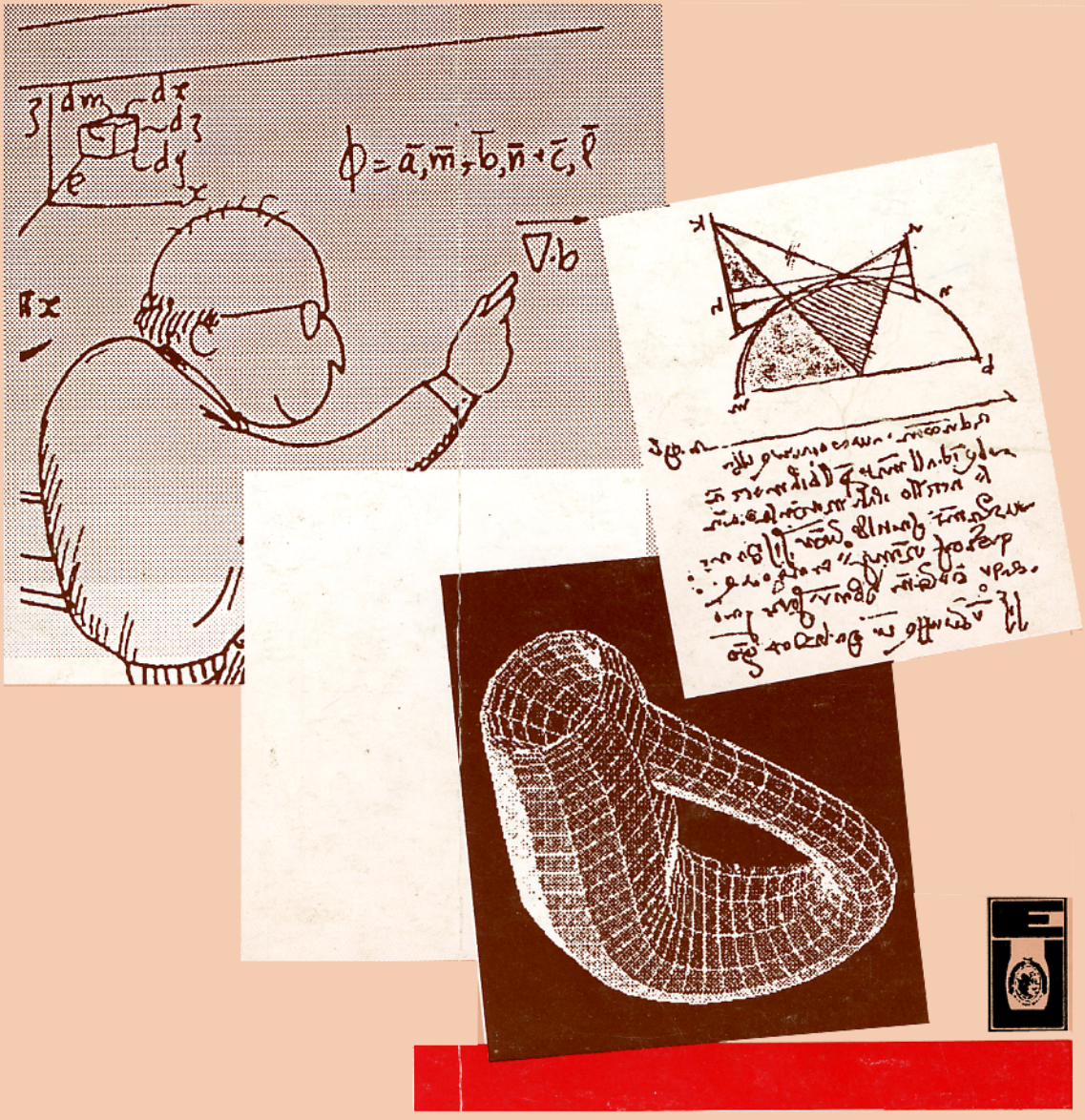
Ingeniería

Revist de la Universidad de Costa Rica
ENERO/JUNIO 1993 VOLUMEN 3 No. 1



Ingeniería 3 (1):21-27, 1992 San José Costa Rica

UNA GENERALIZACIÓN DE LA DIVISIÓN SINTÉTICA

*Raúl Alvarado**

RESUMEN

Presentamos aquí un algoritmo similar al de la división sintética para el caso de que el polinomio divisor sea de grado mayor o igual a uno. El modo de exposición será el siguiente: Primero: una reflexión sobre la división sintética. Segundo: varios ejemplos explicando como funciona el algoritmo generalizado y Tercero: una prueba del mismo.

