end{array} \\ \left\| \begin{array}{ccc} -1 & 0 & 0 \\ 0 & -1 & 0 \\ -1 & 1 & 1 \end{array} \right\| \begin{array}{c} N_1 \\ N_3 \\ N_2 \end{array} \end{array}$$

c) Árbol básico para la Iteración 3 es



$$N_2, e_1, N_1, e_3, N_3$$

y la matriz básica asociada triangulada inferiormente dada por

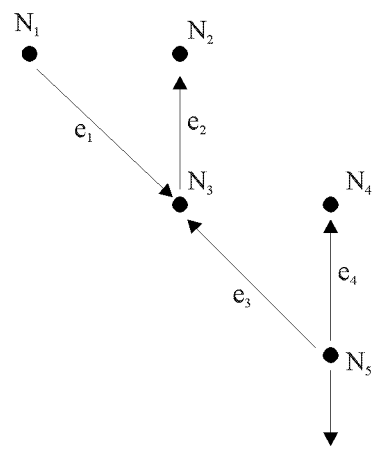
$$\begin{array}{c|ccc|l} & e_3 & e_1 & & \\ & -1 & 0 & 0 & N_3 \\ & 1 & 1 & 0 & N_1 \\ & 0 & -1 & 1 & N_2 \end{array}$$

5.4.4 Ejercicio

Diseñar e implementar un algoritmo para la triangulación de una matriz básica en un grafo

5.4.5 Ejemplo V

Consideremos la siguiente matriz básica (asociada a un árbol generado con raíz)



$$B = \left\|\begin{array}{ccccc} e_1 & e_4 & e_2 & e_3 & a \\ 1 & & & & \\ & & -1 & & \\ -1 & & +1 & & \\ & -1 & & -1 & \\ & 1 & & 1 & 1 \end{array}\right\| \begin{array}{l} \\ N_1 \\ N_2 \\ N_3 \\ N_4 \\ N_5 \end{array}$$

Entonces, $\pi B = c_B$ se reduce al siguiente sistema triangular

$$\begin{array}{cccccl} \pi_1 & & & -\pi_3 & & = c_B^1 \\ & -\pi_4 & & & +\pi_5 & = c_B^4 \\ & & -\Pi_2 & +\pi_3 & & = c_B^2 \\ & & & -\pi_3 & +\pi_5 & = c_B^3 \\ & & & & \pi_5 & = 0 \end{array}$$

Por cierto, este sistema puede ser resuelto por sustitución comenzando con $\Pi_5 = 0$. En general, para una base B y un árbol básico $\mathcal{T}_B$ con nodo raíz l, $\Pi B = c_B$ se reduce a un sistema triangular pues B es triangular dado por

$$\begin{array}{lll} \pi_l & & = 0 \\ \pi_{F(j)} & -\pi_{T(j)} & = e_j \quad \text{para} \;\; e_j \in \mathcal{T}_B \end{array}$$

5.4.6 Ejercicios

Ejercicio 1

Diseñar e implementar un algoritmo para la determinación de las variables duales

Ejercicio 2

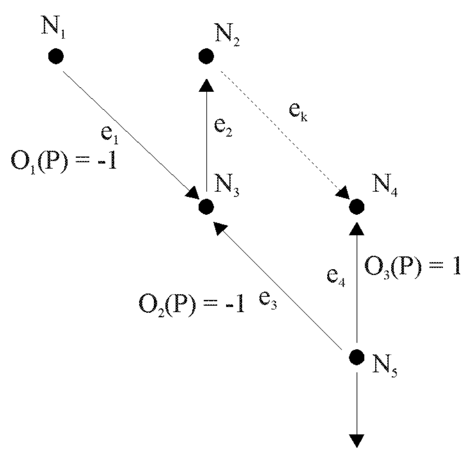
De acuerdo con el árbol básico del Ejemplo V supongamos que el arco fuera del árbol es $e_k = (2, 4)$. Entonces

$$P = \{2, e_2, 3, e_3, 5, e_4, 4\}$$

y

$$O(P) = \{-1, -1, 1\}$$

Determinar el ciclo formado por $(2, 4)$



5.4.7 Especialización del método primal sobre un grafo

El algoritmo correspondiente consta de las siguientes etapas

Etapa 0 - Inicialización

Sean $[x_B, x_N]$ la solución factible básica con el árbol básico $\mathcal{T}_B$. Calcular las variables de π.

Etapa 1 - Costos o Precios

Sean

$$\tau_1 = \{e_j : x_j = 0 \text{ y } \pi_{F(j)} - \pi_{T(j)} - c_j > 0\}$$

y

$$\tau_2 = \{e_j : x_j = u_j \text{ y } \pi_{F(j)} - \pi_{T(j)} - c_j < 0\}$$

si $\tau_1 \cup \tau_2 = \emptyset$ entonces el algoritmo termina con $[x_B, x_N]$ la solución óptima
En caso contrario, seleccionamos $e_k \in \tau_1 \cup \tau_2$ y hacemos

$$\delta = \begin{cases} +1 & \text{si } e_k \in \tau_1 \\ -1 & \text{si } e_k \in \tau_2 \end{cases}$$

Etapa 2 - Test del Cociente

Sea $P = \{S_1, e_{j_1}, S_2, e_{j_2}, \ldots, S_n, e_{j_n}, S_{n+1}\}$ el camino que une $F(k)$ con $T(k)$ en $\mathcal{T}_B$.
Hacemos

$$\begin{aligned} &\Delta_1 = \min_{O_i(P)=\delta}\{x_{ji}, \infty\} \\ &\Delta_2 = \min_{-O_i(P)=\delta}\{u_{ji} - x_{ji}, \infty\} \\ &\Delta = \min\{\Delta_1, \Delta_2, u_k\} \end{aligned}$$

Etapa 3 - Actualización del Flujo

Hacemos $\tilde{x}_k = x_k + \Delta\delta$. Para todo $e_j \in P$ hacemos $\tilde{x}_{ji} = x_{ji} - \Delta\delta O_i(P)$

Si $\Delta = u_k$ entonces volvemos a la etapa 1.

Etapa 4 - Actualización del árbol y de las variables duales

Sean

$$\tau_3 = \{e_{ji} : x_{ji} = 0 \text{ donde } O_i(P) = \delta\}$$

y

$$\tau_4 = \{e_{ji} : x_{ji} = u_{ji} \text{ donde } -O_i(P) = \delta\}$$

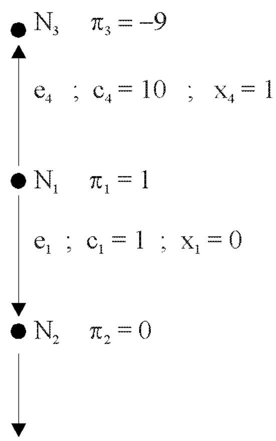
Seleccionamos cualquier $e_m \in \tau_3 \cup \tau_4$. Reemplazamos en $\mathcal{T}_B$ con e_k, actualizamos las variables duales y retornamos a la etapa 1.

Ejemplo VI

Resolvamos el problema del Ejemplo IV con el algoritmo del método primal especializado sobre un grafo

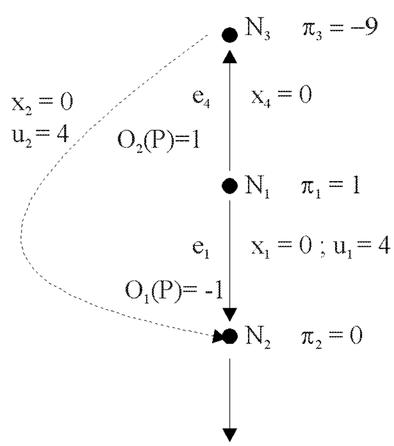
Primero damos los árboles básicos y los tests del cociente correspondientes a los ciclos, a saber

a) Árbol básico para la Iteración 1



Nodo	*Arco*	*Costo*	Π	*Variable*
N_3	e_4	$c_4 = 10$	$\Pi_3 = -9$	
N_1	e_1	$c_1 = 1$	$\Pi_1 = 1$	$x_1 = 0$
N_2			$\Pi_2 = 0$	

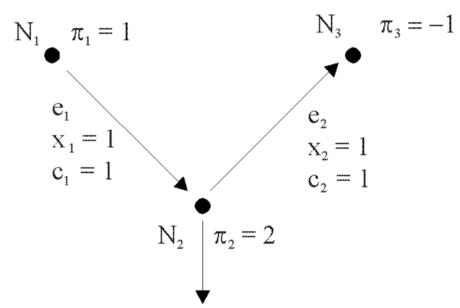
y el Test del cociente y ciclo para la Iteración 2 son



$Nodo$	$Arco$	$O_i(P)$	π	$Variable$	$Capacidad$
N_3	e_4	$O_2(P) = 1$	$\Pi = -9$	$x_4 = 0$	
N_1	e_1	$O_1(P) = -1$	$\Pi_1 = 1$	$x_1 = 0$	$u_1 = 4$
N_2				$\Pi_2 = 0$	

