# Logical-Mathematical Model of Encoder 2D-RS for Hardware Description in VHDL

Cecilia E. Sandoval-Ruiz

*Facultad de Ingeniería, Dirección de Postgrado, Universidad de Carabobo, Venezuela.*

**Abstract.-**

In this research, a logical-mathematical model of the Reed Solomon encoder is developed in two-dimensions, based on the optimized model of the LFSR components (linear feedback shift registers) and RS coders, considering the fractal structure of these circuits and their extrapolation to code concatenation schemes. This is for the purpose of generating the hardware descriptor code in VHDL, applying concepts of iterated functions. The methods considered correspond to the mathematical interpretation of the circuits and identification of correspondence between the equations that describe the mathematical behavior of these elements. In this way, we obtain as a result the model of equations of the constitutive circuits of the 2D-RS, recognizing a highly efficient solution, due to the optimization of circuit stages. This model is a contribution in the design of complex encoders with free hardware, since it simplifies the VHDL description of the encoder and promotes its updating over time.

**Keywords:** Logical-mathematical model; free hardware design; reconfigurable 2D-RS codes; Reed Solomon; VHDL; FPGA.

# Modelo lógico-matemático del Codificador 2D-RS para descripción de hardware en VHDL

**Resumen.-**

En esta investigación se desarrolla un modelo lógico-matemático del codificador Reed Solomon en dos dimensiones, basada en el modelo optimizado de los componentes LFSR (registros desplazamientos con realimentación lineal) y codificadores RS, considerando la estructura fractal de estos circuitos, y su extrapolación a los esquemas de concatenación de códigos. Esto con el propósito de generar el código descriptor de hardware en VHDL, aplicando conceptos de funciones iteradas. Los métodos considerados corresponden a la interpretación matemática de los circuitos e identificación de correspondencia entre las ecuaciones que describen el comportamiento matemático de estos elementos. De esta manera, se obtiene como resultado el modelo de ecuaciones de los circuitos constitutivos del 2D-RS, reconociendo una solución altamente eficiente, debido a la optimización de etapas del circuito. Este modelo constituye un aporte en el diseño de codificadores complejos con hardware libre, ya que simplifica la descripción VHDL del codificador y promueve su actualización en el tiempo.

**Palabras clave:** Modelo lógico-matemático; diseño hardware libre; códigos 2D-RS reconfigurable; Reed Solomon; VHDL; FPGA.

Recibido: octubre 2016
Aceptado: febrero 2017

## 1. Introducción

Entre las actuales tendencias en codificadores de canal compuestos, los cuales buscan garantizar la transmisión de datos con potencia mínima y fidelidad de la información, se han abordado modelos de n-dimensiones, donde se hace indis-

*Autor para correspondencia
*Correo-e:* cecisandova@yahoo.com (Cecilia E. Sandoval-Ruiz)

pensable el estudio de los codificadores base. Al momento de seleccionar estos se han considerado factores de vigencia tecnológica, teniendo presente que si bien existen actualmente alternativas de codificación con buenas prestaciones, es el código Reed Solomon uno de los más competitivos, definidos como codificadores concurrentes.

En tal sentido, que el codificador Reed Solomon [1] resulta interesante de acuerdo a las prestaciones y grado de complejidad del decodificador, siendo necesaria una investigación acerca del modelado y optimización de éste, donde su desarrollo se ha visto definido por las tecnologías disponibles, en este momento los dispositivos reconfigurables FPGA (Field Programmable Gates Arrays), tienen un conjunto de ventajas como: el análisis del consumo de potencia en la etapa de diseño, flexibilidad y capacidad de actualización, propiciando que la adopción de esta tecnología continúe creciendo, convirtiéndose así en la solución para estos desarrollos.

De esta manera el diseñador debe cumplir con la sintaxis del lenguaje estándar de descripción de hardware VHDL (VHSIC Hardware Description Language), lo que ofrece portabilidad del diseño, a diversas plataformas o gamas de dispositivos SoPC (System on Programmable Chip), a la vez que soporta operaciones en la configuración de hardware, tal es el caso del operador denominado 'concatenación', el cual permite ordenar estructuras sin necesidad de una señal de reloj para su manejo. A partir de estos modelos VHDL, se han estudiado los métodos de optimización de la descripción de hardware, esto facilita la adaptabilidad de los productos finales, aspecto importante en los procesos continuos de actualización a las nuevas tecnologías, lo que los hace diseños con características de sostenibilidad.

Estos aspectos demuestran la relevancia de desarrollar modelos lógicos-matemáticos, que permitan extrapolar el diseño a aplicaciones específicas, a través de ecuaciones de comportamiento de hardware resulta más eficiente, a la vez que por ser tratado bajo la filosofía de hardware libre, ofrece a los diseñadores una base importante para desarrollos futuros. Permitiendo el desarrollo de modelos optimizados de codificadores elementales, con procesamiento eficiente y paralelo de los datos de información, que pueden ser concatenados en estructuras 2D, a fin de obtener codificadores compuestos con las mismas características de eficiencia que sus componentes.

El objetivo de esta investigación es obtener un modelo matemático de código híbrido reconfigurable, que permita la adaptación del modelo de concatenación, a fin de establecer las mejores prestaciones, conmutando entre posibles alternativas de codificación multidimensional, dado por ecuaciones con operadores lógico-matemáticos soportados por el lenguaje descriptor de hardware VHDL, a través del cual se pueda generar el código de un codificador multidimensional, bajo el enfoque de hardware libre y orientado a alto rendimiento.

El modelo aplica como técnica de desarrollo la extrapolación de los modelos de componentes auto-similares identificados en el estudio, aplicando los desarrollos de hardware eficiente para codificadores RS y la generalización de las estructuras de concatenación de códigos, a fin de establecer correspondencia entre los codificadores elementales y el codificador 2D. Esta propuesta se presenta como un esquema de concatenación novedoso, que permite avanzar en la descripción de estos sistemas de manera eficiente, orientados a hardware reconfigurables, sobre esta base se plantea estudiar los modelos matemáticos autosimilares entre los esquemas circuitales, y definir las ecuaciones del modelo de descripción lógica para VHDL.