SUMMARY

We show an algorithm simmilar to the algorithm of synthetic division, for the case when the divisor has degree strictely positive. The outline of the article is as follows: First we give some ideas about synthetic division. Second we show some examples explaining how the generalized algorithm works. Third, we prove it.

1. Introducción

El lector notará que al final de este artículo no existe la clásica sección de bibliografía consultada. La razón principal para esto, es que el artículo se basa en una idea muy sencilla y que se encuentra expuesta en casi todo libro de texto de matemática elemental a nivel universitario: la división sintética. La división sintética parece no aportar nada nuevo al conocimiento matemático, para eso está el algoritmo de división de polinomios, pero nadie que haya usado la división sintética negará la utilidad de la misma para aligerar los cálculos y ahorrar tiempo.

La propuesta que hago de un método generalizado para la división sintética, tampoco aporta nada nuevo al conocimiento matemático, pero al igual que en el caso simple, esto no quiere decir que no sea útil ni que carezca de interés académico.

Quien se tome la molestia de seguir los ejemplos que se presentan, se percatará del gran ahorro de cálculo y tiempo que se logra, en comparación con el método estándar de división de polinomios. Tampoco hace falta ser muy perspicaz para darse cuenta que al hacer división de polinomios por computadora, es mucho más simple y eficiente programar el método de división sintética generalizado que propongo, en vez del método estándar.

Este artículo en realidad fue escrito muchos años antes de ser presentado para publicación. Posteriormente encontré la siguiente aplicación.

La Teoría de codificación, detección y corrección de errores estudia el problema siguiente: Se tiene un computador (fuente) el cual genera una tira de bits (tira de ceros y unos) y los envía a otro computador (destino) a través de un medio físico, el cual generalmente es un cable telefónico o medios inalámbricos. La tira de bits que llega al destino no necesariamente es la misma que salió de la fuente; es decir, el medio de transmisión perturbó la tira y le introdujo uno o varios errores. ¿ Cómo detectar si en efecto ocurrió un error, cuál fue ese error y cómo corregirlo?

La teoría matemática detrás de esto es la Teoría de grupos de Galois y sus respectivos polinomios de Galois (nombrados así en honor al matemático francés Evaristo Galois). Muy resumidamente, la técnica funciona más o menos así.

a) Se escoge un código de transmisión (i.e. una convención).

*Escuela de Ciencias de la Computación e Informática, Universidad de Costa Rica

b) Se determina el grupo de Galois asociado y su respectivo polinomio.

c) Se construye un dispositivo electrónico (físico), el cual en realidad es un divisor de polinomios, el polinomio de Galois es el divisor, y el procedimiento está "escrito" en los circuitos del dispositivo.

d) Cuando llega una tira de bits, el dispositivo la interpreta como un polinomio (el dividendo), se efectúa la división; y del análisis del resultado se detecta si hubo error en la transmisión y lo corrige.

Como puede verse, se trata de un caso de división de polinomios en que el grado del divisor en general siempre es mayor que uno. Por lo tanto el método de la división sintética generalizado puede ser de gran utilidad para mejorar el diseño de los circuitos del dispositivo, máxime que se está trabajando en aritmética binaria.

