

EL CRC

Ing. Iselia Ibañez A.

S1 CHEQUEO DE REDUNDANCIA CICLICA (CRC) es una forma de detectar errores en almacenamiento o transmisión de datos. Se trata de un sistema de detección de errores sumamente común, presente no sólo en los sistemas de comunicaciones sino en los propios de almacenamiento (discos, cinta, etc.). En comunicaciones, el CRC se usa especialmente con protocolos sincrónicos como BSC, SDLC y HDLC, usando lo también las redes locales.

Un controlador de disco, por ejemplo, calcula el CRC a medida que escribe un sector de dicho disco y luego anexa el CRC a los datos. Cuando posteriormente tenga que leer los datos nuevamente, calculará el CRC a partir de los datos recuperados y lo comparará con el CRC grabado. Si los valores del CRC difieren se ha producido un error. Por cierto exprofeso hay quienes protegen sus discos de las copias modificando, en bajo nivel, el CRC de algunos sectores, con lo cual el sistema operativo tomará por defectuoso el sector correspondiente.

En los sistemas de comunicaciones el resultado del CRC se puede enviar junto con los datos originales. Cuando se reciben los datos, de nuevo se aplica sobre ellos el algoritmo del CRC comparando el resultado obtenido con el CRC que se ha recibido. Si ha ocurrido un error, es sumamente probable que se obtenga un resultado diferente de CRC. Cuando el resultado es idéntico, el extremo receptor envía un

carácter ACK de Reconocimiento con lo cual el extremo transmisor da por terminada la función de buffering del cuadro en cuestión. En cambio, cuando en el extremo receptor el cálculo de CRC no coincide con el proveniente del transmisor, aquél pide la repetición de la información generalmente vía un cuadro que indica falta de reconocimiento (NAK). El extremo receptor repite este proceso hasta

trarse que un polinomio CRC bien construido detectará:

- Cualquier tren de errores continuos de menor o igual grado que el polinomio.
- Todo número impar de errores a lo largo del bloque.
- Todos los errores de 2 bits en cualquier lugar del bloque.
- La mayoría de los otros casos de cualquier número de errores en cualquier parte de los datos.

Por lo dicho se detectarán todos los errores de menor duración, o sea de 1, 2 ó 3 bits. Por supuesto hay una pequeña posibilidad de que algunos errores no sean detectados. Esto ocurre cuando el patrón de errores resulta en un nuevo bloque que al serle aplicado el algoritmo produzca un mismo CRC. Con un determinado CRC de 16 bits, por ejemplo, por cada 65575 patrones de errores que en promedio se detecten, habrá uno que no alcanzará a serlo. Es decir, se detectará más del 99,998 por ciento de todos los errores posibles, lo que también puede ponerse como un Tasa de Error de Bits o BER ligeramente mayor a $1,5 \times 10^{-5}$.

No existe técnica que se pueda usar para garantizar absolutamente la detección de cualquier tipo de error, pero sí se pueden minimizar los errores no detectados a un costo razonable y con un bajo overhead, tal como en el caso mencionado, de sólo 2 bytes en un mensaje de varios cientos de bytes.

POLINOMIO CRC

El algoritmo del CRC

FIGURA 1

SÍMBOLO Y EXPRESIÓN BOOLEANA
 $Y = A \oplus B$

TABLA DE VERDAD

| Entrada | | Salida |
|---------|---|--------|
| A | B | Y |
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

TUTORIAL

opera sobre un bloque completo de datos. Se puede entender mejor el CRC si se ve este bloque de datos como de un único y gran valor numérico. El algoritmo del CRC divide dicho valor por un número llamado el POLINOMIO GENERADOR del CRC, dejando el residuo, que es nuestro CRC (*).

El Polinomio Generador se diseña y elabora para que tenga ciertas propiedades deseables de detección de errores. La idea es que el efecto de un bit se refleje en varios bits del resultado, lo que lleva a vez a polinomios más de 8 bits para facilitar la detección de trenes de errores de longitud similar. Si los polinomios CRC están bien elaborados, la principal diferencia entre ellos está dada por sus longitudes. Los polinomios de mayor grado proporcionan mayor seguridad en la precisión de los datos y se pueden usar con trenes de datos de mayor longitud. Además, en un polinomio CRC adecuado, tanto el Bit Más Significativo (MSB) como el Bit Menos Significativo (LSB) son siempre iguales a 1.

