

# Códigos RS y su aplicación a la capa física de 802.16 en FPGAs

Sergio Lujan, Sergio Almagro, Andrés Cabrera-Lozoya, Juan Suardíaz-Muro, Fernando Cerdan  
 Departamento Tecnologías de la Información y las Comunicaciones  
 Universidad Politécnica de Cartagena  
 Antiguo Cuartel de Antigones. Plaza del Hospital, Nº 1, 30202 Cartagena (Murcia)  
 {sergio.lujan, sergio.almagro, andres.cabrera, juan.suardiaz, fernando.cerdan}@upct.es

**Resumen.** Los códigos Reed-Solomon suponen una técnica muy útil en la transmisión de datos dentro de sistemas sensibles al retardo. En este artículo los analizamos desde el punto de vista teórico y de aplicación a la tecnología WiMAX, la cual los emplea como parte de su especificación. Dentro del documento discutimos los aspectos clave en la implementación del algoritmo que los genera y su implementación en FPGA's.

## 1 Introducción

Los códigos de corrección de errores se basan en la introducción de redundancia en los mensajes transmitidos con el fin de que, tras sufrir pequeñas alteraciones en la transmisión, los datos puedan ser corregidos sin necesidad de una nueva transmisión. En concreto, los códigos Reed-Solomon (RS) se han convertido en una de las operaciones básicas de procesamiento de señales en los sistemas de comunicaciones digitales.

Entre otras técnicas, tecnologías como WiFi o WiMAX hacen uso de códigos de corrección de errores RS para combatir el desvanecimiento [1]. Estos también están muy presentes en multitud de aplicaciones cotidianas de telefonía, comunicaciones por cable (xDSL) y de video (DVB) o audio (DAB) digitales, como por ejemplo las emisiones vía satélite de radio-televisión o la implantada Televisión Digital Terrestre.

Por otro lado, la gran flexibilidad que ofrecen las FPGAs hace factible la implementación de codificadores RS en ellas. Además, la posibilidad de realizar diseños divididos en módulos o bloques funcionales permite llevar a cabo las optimizaciones oportunas, incluso servir como base de un gran número de sistemas básicos de comunicación digital que utilicen este tipo de codificación. En este artículo se estudia el diseño concreto del código RS especificado en el estándar IEEE 802.16.

El resto del documento se desarrolla como sigue: en la sección 2 se describe cómo se llevan a cabo los procesos de detección y corrección de errores a partir de los códigos RS. En la sección 3 se estudian las especificaciones del estándar IEEE 802.16e para el código RS. La sección 4 trata la implementación de códigos RS en FPGAs. El documento finaliza con unas conclusiones en la sección 5.

## 2 Códigos Reed-Solomon

En este tipo de códigos, el número de posibles mensajes se incrementa al introducir redundancia debido a que el número de bits por mensaje aumenta. Lo que se hace en los códigos de corrección de errores es utilizar únicamente un subconjunto de estos posibles mensajes de modo que, si en recepción no se obtiene una secuencia de bits que coincida con uno de los mensajes válidos (codewords), se sabrá que dicha secuencia contiene errores.

Uno de los aspectos que cuantifica la calidad de estos códigos es la separación o distancia Hamming. Esta distancia se corresponde con el número de posiciones entre dos codewords cuyos bits toman valores diferentes. A partir de esta distancia se obtiene la distancia de código, siendo ésta la mínima distancia Hamming entre todas las posibles combinaciones de codewords. Es obvio que, cuanto mayor sea la distancia de código, mayor será la probabilidad de detectar y corregir los errores, pues la secuencia podrá tener un mayor número de bits erróneos que aún permitan distinguir el codeword al que corresponde. Así, la corrección del error puede llevarse a cabo siguiendo el procedimiento FEC (Forward Error Correction), consistente en encontrar el codeword o mensaje válido más próximo al mensaje recibido.