El artículo está organizado desde la revisión de los esquemas de codificación concatenada en dos dimensiones, realizando una identificación del tipo de procesamiento de las secuencias, seguido de la descripción metodológica, donde se interpretan las ecuaciones matemáticas, se establece un método de modelado que considera la extrapolación de los modelos de los componentes, bajo un enfoque generalizado, hasta obtener como resultado un modelo lógico-matemático del codificador concatenado híbrido 2D-RS, que permite establecer conclusiones sobre los aportes del modelo desarrollado.

*Antecedentes*

El área de estudio de códigos compuestos, comprende codificadores 3DH [2], Turbo Code [3] y Product Code (cuya descripción se presenta en IEEE 802.16 Compatible Turbo Product Code Enconder v1.0 de Xilinx), estos realizan la codificación en dos o más dimensiones, requiriendo alta velocidad de cómputo, a fin de procesar de manera eficiente los datos de información, generando así los símbolos de redundancia. Por este motivo, presentan entre sus requerimientos mayor capacidad y velocidad de procesamiento, a fin de implementarse como un sistema de cómputo de alto rendimiento, donde el consumo energético es uno de los criterios de eficiencia a considerar.

En este orden de ideas, se han desarrollado investigaciones sobre modelos de procesamiento paralelo de los codificadores elementales, y el diseño de módulos para la implementación de códigos concatenados paralelos sobre FPGA [4], en los cuales se puede realizar el procesamiento de los datos a alta velocidad por parte de codificador compuesto. Igualmente, se han estudiado variables como la eficiencia energética en el proceso de codificación [5], donde se compara la estimación de recursos y potencia dinámica de los codificadores, realizando variaciones en la sintaxis de descripción VHDL, se han investigado técnicas de disminución del consumo de potencia para codificadores Reed Solomon sobre hardware reconfigurable [6], que consideran la tesis del modelado concurrente optimizado de las estructuras del codificador [7, 8], en la cual se ha identificado una estructura auto-similar en los componentes LFSR (Linear Feedback Shift Register) del codificador Reed Solomon, característica que se ha tomado como punto de partida para la obtención del modelo 2D-RS.

## 2. Fundamentos del Codificador 2D RS

Para la implementación de códigos concatenados con tecnología FPGA, se procesa un arreglo de datos que alimentará a un par de codificadores. En investigaciones previas se describen las características de los códigos productos aplicados sobre codificadores Reed Solomon como componentes, dado que un código producto es una concatenación de códigos de bloque lineales sistemáticos, éste hereda las propiedades de los códigos elementales que lo componen [9, 10, 11, 12]. Así, partiendo de los códigos de bloque lineal sistemáticos $C_1$ y $C_2$ con parámetros $(n, k, d_{min})$, que representan la longitud del código, el número de símbolos de información y distancia mínima respectivamente. El código producto $P = C_1 \otimes C_2$, consiste en una matriz de $n1 \times n2$. Los parámetros del código producto resultante se dan por: $n_p = n_1 n_2$, $k_p = k_1 k_2$ y $d_{minp} = d_{min1} d_{min2}$, por lo tanto, es posible construir potentes códigos de producto.

Cuando un código $C$ es un código RS $(n, k)$ sobre el campo de Galois GF $(2^m)$, se obtiene un código producto Reed Solomon $RS - PC(n_1 n_2, k_1 k_2)$ sobre GF $(2^m)$. De esta manera, una de las aplicaciones de los codificadores RS $(n, k)$ más interesantes por su arquitectura corresponde a los Reed–Solomon Product-Code (RS-PC) [13, 14]. En el caso de los códigos Reed-Solomon, desarrollados por los ingenieros – matemáticos Irving S. Reed y Gustave Solomon, estos son códigos no binarios, que están clasificados como códigos BCH (por las siglas de sus autores: Bose, Chaudhuri y Hocquenghem), estos son códigos lineales y cíclicos, cuya particularidad consiste en el tratamiento de los datos a través de bloques de longitud fija. El proceso de decodificación debe cumplir que la palabra de código sea divisible de forma exacta entre el polinomio generador, para su comprobación se cuenta con técnicas de decodificación altamente eficientes, incluso con características adaptativas [15], donde la eficiencia del codificador es una variable de interés, en tal sentido los codificadores optimizados – CESR [5], emplean técnicas de optimización para modelos VHDL.

Partiendo de los códigos producto [16] o códigos iterados, concatenados de forma serial [17], donde el codificador funciona sobre una matriz de símbolos de información mediante la codificación de los datos organizados en filas (inner code), seguido de otro codificador concatenado (outer code), que procesará los datos organizados en columnas. Esta configuración se puede interpretar como una operación no lineales de secuencias,

siendo la función $F(x1, x2)$, donde se realizan combinaciones no lineales de secuencias de salida de los LFSRs [18] del codificador RS. La codificación de la columna está formada tanto por los símbolos de información originales, como los símbolos de redundancia generados en la primera codificación [5], tal como se muestra en la Figura 1, donde se genera una matriz de $n1 \times n2$ símbolos.

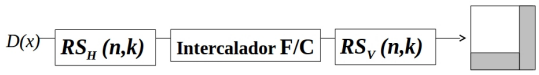



Figura 1: Codificador Concatenado Serial.