2. División general y división sintética

Generalmente utilizamos la división sintética cuando hemos encontrado la raíz de un polinomio. La frecuencia con que se usa la división sintética en el proceso de factorización hace que a veces se olvide que la división sintética no es más que un resumen del proceso de dividir un polinomio P(x) entre el polinomio (x-r). Veamos:

Ejemplo 2.1

$x^4 + 7x^3 - 19x^2 - 103x + 210 / x-3 = x^3 + 10x^2 + 11x - 70$ División general (D.G)

$x^4 + 7x^3 - 19x^2 - 103x + 210 \;/\; x-3$

Tramo 1 $-x^4 \pm 3x^3$

$10x^3 - 19x^2$

Tramo 2 $-10x^3 \pm 30x^2$

$11x^2 - 103x$

Tramo 3 $-11x^2 \pm 33x$

$-70x + 210$

Tramo 4 $\pm 70x - 210$

0

División sintética (D.S)

1	7	-19	-103	210	3
0	3	30	33	-210	3
1	10	11	-70	1	3

Es decir, la división sintética no es más que una observación cuidadosa del método general de división de polinomios, cuando éste es aplicado a los polinomios dividendo P(x) y divisor (x-r)

3. Características esenciales y no esenciales de la división sintética

a) Para fijar ideas supongamos que el polinomio dividendo es

$A(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \; (a \in R)$
y que el polinomio divisor es
$B(x) = x^m - b_{m-1}x^{m-1} - b_{m-2}x^{m-2} \ldots - b_1 x - b_0$. Con $m \leq n$.

Se observa que la condición de que A(x) y B(x) sean mónicos ($a_n=1$, $b_m=1$) podría fácilmente suprimirse, sin embargo esto hace los cálculos un poco engorrosos. En todo caso si $a_n \neq 1$ o $b_m \neq 1$ podemos factorizar para convertir a A(x) y B(x) en mónicos. Más aún, si $b_m=1$ no hay gran inconveniente si $a_n \neq 1$.

b) En ejemplos como el 2.1 tienden a confundirse las características de lo que podría ser un procedimiento general con características muy particulares de estos casos. Por ejemplo en 2.1 (D.S) escribimos 3 y no -3 para evitarnos los cambios de signos o "restas" de las segundas filas de los tramos.

c) En 2.1 (D.G) la primera columna de los tramos, la suma de sus componentes siempre es nula. La suma de los coeficientes de la primer columna no siempre nula (en nuestro caso la segunda y última) es la que da el coeficiente que *genera* el tramo siguiente, es decir, el coeficiente de la potencia inmediatamente inferior del polinomio resultante Q(x).

Para aclarar esta observaciones veamos el siguiente ejemplo.

Ejemplo 3.1 $1x^4+7x^3 - 19x^2-103x+210 /(x^2 -5x + 6) = x2 + 12x + 35$

$1x^4 + 7x^3 - 19x^2 - 103x +210 /(x^2 -5x + 6)$

T1 $-x^4 \pm 5x^3m \mp 6x^2$

$12x^3 - 25x^2 - 103x$

T2 $- 12x^3 \pm 60x^2 \mp 72x$

$35x2 - 175x + 210$

T3 $-35x2 \pm 175x \mp 210$

0

En conclusión, la tercera columna en los tramos 1 y 2 *no era necesario sumar las en ese momento.* Esta idea está implícita en el ejemplo 2.1, pero no se ve claramente por ser la segunda columna la última. Veamos otro ejemplo (con residuo no nulo).

Ejemplo 3.2

$x^{11} -2x^{10} +4x^9 +0x^8 -7x^7 +4x^6 +5x^5 -8x^4 +6x^3 -2x^2 +x -25/(x^4 -3x^3 +2x- 2)$
$= x^7 + x^6 + 7x^5 +19x^4 +50x^3 + 142x^2 + 407x + 1151$

T1

$x^{11} -2x^{10} +4x^9 +0x^8 -7x^7 +4x^6 +5x^5 -8x^4 +6x^3 -2x^2 +x -25/(x^4 -3x^3 +2x- 2)$
$-x^{11} \pm 3x^{10} \mp 0x^9 \mp 2x^8 \pm 2x^7$