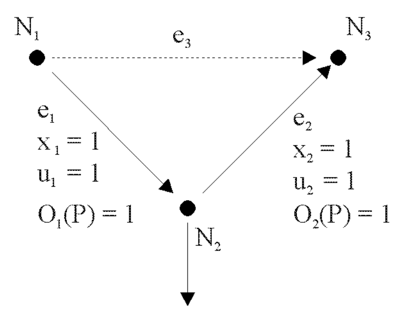
El ciclo lo establece el arco e_2 con $x_2 = 0$ y $u_2 = 2$

b) Árbol básico para la Iteración 2



$Nodo$	$Arco$	$Costo$	π	$Variable$
N_1	e_1	$c_1 = 1$	$\pi_1 = 1$	$x_1 = 1$
N_2			$\pi_2 = 0$	
N_3	e_2	$c_2 = 1$	$\pi_3 = -1$	$x_2 = 1$

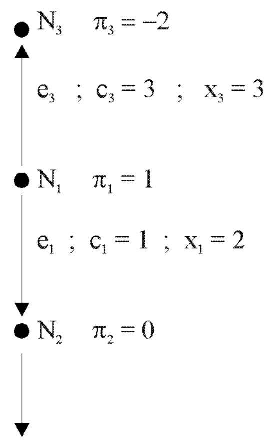
y el Test del cociente y ciclo para la Iteración 2 son



$Nodo$	$Arco$	$O_i(P)$	$Variable$	$Capacidad$
N_1	e_1	$O_1(P) = 1$	$x_1 = 1$	$u_1 = 1$
N_3	e_2	$O_2(P) = 1$	$x_2 = 1$	$u_2 = 1N_2$

El ciclo lo establece el arco e_3

c) Árbol básico para la Iteración 3



Nodo	*Arco*	*Costo*	π	*Variable*
N_3	e_3	$c_3 = 3$	$\pi_3 = 2$	$x_3 = 3$
$Nodo_1$	e_1	$c_1 = 1$	$\pi_1 = 1$	$x_1 = 2$
N_2			$\pi_2 = 0$	

5.4.8 Ejecución del algoritmo

Etapa 0

Sean

$$[x_1\, x_2\, x_3\, x_4\, x_5] = [0\, 0\, 4\, 1\, 0]$$

y

$$x_B = [x_1\, x_4\, x_5] \;\; ; \;\; x_N = [x_2\, x_3]$$

5.4.9 Iteración 1

Etapa 1 - Costos

Para $e_2 : \pi_2 - \pi_3 - e_2 = 0 - (-9) - 1 = 8$ con lo cual $e_2 \in \tau_1$
Para $e_3 : \pi_1 - \pi_3 - e_3 = 1 - (-9) - 3 = 7$ con lo cual $e_3 \notin \tau_1$ ó τ_2
También, $\tau_1 = \{e_2\}; \tau_2 = \emptyset$. Entonces, $e_k = e_2$ y $\delta = 1$

Etapa 2 - Test del Cociente

Sea $P = \{2, e_1, 1, e_4, 3\}$

$$\Delta_1 = \min\{x_4, \infty\} = \min\{1, \infty\} = 1$$
$$\Delta_2 = \min\{u_1 - x_1, \infty\} = \min\{4 - 0, \infty\} = 4$$
$$\Delta = \min\{1, 4, 2\} = 1$$

Etapa 3 - Actualización del Flujo

$$\begin{aligned}\tilde{x}_2 &= 0 + 1(1) = 1\\ \tilde{x}_1 &= 0 - 1(1)(-1) = 1\\ \tilde{x}_4 &= 0 - 1(1)(1) = 0\end{aligned}$$

Etapa 4 - Actualización del árbol y de las variables duales

Sean $\tau_3 = \{e_4\}$; $\tau_4 = \emptyset$. Entonces, $e_m = e_4$

$$x_B = [x_1\, x_2\, x_5] \;;\; x_N = [x_3\, x_4]$$

5.4.10 Iteración 2

Etapa 1 - Costos

Sea $[x_1\, x_2\, x_3\, x_4\, x_5] = [1\,1\,4\,0\,0]$
Para $e_3 : \pi_1 - \pi_3 - e_3 = 1 - (-1) - 3 = -1$ entonces $e_3 \in \tau_2$
Para $e_4 : \pi_1 - \pi_3 - e_4 = 1 - (-1) - 10 = -8$ con lo cual $e_4 \notin \tau_1$ ó τ_2
Entonces, $e_k = e_3$; $\delta = -1$

Etapa 2 - Test del cociente

Sea $P = \{1, e_1, 2, e_2, 3\}$

$$\begin{aligned}\Delta_1 &= \min\{\infty\} = \infty\\ \Delta_2 &= \min\{4-1, 2-1, \infty\} = 1\\ \Delta_3 &= \min\{\infty, 1, 4\} = 1\end{aligned}$$

Etapa 3 - Actualización del Flujo

$$\begin{aligned}\tilde{x}_3 &= 4 + 1(-1) = 3\\ \tilde{x}_1 &= 1 - 1(-1)1 = 2\\ \tilde{x}_2 &= 1 - 1(-1)1 = 2\end{aligned}$$

Etapa 4 - Actualización del árbol y de las variables duales

Sean $\tau_3 = \emptyset$; $\tau_4 = \{e_2\}$. Entonces, $e_m = e_2$

$$x_B = [x_1\, x_3\, x_5] \;;\; x_N = [x_2\, x_4]$$

5.4.11 Iteración 3

Etapa 1 - Costos

Sea $[x_1\, x_2\, x_3\, x_4\, x_5] = [2\,2\,3\,0\,0]$
Para $e_2 : \pi_2 - \pi_3 - e_2 = 0 - (-2) - 1 = 1$ entonces $e_2 \notin \tau_1 \cup \tau_2$
Para $e_4 : \pi_1 - \pi_3 - e_4 = 1 - (-2) - 10 = -7$ con lo cual $e_4 \notin \tau_1 \cup \tau_2$
Por lo tanto, hemos obtenido el óptimo

5.4.12 Observación

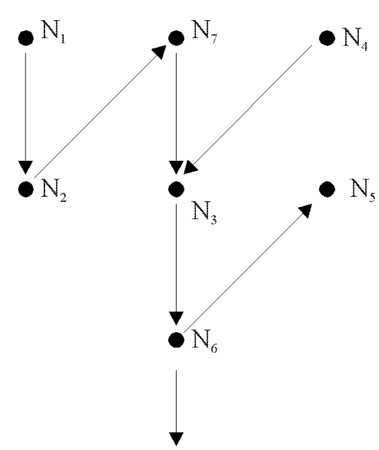
Bajo la suposición de ser $\Delta > 0$ en cada iteración garantizamos la convergencia de este algoritmo. Cuando $\Delta = 0$ simplemente revisamos la partición para obtener una nueva base B y continuamos.
La dificultad reaparece después de un número finito de iteraciones con $\Delta = 0$ pues el algoritmo comienza a ciclar

5.4.13 Ejercicios

Ejercicio 1

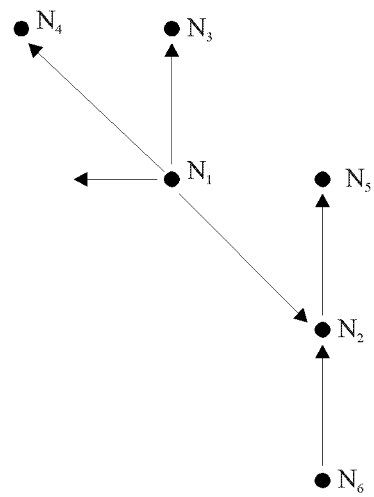
Empleando el algoritmo diseñado e implemetado para la triangulación de una matriz básica de un grafo describir las matrices triangulares inferiores correspondientes a los siguientes árboles dados por sus matrices asociadas

a) Con raíz en el nodo N_6



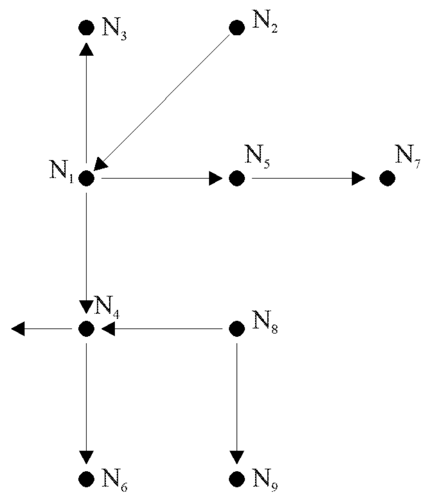
$Nodo$	$Arcos$					
N_1	1	0	0	0	0	0
N_2	-1	1	0	0	0	0
N_3	0	0	-1	-1	1	0
N_4	0	0	0	1	0	0
N_5	0	0	0	0	0	-1
N_6	0	0	0	0	-1	1
N_7	0	-1	1	0	0	0

b) Con raíz en el nodo N_1



$Nodo$	$Arcos$				
N_1	1	1	1	0	0
N_2	0	0	-1	1	-1
N_3	0	-1	0	0	0
N_4	-1	0	0	0	0
N_5	0	0	0	-1	0
N_6	0	0	0	0	1

c) Con raíz en el nodo N_4



Nodo	*Arcos*						
N_1	1	1	1	0	0	0	0
N_2	0	0	0	0	0	0	0
N_3	-1	0	0	0	0	0	0
N_4	0	-1	0	0	-1	1	0
N_5	0	0	-1	1	0	0	0
N_6	0	0	0	0	0	-1	0
N_7	0	0	0	-1	0	0	0
N_8	0	0	0	0	1	0	1
N_9	0	0	0	0	0	0	-1

Sugerencia

Graficar los grafos correspondientes

Ejercicio 2

A partir del algoritmo diseñado e implementado para la determinación de las variables duales, determinar las variables duales para cada una de las siguientes bases

a)

Arco Número j	$F(j)$	$T(j)$	Costo unitario c_j
1	6	5	10
2	3	6	8
3	7	3	6
4	4	3	9
5	6	2	7
6	1	2	3
7	6	0	0

b)

Arco Número j	$F(j)$	$T(j)$	Costo unitario c_j
1	1	0	0
2	1	3	20
3	1	4	5
4	1	2	15
5	2	5	10
6	6	2	0

Ejercicio 3

Implementar, por computadora, el algoritmo dado en el Ejemplo VI.