La codificación concatenada paralela [19], en el cual se realiza una codificación solo sobre los k1 x k2 símbolos de datos, sin generar símbolos de chequeo de los símbolos de redundancia de uno de los codificadores del Turbo block code [3], esta concatenación puede compararse con estructuras de procesamiento de Registros desplazamiento de Realimentación Lineal [20], Registros desplazamiento de Realimentación Dinámica [21], 2D-LFSR [22], Registros desplazamiento de realimentación no lineal [23], bajo el esquema de Multiplexado de secuencias aleatorias, obtenidas a través de estructuras LFSR, el cual se corresponde con la concatenación paralela, sustituyendo los LFSR por codificadores RS(n,k), su esquema de implementación se presenta en la Figura 2.

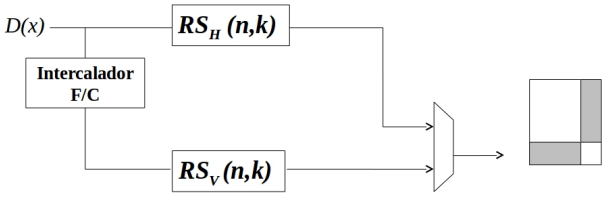



Figura 2: Codificador Concatenado Paralelo.

La estructura de datos de un RS-TPC (Turbo Code Product) de dos dimensiones, compuesto por un codificador de vectores de datos horizontal RS $(n_1, k_1)$ y un codificador de vectores de datos vertical RS $(n_2, k_2)$, viene dada por una matriz $n_1 \times n_2$, que comprende $k_1 \times k_2$ símbolos de datos, un primer bloque de símbolos de redundancia de dimensiones $(n_1 - k_1) \times k_2$, resultado del proceso de codificación interno, quedando una matriz de $n_1 \times k_2$, sobre la cual actúa el codificador externo generando un arreglo de redundancia de dimensiones $n_1 \times (n_2 - k_2)$, la matriz de salida se presenta en la Figura 3.

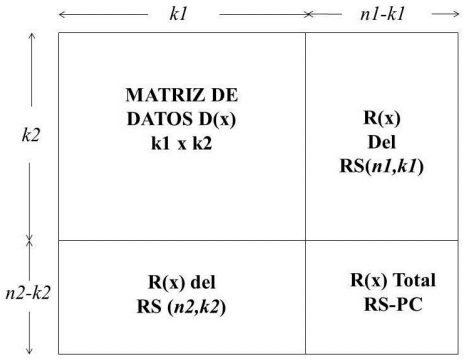
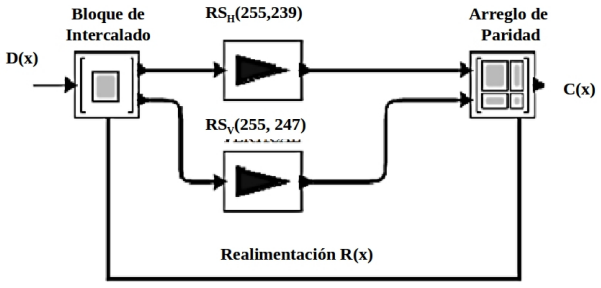



Figura 3: Esquema Matricial de Códigos 2D-RS.

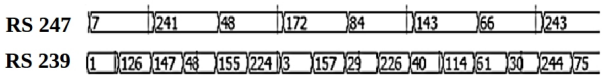
## 3. Metodología

### 3.1. Interpretación del Comportamiento del Circuito 2D-RS

Un ejemplo de éste, puede ser un arreglo compuesto por un codificador horizontal $RS_H(255, 239)$ para el procesamiento de las filas y un codificador vertical $RS_V(255, 247)$ para el procesamiento de las columnas [24], donde la codificación realimentada depende de los resultados de los símbolos de redundancia generados por la primera codificación, como se muestra en la Figura 4.




a) Esquema circuital.




b) Salidas $RS_V(255, 247)$ y $RS_H(255, 239)$.

Figura 4: Modelo del Codificador 2D-Reed Solomon.

A partir de estos esquemas o arreglos de códigos concatenado se estudia un esquema mixto, en el cual se pueda seleccionar la configuración de forma selectiva, la concatenación paralela o concatenación serial, con procesamiento paralelo de los datos $D(x)$, por ambos codificadores RS y una realimentación de los símbolos de redundancia selectiva, la cual se puede habilitar al codificador correspondiente, manejada a través de habilitadores, partiendo de una generalización del modelo, por medio de la concatenación de las salidas de los codificadores RS, esto implementado de forma matricial, como se muestra en la Figura 5.

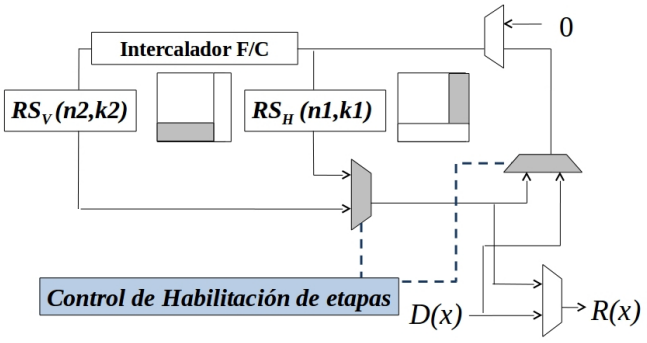



Figura 5: Codificador con método de Concatenación Selectivo 2D-RS.

Es de hacer notar, que para el caso del codificador concatenado paralelo se puede sustituir el multiplexor de salida, por un elemento lógico que permita la concatenación matricial de la salida de cada codificador RS componente, expresado como $R(x) = D_x \& RS_H(D_x) \& RS_V(D_x) \& RS_V(RS_H(D_x))$, igualmente a través de la operación xor entre las matrices resultantes, a fin de adaptar la estructura circuital a un LFSR, el mismo esquema puede ser asumido para la operación de la matriz de datos, con las matrices de redundancia parcial de cada codificador.

