Diseño de un Decodificador Universal de Códigos de Control de Errores, Usando Técnicas Algebraicas

Mat. Ricardo Barrón Fernández
Jefe del Departamento de Matemáticas del CINTEC-IPN
Ing. Valente López Muñoz
Profesor e Investigador del CINTEC-IPN
Ing. Osvaldo Espinosa Sosa
Profesor e Investigador del CINTEC-IPN

En este artículo se presenta un decodificador universal de códigos de control de errores, que permite reconocer y en su caso reconstruir una amplia gama de alfabetos, dentro de los más usados en las comunicaciones digitales. Todo canal de comunicación digital presenta un riesgo de pérdida de la información transmitida, lo cual se pretende resolver codificando la información de tal manera que al recuperarla en el receptor se pueda reconstruir la señal original (dentro de cierto margen de error). Las técnicas algebraicas de tratamiento de código están basadas en las herramientas tradicionales del procesamiento digital de señales: convolución, filtros y sobre todo Transformada de Fourier. Todo esto trabajando no sobre los dominios usuales (números reales y complejos) sino sobre campos finitos (Campos de Galois), haciendo una síntesis interesante entre álgebra moderna, filtrado clásico y teoría de números.

Transformada de Fourier Sobre Campos Finitos

Los ejemplos típicos de campos como conjunto algebraico son los números reales y complejos. La característica principal de estos conjuntos es que constan de dos operaciones, suma y producto, que se relacionan entre si por medio de la propiedad distributiva, y debido a la existencia única de los inversos en la suma y el producto se puede restar y dividir.

Los números reales y complejos no son los únicos conjuntos a los que se puede dotar de una estructura de campo. En diversas áreas de la ingeniería, sobre todo en comunicaciones, surgen conjuntos, especialmente finitos, que por su naturaleza propia tienen estructura de campo.

La teoría de los campos finitos surge a principios del siglo pasado gracias a los trabajos de Evaristo Galois en el problema de demostrar la imposibilidad de resolver una ecuación de quinto orden o más por medio de radicales.

Este concepto de considerar las propiedades generadoras independientes de los objetos donde se plasman fué, a la larga, la base del álgebra moderna.

Sea K igual al conjunto {0,1} con el producto binario usual y la suma modulo 2 forma un campo; para el caso de los campos finitos se puede hacer una tabla para el producto y otra para la suma, donde se puedan observar todas las propiedades. La notación para identificar a los campos finitos es GF(P) donde P es el número de elementos.

+	0	1
0	0	0
1	1	0

*	0	1
0	0	0
1	0	1

Tablas de suma y producto para GF(2)

Si se tiene un campo K siempre es posible construir un campo mayor, el cual está formado por vectores de K; a este campo se le conoce como una extensión de K. A estos vectores de K se les puede acomodar como los coeficientes de un polinomio, es decir, existe una relación 1:1 entre

$$a=[a_0,...,a_n] \text{ y } a(x)=a_0+a_1x^1+,...,a_nx^n$$

donde cada a_k pertenece a K. Siendo este el caso, la suma vectorial equivale a la suma de polinomios y se puede definir el producto entre dos elementos, a(x) y b(x), como $c(x)=a(x)b(x) \bmod p(x)$, donde p(x) es un polinomio irreducible (en este caso de grado n+1). Con la suma definida como la suma usual de polinomios y el producto módulo con el polinomio irreducible, el conjunto de vectores del campo K forma un campo. Se puede observar que el punto clave para que exista una extensión de un orden dado es el polinomio irreducible, que en general no existe para cualquier campo y cualquier orden.

En particular, los números complejos se pueden considerar como una extensión de orden dos si se considera el polinomio $p(x)= 1+X^2$

sobre los reales, $GF(2^n)$; es decir, el conjunto de ceros y unos de tamaño n forma una extensión del campo k={0,1} (en teoría de códigos $GF(2^n)$ es uno de los campos más usados).

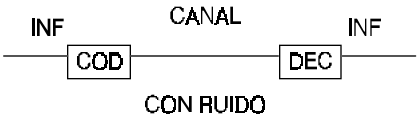
Si se tiene un elemento w en un campo finito y se consideran sus potencias sucesivas w^n, por estar sobre un conjunto finito es claro que en algún momento entre en un ciclo, y como $w^0=1$, el tamaño del ciclo se puede medir a partir de que se repite el valor 1. En general, se dice que w es de orden n si $w^n=1$. En los números complejos existen elementos de cualquier orden, pero en un campo cualquiera esto no es cierto en general. Si en un campo K se cuenta con un elemento w de orden n, entonces se puede definir la transformada de Fourier en base a este elemento como:

$$V_k = \sum_{m=0}^{n-1} v_m w^{mk}$$

Códigos Reed-Solomon

El objetivo principal de la codificación por bloques consiste en construir conjuntos de vectores de longitud n, tales que a pesar de que en cualquiera de ellos se modifiquen hasta t elementos, estos se puedan volver a reconstruir totalmente. Esta propiedad de regeneración es lo que permite que dichos conjuntos de vectores, llamados códigos, se puedan usar como contenedores de mensajes en un canal susceptible a errores.