Ejercicio 4

Resolver el siguiente problema, empleando una variable artificial y un nodo artificial

- Minimizar $2x_1 + 4x_2 + x_3 + x_4 + 9x_5 - 10x_6$ sujeta a las siguientes restricciones:

$$\begin{array}{rcrcrcrcrcrcl}
x_1 & + & x_2 & & & & & & & & & \leq & 6 \\
-x_1 & & & - & x_3 & + & x_4 & + & x_5 & & & \leq & 6 \\
 & - & x_2 & + & x_3 & - & x_4 & & & + & x_6 & \leq & -3 \\
 & & & & & & & - & x_5 & - & x_6 & \leq & -5
\end{array}$$

$$x_1 \in [1,3] \; ; \; x_2 \in [2,3] \; ; \; x_3 \in [2,5]$$

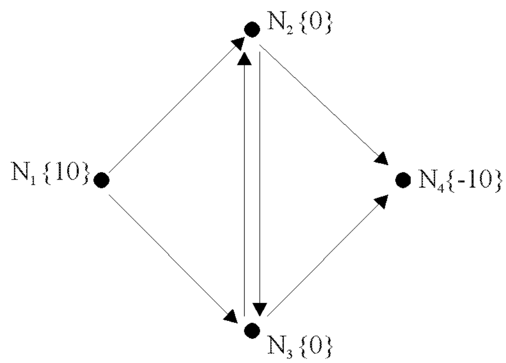
$$x_4 \in [0,3] \; ; \; x_5 \in [1,3] \; ; \; x_6 \in [0,3]$$

<u>*Sugerencia*</u>
Agregar variables slack, una por cada restricción, y una nueva restricción dada por la suma de las otras restricciones. Además, hacer una sustitución de variables del tipo $y_1 = x_1 + 1$ para dar al problema la forma conocida

Ejercicio 5

A partir de la siguiente matriz, asociada a un grafo,

$$\left\|\begin{array}{ccccc}
Nodo & Arcos & & & \\
N-1 & 1 & 1 & 0 & 0 \\
N_2 & -1 & 0 & 1 & 0 \\
N_3 & 0 & -1 & 0 & 1 \\
N_4 & 0 & 0 & -1 & -1
\end{array}\right\|$$



Suponer que requerimos que el flujo a través del nodo N_3 sea al menos 3 y no mayor que 5. Entonces, agregando nuevos arcos y/o nodos, reformular el problema como un problema de grafos en el cual la restricción de la capacidad de este nodo sea reforzada

Ejercicio 6

Dado el siguiente problema reformularlo como una problema sobre un grafo con arcos no dirigidos

- Minimizar $x_1 + x_2 + 3x_3 + x_4 + 10x_5$ sujeta a las siguientes condiciones:

$$\begin{array}{rcrcrcrcrcr} -x_1 & & & - & x_3 & & & & & = & 10 \\ x_1 & + & x_2 & & & & & - & x_5 & = & 0 \\ & - & x_2 & + & x_3 & + & x_4 & & & = & 0 \\ & & & & & & x_4 & + & x_5 & = & -10 \end{array}$$

$$x_i \in [-7, 7] \quad \forall \ i = 1, 2, 3, 4, 5$$

y resolverlo

5.5 Algoritmo de Descomposición

Este algoritmo para la programación en redes "out of kilter" fue desarrollado en 1961 por Fulkerson para la optimización del flujo con costo mínimo en problemas del tipo

- minimizar x=c x sujeta a $Ax = b$, $0 \leq x \leq u$, $u > 0$

Denotemos por $\mathcal{G} = \{\mathcal{A}, \mathcal{N}\}$ el grafo asociado con el problema propuesto. Para este problema, las *condiciones de optimalidad de Kuhn-Tucker* pueden establecerse como sigue $(\forall e_j \in \mathcal{A})$

a) $Ax = b$

b) $\pi_{F(j)} - \pi_{T(j)} - c_j = \mu_j - \lambda_j$

c) $(x_j - u_j)\mu_j = 0$

d) $x_j\lambda_j = 0$

e) $\mu_j \geq\,;\ \lambda_j \geq 0$

Es decir, si obtenemos los vectores (x, π, μ, λ) satisfaciendo (a), (b), (c), (d) y (e) entonces x es el óptimo para el problema propuesto

Denotemos por $\tilde{c}_j = \pi_{F(j)} - \pi_{T(j)} - c_j$; entonces, las indeterminadas λ y μ pueden eliminarse del sistema anterior a partir de los siguientes casos

a) Supongamos que, para algún arco e_j, es $\tilde{c}_j < 0$ con lo cual es $\lambda_j > \mu_j \geq 0$ por (b) y, además, es $x_j = 0$ por (d). Por otra parte, $\lambda_j = -\tilde{c}_j\,;\ \mu_j = 0\,;\ x_j = 0$ resuelve (b), (c), (d) y (e) para el arco e_j

b) Supongamos que, para algún arco e_j, es $\tilde{c}_j > 0$ con lo cual es $\mu_j > \lambda_j \geq 0$ por (b) y, además, es $x_j = u_j$ por (c). Por otra parte, $\mu_j = \tilde{c}_j\,;\ \lambda_j = 0\,;\ x_j = u_j$ resuelve (b), (c), (d) y (e) para el arco e_j

c) Supongamos que, para que algún arco e_j, es $\tilde{c}_j = 0$ con lo cual es $\mu_j = \lambda_j \geq 0$. Entonces, $\mu_j = \lambda_j = 0$ resuelve (b),(c),(d) y (e)
A partir de estos tres casos podemos reescribir las condiciones de optimalidad da la siguiente manera

a) $Ax = b$

b) Para el arco e_j tenemos $c_j \begin{cases} < 0 & \text{si} \quad x_j = 0 \\ = 0 & \text{si} \quad 0 \leq x_j \leq u_j \\ > 0 & \text{si} \quad x_j = u_j \end{cases}$

Por lo tanto, x es un punto optimal para el problema propuesto si y sólo si existe un vector π tal que (x, π) satisfacen (a) y (b)
La estrategia básica del algoritmo de descomposición consiste en lo siguiente
Comienza con cualquier vector π de variables duales y con un conjunto de flujos x satisfaciendo las condiciones $Ax = b$; $0 \leq x \leq u$. Entonces, si (x, π) satisfacen (a) y (b), x ya es el óptimo. Si esto no sucede, se cambian los flujos, las variables duales o ambos hasta alcanzar el óptimo

Sea (x, π) dado y sea e_j algún arco. Entonces, si las condiciones (a) y (b) se satisfacen para este arco e_j, decimos que el arco e_j está en arreglo; de lo contrario decimos ques está fuera de arreglo

En la siguiente table aparecen las posibles condiciones del arco e_j (las zonas con guiones indican condiciones de arreglo para el arco)

	$\tilde{c}_j < 0$	$\tilde{c}_j = 0$	$\tilde{c}_j > 0$
$x_j = u_j$		$------$	$------$
$0 < x_j < u_j$		$------$	
$x_j = 0$	$------$	$------$	

Ahora bien, a fin de asegurar la convergencia del algoritmo, es necesario contar con una medida de la distancia a la optimalidad puesto que si se construye un algoritmo que, periódicamente, (en intervalos finitos) reduce tal distancia, el algoritmo convergerá. Existen distintas medidas de tal distancia para este problema. Una de ellas es la llamada "número de arreglo K_j para el arco j" definida como

> "El mínimo cambio de flujo sobre el arco necesario para estar en arreglo."