### *3.2. Interpretación Matemática de los componentes del 2D-RS*

Partiendo del codificador Reed Solomon, en la definición de la palabra de código Reed Solomon $C(x)$, cada palabra debe ser múltiplo del polinomio generador $G(x)$, expresada ésta en su forma sistemática, corresponde al bloque de información $D(x)$ adicionando los símbolos de redundancia calculados sobre el bloque de información. Este cálculo es el bloque resultante como residuo de la operación de división entre el polinomio generador G(x), dada como $R_{g(x)}[arg]$ aplicada sobre los símbolos de datos. Tal como se expresa en la Ecuación (1).

$$C(x) = x^{n-k}D(x) + R_{G(x)}\left[D(x)x^{n-k}\right] \quad (1)$$

La expresión matemática corresponde a ensamblar dos polinomios con desplazamiento, definido como: $c = (D << (n\text{-}k)) + (D << (n\text{-}k))\ \%\ g$ ; donde se desplaza el polinomio de datos de información $n - k$ posiciones a la izquierda, y los $n - k$ símbolos menos significativos son completados con el residuo de la operación mod del polinomio $G(x)$. De manera tal que la expresión polinomial de la palabra de código queda definida, como la suma de los polinomios mencionados, presentada en la Ecuación (2).

$$C(x) = x^{n-k}D(x) + x^{n-k}D(x) \mod G(x) \quad (2)$$

Encontrando así la expresión matemática del generador de símbolos de redundancia, dada por la Ecuación (3), correspondiente a la reducción modular del polinomio de datos, entre el polinomio generador $G(x)$.

$$R(x) = x^{n-k}D(x) \mod G(x) \quad (3)$$

Similar a la expresión de los polinomios generados como residuos parciales en la operación de multiplicación en campos finitos, definida por la Ecuación (4), que se expresa en función de los $i$ desplazamientos $x^i$, que se realizan en el proceso de multiplicación para la operación con el coeficiente $B_i$ correspondiente.

$$a_m(x) = x^i A(x) \mod p(x) \quad (4)$$

Donde $a_m(x)$ corresponde a la reducción modular, del polinomio $A(x)$ respecto al polinomio irreducible del campo de Galois $p(x)$. Lo que permite evidenciar una definición matemática similar, entre ambas estructuras. Seguidamente se analiza la implementación de las ecuaciones, las cuales corresponden a la salida de un generador de secuencia LFSR, en su representación de

Galois. Partiendo de la ecuación de convolución, se sustituye la salida de datos, por el vector de símbolos de redundancia $R(x)$, la entrada de datos, por los datos a codificar (compuesto con la realimentación) $d(x)$, y los coeficientes de la función de transferencia, por los coeficientes del polinomio generador del código $g(n-k)$, obteniendo así la Ecuación (5).

$$R(x) = \sum_{k=0}^{n} d(x)g(n-k) \tag{5}$$

para los $n-k$ símbolos generados

Para dicha expresión se ha empleado un término $d(x)$ que corresponde a un arreglo compuesto entre $d(k)$ y la realimentación del residuo en la posición menos significativa del polinomio $r_{k-1}(0)$, esto con el propósito de conservar la similitud de la expresión matemática (sin realimentación), al sustituir en función de la entrada del codificador $d(k)$, correspondiente a una muestra k del vector de datos, se obtiene así la Ecuación (6).

$$R(x) = \sum_{k=0}^{n} (d(k) \oplus r_{k-1}(n-k))G(x) \tag{6}$$

Del mismo modo, la ecuación que define el producto de $A(x)$ (correspondiente al primer operando) *mod* el polinomio generador del campo $p(x)$. Se puede expresar como la convolución, mostrada en la Ecuación (7).

$$a(x) \mod p(x) = \sum_{k=0}^{m} A(x)p(m-k) \tag{7}$$

Donde $a_m(x)$ se sustituye de igual modo, se puede expresar en correspondencia con la Ecuación (8).

$$a_m(x) = \sum_{k=0}^{m} (a(k) \oplus a(m))p(x) \tag{8}$$

Siendo $a_m(x)$ el polinomio de la reducción modular, $a(k)$ y $a(m)$ los elementos $k$ y $m$ respectivamente del polinomio $A(x)$ y $p(x)$ el polinomio irreducible del campo finito. En este punto, una vez establecida la similitud de los modelos matemáticos entre ambos componentes, se considera la descripción matemática de un codificador concatenado serie, descrito por la Ecuación (9), en el cual se expresa el procesamiento del codificador interno sobre las $k_2$ y el codificador externo sobre las $n_1$ filas.

$$2D - R(x) = \sum_{i=0}^{n1} \left( \sum_{j=0}^{k2} D(x_{i,j}).f_C(x) \right) f_F(x) \tag{9}$$

Donde $D(x)$ será la entrada de datos, operada en función de la codificación Reed Solomon sobre filas $f_F(x)$ y la función Reed Solomon sobre columnas $f_C(x)$. Dada la similitud entre los modelos matemáticos de los tres circuitos, se consideran los avances desarrollados en las etapas del codificador concatenado [7], con el objetivo de realizar un modelo iterado, la descripción del codificador Reed Solomon $(255, k)$ con el parámetro $k$ configurable, y así permite la descripción de ambos codificadores en la estructura 2D-RS, donde elementos de memoria corresponden a arreglos matriciales.

### *3.3. Métodos de optimización aplicados al circuito 2D-RS*

Las consideraciones realizadas partieron de los postulados que los *circuitos más rápidos consumen menor potencia* [25] y al igual que la reducción de la complejidad lógica, para la implementación de un codificador altamente eficiente en cuanto a velocidad de procesamiento. El método de modelado concurrente de las estructuras LFSR se presenta en la investigación del codificador RS(n,k) basado en LFCS - Linear Feedback Concurrent Structure [8], donde se realizó el cálculo de los símbolos en función de variables tiempo-espacio, para la descripción de los componentes LFSR del codificador Reed Solomon de forma concurrente. Se obtiene como resultado un conjunto de términos correspondientes a la descripción tiempo – espacio de los elementos del modelo, para su descripción en hardware paralelo la cual ha sido abordada en [7].

