Proyecciones (Antofagasta. On line) | vol. 40, n. 3 (2021) | pp. 731-742.

doi 10.22199/issn.0717-6279-4322

PROYECCIONES
Journal of Mathematics

ISSN 0717-6279 (On line)

Fractal mathematical over extended finite fields $F_p[x]/(f(x))$

Cecilia E. Sandoval-Ruiz[1] orcid.org/0000-0001-5980-292X

[1]Universidad de Carabobo, Instituto de matemática y cálculo aplicado, Valencia, Venezuela.
cesandova@gmail.com

Received: 08 July 2020 | Accepted: 02 November 2020

Abstract:

In this paper, we have defined an algorithm for the construction of iterative operations, based on dimensional projections and correspondence between the properties of extended fields, with respect to modular reduction. For a field with product operations $R(x) \bigotimes D(x)$, over finite fields, $GF[(p_m)^{n-k}]$. With $\mathbf{G}_p[x]/(g(f(x))$, whence the coefficient of the $g(x)$ is replaced after a modular reduction operation, with characteristic p.

$$R(x) = D(x)\epsilon_k \sum_{k=1}^{r} \ldots g_i \sum_{j=1}^{n-k} [\sum_{i=1}^{m} a_i (x^i)^j]^k \ mod_e(mod_g(mod\ p(x))).$$

Thus, the reduced coefficients of the generating polynomial of $\mathbf{G}$ contain embedded the modular reduction and thus simplify operations that contain basic finite fields. The algorithm describes the process of construction of the GF multiplier, it can start at any stage of LFSR; it is shift the sequence of operation, from this point on, thanks to the concurrent adaptation, to optimize the energy consumption of the GF iterative multiplier circuit, we can claim that this method is more efficient. From this, it was realized the mathematical formalization of the characteristics of the iterative operations on the extended finite fields has been developed, we are applying a algorithm several times over the coefficients in the smaller field and then in the extended field, concurrent form.

Keywords: Finite Galois extensions; Iterative multiplication over GF; Fractal design techniques; LFSR schemes; Self-similar circuits automorphism.
MSC (2020): 12F05, 12F10, 12K10

Cite this article as (IEEE citation style):

C. E. Sandoval-Ruiz, "Fractal mathematical over extended finite fields $F_p[x]/(f(x))$", *Proyecciones (Antofagasta, On line)*, vol. 40, no. 3, pp. 731-742, 2021, doi: 10.22199/issn.0717-6279-4322

1. Introduction

The theory of field extensions was developed by Galois [1, 2, 3, 4]. The number of elements of a finite field, also called a Galois Field GF [2] is of the form p^m. corresponds to the number of field, for a prime number p and a natural number m. For every power p^m exists a unique field of p^m elements up to isomorphism, denoted by $GF(p^m)$. Suppose that $F = GF(p^m)$ and that K is a subfield of F with p^k elements. Then k is a divisor of m and F is isomorphic to the quotient $K[x]/(f)$ of the polynomial ring $K[x]$ with coefficients in K on the ideal generated by a irreducible polynomial $f \in K[x]$ of degree $r = m/k$. Hence we can express the elements of F in the forma $A(x) = \sum_{i=0}^{r-1} a_i(x^i)$, with $a_i \in K, 0 \leq i \leq r-1$.

The field $GF(2^m)$ is an extension of the field $GF(2)$, called finite binary field, in which each element of $GF(2^m)$ can be represented by a vector of m elements in $GF(2)$. For an element $a \in GF(2^m)$ the operation of multiplication by x corresponds to a shift in the form:

$$x \cdot a(x) mod\ f = \begin{cases} \sum_{i=1}^{m} a_{i-1}x^i, & if\ a_{m-1} = 0 \\ \sum_{i=1}^{m}(a_{i-1} + a_{i-1}f_i)x^i + a_{m-1}f_0, & if\ a_{m-1} \neq 0 \end{cases}$$

(1.1)

where a_{m-1} is the feedback from LFSR (Linear Feedback Shift Register). In abstract algebra, Finite Galois Extensions are defined (see chapter 15 in [1]): $L|K$ is a (finite) Galois extension if there exists a finite subgroup $G \subset Aut(L)$, such that $K = Fix(L, G)$, where K is a subfield of L called the Fix field of G over L. Theorem of Galois theory describes the interplay between the Galois group and Galois extensions. In particular the result ties together subgroups of the Galois group and intermediate fields between L and K, this is presented in [1]. From the study of the extended finite fields and its properties, the description of the fractal (concatenated) operation of multiplication for extended fields was developed in this investigation, from a circuit interpretation LFSR [5] (see Figure 1).