El número de arreglo de una solución (x, π) está dado por $\sum_{j \in \mathcal{A}} K_j$ donde $K_j \geq 0 \ \ \forall\, j$. Por cierto, una solución cuyo número de arreglo sea nulo es optimal

La estrategia básica del algoritmo de descomposición involucra cambios de (x, π) de modo tal que se verifiquen las siguientes condiciones

a) El número de arreglos de un arco nunca crece

b) En intervalos finitos el números de arreglos de algún arco se reduce por un entero

Para cada una de las nueve condiciones dada en la tabla anterior se define un número de arreglo en la siguiente tabla

	$\tilde{c}_j < 0$	$\tilde{c}_j = 0$	$\tilde{c}_j > 0$
$x_j = u_j$	x_j	0	0
$0 < x_j < u_j$	x_j	0	$u_j - x_j$
$x_j = 0$	0	0	$u_j - x_j$

Este algoritmo tiene dos fases: la fase primal (1) para el cambio de flujo, y la fase dual (2) para reducir el valor de la variable dual con el propósito de reducir el número de arreglo. A ambas fases se las itera hasta alcanzar $\sum_{j \in \mathcal{A}} K_j$

5.5.1 Fase primal para el cambio de flujo

Durante esta fase las variables duales permanecen fijas y los flujos que cambian están siempre asociados con arcos en el ciclo

$$C = \{S_1, e_{j_1}, S_2, e_{j_2}, \ldots, S_n, e_{j_n}, S_{n+1}\}$$

del grafo $\mathcal{G} = \{\mathcal{A}, \mathcal{N}\}$.

Sabemos que la orientación de la sucesión de los arcos en tal ciclo satisface

$$\sum_{i=1}^{n} O_i(c)A(ji) = 0$$

y haciendo

$$y_K = \begin{cases} O_i(c) & \text{si } e_{j_i} = e_k \\ 0 & \text{en caso contrario} \end{cases}$$

tenemos $Ay = 0$
En esta fase, el problema se plantea de la siguiente forma
Dado cualquier arco e_s fuera de arreglo pretendemos hallar un ciclo que incluya e_s y que permita un incremento en el flujo según la siguiente tabla

	$\tilde{c}_j < 0$	$\tilde{c}_j = 0$	$\tilde{c}_j > 0$
$x_j = u_j$	decrece por x_j	decrece por x_j	no se permite cambio
$0 < x_j < u_j$	decrece por x_j	decrece por x_j	crece por $u_j - x_j$
$x_j = 0$	no se permite cambio	crece por $u_j - x_j$	crece por $u_j - x_j$

Supongamos que el arco fuera de arreglo e_s tiene $\tilde{c}_s > 0$. Entonces la estrategia para determinar si tal ciclo existe involucra el desarrollo de un árbol especial $\mathcal{T}$ con raíz $F(s)$. Tal árbol se construye de la siguiente forma
Si el nodo $i \in \mathcal{T}$ entonces se permite un incremento del flujo en el único camino desde i hasta la raíz. Además, si $T(s) \in \mathcal{T}$, entonces el ciclo C es el único camino en $\mathcal{T}$ desde $T(s)$ hasta $F(s)$ junto con e_s
El algoritmo para la fase primal comienza con un arco e_s fuera de arreglo y tiene las siguientes etapas

5.5.2 Fase Primal

Etapa 0 - Inicialización

Si $\tilde{c}_s < 0$ entonces $\tilde{\mathcal{N}} = \{T(s)\}$ y $\Delta_{T(s)} = x_s$ y si $\tilde{c}_s > 0$ entonces $\tilde{\mathcal{N}} = \{F(s)\}$ y $\Delta_{F(s)} = u_s - x_s$.
Además, $\tilde{\mathcal{A}} = \emptyset$

Etapa 1 - Determinación de candidatos para el árbol

Sean los siguientes conjuntos de arcos

$$\psi_1 = \{e_j : e_j \neq e_s; \tilde{c}_j \geq 0; x_j < u_j; F(j) \notin \tilde{\mathcal{N}}; T(j) \in \tilde{\mathcal{N}}\}$$

$$\psi_2 = \{e_j : e_j \neq e_s; \tilde{c}_j < 0; x_j > 0; F(j) \in \tilde{\mathcal{N}}; T(j) \notin \tilde{\mathcal{N}}\}$$

Si $\psi_1 \cup \psi_2 = \emptyset$ entonces concluimos que tal ciclo c no existe y finalizamos el algoritmo

Etapa 2 - Agregar un nuevo arco al árbol

Elegimos un arco $e_k \in \psi_1 \cup \psi_2$ entonces si
$e_k \in \psi_1$ hacemos $\Delta_{F(k)} = \min\{\Delta_{T(k)}, u_k - x_k\}$ y
si $e_k \in \psi_2$ hacemos $\Delta_{T(k)} = \min\{\Delta_{F(k)}, x_k\}$
Modificamos $\tilde{\mathcal{N}}$ por $\tilde{\mathcal{N}} \cup \{F(k), T(k)\}$ y $\tilde{\mathcal{A}}$ por $\tilde{\mathcal{A}} \cup \{e_k\}$.
Entonces, si $\{F(s), T(s)\} \in \tilde{\mathcal{N}}$ vamos a la Etapa 3; de lo contrario volvemos a la Etapa 1

Etapa 3 - Abrirse Paso

Si $\tilde{c}_s < 0$, incrementamos el flujo en el ciclo mediante $\Delta_{F(s)}$ y, en caso contrario, lo incrementamos mediante $\Delta_{T(s)}$

5.5.3 Fase dual para reducir el valor de las variables duales

Si en la fase primal se concluye que no existe ciclo, entonces se intenta reducir el número de arreglo para la solución dado por $\sum_{j\in\mathcal{A}} K_j$ mediante el ajuste de las variables duales manteniendo fijos los flujos
Sea $\mathcal{T} = \{\tilde{\mathcal{A}}, \tilde{\mathcal{N}}\}$ el árbol desarrollado en la fase primal. En la fase dual se reduce cada variable dual asociada con un nodo en $\tilde{N}$ mediante un monto $\theta > 0$ determinado de la siguiente manera

Sea $e_r \in \tilde{\mathcal{A}}$ y supongamos que $\hat{\pi}_{F(r)} = \pi_{F(r)} - \theta$ y que $\hat{\pi}_{T(r)} = \pi_{T(r)} - \theta$ con lo cual es:

$$\tilde{\pi}_{F(r)} - \tilde{\pi}_{T(r)} = \pi_{F(r)} - \pi_{F(r)}$$

Por lo tanto, la reducción de cada variable dual correspondiente a un nodo en $\mathcal{T}$ no afecta los números de arreglo para los arcos en $\mathcal{T}$. Los únicos arcos con número de arreglo afectado por tal cambio son aquellos que inciden sobre un nodo $\tilde{\mathcal{N}}$ y sobre un nodo en $\mathcal{N} - \tilde{\mathcal{N}}$

El objetivo de la fase dual es determinar el decrecimiento permitido en las variables duales asociados con nodos en $\mathcal{T}$ que no incrementará cualquier número de arreglo y que decrecerá al menos un número de arreglo

En las siguientes tablas damos el posible cambio para el arco e_j con $T(j) \in \tilde{\mathcal{N}}$ y $F(j) \in \mathcal{N} - \tilde{\mathcal{N}}$ y al revés, es decir, el posible cambio para el arco e_j con $F(j) \in \tilde{\mathcal{N}}$ y $T(j) \in \mathcal{N} - \tilde{\mathcal{N}}$

Decrecimiento permitido en $\pi_{T(j)}$

	$\tilde{c}_j < 0$	$\tilde{c}_j = 0$	$\tilde{c}_j > 0$
$x_j = u_j$	$-\tilde{c}_j$	∞	∞
$0 < x_j < u_j$	$-\tilde{c}_j$	$------$	$------$
$x_j = 0$	$-\tilde{c}_j$	$------$	$------$

Decrecimiento permitido en $\pi_{F(j)}$

	$\tilde{c}_j < 0$	$\tilde{c}_j = 0$	$\tilde{c}_j > 0$
$x_j = u_j$	$------$	$------$	$+\tilde{c}_j$
$0 < x_j < u_j$	$------$	$------$	$+\tilde{c}_j$
$x_j = 0$	∞	∞	$+\tilde{c}_j$

5.5.4 Fase Dual

El algoritmo para la fase dual comienza con un árbol $\mathcal{T} = \{\tilde{\mathcal{A}}, \tilde{\mathcal{N}}\}$ desarrollado en la fase primal, y tiene las siguientes etapas

Etapa 0 - Determinación de arcos incidentes sobre T

Sean los siguientes conjuntos de arcos

$$\psi_1 = \{e_j : T(j) \in \tilde{\mathcal{N}}; F(j) \notin \tilde{\mathcal{N}}; \tilde{c}_j < 0\}$$

$$\psi_2 = \{e_j : T(j) \notin \tilde{\mathcal{N}}; F(j) \in \tilde{\mathcal{N}}; \tilde{c}_j > 0\}$$

Etapa 1 - Determinación del máximo cambio permitido

Sea

$$\theta = \min_{e_j \in \psi_1 \cup \psi_2} \{|\tilde{c}_j|\}$$

Etapa 2 - Reducción de las variables duales

Sea

$$\hat{\pi}_i = \pi_i - \theta \ \ \forall\, i \notin \tilde{N}$$

Observemos que un arco $e_k \in \psi_1 \cup \psi_2$ que en la Etapa 2 de esta fase tuvo $|\tilde{c}_k| = \theta$ tendrá $\tilde{c}_k = 0$ después de esta etapa.
Luego, si $|\tilde{c}_s| \neq \theta$ y la fase primal se repitió, se podrá construir el mismo árbol que antes con el agregado de e_k y de un nuevo punto terminal.
Si $|\tilde{c}_s| = \theta$ entonces e_s estará en arreglo

5.5.5 Algoritmo de descomposición

En base a todo lo dicho, el algoritmo de descomposición puede establecerse así

Etapa 0 - Inicialización

Sea X un conjunto de flujos $Ax = b; 0 \leq x \leq u$ y sea π el vector de variables duales.