Dado que se trata de códigos lineales, sería lógico decir que para  $k$  bits existen  $M=2^k$  vectores distintos. Pero  $k$  se corresponde con el número de bits del mensaje que se desea transmitir, sin contar la redundancia. Por lo tanto, el tamaño del codeword que se transmite será  $n$  y la redundancia tendrá un tamaño  $n-k$ .

Los codewords ( $c$ ) se obtienen a partir del producto vectorial de una porción  $k$  del mensaje ( $m$ ) original por una matriz generatriz ( $G$ ) de tamaño  $k \times n$ . De modo que el resultado es un codeword de tamaño  $n$ :  $c[n] = m[k] \times G[k, n]$ .

## 2.1 Campos finitos o de Galois

Un código RS se define mediante un polinomio generatriz  $g(x)$ , un polinomio que define la base  $p(x)$  con raíz  $\alpha$ , un campo finito  $GF(2^m)$  y los tamaños de los datos de entrada y salida,  $k$  y  $n$ , respectivamente. Además, los elementos que componen cada codeword no son bits sino símbolos, los cuales forman parte de un campo finito o de Galois.

Cada secuencia de  $m$  bits de un mensaje original se codifica según los pesos:  $\{\alpha^{m-1}, \alpha^{m-2}, \dots, \alpha, 1\}$ . De modo que, para  $GF(2^3)$ , la secuencia binaria "100 000 010 001" correspondería a los símbolos " $\alpha^2 0 \alpha 1$ ".

La obtención analítica de la matriz  $G$  precisa de la utilización de operaciones definidas en campos finitos. Para el cálculo de cada una de las filas de la matriz se emplea la fórmula:

$$fila(j) = x^{n-j} + r^{n-j}(x)$$

Donde  $r^{n-j}$  es el resto de dividir  $x^j$  entre  $g(x)$ . La dificultad de esta división se encuentra en que se parte de un polinomio  $g(x)$  de la forma:

$$g(x) = \prod_{i=0}^{m-1} (x - \alpha^i)$$

La expansión de dicho polinomio para la división requiere ceñirse a una serie de reglas dado que los elementos que lo constituyen forman parte de un campo finito. Una de las principales propiedades es que la suma de los dos mismos elementos de un campo en nula:  $\alpha^n + \alpha^n = 0$ ; por tanto:  $\alpha^n = -\alpha^n$ . Con esta propiedad y partiendo del polinomio que define la base se puede obtener  $g(x)$  como suma de potencias de  $\alpha$  para poder realizar las divisiones polinómicas y obtener cada una de las filas de la matriz generatriz, que tiene la siguiente forma:

$$g(x) = \begin{pmatrix} 1 & 0 & \dots & 0 & p_{1,k+1} & \dots & p_{1,n} \\ 0 & 1 & \dots & 0 & p_{2,k+1} & \dots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & p_{k,k+1} & \dots & p_{k,n} \end{pmatrix}$$

## 2.2 Detección y corrección de errores

Cuando se generan los codewords, los  $k$  primeros símbolos corresponden a la misma secuencia de símbolos de entrada, ya que las primeras  $k$  columnas de la matriz  $G$  son una matriz identidad (figura 1).

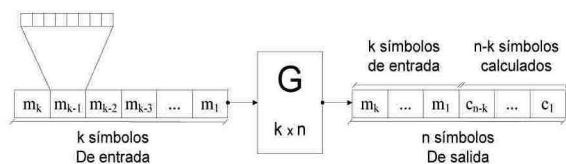


Fig. 1. Generación de codewords en los códigos RS.

Los  $n-k$  símbolos restantes forman parte de la redundancia del código RS.

En función de la distancia ( $d$ ) de este código, el número de símbolos erróneos corregibles viene dado por la fórmula:

$$t = \frac{d-1}{2}$$

Para la detección y corrección de errores es necesario obtener una matriz  $H$  tal que, si  $G = [I_k | P_{n-k}]$ , entonces  $H = [P^T | I_{n-k}]$ , de tamaño  $(n-k) \times n$ , y cumpliendo que el producto de  $G$  con  $H^T$  sea nulo.