Por otra parte, *la habilitación selectiva de módulos* para el procesamiento paralelo permite manejar a través de tri-estados la configuración de etapas de forma óptima, con el menor consumo de

potencia. Esto corresponde a habilitar el número de codificadores Reed Solomon en paralelo, de acuerdo a la configuración de la concatenación.

Finalmente, considerar que los circuitos tienen un *consumo de energía proporcional a la complejidad computacional y la profundidad lógica del diseño*, por lo tanto la optimización de los recursos de hardware en el diseño, resultará en un consumo de energía proporcional.

En este sentido, se estableció la ecuación de estimación del consumo de potencia del diseño propuesto, basado en los elementos lógicos de las operaciones del circuito, considerando el modelo de estimación presentado por [26] para el componente multiplicador $P_M = 0{,}4(m^2 + 3(m-1)^2/2)$. A partir de esta se definió la potencia del multiplicador optimizado $P_{M\_OPT} = 0{,}4\,(m^2 + (p\,m - p - 2m + 2)\,(m-1))$, se adaptó a la configuración propuesta, resultando la potencia estimada $P_E$ dada por la Ecuación (10).

$$P_E = P_{M\_OPT}(n_2 - k_2)k_1\,D \tag{10}$$

Donde $m$, es el número de bits por símbolo; $p$, el número de bits no nulos del polinomio generador de campo GF; $n_2 - k_2$, los estados del generador de redundancia para el codificador RS2 multiplicado por el número de filas/columnas a procesar $k_1$, siendo éste el número de símbolos de datos para el codificador RS1; y $D$, la dimensión del codificador concatenado, de esta manera la optimización desarrollada para los codificadores RS, cuyos reportes de eficiencia están documentados en [5, 6], es extrapolada para el modelo de codificador concatenado 2D-RS.

### *3.4. Método de Modelado de Generalización Estructural*

El método de modelado está basado en el análisis de la similitud entre los circuitos componentes del sistema, asociado con modelos fractales de codificadores RS [27], en este caso se realizó la descripción en VHDL del comportamiento del codificador bajo un tratamiento de concreción, a fin de describir las ecuaciones espacio – temporal involucradas en la configuración del hardware, lo que se ha considerado un método aplicable para el modelado del circuito, con los resultados obtenidos se han generado las ecuaciones en forma de funciones iteradas. El análisis matemático de los circuitos generadores de códigos Reed-Solomon, permite un nuevo enfoque en el modelado de sistemas con características auto-similares, así como algoritmos recurrentes. Así pueden ser extrapolados para la generalización de circuitos. En el cual, el tratamiento del modelo optimizado se puede desarrollar en base a la algoritmia característica de las estructuras fractales identificadas.

## 4. Resultados

### *4.1. Estructura LFSR del Codificador Concatenado Híbrido 2D-RS*

En este caso se identificó que el generador de símbolos de redundancia del codificador Reed Solomon y el componente de reducción modular del multiplicador en el campo GF, presentan la misma estructura LFSR, y las funciones que definen su comportamiento matemático, como un sistemas de funciones iteradas, de manera tal que el codificador concatenado puede aprovechar esta característica, a fin de obtener un modelo simplificado. Así, considerando el principio de correspondencia permitió extender el diseño del multiplicador desarrollado, hacia la aplicación del codificador Reed Solomon, donde aplican los fundamentos para la paralelización del circuito LFSR y a su vez definir un esquema circuital similar para el codificador concatenado 2D-RS. En la Tabla 1 se presenta la correspondencia entre los elementos del LFSR de los circuitos estudiados, donde se identifican las dimensiones de los elementos de memoria, las operaciones que se realizan en las ramas del circuito y el polinomio que identifica la función de realimentación del LFSR.

Donde el polinomio generador del campo $p(x)$, el polinomio generador del código $g(x)$ y el polinomio generador de concatenación $f(x)$, definen los coeficientes para cada caso. Es de hacer notar que la definición de un polinomio $f(x)$, cuyos coeficientes controlan el procesamiento paralelo de codificación RS en cada rama del codificador concatenado, a través de la habilitación

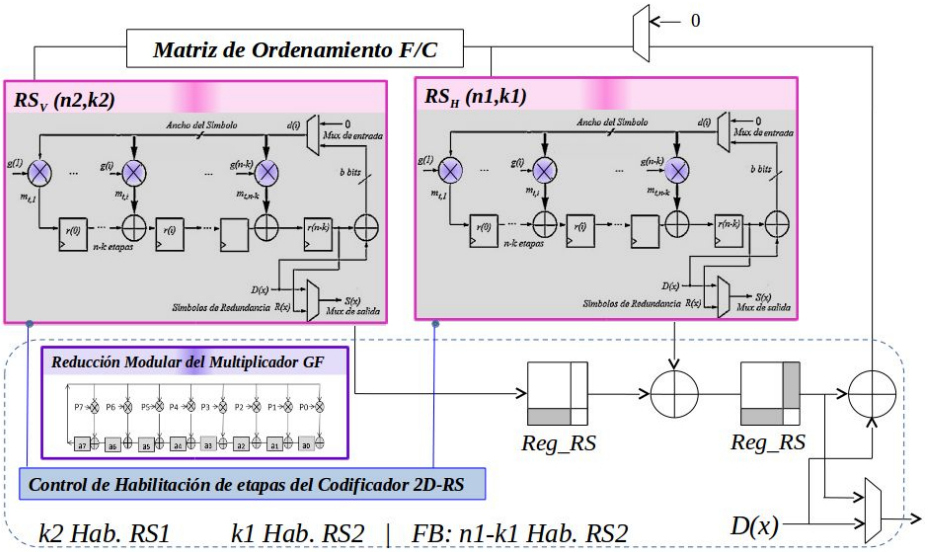



Figura 6: Estructura generalizada del codificador RS-2D.