Etapa 1 - Hallar un arco fuera de arreglo

Sea e_s cualquier arco fuera de arreglo. Si todos los otros arcos están en arreglo entonces x es optimal

Etapa 2 - Fase primal

Ejecutamos la fase primal con el arco e_s. Si este algoritmo primal concluye que el ciclo no existe entonces vamos a la etapa 3. De lo contrario, volvemos a la etapa 1

Etapa 3 - Fase dual

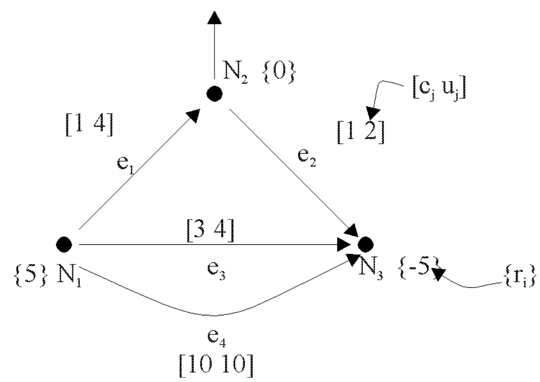
Ejecutamos el algoritmo dual con el árbol desarrollado en la Etapa 2.
Entonces, si
e_s está fuera de arreglo volvemos a la etapa 2. De lo contrario, volvemos a la etapa 1

Finalmente, observemos que en cuanto a la convergencia del algoritmo suponemos que los vectores b, u, x, c, π tienen componentes enteras
En base a esta hipótesis de integridad, cada vez que logramos abrirnos paso y cambiar el flujo de la fase primal, el número de arreglo para e_s se reduce al menos en uno. Cada vez que cambiamos las variables duales en la fase dual o

bien el árbol desarrollado en la próxima fase primal tiene al menos un nodo (y un arco) más, o bien el número de arreglo se reduce al menos en uno. De esta forma, en un número finito de etapas $\sum_{e_j \in \mathcal{A}} K_j$ puede llevarse a cero

5.5.6 Ejemplo VII

Teniendo en cuenta el problema de nuestro Ejemplo IV lo resolvemos mediante el algoritmo "out-of-kilter" como sigue



Etapa 0 - Inicialización

Sean $[x_1\ x_2\ x_3\ x_4] = [0\ 0\ 4\ 1]$ y sean $[\pi_1\ \pi_2\ \pi_3] = [5\ 0\ -1]$

Etapa 1 - Hallar el arco fuera de arreglo

Dado que $\tilde{c}_4 = -4; x_4 = 1$ resulta e_4 fuera de arreglo

5.5.7 Fase primal

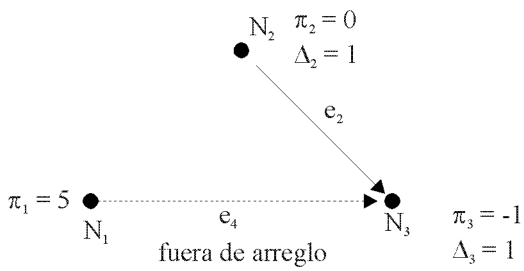
Etapa 0 - Inicialización

$\tilde{\mathcal{N}} = \{3\} \quad \Delta_3 = 1; \tilde{\mathcal{A}} = \emptyset$

Etapa 1 - Arcos candidatos

$\psi_1 = \{e_2\}; \psi_2 = \emptyset$

Etapa 2 - Agregar un nuevo arco



$e_k = e_2$; $\Delta_2 = \min\{1, 2\} = 1$; $\tilde{\mathcal{N}} = \{3, 2\}$; $\tilde{\mathcal{A}} = \{e_2\}$
Con el arco e_4 fuera de arreglo la información es la siguiente

$Nodo$	$Arco$	π	Δ
N_1	e_4	$\pi_1 = 5$	
N_3		$\pi_3 = -1$	$\Delta_3 = 1$
N_2	e_2	$\pi_2 = 0$	$\Delta_2 = 1$

Etapa 1 - Arcos candidatos

$\psi_1 = \{e_1\}; \psi_2 = \emptyset$

Etapa 2 - Agregar un nuevo arco

$e_k = 1$; $\Delta_1 = \min\{1, 4\} = 1$; $\tilde{\mathcal{N}} = \{3, 2, 1\}$; $\tilde{\mathcal{A}} = \{e_2, e_1\}$

Etapa 3 - Abrirse paso

El ciclo es $\{1, e_1, 2, e_2, 3, e_4, 1\}$ y el/los nuevos flujos son $[x_1\ x_2\ x_3\ x_4] = [1\ 1\ 4\ 0]$

Donde nuevamente hallamos un arco fuera de arreglo, por lo que debemos recomenzar la fase primal

Etapa 0 - Inicialización

$\tilde{\mathcal{N}} = \{1\} \quad \Delta_1 = 1; \tilde{\mathcal{A}} = \emptyset$

Etapa 1 - Arcos candidatos

$\psi_1 = \psi_2 = \emptyset$

5.5.8 Fase Dual

Etapa 0 - Determinación del arco incidente sobre T (árbol)

$\psi_1 = \emptyset$; $\psi_2 = \{e_1, e_3\}$

Etapa 1 - Determinación de máximo cambio

Sea $\theta = \min\{|\tilde{c}_1|, |\tilde{c}_3|\} = \min\{4, 3\} = 3$

Etapa 2 - Reducción de variables duales

$\pi_1 = 5 - 3 = 2$

Ahora debemos volver nuevamente a la fase primal

5.5.9 Fase Primal

Etapa 0 - Inicialización

$\tilde{\mathcal{N}} = \{1\}$; $\Delta_1 = 3$; $\tilde{\mathcal{A}} = \emptyset$

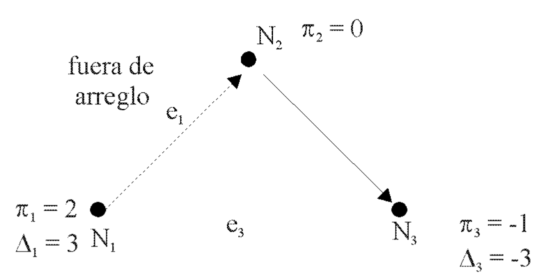
Etapa 1 - Arcos candidatos

$\psi_1 = \emptyset$; $\psi_2 = \{e_3\}$

Etapa 2 - Agregar un nuevo arco

$e_k = e_3$; $\Delta_3 = \min\{3, 4\} = 3$; $\tilde{\mathcal{N}} = \{1, 3\}$; $\tilde{\mathcal{A}} = \{e_3\}$

Con el arco e_1 fuera de arreglo la información es la siguiente



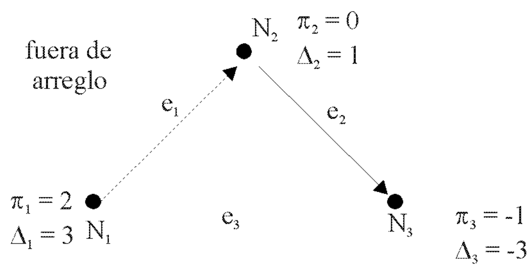
$Nodo$	$Arco$	π	Δ
N_1	e_1	$\pi_1 = 2$	$\Delta_1 = 3$
N_2		$\pi_2 = 0$	
N_3	e_2	$\pi_3 = -1$	$\Delta_3 = -3$

Etapa 1 - Arcos candidatos

$\psi_1 = \{e_2\}$; $\psi_2 = \emptyset$

Etapa 2 - Agregar un nuevo arco

$e_k = e_2$; $\Delta_2 = \min\{3, 1\} = 1$; $\tilde{\mathcal{N}} = \{1, 3, 2\}$; $\tilde{\mathcal{A}} = \{e_3, e_2\}$



La información es idéntica a la de la etapa anterior

Etapa 3 - Abrirse paso

El ciclo es $\{2, e_2, 3, e_3, 1, e_1, 2\}$ y los nuevos flujos son

$$[x_1\ x_2\ x_3\ x_4] = [2\ 2\ 3\ 0]$$

Ahora, volvemos a buscar un arco fuera de arreglo, pero no lo encontramos todos los arcos están en arreglo