Cuando se recibe un codeword se calcula su síndrome como el producto entre el codeword y la matriz  $H^T$ , de modo que, si se obtiene un resultado nulo, el codeword no contendrá errores y, si es distinto de cero, se habrá detectado un error.

Para corregir el error se calcula el síndrome del codeword recibido. Como es conocido el número de errores máximo que se pueden corregir, se pueden tener almacenados los síndromes de todos los posibles codewords erróneos y, a su vez, el codeword correcto al que se corresponde. De modo que, si el número de errores que contenía el codeword recibido no supera el límite máximo establecido por el código RS utilizado, se podrá obtener el mensaje correcto de forma directa.

Es importante destacar que los códigos RS son capaces de detectar y corregir los errores producidos en símbolos, no en bits. Es decir, si se tiene un  $GF(2^8)$  con el que se puedan corregir 8 símbolos, como cada uno de ellos equivale a  $m=8$  bits, se podría decir que sería capaz de corregir hasta  $8 \times 8 = 64$  bits. Para que esto fuese cierto, los 64 bits erróneos deberían de estar repartidos entre 8 símbolos como máximo, de lo contrario habría 9 o más símbolos con errores y este método no podría corregirlos.

## 3 Código RS en WiMAX

El estándar IEEE 802.16[4] define a nivel físico un sistema de modulación OFDM que incluye dos bloques de corrección de errores de codificación redundante (FEC) que emplean códigos RS y Códigos Convolucionales (CC) de Viterbi o turbo códigos (CTC) [5]. Éstos juegan un papel importante a este nivel puesto que evitan en buena medida la utilización de otros algoritmos de corrección de capa MAC como es el ARQ híbrido, el cual implica la retransmisión de tramas y la consiguiente aparición de retardos. La figura 2 contiene un esquema en el que aparecen los diferentes bloques incluidos en el codificador de cualquier dispositivo que integre una red 802.16.

Como se puede apreciar en la fig.2, una cadena binaria que se introduce como entrada al codificador es en primer lugar procesada por un bloque

denominado aleatorizador, que altera el orden de su secuencia. En el siguiente paso, se implementa la corrección de errores, para la cual el estándar 802.16 especifica la concatenación de un codificador RS (255, 239) con un otro convolucional de Viterbi de tasa 1/2 [6].

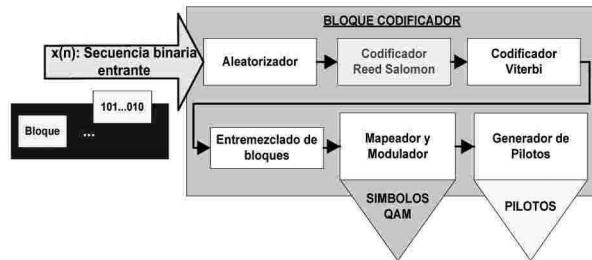


Fig. 2. Esquema de un codificador OFDM en 802.16.

En cuanto al bloque RS, la secuencia es segmentada en pequeños conjuntos de 239 octetos, quedando a la salida 255 (16 octetos redundantes). Esto se consigue empleando un polinomio característico  $p(x) = x^8 + x^4 + x^3 + x^2 + 1$ , y uno generador  $g(x) = (x + \lambda_0) \cdot (x + \lambda_1) \cdot (x + \lambda_2) \dots (x + \lambda_{2T-1})$ , donde  $\lambda = 2$  es la raíz y T es el número de caracteres que pueden ser corregidos, que en este caso llega a un máximo de 8. Se utilizan campos de Galois de 8 bits.