$x^{10} + 4x^9 - 2x^8 - 5x^7 + 4x^6$

T2 $-x^{10} \pm 33x^9 \mp 0x^8 \mp 2x^7 \pm 2x^6$

$7x^9 - 2x^8 - 7x^7 + 6x^6 + 5x^5$

T3 $- 7x^9 \pm 21x^8 \mp 0x^7 \mp 14x^6 \pm 14x^5$

$19x^8 - 7x^7 - 8x^6 +19x^5 - 8x^4$

T4 $-19x^8 \pm 57x^7 \mp 0x^6 \mp 38x^5 \pm 38x^4$

$50x^7 - 8x^6 - 19x^5 + 30x^4 + 6x^3$

T5 $-50x^7 \pm 150x^6 \mp 0x^5 \mp 100x^4 \pm 100x^3$

$142x^6 - 19 x^5 - 70x^4 +106x^3 - 2x^2$

T6 $-142x^6 \pm 426x^5 \mp 0x^4 \mp 284x^3 \pm 284x^2$

$407x^5 - 70x^4 - 178x^3 - 282x^2 + x$

T7 $-407x^5 \pm 1121x^4 \mp 0x^3 \mp 814x^2 \pm 814x$

$1151x^4 - 178x^3 - 532x^2 + 815x - 25$

T8 $-1151x^4 \pm 3453x^3 \mp 0x^2 \mp 2302x \pm 2302$

$3275x^3 - 532x^2 - 1487x + 2277$

En este caso se ve claramente que (por ejemplo) los términos x^7 en los tramos 1, 2, 3, 4 realmente viene a interesarnos solo en el quinto tramo. Además, en cada tramo los coeficientes de la segunda fila son los negativos de los coeficientes del polinomio divisor multiplicados por el generador de este tramo. De estas dos últimas observaciones podemos sacar dos conclusiones:

primero, que podemos evitarnos estas sumas parciales en cada tramo y efectuar una sola suma en el momento que se necesite para determinar un generador.

segundo, que podemos suprimir todas las potencias de x y trabajar solo con los coeficientes.

4. La división sintética generalizada (dividendo y divisor mónicos)

Si observamos el ejemplo 3.1 y tomamos en cuenta los expresado en el parágrafo 3, podemos entonces construir una tabla similar a la tabla (D.S) en el ejemplo 2.1.

sección I	1	-19	-103	210			
sección II	0	5	60	175	0	5	
sección II	0	0	-6	-72	-210		-6
sección III	1	12	35	0	0		

Para entender como se construye esta tabla, dividiremos el procedimiento en varios pasos y subpasos.

Paso 1

a) En la primera sección (única línea) ponemos los coeficientes del polinomio dividendo.

b) Como el "divisor" es "doble" (5; -6) en la segunda sección de la tabla ponemos dos líneas.

c) En la primera posición de la primera columna escribimos un cero; construimos un triángulo de ceros a partir de esa posición (hacia abajo).

sección I	1	7	-19	-103	210		
sección II	0						
sección II	0	0					

d) Colocamos el "divisor" en sentido diagonal (esto sólo por razones pedagógicas) al lado derecho de la tabla.

e) En la última columna de la segunda sección, escribimos un cero en la penúltima posición. A partir de esta posición hacemos un triángulo de ceros (hacia arriba)

sección I	1	7	-19	-103	210		
sección II	0				0	5	
sección II	0	0					-6

Con esto ya estamos listos para empezar a operar la tabla

Paso 2

a) Se suma la primera columna completa (secciones I y II) y se coloca el resultado (en este caso, por ser mónico el dividendo) en la primera posición de la tercera sección.

b) Se toma este multiplicador 1 (i.e. el generador del primer tramo en la división general) y se multiplica por cada uno de los números del "divisor" y se coloca en la tabla como indica la siguiente figura:

sección I	1	7	-19	-103	210		
sección II	0	5			0	5	
sección II	0	0	-6				-6
sección III		1					

c) Se suma la última columna completa (7+5+0) y se coloca el resultado en la posición correspondiente (tercera sección)

d) Se repiten los pasos b) y c) usando como multiplicador del divisor el número que aparezca en la última posición llena de la tercera sección. Esto hasta que estén llenas todas las posiciones de la segunda sección

sección I	1	7	-19	-103	210		
sección II	0	5	60	175	0	5	
sección II	0	0	-6	-72	-210		-6
sección III	1	12	35				

e) Se suman las columnas restantes

f) Como el "divisor" es de dos componentes entonces las dos últimas posiciones son los coeficientes del polinomio residuo.