Tabla 1: Identificación de Componentes de los Modelos propuestos.

| Componente LFSR | RS-PC | Codificador RS | Mult. GF |
|---|---|---|---|
| Elemento de memoria | Bloque $(n \times k)$ símbolos | Símbolos (m bits) | bit |
| Operador de ramas | RS(n,k) | Mult_GF | and |
| Polinomio Generador | $f(x)$ | $g(x)$ | $p(x)$ |

de codificación en procesamiento paralelo y en realimentación. Esto corresponde a un enfoque novedoso, este polinomio permite el diseño de códigos RS-PC más complejos y con mayor ganancia, como los presentados en [11].

En este punto se realizó una generalización, a fin de adaptar el modelo del codificador concatenado a la estructura LFSR de los componentes internos, multiplicador GF y codificador RS, motivo por el cual la selección (implementada a través de los multiplexores de salida de datos codificados, se ha remplazado por habilitadores de los componentes codificadores) y concatenación matricial simple (presentada en la Figura 5) se ha reacomodado en la expresión de suma módulo2 de segmentos de la matriz, para obtener la concatenación del arreglo de datos con los arreglos de redundancia resultante, como se muestra en la Figura 6.

A partir de la estructura, se puede obtener una función de transferencia similar en los tres casos, así se puede observar la relación entre los LFSR del componentes reducción modular del multiplicador GF (la vista del esquema detallado se observa en términos de $a7 \ldots a0$, estado del LFSR y $p7 \ldots p0$, elementos del polinomio irreducible del campo), en una estructura anidada con relación al LFSR dpl codificador RS, y éste con el 2D-RS, donde se reconoce una arquitectura fractal. Finalmente, se adapta la concatenación a la estructura LFSR, integrando un componente de control de habilitadores, que permite la selección de etapas de codificación, a fin de deshabilitar los módulos en alta impedancia, mientras no se estén utilizando.

En el primer ciclo se emplean los codificadores paralelos para $k$ vectores de datos, definidos estos por los habilitadores $k_1$ y $k_2$ respectivamente, en el ciclo de realimentación se habilitarán solo $n - k$ codificadores para la matriz de símbolos de redundancia parcial, habilitado por FB. De manera selectiva se puede habilitar uno ambos bloques de codificación, teniendo la paridad compuesta como el resultado de paridad de los símbolos de redundancia de uno de los codificadores o la operación *xor* entre la paridad de cada uno.

Una vez definido el esquema del codificador RS-2D generalizado en la estructura base LFSR,

se ha realizado la descripción VHDL, a través de la operación VHDL "concatenación", el cual permite el manejo de los fragmentos de datos y la composición de la matriz total codificada, el código de descripción del RS-2D se presenta en la Figura 7.

```
architecture Behavioral of nDRS is
component Codificador_RS is
--Codificador paralelo como un procesador matricial
Port     ( Mdato : matriz is array (0 to k1)
           of std_logic_vector(width-1 downto 0);
           Mred  : matriz is array (k1+1 to n1)
           of std_logic_vector(width-1 downto 0);
end component;
begin
process (clk)
C1: Codificador_RS port map (Mdato, Mred_hor);
   --Codificación horizontal paralelo
C2: Ordenador_mat  port map (Mdato, Mdato_vert);
   --Ordenador fila/columna
C3: Codificador_RS port map (Mdato_vert, Mred_vert);
   --Codificación vertical paralelo
     if (clk'event and clk='1') then
            dato <= Mdato & Mred_hor
            -- equivalente a suma matricial estructurada
     end if;
C4: Ordenador_mat  port map (dato, Mdato_vert);
   --Ordenador f/c de redundancia
C5: Codificador_RS port map (Mdato_vert, Mred_total);
     --Codificación vertical de redundancia
2D-RS <= Mdato & Mred_hor & Mred_ver & Mred_total;
--Concatenación matricial 2D-RS <= dato & Mred_total
end process;
end Behavioral;
```

Figura 7: Descripción VHDL del Codificador 2D-RS.

### 4.2. *Modelo del Codificador Concatenado Híbrido 2D-RS*

Una vez definido el modelo a partir de los términos particularizados, y considerando las variables estudiadas, se generaliza el modelo de forma condensada, partiendo de la descripción que modela el componente multiplicador, dada por la Ecuación (11)

$$m_{i,x} = \oplus_{t=1}^{m} (a_m(x)\, b_i) \tag{11}$$

siendo:

$$a_m(x) = \&_{i=0}^{m-1} a_{t-1}\,(i-1) \oplus (a_{t-1}\,(m-1)\;\; p(i))$$

La cual corresponde a la reducción modular de a(x) con respecto al polinomio irreducible p(x), por el coeficiente $i$ de $b(x)$. La ecuación del modelo del codificador paralelo, se puede expresar a través de la Ecuación (12).

$$r_t = \&_{i=0}^{n-k} r_{t-1}(i) \oplus [(D(i) \oplus r_{t-1}(n-k)) \otimes g(x)] \tag{12}$$

Donde $r_t$ corresponde al elemento actual generado en la posición $i$, el cual es el resultado de la operación *xor* entre el elemento en la posición anterior con un retardo de tiempo $r_{t-1}(i-1)$ y el término generado por la operación entre la xor del dato de entrada $x(t)$ y el elemento de mayor peso un instante de tiempo anterior $r_{t-1}(n)$ con el coeficiente de la función $g(i)$. Al sustituir el modelo del codificador Reed Solomon desarrollado en el modelo del codificador concatenado *n-dimensional*, para $n = 2$ se tiene como salida la concatenación de símbolos dada por: $f_1(D(x)) \& f_0(D(x)) \& [f_1(rs_{t-1}(0) \oplus f_0(rs_{t-1}(1))]$, se obtiene así el modelo presentado en la ecuación 13, para un $nD-RS$, siendo éste similar a los componentes.