5.5.10 Ejercicios

Ejercicio 1

Implementar, por computadora, el algoritmo de descomposición

Ejercicio 2

Dada la siguiente tabla correspondiente a un problema de flujo con costo mínimo y sólo cuatro nodos

Nodo No.	Suministro	Demanda
1	11	10
2	0	1
3	3	0
4	0	3

Arco No.	Dirigido en sentido opuesto (away from)	Dirigido hacia (towards)	Costo unitario	Capacidad del arco
1	1	2	10	1
2	1	3	1	2
3	3	2	-3	4
4	2	4	3	2
5	3	4	2	2

Resolver el problema mediante el algoritmo ”out-of-killer” comenzando con todas la variables duales en 10

Ejerccicio 3

A partir del algoritmo de descomposición resolver el problema propuesto en las siguientes tablas respetando las siguientes condiciones

a) Comenzar con las variables duales y los flujos iniciales que aparecen en la tabla. En la etapa uno, cuando selecciona el arco fuera de arreglo, siempre seleccione el arco fuera de arreglo con menor número de arco

Nodo No.	Suministro	Demanda
1	10	10
2	0	0
3	0	0
4	-10	10

Arco No.	Desde el nodo (from)	Hacia el nodo (to)	Costo unitario	Capacidad del arco	Punto inicial
1	1	2	1	10	5
2	1	3	4	5	5
3	2	3	2	9	0
4	2	4	6	10	5
5	3	4	3	8	5

Ejercicio 4

Desarrollar una estructura de datos para la implementación computacional del algoritmo de descomposición

5.5.11 Sugerencias

Es importante conocer procedimientos recursivos para el recorrido de un árbol. Cuando un procedimiento A es conocido, por ejemplo, $\underline{recorrer(x)}$ (recorrer un árbol) diremos: si $x = 0$ entonces no hay nada que recorrer, y si $x \neq 0$ entonces, escribir (x), recorrer (izq.x), recorrer (der.x) y finalizar. De esta manera, podemos recorrer caminos

Rótulos para árboles con raíces

Existe una estructura particular de datos que emplea un rótulo conocido como enlace, a saber
Sea $\mathcal{T} = \{\mathcal{N}, \mathcal{A}\}$ un árbol con raíz en el nodo l. Sabemos que existe un único camino $P(i)$ que une cualquier nodo i con el nodo l
Así, el nodo i se llamará sucesor del nodo n si $n \in P(i)$.
El conjunto de sucesores de un nodo n se denotará por $U(n)$ y el número de sucesores del nodo n se denotará por t_n
Definimos un rótulo distancia, denotado por d_i como sigue

$$d_i = \begin{cases} 0 \text{ si } i = l \\ \text{longitud de } \; P(i) \; \text{ en caso contrario} \end{cases}$$

El rótulo predecesor, denotado por p_i está dado por

$$p_i = \begin{cases} 0 \text{ si } i = l \\ P(i) \; \text{ en caso contrario} \end{cases}$$

Para cualquier aplicación S_i uno a uno de $\mathcal{N}$ en sí mismo definimos una familia de aplicaciones recursivamente como sigue

$$S^1(i) = s_i$$

$$S^{j+1}(i) = S^j(s_i)$$

Entonces, se llamará rótulo enlace si

$$U(i) = \{s^j(i) : j = 1, 2, \ldots, t_i\} \text{ cuando } \; t_i \neq 0$$

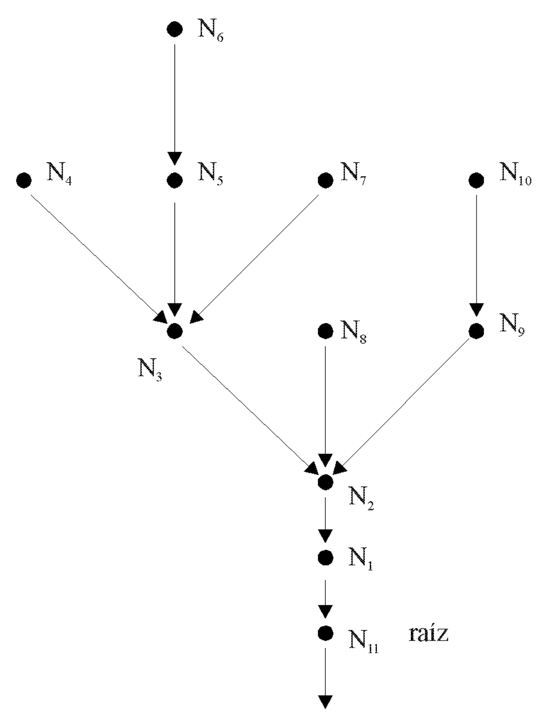
Dado un rótulo enlace, el rótulo distancia pre-orden, denotado por g_i, es una aplicación de $\mathcal{N}$ en sí mismo tal que

$$g_i = \begin{cases} 1 & \text{si} \quad i = l \\ j+1 & \text{si} \quad i = s^j(l) \end{cases}$$

Dado un rótulo enlace, el rótulo último sucesor, denotado por n_i, está dado por

$$n_i = \begin{cases} i & \text{si } U(i) = \emptyset \\ S^j(i) & \text{en caso contrario, donde } S^j(i) \in U(i) \text{ y } S^{j+1}(i) \notin U(i) \end{cases}$$

Supongamos que tenemos un árbol con I nodos, entonces tal árbol $\mathcal{T}$ tiene $I - \{1\}$ arcos y un arco raíz. Entonces, para cada $i \neq l$ es necesario tener información respecto de los arcos conectando nodos i y, también, es necesario conocer p_i asociado con cada nodo i. Supongamos que el arco e_k conecta nodos i y p_i. Podemos, entonces, emplear un arco orientado identificador definido por $m_i = \begin{cases} +K & \text{si} \quad e_k = (p_i, i) \\ -K & \text{si} \quad e_k = (i, p_i) \end{cases}$ La siguiente tabla da los rótulos para el árbol, con raíz en el nodo N_{11}, dado por



N_1	1	-1	0	0	0	0	0	0	0	0
N_2	0	1	-1	0	0	0	0	-1	-1	0
N_3	0	0	1	-1	-1	0	0	0	0	0
N_4	0	0	0	1	0	0	0	0	0	0
N_5	0	0	0	0	1	-1	-1	0	0	0
N_6	0	0	0	0	0	1	0	0	0	0
N_7	0	0	0	0	0	0	1	0	0	0
N_8	0	0	0	0	0	0	0	1	0	0
N_9	0	0	0	0	0	0	0	0	1	-1
N_{10}	0	0	0	0	0	0	0	0	0	1
N_{11}	-1	0	0	0	0	0	0	0	0	0

Nodo i	Distancia d_i	Predecesor p_i	Enlace s_i	Ultimo sucesor n_i	Número de sucesores t_i	Distancia pre-orden g_i
1	1	11	2	10	10	2
2	2	1	3	10	9	3
3	3	2	4	7	5	4
4	4	3	5	4	1	5
5	4	3	6	6	2	6
6	5	5	7	6	1	7
7	4	3	8	7	1	8
8	3	2	9	8	1	9
9	3	2	10	10	2	10
10	4	9	11	10	1	11
11	0	0	1	10	11	1

El flujo sobre el arco e_k es denotado por α_i:

5.5.12 Ejercicios

Ejercicio 1

Teniendo en cuenta las sugerencias de la sección anterior, implementar computacionalmente los siguientes algoritmos

a) predecesor/enlace: test del cociente y actualización

b) predecesor/enlace/distancia: test del cociente y actualización

c) predecesor/enlace/nro. de sucesores: test del cociente y actualización

d) predecesor/enlace/distancia pre-orden: test del cociente y actualización

e) predecesor/enlace/número de sucesores/último sucesor: actualización

5.6 Aplicaciones

5.6.1 El problema de flujo máximo en una red con una sola fuente y un solo vertedero

Sabemos que una red está dada por la terna $\mathcal{G} = (\mathcal{N}, \mathcal{A}, c)$ donde $\mathcal{N}$ es un conjunto no vacío finito de nodos, $\mathcal{A}$ es un conjunto de pares ordenados de nodos llamados arcos y $c : A \to \Re^+$ es una función llamada capacidad. De modo entonces, que, a cada arco $(x, y) \in \mathcal{A}$ le asociamos un número no negativo $c(x, y)$ que es la capacidad de dicho arco
Para todo par X e Y de subconjuntos de nodos, denotamos por

$$(X, Y) = \{(x, y) : x \in X; y \in Y; (x, y) \in \mathcal{A}\}$$

En particular, si consideramos $S = \{s\}$ (un solo nodo fuente) y $T = \{t\}$ (un solo nodo vertedero) entonces para todo conjunto $X \subset \mathcal{N}$ tal que X contiene al nodo s y no al nodo t, si denotamos por $\overline{X} = \mathcal{N} - X$, el par ordenado $(X, \overline{X})$ se denomina cortadura que separa al nodo t del nodo s
Para cada aplicación $g : \mathcal{A} \to \Re$ denotamos por

