Instituto Politécnico Nacional
Escuela Superior de Cómputo
Redes de Computadoras
Tarea 3: Polinomio
Alumno: Meza Zamora Abraham Manuel

1. Comprobación de redundancia cíclica

Comprobación de redundancia cíclica o control de redundancia cíclica (en informática, CRC). Hace referencia a cyclic redundancy check, también llamado polynomial code checksum. El CRC es una función diseñada para detectar cambios accidentales en datos de computadora y es comúnmente usada en redes digitales y dispositivos de almacenamiento (como discos duros).

El CRC fue creado por W. Wesley Peterson en 1961; el polinomio de 32 bits usado en funciones CRC de Ethernet (y otros estándares) fue publicado en 1975. Es muy popular por su simpleza de implementación, fácil de analizar matemáticamente y es muy bueno detectando errores causados por ruidos en los canales de transmisión.

2. Descripción del Algoritmo

La comprobación de redundancia cíclica consiste en la protección de los datos en bloques, denominados tramas. A cada trama se le asigna un segmento de datos denominado código de control (al que se denomina a veces FCS, secuencia de verificación de trama, en el caso de una secuencia de 32 bits, y que en ocasiones se identifica erróneamente como CRC). El código CRC contiene datos redundantes con la trama, de manera que los errores no sólo se pueden detectar sino que además se pueden solucionar.

El término suele ser usado para designar tanto a la función como a su resultado. Pueden ser usadas como suma de verificación para detectar la alteración de datos durante su transmisión o almacenamiento. Las CRC son po-

pulares porque su implementación en hardware binario es simple, son fáciles de analizar matemáticamente y son particularmente efectivas para detectar errores ocasionados por ruido en los canales de transmisión.

3. Funcionamiento del CRC

A cada bloque de datos le corresponde una secuencia fija de números binarios conocida como código CRC (esto se calcula con una misma función para cada bloque). Ambos se envían o almacenan juntos. Cuando un bloque de datos es leído o recibido, dicha función es aplicada nuevamente al bloque, si el código CRC generado no coincide con el código CRC original, entonces significa que el bloque contiene un error. Eso hará que el dispositivo intente solucionar el error releyendo el bloque o requiriendo que sea enviado nuevamente.

Si coinciden ambos códigos CRC, entonces se asume que el bloque no contiene errores (existe una remota posibilidad de que haya un error sin detectar). El nombre çontrol/comprobación de redundancia cíclica"se debe a que se çontrola"(verificación de datos) un código redundante (no agrega nueva información, el código CRC representa el mismo bloque de datos) y el algoritmo está basado en códigos cíclicos. Es importante destacar que el número de caracteres de entrada a la función CRC puede tener cualquier longitud, pero siempre producirá un código CRC de igual longitud.

4. Polinomios generadores

Los polinomios generadores más comunes son:

- CRC-12: X12 + X11 + X3 + X2 + X + 1
- CRC-16: X16 + X15 + X2 + 1
- CRC CCITT V41: X16 + X12 + X5 + 1(este código se utiliza en el procedimiento HDLC)
- CRC-32 (Ethernet): = X32 + X26 + X23 + X22 + X16 + X12 + X11 + X10 + X8 + X7 + X5 + X4 + X2 + X + 1

- CRC ARPA: X24 + X23+ X17 + X16 + X15 + X13 + X11 + X10 + X9 + X8 + X5 + X3 + 1