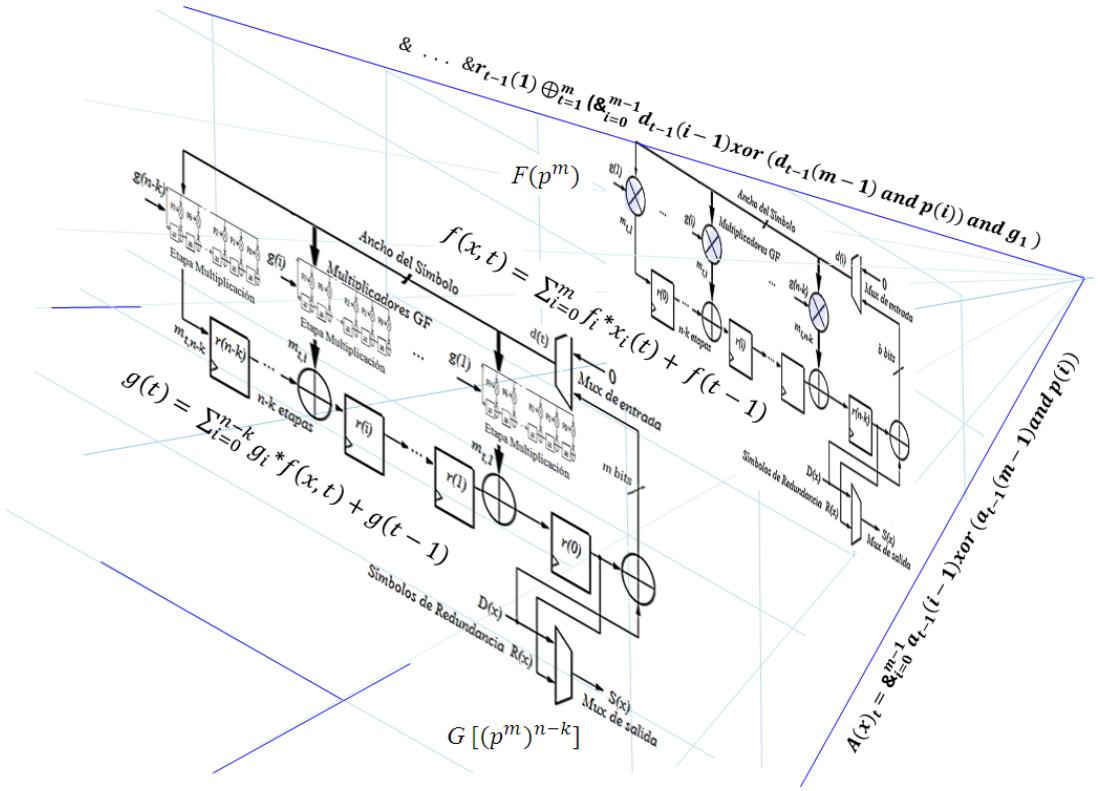

Figure 1. Fractal structure for iterative multiplication $GF[(p^m)^{n-k}]$.