La manera de diseñar este código consiste en construir sus elementos de tal forma que difieran entre si en al menos 2t +1 elementos. Si en un conjunto de vectores estos difieren entre si en al menos 2t +1 localidades correspondientes, al modificar cualquiera de ellos en t localidades diferirá de los demás en al menos t+1, por lo que su vector más próximo será él mismo antes de ser modificado. Esto quiere decir que, para decodificar un vector que se modificó en a lo más t localidades, basta encontrar el elemento del código más próximo a el.



Transferencia de información

Una manera de caracterizar a un vector de longitud n es a través de su complejidad cíclica, la cual se define como la capacidad que tiene el vector de producirse a si mismo a partir de sólo una parte de él.

$$v_k = -\sum_{m=1}^{t} h_m v_{<k-m>_n}$$

Esta ecuación puede verse en términos polinomiales como $h(x)v(x) = 0 \bmod x^n-1$, donde :

$$v(x)=v_0 + v_1 x +,...,+ v_{n-1} x^{n-1} \quad y$$

$$h(x)=h_0 + h_1 x +,...,+ h_t x_t,$$

donde $h(x)v(x)=0 \bmod x^n-1$ implica la convolución cíclica de los coeficientes de los polinomios y la complejidad cíclica como tal es el orden mínimo de h(x).

Suponiendo que los vectores H y V son la Transformada de Fourier de h y v, respectivamente, y que

$$H(x)V(x)=0 \bmod x^n-1$$

es decir, $V*H=0$

entones, por el teorema de convolución $h_k v_k=0$ (k=0,...,n-1) y si $v_k \neq 0$, entonces $h_k=0$; pero h_k es la Transformada Inversa de Fourier de H, por lo que:

$$h_k = 1/n \sum_{m=0}^{n-1} H_m w^{-mk} = 1/n\ H(x)\big|_{x=w^{-k}}$$

Esto significa que los valores de $v_k \neq 0$ están relacionados directamente con las raíces de H(x), y como el orden de un polinomio no puede ser menor que su número de raíces, el polinomio H(x) mínimo que anula a V(x) bajo la convolución cíclica tiene un orden igual al número de elementos de v_k que son diferentes de cero.

Al polinomio H(x) también se le conoce como polinomio localizador, dado que sus ceros $x=w^{-k}$ indican la posición donde v_k es diferente de cero.

En conclusión, se tiene que la complejidad cíclica de la Transformada de Fourier de un vector v es igual a su peso, donde el peso del vector es igual al número de elementos diferentes de cero.

De lo anterior se sigue que si H_k tiene 2t componentes consecutivos iguales a cero su transformada inversa h_k debe tener al menos 2t +1 elementos diferentes de cero para que la complejidad cíclica de H sea mayor que 2t y no se anule al autogenerarse cíclicamente; esta es precisamente la clave para la codificación.

Sea F un campo con un elemento de orden n. El código Reed-Solomon (n,n-2t) de longitud n con símbolos en F es el conjunto de todos los vectores con elementos en F que contienen 2t elementos consecutivos iguales a cero.

Normalmente las primeras n-2t localidades del vector son ocupadas por la información a codificar y las restantes son llenadas con ceros. Hay que notar que, en el dominio temporal, estos vectores difieren al menos en 2t+1 lugares, lo que era precisamente el objetivo.

0 0 0 7 0 7 7
0 0 0 7 1 1 4
0 0 0 7 2 0 1
0 0 0 7 3 6 2

*
*
*

Código Reed-Solomon (7,5)

Decodificación

Si se transmite un vector c miembro del código C, entonces del lado del receptor se tiene el vector v=c+e, donde el error e tiene a lo más t elementos diferentes de cero. Cada lugar donde e es cero indica que no hubo error en la transmisión, y donde e es diferente de cero se tiene un error. La función del decodificador es detectar el error (si lo hubo) y corregirlo, es decir, eliminarlo. En el dominio espectral el vector recibido tiene la forma siguiente:

$$V_k = \sum_{m=0}^{n-1} w^{mk} v_m \qquad (k=0,...,n-1)$$

con componentes :

$$V_k = C_k + E_k \quad (k=0, ..., n-1)$$

esto es porque en el dominio temporal se tiene $v_i=c_i+e_i$ (i=0,...,n-1) y la Transformada de Fourier es lineal.