$$nD-RS = \&_{i=0}^{n-1} rs_{t-1}(i) \oplus [(D(x) \oplus rs_{t-1}(i)) \otimes f(x)] \tag{13}$$

Donde $f(x)$ corresponde a la operación Reed Solomon sobre los datos de información, para cada rama en paralelo del codificador concatenado (con habilitación de la etapa correspondiente y el número de arreglos a procesar), y $rs_{t-1}(i)$ los símbolos de redundancia generados en la operación anterior. El modelo optimizado para funciones iteradas, acá propuesto será útil en estas aplicaciones, ya que permite mejorar el desempeño del RS-PC, lo que justifica la paralelización de los codificadores RS que lo componen. De modo que, este desarrollo podrá servir de insumo para futuras aplicaciones de codificadores híbridos con características adaptativas, basados en la capacidad de reconfiguración dinámica de los FPGAs y las características que estos dispositivos presentan [32]. Todo esto con el fin de reducir el tiempo de desarrollo y optimizar el desempeño de las etapas de los sistemas compuestos por codificadores concatenados en sus diversas combinaciones y aportando un cambio de paradigma en el diseño.

## 5. Conclusiones

Gracias a la naturaleza del código Reed Solomon, "cíclico de bloques" y la definición del producto en campos finitos GF, en trabajos previos [7], se analizó la realimentación en ciclos iterados para la paralelización de sus componentes, definiendo el procesamiento por bloques para un tratamiento concurrente del conjunto de datos. En esta investigación se han considerado estos avances para definir un nuevo modelo, al que hemos llamado "Código Concatenado Híbrido 2D-RS", por permitir la configuración de concatenación serial/paralelo, a través del polinomio generador de la concatenación $f(x)$, siendo éste un elemento nuevo que se ha incorporado para optimizar el modelado. En este esquema de codificación se aplica el procesamiento optimizado de los datos en los códigos Reed Solomon definidos en VHDL, incorporándolos como códigos elementales en este modelo multidimensional 2D.

De esta manera, se evidencia la similitud entre las estructuras circuitales LFSR, con operadores de diferentes dimensiones, lo que permite observar el Isomorfismo estructural entre los componentes, y la correspondencia de los modelos matemáticos. En tal sentido, se aplica el modelo optimizado de los componentes RS [7], partiendo de su análisis temporal e interpretación del comportamiento del LFSR para la obtención de las ecuaciones, este tratamiento es un enfoque del Principio Holográfico, de coexistencia en el espacio de resultados secuenciales. En este análisis se reconoce la presencia de (*i*) Funciones Iteradas, las cuales se pueden modelar para la implementación concurrente del circuito secuencial, (*ii*) Auto-similitud entre los componentes LFSR de las estructuras del multiplicador GF y del codificador RS, de las mismas características, pero a diversas escalas, por lo que se puede identificar la posibilidad optimizar la aplicación, como un circuito fractal en VHDL.

Igualmente, la trascendencia científica corresponde al logro de la optimización del modelo de una aplicación compleja, a través de un método de concatenación de elementos eficientes, cuyos modelos para configuración en VHDL, comprende la descripción circuital de circuitos concurrentes, generados haciendo uso de la operación de concatenación "&", soportada en las nuevas tecnologías de diseño de hardware. Esta técnica para la reducción del consumo de potencia mediante el procesamiento paralelo, simplificación de variables, concatenación para ordenamiento de símbolos, etc., permitió desarrollar un modelo para la generación de código VHDL, enfocado en hardware libre por ofrecer las ecuaciones para la descripción del codificador, sobre tecnología FPGA.

Obteniendo en el método de modelado un avance significativo en la descripción de las ecuaciones para VHDL por extrapolación de optimizaciones de los módulos componentes, donde se busca el equilibrio entre (a) el procesamiento paralelo, mediante la codificación paralela de la matriz de datos en filas/columnas), (b) la eficiencia energética, esto a través de la deshabilitación de etapas para ahorro de energía, y (c) el menor número de recursos de los dispositivos FPGA, reutilizando componentes diseñados mediante la realimentación selectiva de resultados previos, como es el caso de la matriz de redundancia parcial. Destacando, la obtención de las ecuaciones del código concatenado, que aporta un método de configuración de hardware en VHDL, basado en modelado matemático-lógico, aprovechando la correspondencia matemática-circuital, en las estructuras de realimentación LFSR, de los componentes del código RS(n,k), el elemento multiplicador y el codificador 2D-RS.

Se presenta el modelo desarrollado con características innovadoras, tanto en el método abordado como en los resultado, a la vez de promover la investigación en el área de cómputo de alto rendimiento, donde se extrapola el modelo del codificador $RS(n,k)$, a través del método de modelado lógico-matemático, para alcanzar la optimización de rendimiento, sobre hardware reconfigurable. Lo que representa un aporte a la comunidad científica, donde los avances pueden ser aplicados en futuras actualizaciones, sirviendo de insumo en la generación de nuevo conocimiento en el área de hardware reconfigurable aplicado en comunicaciones digitales. Este proyecto pretende dar continuidad a desarrollos previos en el

área, cuyo aporte está dado por el tratamiento matemático-lógico de las funciones iteradas reconocidas, dentro de la aplicación objeto de estudio, tomando como base la investigación en modelado optimizado, a través de estructuras LFSR [7], para las estructuras afines.

## Referencias


[1] Johnny Phuong Nguyen. *Applications of Reed-Solomon codes on optical media storage*. Doctoral Thesis, San Diego State University, USA, 2011.

[2] Chagun Basha Basheer Ahmed. *Fault mitigation strategies for reliable FPGA architectures*. Thése de Doctorat, Université De Rennes 1, France, 2016.

