Guion o Resumen.

La aplicación de la aritmética de residuos a las computadoras

Esta sección se ocupa del tema de la aritmética de residuos y su aplicación a la organización de computadoras digitales.

Se enfoca en la descripción del sistema numérico de residuos como una alternativa a los sistemas numéricos ponderados de base fija de los cuales el sistema decimal y binario son ejemplos típicos. Aunque los sistemas numéricos de base fija tiene muchas ventajas, también tienen desventajas que limitan la velocidad al efectuar operaciones aritméticas, todas las operaciones aritméticas excepto la división, son por principio sin acarreos; eso es, cada digito en el resultado es una función que solo de los dígitos correspondientes a los operandos.

Por consecuencia la suma, sustracción y multiplicación se pueden efectuar en un "computador de residuos" en menos tiempo del que sería posible en un computador binario equivalente.

Introducción a los sistemas numéricos.

Los sistemas numéricos se pueden clasificar en posicionales y no posicionales. Los números romanos, son un ejemplo típico de un sistema no posicional. Los posicionales no fueron posibles sino hasta que los hindúes introdujeron el concepto del número 0 en alrededor del siglo XII D.C.

En esos sistemas, la posición del digito en un numero implica cierto peso por el cual se multiplica este digito.

Se dice que el sistema numérico tiene una base fija o radical fijo. Por ejemplo, si Wi=10^i o Wi=2^i se obtienen los sistemas numérico decimal y binario conocidos respectivamente. El sistema numérico binario se usa en los computadores con mucha más frecuencia que su contra parte decimal, un sistema numérico que no es de base fija se dice que es de base mixta, un ejemplo de un sistema de base mixta llamado sistema numérico de residuos, en particular un sistema numérico puede tener la propiedades de rango, unicidad y no redundancia.

El rango del sistema numérico se define como el máximo intervalo en el que cada entero se puede representar de manera única. Los numéricos como el binario y el decimal pueden representar cualquier entero y se que tiene un rango ilimitado.

Un sistema numérico tiene la propiedad de unicidad si cada número en el sistema se puede representar de una sola manera.

Los sistemas numéricos decimal y binario se han usado para efectuar aritmética en los computadores digitales debido a las siguientes ventajas

1. La comparación algebraica de los 2 números se puede mecanizar con facilidad
2. El rango de estos sistemas numéricos se puede extender al añadir mas posiciones de dígitos
3. La multiplicación por el radical fijo se pueden hacer desplazando las posiciones de los dígitos en la memoria

4. La lógica requerida para efectuar una operación aritmética en particular (como la suma) es más o menos la misma para todas las posiciones de dígitos
5. La detección de rebasamiento es fácil

Los sistemas numéricos decimal y binario poseen propiedades que son directamente responsable de las ventajas mencionadas con anterioridad, pero estas misma propiedades limitan la velocidad a la cual se pueden efectuar las operaciones aritméticas.

Para eliminar el problema de propagación del acarreo, se pueden usar las siguientes alternativas:

1. Usar circuitos especiales de acarreo "que vean hacia adelante"
2. Escoger un sistema numérico que tenga atributos especiales de acarreo

Muchos computadores tienen cierto número máximo de bits o de tamaño de palabra para la representación de un entero. El número de bits varia de un mínimo a un máximo de 64. Consideres el caso en el que solo están disponibles 30 bits para la representación de la magnitud de un número. Es obvio que un sistema así solo es posible representar m=2^30 números distintos, y cada número real se puede considerar como equivalente de los 2^30 números.

Aritmética Residual

En el sistema numérico residual todas la operaciones aritméticas excepto la división son sin acarreo; o sea cada digito en el resultado es una función de solo los dígitos correspondientes a los operados. Por consecuencia como la suma, sustracción y la multiplicación se pueden efectuar en un "Computador de residuos" en menos tiempo que lo que sería posible en un computador binario equivalente (en lo que se refiere a velocidad y rango numérico).

Algunas de las desventajas del sistema numérico residual cuando se compara con los sistemas numéricos de base numérico como sigue:

1. La comparación de los números es difícil
2. Es difícil de terminar si ha ocurrido un rebasamiento
3. La división es compleja
4. El sistema numérico residual no es conveniente para la representación de fracciones
5. La aritmética residual solo se puede justificar si hay métodos eficientes de conversión hacia el sistema numérico residual

$$<x1,x2,x3,\ldots,xr>=<x \bmod m1, x \bmod m2, x \bmod m3,\ldots,x \bmod mr>$$

Esto se llama representación modular o de residuo de x

Como un ejemplo, Sea m=30 de manera que m1=2, m2=3, m3=5 con Z30 =Z2 X Z3 X Z5

	Dígitos de residuos				Dígitos de residuos		
	Módulos				Módulos		
x	2	3	5	x	2	3	5
0	0	0	0	15	1	0	0
1	1	1	1	16	0	1	1
2	0	2	2	17	1	2	2
3	1	0	3	18	0	0	3
4	0	1	4	19	1	1	4
5	1	2	0	20	0	2	0
6	0	0	1	21	1	0	1
7	1	1	2	22	0	1	2
8	0	2	3	23	1	2	3
9	1	0	4	24	0	0	4
10	0	1	0	25	1	1	0
11	1	2	1	26	0	2	1
12	0	0	2	27	1	0	2
13	1	1	3	28	0	1	3
14	0	2	4	29	1	2	4

<x1,x2,x3>=<x mod m1,x mod m2, x mod m3>

Una propiedad importante de la aritmética es la ley de cancelación de la multiplicación.

(ca) mod m=(cb) mod m → a mod m = b mod m

Teorema de Fermat: Si a es un entero y m es un primo, entonces:

a^m mod m = a mod m