Sin embargo, por construcción :

$$C_k=0 \quad (k=0,...,2t-1)$$

lo que implica que para estos valores de k, $V_k=E_k$, es decir, el vector en el receptor permite conocer una parte de la transformada del vector de error, con lo que el problema es encontrar la parte que falta. Si el vector de error e en el dominio temporal tiene a lo mas t elementos diferentes de cero, se puede encontrar un polinomio localizador H(x) de grado a lo más t y que

$$H(x)E(x)=0 \bmod x^n-1$$

es decir :

$$V_k = -\sum_{m=1}^{n-1} HmE<k-m>_n \quad (k=0,...,n-1)$$

Si los coeficientes del filtro H_m fueran conocidos se podría conocer el vector E en su totalidad, e invirtiéndolo conocer el vector de error e para descontarlo del vector recibido v y finalmente conocer el vector enviado, con lo cual estaría resuelto el problema. Pero, aunque los coeficientes H_m son desconocidos de entrada, se conocen los E_k para (k=0, ...,2t-1) con los cuales se puede plantear un sistema de ecuaciones para encontrar los coeficientes del filtro.

$$V_k=E_k = -\sum_{m=0}^{t} H_m E<k-m>_n \,(k=t,...,2t-1)$$

$$\begin{bmatrix} V_{t-1} & \cdots & V_0 \\ V_t & \cdots & V_1 \\ \cdot & & \cdot \\ \cdot & & \cdot \\ V_{2t-2} & \cdots & V_{t-1} \end{bmatrix} \begin{bmatrix} H_1 \\ \cdots \\ \cdot \\ \cdot \\ H_t \end{bmatrix} = - \begin{bmatrix} V_t \\ \cdots \\ \cdot \\ \cdot \\ V_{2t-1} \end{bmatrix}$$

En este caso se tiene t ecuaciones con t incógnitas, que son precisamente los coeficientes del filtro que se anda buscando.

Este sistema resulta tener una matriz tipo Toeplitz y que se puede resolver por diferentes métodos; sin embargo, en la práctica resulta mas eficiente usar el método de Berlekamp-Massey. Este método es un algoritmo iterativo que va encontrando los coeficientes del filtro por medio de aproximaciones sucesivas, que es más adecuado para ejecutarse en un sistema digital dedicado. El algoritmo se puede modificar para que no solo encuentre los coeficientes, sino que simultáneamente construya el vector de error en el dominio temporal, lo que es el objetivo central.

En **figura 1** se muestra una arquitectura que efectúa un algoritmo de Berlekamp-Massey modificado. Está constituida por un banco de registros de corrimiento auxiliares, un registro de entrada y uno de salida, y una unidad aritmética que efectúa suma y multiplicaciones de campo finito de acuerdo a un modulo programable. La unidad de control es la que se encarga de proporcionar todas las señales de sincronización y comandos necesarios para el funcionamiento del decodificador.

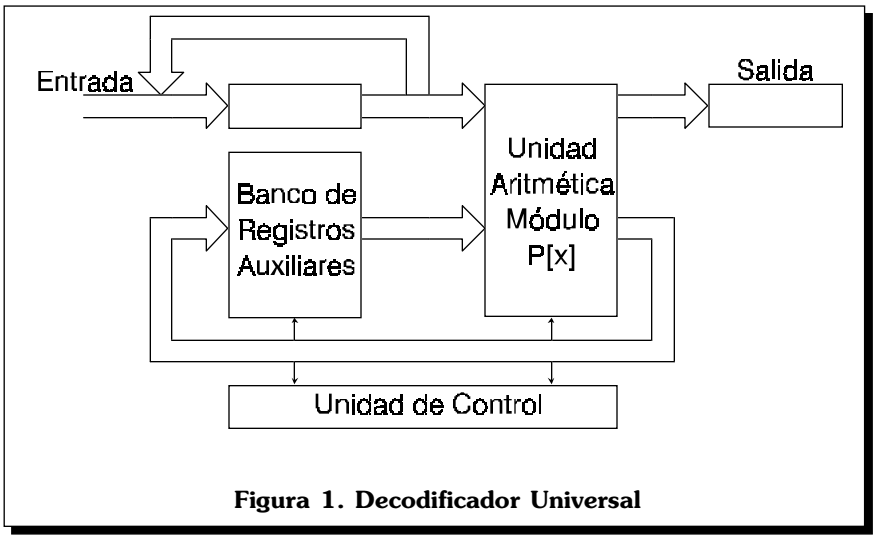


Figura 1. Decodificador Universal

Conclusiones

Las técnicas algebraicas permiten un trabajo simultáneo en el dominio temporal y de la frecuencia, a través de resultados duales que establecen una correspondencia uno a uno entre características espectrales y temporales de los códigos; algunas características de los códigos pueden fijarse más fácilmente en el dominio espectral y luego aplicar transformada inversa, que si se hiciera directamente en el dominio temporal. Esta visión dual permite economía y eficiencia en los algoritmos, y un mejor dominio conceptual del proceso global. La simplicidad de los algoritmos es trascendente sobre todo cuando estos tienen que implementarse en hardware.

Bibliografía y Referencias

[1] Salvatorre D. Morgera. *"Digital Signal Procesing"*. Academic Press,1989.

[2] E. R. Berlekamp. *"Agebraic Coding Theory"*. Mc Graw-Hill, 1968.

[3] D. G. Hoffman. *"Coding Theory"*. Dekker,1991

[4] R. E. Blahut. *"Algebraic fields, signal processing, and error control"*. Proc. IEEE, 73, 874-893 (1985).

[5] Emil Artin. *"Galois theory"*. Notre Dame, 1971.