[3] Todd K. Moon. *Error correction coding: mathematical methods and algorithms*, chapter 14. Turbo codes, pages 581–633. John Wiley & Sons, Inc., 2005.

[4] Cecilia Sandoval. Diseño de módulos funcionales para implementación de códigos concatenados paralelos sobre FPGA. In *VI Congreso de Investigación Universidad de Carabobo. La investigación en el siglo XXI: oportunidades y retos*, pages 535–539, Venezuela, 2008.

[5] Cecilia Esperanza Sandoval Ruiz and Antonio S. Fedón Rovira. Efficient RS (255, k) encoder over reconfigurable systems. *Revista Técnica de la Facultad de Ingeniería Universidad del Zulia*, 37(2):151 – 159, 08 2014.

[6] C. Sandoval. Power consumption optimization in Reed Solomon encoders over FPGA. *Latin American Applied Research*, 44:81–85, 2014.

[7] C. E. Sandoval Ruiz. *Modelo optimizado del codificador Reed-Solomon (255, k) en VHDL a través de un LFSR paralelizado*. Tesis Doctoral, Dirección de Postgrado, Facultad de Ingeniería, Universidad de Carabobo, Venezuela, 2013.

[8] Cecilia Sandoval-Ruiz. Codificador rs (n, k) basado en lfcs: caso de estudio rs (7, 3). *Revista Facultad de Ingeniería Universidad de Antioquia*, (64):68–78, 2012.

[9] C. Leroux, G. Le Mestre, C. Jego, P. Adde, and M. Jezequel. A 5-Gbps FPGA prototype of a (31,29)2 Reed-Solomon turbo decoder. In *2008 5th International Symposium on Turbo Codes and Related Topics*, pages 67–72, Sept 2008.

[10] Raphaël Le Bidan, Camille Leroux, Christophe Jego, Patrick Adde, and Ramesh Pyndiah. Reed-Solomon turbo product codes for optical communications: from code optimization to decoder design. *EURASIP Journal on Wireless Communications and Networking*, 2008:14, 2008.

[11] Bingrui Wang, Xiaofei Yang, Xingzhong Yao, Hongzhi Zhang, and Yue Zhang. Highly reliable product code for error correction. *International Journal of Multimedia and Ubiquitous Engineering*, 10(8):277–286, 2015.

[12] Jorge Castiñeira Moreira and Patrick Guy Farrell. *Essentials of error-control coding*. John Wiley & Sons, 2006.

[13] Hsie-Chia Chang, C. Bernard Shung, and Chen-Yi Lee. A Reed-Solomon product-code (RS-PC) decoder chip for DVD applications. *IEEE Journal of Solid-State Circuits*, 36(2):229–238, 2001.

[14] C. Kim, S. Rhee, J. Kim, and Y. Jee. Product Reed-Solomon codes for implementing NAND flash controller on FPGA chip. In *2010 Second International Conference on Computer Engineering and Applications*, volume 1, pages 281–285, March 2010.

[15] Jonathan D. Allen. Energy efficient adaptive Reed-Solomon decoding system. Master's thesis, Department of Electrical and Computer Engineering, University of Massachusetts Amherst, USA, 2008.

[16] Shu Lin and Daniel J. Costello. *Error control coding*. Pearson Education International, 1983.

[17] Ramesh Mahendra Pyndiah. Near-optimum decoding of product codes: block turbo codes. *IEEE Transactions on Communications*, 46(8):1003–1010, 1998.

[18] Patrik Ekdahl. *On LFSR based Stream Ciphers - analysis and design*. PhD thesis, Lund University, Sweden, 2003.

[19] Ken Harima. Decodificaón de salida suave para códigos Reed-Solomon y su aplicación a códigos concatenados. Tesis de Maestría, Decanato de Estudios de Postgrado, Universidad Simón Bolívar, Venezuela, 2006.

[20] Claudio Mucci, Luca Vanzolini, Ilario Mirimin, Daniele Gazzola, Antonio Deledda, Sebastian Goller, Joachim Knaeblein, Axel Schneider, Luca Ciccarelli, and Fabio Campi. Implementation of parallel lfsr-based applications on an adaptive dsp featuring a pipelined configurable gate array. In *Design, Automation and Test in Europe, 2008. DATE'08*. IEEE, 2008.

[21] A. Peinado, J. Munilla, and A. Fúster Sabater. Diseño de cifradores en flujo DLFSR con alta complejidad lineal para implementacion hardware. In *Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información*, pages 63–68, Alicante, España, 2014.

[22] Chien-In Henry Chen. Synthesis of configurable linear feedback shifter registers for detecting random-pattern-resistant faults. In *Proceedings of the 14th International Symposium on Systems Synthesis*, ISSS '01, pages 203–208, New York, NY, USA, 2001. ACM.

[23] Elena Dubrova, Maxim Teslenko, and Hannu Tenhunen. On analysis and synthesis of (n, k)-non-linear feedback shift registers. In *Design, Automation and Test in Europe, 2008. DATE'08*, pages 1286–1291. IEEE, 2008.

[24] J. Lee and K. A. Schouhamer Immink. An efficient

decoding strategy of 2D-ECC for optical recording systems. *IEEE Transactions on Consumer Electronics*, 55(3):1360–1363, August 2009.

[25] Andreas Genser, Christian Bachmann, Christian Steger, Jos Hulzink, and Mladen Berekovic. Low-power asip architecture exploration and optimization for reed-solomon processing. In *Application-specific Systems, Architectures and Processors, 2009. ASAP 2009. 20th IEEE International Conference on*, pages 177–182. IEEE, 2009.

[26] Lionel Biard and Dominique Noguet. Reed-Solomon Codes for low power communications. *Journal of Communications*, 3(2):13, 2008.

[27] A. Astarloa. *Reconfiguración dinámica de sistemas modulares multi-procesador en dispositivos SoPC*. Tesis Doctoral, Universidad del País Vasco, España, 2005.