Por lo dicho antes, lo que nos interesa es el resto de la operación CRC, que por cierto es de un grado menor que el Polinomio Generador. Así, se puede pensar en un CRC de 16 bits, aunque su polinomio generador verdaderamente contiene 17 bits (desde el bit 16 hasta el 0). En este caso entonces es suficiente un registro de 16 bits para operaciones con CRC.

FIGURA 2

- 1) Polinomio Mensaje $M = 110101$ ($X^5 + X^4 + X^2 + X^0$)
Polinomio Generador $G = 11001$ ($X^4 + X^3 + 1$)

M tiene 6 bits de datos
G tiene 5 bits por lo que producirá un CRC de 4 bits; en consecuencia: $k = 4$.

- 2) Multiplicando el mensaje M por X^k da:
 $X^k \times M = X^4(X^5 + X^4 + X^2 + X^0) = X^9 + X^8 + X^6 + X^4$
El equivalente binario de este producto tiene 10 bits y es igual a:
1101010000
- 3) Se divide por G el producto obtenido

$$\begin{array}{r} X^k \times M \longrightarrow 1101010000 \\ \underline{11001} \\ 11100 \\ 11001 \\ \hline 10100 \\ 11001 \\ \hline 1101 \end{array} \quad \begin{array}{c} 11001 \leftarrow G \\ 100101 \leftarrow C \text{ (Cociente)} \\ \hline R = \text{Resto} = \text{CRC} \end{array}$$

- 4) El resto R se suma a $X^k \times M$ para dar la información a transmitir:
1101011101
- 5) La información recibida se divide por G dando un resto nulo:

$$\begin{array}{r} 1101011101 \\ \underline{11001} \\ 11111 \\ 11001 \\ \hline 11001 \\ 11001 \\ \hline 00000 \end{array} \quad \begin{array}{c} 11001 \\ \hline 100101 \end{array}$$

Pero hay algo más: el CRC usa el polinomio binario de módulo 2. El polinomio en cuestión difiere ligeramente de la aritmética normal y es generalmente la parte más confusa del CRC. Lo anterior significa que se trabaja con el valor absoluto (no relativo) de cada uno de los dígitos

que lo componen, por lo que no hay operación de acarreo o pedido de prestado entre posiciones contiguas ya que cada dígito se calcula por separado.

Las operaciones en módulo 2 se efectúan lógicamente, bit por bit; en módulo 2, la operación de suma es un "O EXCLUSIVO" lógico de los valores dados mientras la resta en módulo 2 es exactamente la misma operación. Esta operación es conocida también como XOR (EXCLUSIVO OR).

La salida de un O EXCLUSIVO de dos entradas es un '1' si una y sólo una de las entradas es '1' como puede verse en la Tabla de Verdad

El CRC se implementa en hardware con registros por desplazamiento del tipo Flip-Flop y compuertas XOR

TUTORIAL

de la Figura 1, donde también se ilustra el símbolo de la compuerta electrónica que ejecuta esta operación así como la expresión booleana correspondiente.

En realidad se usa el álgebra de módulo para los CRC por tratarse de un procedimiento simple que, como se dijo, no requiere operaciones de acarreo o pedir prestado. Ocurre que en el hardware de computación, un circuito de acarreo contribuye a la mayor parte del tiempo de un cálculo, lo cual implica una limitación en la velocidad del sistema. Por otra parte téngase en cuenta que las operaciones tipo módulo disponibles en los lenguajes de programación, operan en un número como conjunto y no precisamente en cada uno de los bits que lo componen.

OPERACION CON EL CRC

Siguiendo el esquema previsto, podemos decir que una división de polinomios módulo 2 es muy similar a la división binaria común, excepto que efectúa una operación lógica XOR.

Dado un polinomio mensaje M y un polinomio generador G , el objetivo es construir un nuevo polinomio que pueda dividirse íntegramente por G . Llamando C al cociente y R al resto tenemos:

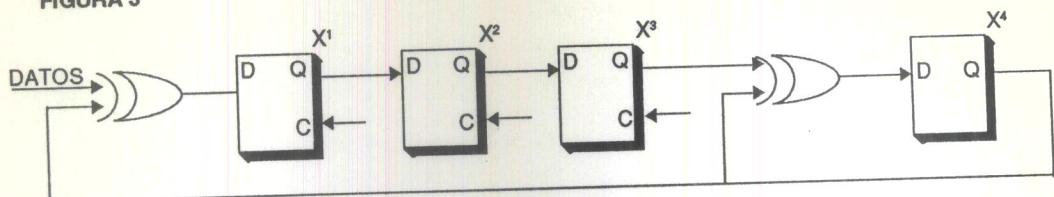
$$\frac{M}{G} = C \oplus \frac{R}{G}$$

Ya dijimos que en la aritmética del módulo 2, el resultado de una resta es equivalente al resultado de la suma. Aplicando esta propiedad más algunos pasos algebraicos se obtiene:

$M \oplus R = C \times G$
El algoritmo CRC calcula R y lo coloca a continuación del mensaje a enviar. Puesto que $M \oplus R$ es igual a $C \times G$, el mensaje codificado resultante será igualmente divisible por G , si y sólo si no haya cambiado

- 1) Multiplicar el mensaje M por X^k , donde k es el grado del CRC.
- 2) Dividir el producto resultante $X^k \times M$ por el polinomio generador G .
- 3) Desechar el cociente y agregar el resto R al producto para obtener el polinomio mensaje codificado, todo

FIGURA 3



ningún bit. En el extremo receptor, el mensaje recibido se divide por el polinomio generador G . Si el resto no es cero, se asume que se está frente a un error. En cambio si el resto vale cero, se asume que no han ocurrido errores o si así hubiera ocurrido, no ha podido ser detectado por el algoritmo.

Debe reconocerse que al no haber

El CRC usa el polinomio binario de módulo 2

acarreos o pedidos de prestado, el efecto de las sucesivas divisiones de los bits de datos en los correspondientes restos, perduran hasta que se hayan seguido "bajando ceros" en una cantidad igual al grado del polinomio generador, que también será la cantidad de bits del resto CRC buscado. Esto explicará el paso 1) del procedimiento algebraico detallado que sigue.

lo cual se representa como:

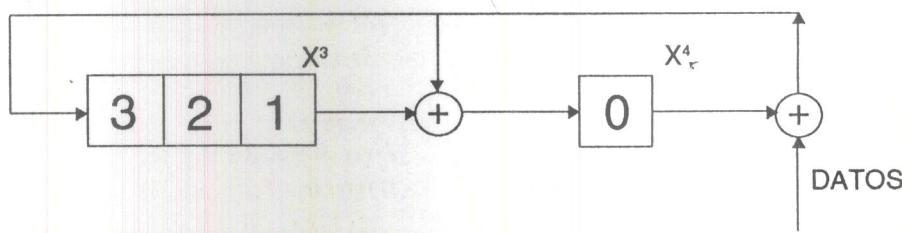
$$X^k \times M \oplus R$$

En la Figura 2 puede apreciarse un ejemplo bastante simple para visualizar este proceso. Dados los polinomios Mensaje y Generador (Paso 1), se multiplica el primero por el monomio de grado igual al grado del polinomio generador (Paso 2). A continuación se efectúa la división del producto recién obtenido por el polinomio generador (Paso 3). La información a transmitir se forma (Paso 4) con el agregado a continuación del Mensaje, del Resto obtenido en el paso anterior. Finalmente la estación receptora divide la información recibida por el mismo polinomio generador (Paso 5). Si no ha habido error, la división dará un resto nulo por lo que supuestamente el mensaje es correcto. Un resto distinto de cero indicará error.

IMPLEMENTACIONES POR HARDWARE

Puesto que la aritmética del CRC se realiza en módulo 2, es fácilmente

FIGURA 4



TUTORIAL

implementada en hardware con registros por desplazamiento del tipo Flip-Flop y compuertas XOR. La configuración del registro se basa en el código CRC que se desea implementar. El número de etapas del registro es igual al grado del polinomio generador; el número de elementos O EXCLUSIVO también es función de dicho polinomio. Debe también tenerse presente que en estas implementaciones, el bit tratado en primer término es el menos significativo, precisamente por ser el primero en enviarse.

La Figura 3 presenta un primer acercamiento a la solución por hardware siempre para el ejemplo dado. Como puede observarse basta realimentar la salida a los puntos donde el divisor no es nulo (o sea vale '1'), entre ellos la entrada que justamente siempre es '1' en los casos prácticos del CRC. En dicha figura además de las compuertas XOR ya vistas, los

FIGURA 5

| FF3 | FF2 | FF1 | FF0 | DATOS REALIM. |
|-----|-----|-----|-----|---------------|
| 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 | |

Realimentación = estado anterior FF0 + bit actual de datos

FF3 = Realimentación

FF2 = estado anterior FF3

FF1 = estado anterior FF2

FF0 = estado anterior FF1 + Realimentación

Compuworld s.r.l. Communications Division

Capacitación: Curso Lectivo 1993

CURSOS REGULARES

Teleprocesamiento de Datos: Introducción, nivel avanzado y Senior - Comunicación de datos con la PC - Medios de comunicación - Normas de la comunicación de datos - Líneas telefónicas, coaxil y fibra óptica - Introducción a los protocolos: X.25, SDLC - Integración de voz, fax, video y datos - Comunicaciones vía satélite.