5. Otros ejemplos

Ejemplo 5.1 Aplicar el método al ejemplo 3.2
Polinomio resultante: $x^7 + x^6 + 7x^5 + 19x^4 + 50x^3 + 142x^2 + 407x + 1151$

SI	1	-2	4	0	-7	4	5	-8	6	-2	1	25				
SII	0	3	3	21	57	150	426	1221	3453	0	0	0	3			
SII	0	0	0	0	0	0	0	0	0	0	0	0		0		
SII	0	0	0	-2	-2	-14	-38	-100	-284	-814	-2302	0			-2	
SII	0	0	0	0	2	2	14	38	100	284	814	2302				2
SIII	1	1	7	19	50	142	407	1151	3275	-532	-1487	2277				

Polinomio residuo: $3275x^3 - 532x^2 - 1487x + 2277$

6. Demostración del algoritmo.

Sea $A(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$
$B(x) = x^m - b_{m-1}x^{m-1} - b_{m-2}x^{m-2} \ldots - b_1 x - b_0$ con $n \geq m$

La tabla puede verse como una matriz $(m+1)\times(n+1)$, por conveniencia de notación indizaremos las entradas desde la (0,0) hasta la (m,n), quedando de la siguiente forma:

0	1	2	3	.....	n-m	n-m+1	n-m+2	...	n-2	n-1	n
a_n	a_{n-1}	a_{n-2}	a_{n-3}						a_2	a_1	a_0
0	c_0b_{m-1}	c_1b_{m-1}				$c_{n-m}b_{m-1}$	0	....	0	0	0
											:
											:
											0
0				c_0b_0							$c_{n-m}b_0$
c_0	c_1		...	c_m						c_{n-1}	c_n

La fila cero y columna cero no son de gran interés para nosotros, sea d_{ij} la entrada (i,j) de esta matriz, note que para $i \geq 1$, $j \geq 1$ se tiene

$$d_{ij} = \begin{cases} 0 & \text{si } i>j \\ c_{j-i}\, b_{m-i} & \text{si } i \leq j \leq n-m+i \\ 0 & \text{si } j > n-m+i \end{cases}$$

Además $c_0 = a_n$ y $c_j = \sum_{i=1}^{m} d_{ij} + a_{n-j}$ para $j=1, \ldots, n$

Sea $Q(x) = a_n x^{n-m} + \sum_{j=1}^{n-m} c_j\, x^{n-m-j}$ y $R(x) = \sum_{j=n+m-1}^{n} c_j\, x^{n-j}$

Note que grad(Q) = n-m y grad(R) = n-(n-m+1) = m-1 < m = grad(B).

Vamos a probar que A(x) = Q(x) B(x) + R(x)

Por la unicidad de los polinomios resultantes y residuo, se sigue que Q y R son precisamente esos polinomios.

$$Q(x)\,B(x) + R(x) = [\, a_n x^{n-m} + \sum_{j=1}^{n-m} c_j x^{n-m-j} \,][\, x^m + \sum_{j=1}^{m} -b_{m-j} x^{m-j}] + \sum_{j=n-m+1}^{n} c_j x^{n-j}$$

$$= a_n x^n + \sum_{j=1}^{n-m} c_j x^{n-j} + a_n \sum_{j=1}^{m} -b_{m-j} x^{n-j} + \sum_{j=1}^{n-m} c_j x^{n-m-j}][\sum_{j=1}^{m} -b_{m-j} x^{m-j}] + \sum_{j=n-m+1}^{n} c_j x^{n-j}$$

$$= a_n x^n + \sum_{j=1}^{n}. c_j x^{n-j} + a_n \sum_{j=1}^{m}. -b_{m-j} x^{n-j} + x^{n-m} [\sum_{j=1}^{n-m} c_j x^{j}][\sum_{j=1}^{m}. -b_{m-j} x^{m-j}]$$