$$g(X, Y) = \sum_{(x,y)\in(X,Y)} g(x, y)$$

el valor de tal aplicación sobre (X, Y). En el caso particular de tomar $g = c$ obtenemos $c(X, Y)$, es decir, la capacidad de flujo entre dos subconjuntos de nodos. Si, además, (X, Y) es una cortadura entonces $c(X, Y)$ es la capacidad de dicha cortadura. Cuando esta capacidad es mínima, la cortadura (X, Y) se llama corte minimal
Para todo nodo x, denotamos por

$$net(g, x) = g(\mathcal{N}, \{x\}) - g(\{x\}, \mathcal{N})$$

Finalmente, el flujo es una función $f : \mathcal{A} \to \Re^+$ que verifica las siguientes ecuaciones de conservación de flujo

$$net(f, x) = \begin{cases} \leq 0 & \text{si} \quad x \in S \\ 0 & \text{si} \quad x \notin S \cup T \\ \geq 0 & \text{si} \quad x \in T \end{cases}$$

y la restricción de capacidad en cada arco es

$$0 \leq f(x, y) \leq c(x, y) \ \ ; \ \ (x, y) \in \mathcal{A}$$

5.6.2 El problema de flujo máximo

Consideremos una red $\mathcal{G} = (\mathcal{N}, \mathcal{A}, c)$ con m nodos y n arcos a través de la cual fluye un solo tipo de bien y supongamos que las capacidades de los arcos $c(x, y)$ son números enteros no negativos. En el problema de flujo máximo no intervienen costos y su objetivo es hallar el costo máximo desde el nodo 1 hasta el

nodo m
Representemos por F la cantidad de flujo en la red desde el nodo 1 hasta el nodo m, es decir $F = net(f, m)$. De este modo, enunciamos el problema de flujo máximo como sigue
Sea $f : \mathcal{A} \to \Re^+$ un flujo
Maximizar F sujeta a

$$net(f,i) = \begin{cases} -F & \text{si} \quad i = 1 \\ 0 & \text{si} \quad i \neq 1, i \neq m \\ F & \text{si} \quad i = m \end{cases}$$

Esta es la clásica formulación nodo/arco dado que la matriz de restricciones es la matriz de incidencia nodo/arco. Observando que F es variable y denotando por B a la matriz de incidencia nodo/arco describimos el problema de flujo máximo en forma matricial como sigue
Dado el flujo $f : A \to \Re^+$
Maximizar F sujeta a

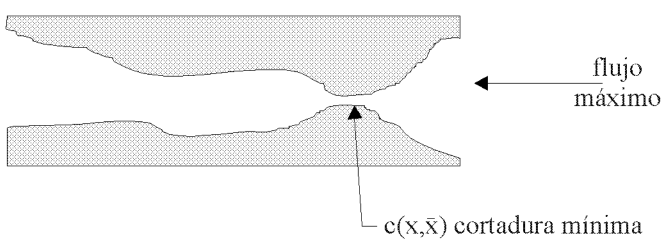
$$(e_m - e_1)F + Bf = 0 \qquad 0 \leq f \leq c$$

Ahora bien, si consideramos el dual del problema de flujo máximo decimos

Minimizar $\sum_{(i,j)\in\mathcal{A}} c(i,j)h_{ij}$, sujeto a

$$\begin{array}{lll} w_m - w_1 & = 1 & \\ w_i - w_j + & h_{ij} \geq 0 & \text{para} \ \ (i,j) \in \mathcal{A} \\ & h_{ij} \geq 0 & \text{para} \ \ (i,j) \in \mathcal{A} \end{array}$$

donde w corresponde a las ecuaciones de conservación y h corresponde a la restricción de capacidad $0 \leq f \leq c$. La primera restricción dual está asociada con F cuya columna es $e_m - e_1$. Una columna cualquiera de la matriz de incidencia nodo/arco tiene $(+1)$ en la i-ésima posición y (-1) en la j-ésima posición que, por cierto, nos lleva a las restricciones duales $w_i + w_j + h_{ij} \geq 0$. Para interpretar este problema dual, hagamos una analogía entre una red y un caño de la siguiente forma: el flujo que va de la fuente al vertedero será la cantidad de fluido que se transporta a través del caño mientras que las capacidades de las cortaduras de la red serían los diferentes diámetros del caño



Intuitivamente, podríamos decir que el flujo máximo estará relacionado con el menor diámetro, es decir, con la cortadura mínima. Por lo tanto, maximizar

el flujo equivaldría a minimizar las capacidades de las cortaduras. Luego, el problema dual es el de hallar la cortadura mínima.
En efecto
Sea $(X, \overline{X})$ cualquier cortadura y consideremos el dual del problema de flujo máximo presentado. Si tomamos

$$w_i = \begin{cases} 0 & \text{si} \quad i \in X \\ 1 & \text{si} \quad i \in \overline{X} \end{cases}$$

y

$$h_{ij} = \begin{cases} 1 & \text{si} \quad (i,j) \in (X, \overline{X}) \\ 1 & \text{si} \quad (i,j) \notin (X, \overline{X}) \end{cases}$$

esta elección particular de w y de h constituye una solución factible del problema dual puesto que $w_m - w_1 = 1$ ya que $1 \in X$ y $m \in \overline{X}$, y $w_i - w_j + h_{ij} \geq 0$ ya que

a) Si $(i,j) \in (X, \overline{X})$ entonces $h_{ij} = 1$ y $w_i - w_j = -1$ con lo cual es $w_i - w_j + h_{ij} = 0$

y

b) Si $(i,j) \notin (X, \overline{X})$ entonces, o bien $i, j \in X$ o bien $i, j \in \overline{X}$
Luego $w_i - w_j + h_{ij} = 0$ siendo $h_{ij} \geq 0$ por definición

De esta forma vemos que la capacidad de la cortadura mínima es mayor o igual que la solución del problema dual y por ende mayor o igual que el flujo máximo. Para mostrar que la capacidad de la cortadura mínima es igual al flujo máximo tenemos que ver que la solución del problema dual coincide con la capacidad de la cortadura mínima. Es decir, si podemos hallar un flujo f y una cortadura tales que $c(X, \overline{X}) = net(f, n)$ tendremos el flujo máximo (es decir, la cortadura mínima)
Para esto diseñamos un algoritmo en la siguiente sección

5.6.3 Un Algoritmo para el problema de flujo máximo

Supongamos que comenzamos con cualquier flujo factible en $\mathcal{G} = (\mathcal{N}, \mathcal{A}, c)$, por ejemplo, cada $f(i,j) = 0$. A partir de esta red $\mathcal{G}$ construimos una nueva red $\mathcal{G}' = (\mathcal{N}, \mathcal{A}', \Delta)$ como sigue

Etapa 0

Supongamos que N_s (fuente) $\in X$

Etapa 1

Si el arco $(i,j) \in \mathcal{A}$ y si $f(i,j) < c(i,j)$ (es decir, si $N_i \in X$ y si $f(i,j < c(i,j)$ entonces $N_j \in X$) entonces colocamos el arco (i,j) en $\mathcal{A}'$ con valor $\Delta(i,j) = c(i,j) - f(i,j)$ como cambio permitido de flujo

Etapa 2

Si el arco $(i,j) \in \mathcal{A}$ y si $f(i,j) > 0$ (es decir, si $N_i \in X$ y si $f(i,j) > 0$ entonces $N_j \in X$) entonces colocamos el arco (j,i) en $\mathcal{A}'$ con valor $\Delta(j,i) = f(i,j)$ como cambio permitido para el flujo

Ahora, en $\mathcal{G}'$ existen dos posibilidades

a) Caso 1:
$N_t \in X$, es decir, existe en $\mathcal{G}'$ un camino P desde el nodo $1 = N_s$ (fuente) hasta el nodo $m = N_t$ (vertedero) dado por

$$N_s, \ldots, N_i, A_{i,i+1}, \ldots, N_t$$

para el cual en todo arco, o bien $f_{i,i+1} < c_{i,i+1}$ o bien $f_{i+1,i} > 0$. Sea, entonces, $\Delta_1 = \min_i\{c_{i,i+1} - f_{i,i+1}\}$ en tal camino P y sea $\Delta_2 = \min_i\{f_{i,i+1}\}$ en tal camino P y $\Delta = \min\{\Delta_1, \Delta_2\}$ un entero positivo