The modular arithmetic can be applied in Cryptography, Theory of Code, Circuits on Systems, Galois Theory and Digital Communications and other areas as extended GF (see, for instance, [6-7] and references therein). This analysis starts from the study of the mathematical model of the polynomial representation, in which: If $p(x)$ is the irreducible polynomial, then the multiplication of two elements of the field, represented as the polynomials $A(x)$ and $B(x)$ is the algebraic product of the two polynomials, and the module operation of the polynomial $p(x)$, also known as modular reduction:

$$C(x) = A(x) \bigotimes B(x) \rightarrow C(x) = A(x) \cdot B(x) (mod\ p(x)) \tag{1.2}$$

The multiplication of polynomials is associative, commutative and distributive with respect to addiction [11-13], which is why we obtain:

$$(1.3) C(x) = B(x)\sum_{i=1}^{m} A_i x^i mod\ p(x) \rightarrow C(x) = \sum_{i=1}^{m} B_i (A(x)x^i mod\ p(x)$$

where $r(x) = A(x) mod\, p(x)$, corresponds to modular reduction over $GF(p^m)$. On the other hand, in the definition of the code word Reed Solomon [9], expressed through a generator polynomial G(x). This calculation is the resulting given as the operator $R_{g(x)}[.]$, applied on the data symbols $D(x)$.

$$(1.4) \qquad C(x) = x^{n-k}D(x) + R_{g(x)}[D(x)x^{n-k}]$$

Where $C(x)$ is the code word; n is the number of symbols in the code word and k is the number of symbols in the data word. The mathematical expression corresponds to assembling two polynomials, defined as: $c = (D << (n-k)) + (D << (n-k))\%g$. In the form: $C(x) = x^{n-k}D(x) + x^{n-k}D(x) mod\ g(x)$ Finding the mathematical expression of the redundancy symbol generator:

$$(1.5) \qquad R(x) = x^{n-k}D(x) mod\ g(x)$$

D(x) being a word of data of size k, which is operated by the polynomial $G(x) = g_{n-k}x^{n-k} + g_{n-k-1}x^{n-k-1} + \ldots + g_1$, an irreducible polynomial of length $n-k$. If F is a field, then F[x] forms an integral domain. F can be naturally embedded into F[x] by identifying each element of F with the corresponding constant polynomial. The only units in F[x] are the nonzero elements of F [1]. After studying the fundamentals of finite fields, it was possible to establish the commutative property for iterative operations, in a fractal structure, over extended fields. This algebraic property has application in various engineering fields.

$$\forall x \in F: \text{ and } \ f(x) \in G : mod(g(x)) = \sum_{j=1}^{n} g_j \bigotimes f(x_i(t)) + g_0(t-1)$$

Where the multiplication is defined as a convolution between the polynomials $G(x)$ and $D(x)$, detailed as the product operation over finite fields between the coefficient of the LFSR array at position i and the polynomial F(x), expressed by $g_j(x)$, plus the feedback of the independent term of the

polynomial in $t-1$. Some works define multiplication in a specific structure [14], in this case the objective is to define the iterative operation over extended finite fields.

The idea behind the paper is to make the calculations in $GF(q^n)$ when $n = mr$, in by applying equation (1.1) in two steps: we can consider $a \in GF(q^n)$ as a polynomial with coefficients in $GF(p^m)$ by using the irreducible polynomial in $GF(p^m)[x]$ of degree r and the operations needed in equation (1.1) can be done by applying again equation (1.1) with the elements of $GF(p^m)$ considered as elements of $Z_p[x]$ and an irreducible polynomial of $Z_p[x]$ of degree m. The description of the algorithm present fractal form, we are applying a similar algorithm several times to concurrent compute the coefficients in the smaller field and in the bigger field. We can claim that this method is more efficient is demonstrated by computing the number of operations and resources, as such as is proved in [15].

2. Preliminaries

Let $p[x]$ with characteristic p, that is, a prime field p that has been extended module an irreducible polynomial $f(x)$ of degree n. The extension field $\mathbf{F}_p[x]/(f(x))$ extends module another irreducible polynomial $g(x)$ of degree n/m, generating a field with a greater number of elements. For the case, arithmetic over Binary Extension Fields, the finite field $GF(2^m)$ is isomorphic to $GF(2)[x]/(p(x))$ whereby $p(x)$ is an irreducible polynomial of degree m with coefficients from $GF(2)$. We represent the elements of $GF(2^m)$ as binary polynomials of degree up to $m-1$ [16]. Addition is the simple logical XOR operation, while the multiplication of field elements is performed module the irreducible polynomial $p(x)$, some algorithm for GF_{mult} is presented in [17].