CURSOS ESPECIALES

Cálculo de radioenlaces. Integración de centrales telefónicas y sistemas mediante enlaces digitales. Actualización sobre nuevas tecnologías. Seguridad en las comunicaciones. Interconexión de LANs. Actualización a nivel gerencial.

Estos cursos se dictan en nuestras aulas y laboratorios por profesionales de destacada trayectoria en empresas de comunicaciones de primer nivel combinando un 70% de teoría y un 30% de práctica, para un cupo limitado a 12 participantes que redibuirán material didáctico, refrigerio y certificado de asistencia.

CURSOS A PEDIDO

En su empresa, de acuerdo al equipamiento y horario solicitado.

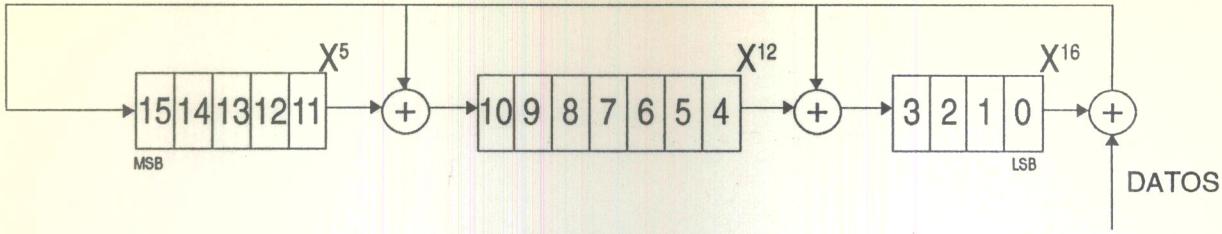
SERVICIOS

Soporte de ingeniería, confección de pliegos de licitaciones del área, auditoria de comunicaciones, diseño de redes y enlaces. Adaptación de tecnologías y configuraciones. Orientación y gestión de demostraciones. Soporte para proveedores del exterior. Verificación y puesta en marcha de nuevos productos, etcétera.

Diagonal Roque Sáenz Peña 1116, Piso 7. Tel.: 35-8727/7708/7806

TUTORIAL

FIGURA 6 - CRC - CCITT



bloques rectangulares representan las etapas del registro por desplazamiento que se realizan con Flip-Flops de retardo (D) activados por un mismo reloj (C) para provocar los sucesivos desplazamientos.

Esta configuración reproduce la disposición de la división anterior-

En cambio, si cada vez que un bit de datos entra a la cadena de desplazamiento se procesa con las funciones XOR existentes, la operación siguiente al ingreso del último bit del mensaje (dividendo) dará lugar directamente al resto (Figura 4). Es conveniente observar que el ordena-

Con esta última implementación, en la Figura 5 puede verse el esquema correspondiente a los estados de los diferentes Flip-Flops para cada una de las secuencias de reloj. Para la construcción de este esquema debe tenerse presente el siguiente procedimiento:

1) Cuando un FF recibe información sólo de otro FF: *el estado de un Flip-Flop en un momento dado es igual al estado del Flip-Flop que lo antecede en el ciclo anterior.*

2) Cuando un FF recibe información a la salida de una compuerta XOR: *el estado de un Flip-Flop en un momento dado es el resultado XOR entre el estado, en el ciclo anterior, del Flip-Flop que lo antecede y la realimentación correspondiente.*

En la Figura 5 puede verse el resultado XOR (Realimentación) del FF0 y el bit de datos que está entrando, ubicado ANTES de un nuevo ciclo de reloj (por eso está un renglón por arriba). Cada valor de esta columna será de hecho el correspondiente al FF3 en el ciclo siguiente. El resto así determinado es el mismo de la división efectuada antes, sólo que el orden está invertido puesto que el bit del FF0 es el primero que se envía.