Este bloque se caracteriza por un parámetro denominado tasa de redundancia, el cual no es más que la relación  $k/n$ . A este nivel es muy importante entender que no en todas las situaciones es necesaria una alta redundancia para poder transmitir, en este sentido el estándar proporciona una forma de reducir tal redundancia mediante supresión de bits. En 802.16 se hace uso de máscaras binarias, conocidas como “plantillas de perforación” o puncturing. El estándar define una serie de plantillas de mayor a menor eficiencia/redundancia. La combinación de las tasas de los codificadores con la de supresión de bits de la plantilla, da lugar a la tasa de redundancia del codificador, que se calcula a partir de la fórmula:

$$R_{BLOQUE} = R_{RS} \cdot R_{CC} \cdot R_{PLANTILLA}$$

Donde  $R_{BLOQUE}$  es la tasa de salida del codificador,  $R_{RS}$  y  $R_{CC}$  la de los bloque RS y CC, respectivamente y  $R_{PLANTILLA}$  la relación de supresión dada por la plantilla.

Como ejemplo, pongamos una modulación QPSK 1/2, para la cual el estándar define bloques de entrada RS de 24 bytes y de salida de 32 bytes. De esta forma, la tasa RS es 3/4 y la tasa CC es 1/2. La plantilla ha de tener 4 bits de entrada y 3 de salida, ésta se define en el estándar como [1 1 0 1].

## 4 Avances en las implementaciones de los códigos RS sobre FPGAs

Una de las posibles implementaciones de los bloques codificador y decodificador RS en hardware

reconfigurable es la descrita en [2], la cual puede extenderse para cualquier código RS.

Con el fin de desarrollar el sistema de detección y corrección de errores FEC del estándar 802.16, se ha implementado un modelo de codificador RS(255, 239) bajo la sintaxis VHDL y basada en una implementación que utiliza el algoritmo Berlekamp Massey [3]. Este modelo permite alcanzar unas mayores velocidades de trabajo ya que se puede extender la arquitectura de forma que se trabaje con más de un símbolo al mismo tiempo. Este aspecto tiene un gran interés en los sistemas de comunicaciones digitales que se caractericen por tener grandes tasas de transmisiones de datos, como es el caso de WiMAX.

## 5 Conclusiones

En este trabajo se describen las bases del funcionamiento de los códigos RS y su papel en tecnologías como WiMAX. Asimismo, se plantean las pautas para su implementación en FPGAs, objeto de estudio y publicación en diversas disciplinas.

## Agradecimientos

Este trabajo se ha desarrollado en el marco de los siguientes proyectos: “TEC2007-67966-01/TCM (CON-PARTE-1)”, “Becas Asociadas a la Realización de Proyectos en I+D, Innovación y Transferencia de Tecnología 2009” de la Fundación Séneca, Agencia de Ciencia y Tecnología de la RM, (expediente nº 13076/BPS/09), y “Programa de Ayudas a Grupos de Excelencia de la Región de Murcia, Fundación Seneca”.

## Referencias

- [1] Abderrahmane, Anou, Mehdi Merouane and Bensebti Messaoud. “Diversity techniques to combat fading in WiMAX”. WSEAS Transactions on Communications 7.2 (2008):43-51.
- [2] Celia E. Sandoval R., Antonio Fedón. “Reed-Solomon Digital Encoder/Decoder for Reconfigurable Hardware”. Ingeniería y Universidad, vol. 11, num. 001 (2007): pp. 17-31.
- [3] He, N., et al. “Design and implementation of Reed-Solomon codes on FPGA for the multi-wavelength optical storage system”. Proceedings of SPIE--the international society for optical engineering 4930(2002):232-235.
- [4] IEEE. 802.16e IEEE “Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands”, 2005.
- [5] C. Berrou, A. Glavieux, and P. Thitimajshima, “Near Shannon limit error-correcting coding and decoding: Turbo Codes,” in Proc. ICC, 1993, pp. 1064-1070.
- [6] A. J. Viterbi, "Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm," IEEE Transactions on Information Theory , vol. IT-13, April, 1967, pp. 260-269.