Theorem 2.1. Let R(x) is the modular reduction defined on the polynomial $G(x) = g_{n-k}x^{n-k} + g_{n-k-1}x^{n-k-1} + \ldots + g_1$, of the element $D(x)$. An LFC(n,k) transformation is defined; it is interpreted as the sum of products in the finite field, representing the concatenation of self-similar operators, which defines an extended field of dimensions $n-k$.

Theorem 2.2. Let the function f be an operation defined as the product in finite fields on the polynomial $p(x)$, and the function g be a concatenation operation of products on the polynomial $g(x)$, then:

$$g(f(x)) = \&_{i=n-k}^{k} g_{i-1} + g_i(f(x))$$

When replacing each operator, a fractal operator is obtained, a product of convolution. If the function $g(x)$ corresponds to $n-k$ elements operated in the finite field product of the function $f(x) \in GF(2^m)$, then $g(x) \in GF(2^{m \cdot n-k})$. For a proof of theorem 2.1 and theorem 2.2, see [18].

Lemma 2.1. Let F, B, and E be fields with $F \subseteq B \subseteq E$. Then

$$(E/F) = (E/B)(B/F)$$

.

Proof. Let $\epsilon_1, ..., \epsilon_m$ be a basis for **E** as a **B**-vector space and $\beta_1, ..., \beta_n$ be a basis for **B** as an **F**-vector space. We claim that $\epsilon_i b_j | i = 1, ..., m, j = 1, ..., n$ is a basis for **E** as an **F**-vector space, yielding the lemma. First, we show that this set spans **E**. Let $\alpha \in \mathbf{E}$.
Then $\alpha = \sum_{i=1}^{m} x_i \epsilon_i$, with $x_i \in \mathbf{B}$.
But for each $i, x_i = \sum_{i=1}^{m} (\sum_{j=1}^{n} \gamma_{i,j} \beta_j) \epsilon_i = \sum_{i,j=1}^{m,n} \gamma_{i,j} (\epsilon_i \beta_j)$.
For a proof of this, see [19]. Its application is present in concatenated systems; such is the case of 2D-RS codes.

3. Main results

In this section, we present the lemmas derived from the observation and identification of correspondence, and our main results:

Conjecture 3.1. Let **G** extended finite field of **F** and $\mathbf{G} = Aut(\mathbf{F})$ then

(i) Being $F \subset G$, the GF-multiplication operation over **F** is embedded in GF-multiplication operation on **G**.

(ii) The multiplication of elements on the extended Galois field **G** is iterative on the Galois field **F**.

(iii) If the fixed coefficients of the extended field generating polynomial g(x) have been reduced by **F**, the multiplication operation in the extended field is simplified.
If

$$g_i, d_i \in \mathbf{G} \text{ and } gf_i = g_i \ mod \ f(x) \in \mathbf{F} \text{ then } g_i \cdot d_i \in \mathbf{F}.$$

Proof. Starting from property of automorphism (same structural form between the field and its composition) [1], this are identified by correspondence in the structure by observation and circuit interpretation of the LFSR

scheme.

$$r(t) = \sum_{j=1}^{n} g_j(t) * d_j(t) + r_n(t-1),$$

with: $g_j(t) * d_j(t) = g_j(t) \sum_{i=1}^{m} d_i(t) * x_i(t) + p_0(t-1)$
$= d_j(t) \sum_{i=1}^{m} g_i(t) * x_i(t) + p_0(t-1)$

Finally, we obtain the expression of the form:

$$r(t) = d_j(t) \sum_{j=1}^{n} (g_i(t) * x_i(t) + p_0(t-1)) + r_n(t-1)$$

Theorem 3.2. For a finites field, if $\mathbf{F}$ is a field defined for $GF(p^m)$ and $\mathbf{G}$ a field defined $GF(q^n)$. Where $\mathbf{G}_q[x]/(g(x))$ and $\mathbf{F}_p[x]/(f(x))$, with p prime, then:
(i) $A(x) \bigotimes B(x) = A(x) \sum_{i=1}^{m} b_i x^i \ mod\ p(x) = B(x) \sum_{i=1}^{m} a_i x^i \ mod\ p(x)$
(ii) $G(x) \bigotimes D(x) = G(x) \sum_{j=1}^{n} D_j x^j \ mod\ g(x) = D(x) \sum_{j=1}^{n} G_j x^j \ mod\ g(x)$