$$= a_n x^n + \sum_{j=1}^{n} c_j x^{n-j} + a_n \sum_{j=1}^{m} -b_{m-j} x^{n-j} + [\sum_{j=1}^{n-m} c_j x^{j}][\sum_{j=1}^{m}. -b_{m-j} x^{n-j}]$$

$$= a_n x^n + \sum_{j=1}^{n} c_j x^{n-j} + \sum_{j=1}^{m} -b_{m-j} x^{n-j} [\sum_{j=1}^{n-m} c_j x^{j} + a_n]$$

$$= a_n x^n + \sum_{j=1}^{n} c_j x^{n-j} + \sum_{j=1}^{m}. -b_{m-j} x^{n-j} [\sum_{j=0}^{n-m} c_j x^{j}]$$

$$= a_n x^n + \sum_{j=1}^{n} (\sum_{i=1}^{m} d_{ij} + a_{n-j}) x^{n-j} + \sum_{j=1}^{m}. -b_{m-j} x^{n-j} [\sum_{j=0}^{n-m} c_j x^{j}]$$

$$= a_n x^n + \sum_{j=1}^{n} a_{n-j} x^{n-j} + \sum_{j=1}^{n} (\sum_{i=1}^{m} d_{ij} x^{n-j}) + \sum_{j=1}^{m}. -b_{m-j} x^{n-j} [\sum_{j=0}^{n-m} c_j x^{j}]$$

$$= A(x) + \sum_{j=1}^{n} (\sum_{i=1}^{m} d_{ij} x^{n-j}) + \sum_{j=1}^{m}. -b_{m-j} x^{n-j} [\sum_{j=0}^{n-m} c_j x^{j}]$$

Por lo tanto $Q(x)\,B(x) + R(x) = A(x) + D(x)$ donde

$$D(x) = \sum_{j=1}^{n} (\sum_{i=1}^{m} d_{ij} x^{n-j}) + \sum_{j=1}^{m}. -b_{m-j} x^{n-j} [\sum_{j=0}^{n-m} c_j x^{j}]$$

El problema se reduce entonces a probar que $D(x) = 0$. El primer término de D(x) se expresa como:

$$\sum_{j=1}^{n} \sum_{i=1}^{m} d_{ij} x^{n-j} = \sum_{i=1}^{m} \sum_{j=1}^{n} d_{ij} x^{n-j} = \sum_{i=1}^{m} \sum_{j=i}^{n-m+i} c_{j-i} b_{m-i} x^{n-j} = \sum_{i=1}^{m} \sum_{k=0}^{n-m} c_k b_{m-i} x^{n-i-k}$$

Esto por la definición de d_{ij}, y haciendo el cambio de variable j = i+k. Por otra parte, el segundo término de D(x) se expresa como:

$$\sum_{j=1}^{m} . -b_{m-j}x^{n-j} [\sum_{j=0}^{n-m} c_j x^{-j}] = \quad \text{(sustituyendo j por i)}$$

$$\sum_{i=1}^{m} . -b_{m-i}x^{n-i} [\sum_{j=0}^{n-m} c_j x^{-j}] = \quad \text{(i y j son variables independientes)}$$

$$-\sum_{i=1}^{m} .[\sum_{j=0}^{n-m} b_{m-i}c_j x^{n-i-j}] = \quad \text{(sustituyendo j por k)}$$

$$-\sum_{i=1}^{m} [\sum_{k=0}^{n-m} b_{m-i}c_k x^{n-i-k}] \text{ . Por lo tanto D(x) = 0 Q.E.D.}$$

Nota. Como puede observarse, la prueba se hizo asumiendo que el polinomio B(x) es mónico (i.e. b_m=1), no así con el polinomio A(x). Podría hacerse la prueba con toda generalidad, sin embargo, esto hace la prueba sumamente engorrosa (y también la aplicación del algoritmo). En la práctica es más cómodo factorizar b_m y luego aplicar el algoritmo.