Téngase en cuenta que los diagramas de hardware se dan sólo como ejemplos. Los CRCs muy cortos son de uso práctico limitado y hay mejores formas de realizar el trabajo en

POLINOMIOS

Un polinomio es un valor expresado en una forma algebraica particular, tal como:

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x^1 + a_0$$

Ya que la aritmética decimal usa polinomios de base constante, todos nosotros sabemos como hacer polinomios aritméticos con base constante igual a 10 y no es difícil extrapolar el concepto a la base binaria,

Nuestro sistema de numeración común es un polinomio implícito de base 10, o sea $x=10$. Cada dígito en realidad significa que su valor se multiplica por la potencia de 10 asociada. Otro polinomio aritmético que todos conocemos es el sistema de numeración de base 2 ó binario, donde el peso relativo de los dígitos será de derecha a izquierda: 1, 2, 4, 8, 16, etc. Tampoco falta quien maneje con bastante facilidad el sistema de base 16 o hexadecimal: 1, 16, 256, 4096 (4 K), 65536 (64 K), 1048576 (1 M), etcétera.

Los polinomios están clasificados por el coeficiente distinto de cero y correspondiente al mayor grado o exponente de la variable "x". Por ejemplo, para el CRC se usan el CRC-16 y el CRC-CCITT que son de grado 16, lo que significa que los bits desde 16 hasta 0 son significativos lo que nos dice que un polinomio de grado 16 tiene 17 bits.

mente realizada y por lo tanto se deben entrar ceros adicionales (4 en nuestro ejemplo) para expulsar el último bit de los datos y así recuperar totalmente el resto en el registro por desplazamiento.

miento se lo ve invertido debido a que por norma las etapas de los circuitos electrónicos "avanzan" de izquierda a derecha, mientras que en el sistema de numeración el LSB está a la derecha y el MSB a la izquierda.

(Continúa en pág 45)

EL CRC

(Viene de pág. 34)

cuestión. En la práctica, el polinomio generador es más elaborado que el usado en nuestro análisis. Para el caso hay dos polinomios de 16 bits muy conocidos: CRC-16 (que se usó originalmente con el protocolo Bisíncrónico) y el CRC-CCITT (que se usa con el SDLC, HDLC, almacenamiento en discos y en la versión correspondiente del XMODEM). Mientras el CRC-16 está dado por:

100 Mbp por UTP

(Viene de pág. 38)

con lo que se reduce la frecuencia de trabajo y por ende la atenuación. A su vez, al no haber transmisiones

$$X^{16} + X^{15} + X^2 + 1$$

el polinomio CRC-CCITT responde a la expresión:

$$X^{16} + X^{12} + X^5 + 1$$

y su implementación puede verse en la Figura 6.

Finalmente podemos comentar que algunas rutinas CRC implementadas por software emulan el procedimiento por hardware, o sea de a un bit por vez. Sin embargo como los procesadores comunes no operan directamente en el modo bit (sino byte,

palabra, etc.), el método por software requiere una gran cantidad de ciclos de la CPU. Debido a esto la mayoría de las rutinas tratan de explotar el cálculo a nivel de byte, de la mejor manera posible tratando de afectar lo menos posible al rendimiento del sistema. ▲

(*) En realidad el residuo debiere considerarse como un BCC (Carácter de Chequeo del Bloque) reservando el nombre CRC para el sistema de detección. La práctica usual, sin embargo le da también el nombre CRC al residuo en cuestión.

simultáneas en ambos sentidos no existe el NEXT. Como además se puede trabajar hasta 100 metros con UTP 3, según los propulsores del sistema, los costos totales (con tarjetas específicas) pueden estar en poco más del doble del 10BASE-T actual.

De cualquier manera todavía no está muy definida la ventaja de este último método ya que por ejemplo una tarjeta binorma (10 y 100 Mbps) sería bastante más costosa y los hubs adecuados -que deberán cumplir ciertas funciones de enrutado- serán también más costosos de lo supuesto. ▲

COLABORADORES

SEA UD. TAMBIEN PARTE DE LAN & WAN

Si Ud. posee experiencia en LANs, WANs o temas de comunicaciones y desea colaborar en notas para ser publicadas, contáctese con **LAN & WAN**.

Hay un espacio reservado para su nota, tanto sea de índole práctica, conceptual o bien que se trate de trabajos específicos que puedan ser de interés para nuestros lectores.

Si está interesado en esta propuesta, concerte una entrevista personal con nuestra redacción por los teléfonos **40-4638 o 46-8980** o bien diríjase por carta -acompañando un breve currículum- a **LAN & WAN**, Casilla de Correo 1975, 1000 Buenos Aires, Argentina.