Luego, podemos incrementar por Δ el flujo en todos los arcos del camino que tengan $f_{i,i+1} \geq 0$ o bien reducir el flujo en todos los arcos del camino que tengan $f_{i+1,i} > 0$. Por lo tanto, el flujo se incrementa por Δ y los nuevos valores de f_{ij} satisfacen las condiciones del problema. Ahora, se redefine X a partir del nuevo flujo
Si aún $N_t \in X$ entonces volvemos a incrementar por Δ. Asi, como la capacidad del corte mínimo es finita e incrementamos el flujo al menos en una unidad, en proceso terminará en un número finito de pasos
Esto significa que en este caso podemos construir un nuevo flujo facitble con mayor valor objetivo pues si Δ es el flujo mínimo permitido sobre la trayectoria o camino P desde el nodo 1 hasta el nodo m en $\mathcal{G}'$, es decir,

$$\Delta = \min\{\Delta(i,j) : (i,j) \text{ pertenece a la trayectoria}\}$$

construimos un nuevo flujo sumando Δ a los flujos sobre los arcos de la cadena (trayectoria no dirigida) asociada en $\mathcal{G}$ que tienen la dirección de la trayectoria en $\mathcal{G}'$; restamos Δ de los flujos sobre los arcos de la cadena asociada en $\mathcal{G}$ que tienen dirección contraria a la de la trayectoria en $\mathcal{G}'$ y no cambiamos todos los otros flujos sobre los arcos. Así, el nuevo flujo es factible y el valor objetivo es $F' = F + \Delta$

b) Caso 2;
$N_t \in X^c$. Esto significa que en todos los arcos desde X hasta X^c tenemos

$f_{ij} = c_{ij}$ según la Etapa 1. Así, no existe flujo f_{ij} sobre arcos desde X^c hasta X por Etapa 2. Entonces

$$\sum_{\substack{i \in X \\ j \in X^c}} f_{ij} = \sum_{\substack{i \in X \\ j \in X^c}} c_{ij} \quad \text{y} \quad \sum_{\substack{i \in X \\ j \in X^c}} f_{ji} = 0$$

Lo que acabamos de afirmar significa que no existe en $\mathcal{G}'$ un camino desde el nodo 1 hasta el nodo m. Cuando esto ocurre tomamos X como el conjunto de los nodos en $\mathcal{G}'$ que pueden alcanzarse desde el nodo 1 a lo largo de alguna ruta en $\mathcal{G}'$. Sea $\overline{X} = \mathcal{N} - X$ y observemos que el nodo m pertenece a $\overline{X}$. Consideremos los arcos en $\mathcal{G}$ entre X y $\overline{X}$. En primer lugar, cada arco (i, j) en $\mathcal{G}$ de X a $\overline{X}$ debe tener $f_{ij} = c_{ij}$ pues sino habría un arco (i, j) en $\mathcal{G}$ y j sería miembro de X, lo cual es contradictorio. En segundo lugar, cada arco (i, j) en $\mathcal{G}$ de $\overline{X}$ a X debe tener $f(i, j) = 0$ pues de lo contrario habría un arco (j, i) en $\mathcal{G}'$ e i sería miembro de X, lo cual es contradictorio. Luego, tenemos

$$\sum_{(i,j)\in(X,\overline{X})} f_{ij} = F \text{ ó } c(X, \overline{X}) = F$$

Ahora bien, como todo corte es solución factible del problema dual, tenemos que su capacidad es mayor o igual que el flujo que llega al vertedero, es decir, $c(X, \overline{X}) \geq net(f, m)$. Por lo tanto, el flujo obtenido es el flujo máximo. Así quedó probado el Teorema de Flujo Máximo - Cortadura Mínima, que afirma

Teorema

El valor del flujo máximo en $\mathcal{G}$ es igual a la capacidad de la cortadura mínima en $\mathcal{G}$

5.6.4 Condiciones de optimalidad de Kuhn-Tucker

Dado el problema de

Minimizar $z = \sum_{j=1}^{n} c_j x_j$
sujeta a

$$\sum_{j=1}^{n} a_{ij} x_j = b_i \quad ; i = 1, 2, \ldots, m$$
$$x_j \geq 0 \quad j = 1, 2, \ldots, n$$

Lo interpretamos como un simple problema de extremos ligados, a saber
Minimizar

$$\mathcal{Z} = \sum_{j=1}^{n} c_j x_j + \sum_{i=1}^{m} p_i (b_i - \sum_{j=1}^{n} a_{ij} x_j) + \sum_{j=1}^{n} q_j (\alpha_j^2 - x_j)$$

$$= \sum_{i=1}^{m} p_i b_i + \sum_{j=1}^{n} (c_j - q_j - \sum_{i=1}^{m} p_i a_{ij}) x_j + \sum_{j=1}^{n} q_j \alpha_j^2$$

donde por tratarse de un mínimo irrestricto, pedimos

a) $q_j \geq 0 \; \forall \; j = 1, 2, \ldots, n$

b) $c_j - q_j - \sum_{i=1}^{m} p_i a_{ij} = 0$ lo cual implica $q_j = c_j - \sum_{i=1}^{m} p_i a_{ij} \geq 0$ Además, la condición necesaria para la existencia de extremo debe ser $\frac{dZ}{dx_j} = 0$ lo cual proporciona la condición b).
Por otra parte, $\frac{dZ}{d\alpha_j} = Z\alpha_j q_j = 0$ lo cual implica $\alpha_j q_j = 0$ o bien $\alpha_j \alpha_j q_j = x_j q_j = 0$, es decir, $xq = 0$

Por lo tanto, $x = (x_1 \ldots x_m)$ es optimal sí y sólo síexisten vectores $p = (p_1 \ldots p_m)$ irrestricto y $q = (q_1 \ldots q_n)$ no negativo tales que las siguientes condiciones son válidas

a) $Ax = b$; $x \geq 0$ (factibilidad primal)

b) $c - pA - q = 0$; p irrestricto ; $q \geq 0$ (factibilidad dual)

c) $p(Ax - b) = 0$; $xq = 0$ (holgura complementaria)

Los vectores p y q se llaman multiplicadores de Lagrange (variable duales) correspondientes a las restricciones $Ax = b; x \geq 0$. Estas condiciones son las llamadas condiciones de optimalidad de Kuhn-Tucker. A ellas nos hemos referido al tratar el problema de optimizar el flujo sobre una red

5.6.5 Ejercicios

Ejercicio 1

Verificar la formulación de las condiciones de optimalidad de Kuhn-Tucker para el problema de flujo máximo

Capítulo 6

Programa

6.1 Números naturales y enteros

6.1.1 Números Naturales

Principios de inducción matemática y de buena ordenación.

6.1.2 Números Enteros

Dominios de integridad. Divisores de cero y ley de cancelación. Propiedades de orden. Divisibilidad. Divisores enteros de 1. Enteros asociados. Algoritmo de división de enteros o algoritmo de Euclides. Números primos. Función de Euler. Máximo común divisor y mínimo común múltiplo. Teorema fundamental de la aritmética. Análisis de la complejidad del algoritmo de Euclides.

6.1.3 Relaciones de recurrencia

Relaciones de recurrencia homogéneas y no homogéneas, lineales y no lineales de primero y de segundo órdenes. Resolución: método de la función generadora de Taylor. Ejemplos de algoritmos recursivos y análisis de su complejidad.

6.2 Anillos y aritmética modular

Estructura de anillo: definición, ejemplos y propiedades. Homomorfismos e isomorfismos de anillos. Enteros módulo n. Congruencias: definición, propiedades y teoremas relativos. Clases residuales. Teorema de Fermat. Generalización de Euler. Aplicación de la noción de congruencia a la recuperación de información.

6.3 Funciones generadoras y representaciones asintóticas

6.3.1 Funciones Generadoras

Definición y propiedades. Operaciones: combinaciones lineales. Producto por potencias. Producto de Cauchy. Derivación e integración.
Números armónicos: propiedades. Estimación y constante de Euler. Números y polinomios de Bernoulli.

6.3.2 Representaciones asintóticas

Definición de orden. Propiedades y teoremas relativos.

6.4 Álgebras booleanas y funciones de conmutación

Estructura de un álgebra booleana, definiciones. Propiedades y teoremas relativos.
Funciones de conmutación: formas normales conjuntiva y disyuntiva. Compuertas AND, OR, NOT. Expresiones booleanas. Circuitos combinatorios y síntesis.
Redes de compuertas: sumas minimales de productos y diagramas de Karnaugh.

6.5 Teoría de grafos y Algoritmos en redes

Definiciones: arcos, ramas o ejes, matriz de adyacencias o de incidencia nodo-arco. Caminos simples y compuestos, orientación. Cadenas. Redes.
Definiciones, propiedades y ejemplos de árboles. Árboles con raíz. Matrices asociadas y triangulación inferior. Teoremas relativos. Modelos matemáticos y algoritmos. Aplicaciones algorítmicas: Algoritmos de Kruskal y Prim. Algoritmos para la optimización de la programación en redes: máximo flujo-mínimo corte y de descomposición (out-of-kilter).

6.6 Bibliografía

[1] Discrete Mathematics with algorithms - Michael O.Albertson - Joan P. Hutchinson - John Wiley & Sons - 1988
[2] Matemáticas discreta y combinatoria - Ralph P. Grimaldi - Addison Wesley Iberoamericana - 1985
[3] The art of computer programming - Vol.I - Donald E. Knuth - Addison Wesley Publishing Company - 1973
[4] Concrete Mathematics - A Foundation for Computer Science - Graham-

Knuth - Patashnik - 1994
[5] Álgebra para informáticos - Telma Caputti - Universidad Austral - 1996
[6] Matemática Discreta - Telma Caputti - Universidad Austral - 1997