This defines the field with iterative operations for $GF[(p^m)^n]$. Rewriting $\mathbf{F}_p[x]/(g(f(x))$, in which we can substitute the reduced operand on the $GF(p^m)$.

$$G(x) \bigotimes D(x) = D(x) \sum_{j=1}^{n} (\sum_{i=1}^{m} G_i x^i \ mod\ p(x))^j \ mod\ g(x)$$

With i, j determines the order of the element in the polynomial (position in the LFSR).

NOTE: For the particular application RS(n,k), the relation of degree of the polynomials on $\mathbf{F}$ and $\mathbf{G}$: $deg(a) < deg(p)$ and $deg(d) > deg(g)$, where $g(x)$ is a polynomial of $n-k$ elements, the index of the independent term of polynomial should be $n-k$, by the specific organization of the Galois LFSR array.

Proof. By commutative property with respect to the product [1], [12] is applied for the iterative modular reduction, from which it can be expressed:

$$G(x) \bigotimes D(x) = G(x) \sum_{j=1}^{n} (\sum_{i=1}^{m} (D_j x^j)^i \ mod_q\ (mod\ p(x))$$

The main difference with results presented in [17] is that in this paper is obtained the descriptor equation for definability of iterative multiplication over extended finite fields.

Lemma 3.3. If $\mathbf{C} = \text{Aut}\ (\mathbf{G}/\mathbf{F})$, with
(i) $a = \sum_{i=1}^{m} a_i x^i \in \mathbf{F}$ and $g = \sum_{j=1}^{n} g_j x^j \in \mathbf{G}$
(ii) $G(x) \bigotimes D(x) = D(x) \sum_{j=1}^{n} G_j x^j \ mod\ g(x)$
(iii) $A(x) \bigotimes B(x) = A(x) \sum_{i=1}^{m} b_i x^i \ mod\ p(x)$

Then

$$g(i) \bigotimes d(i) = d(i) \sum_{i=1}^{m} g_i x^i \ p(x)$$

Proof. See Theorem 3.2. With which the iterative form of the operation and fractal structure of the LFSR scheme is proven.

Lemma 3.4. If $\mathbf{C} = \text{Aut}\ (\mathbf{G}/\mathbf{F})$, $a = \sum_{i=1}^{m} a_i x^i \in \mathbf{F}$ and $g = \sum_{j=1}^{n} g_j x^j \in \mathbf{G}$ then

$$Aut(\mathbf{G}/\mathbf{F}) = Aut(GF_{mult}(\mathbf{G})/GF_{mult}(\mathbf{F}))$$

Proof. See Theorem 3.2. GF multiplication operation on each field has the same structure with an n/m dimensional relationship (see Figure 1).

Algorithm 3.5. Circuit description for iterative multiplication on extended field

For $k = 1$ to r generate –extended field $\mathbf{E} \subset \mathbf{G}$ with polynomial $e(x)$
For $j = 1$ to n generate –extended field $\mathbf{G} \subset \mathbf{F}$ with polynomial $g(x)$
For $i = 1$ to m generate –Field F with polynomial $p(x)$
$R(x) = D(x)\epsilon_k \sum_{k=0}^{r} g_i \sum_{j=1}^{n-k} [\sum_{i=1}^{m} a_i (x^i)^j]^k mod_e(mod_g mod\, p(x)))$.
–$mod(f(x)) \rightarrow LFSR$ Structure:
–With $LFSR_f : \sum_{i=1}^{m} f_i \cdot x_i(t) + f_0(t-1)$
–Concurrent form: $a_t = \&_{i=0]^{m-1}} a_{t-1}(i-1)x$ or $(a_{t-1}(m-1)$ and $p(i))$
–With $LFSR_g : \sum_{j=k+1}^{n-k} g_j \bigotimes D(x) + g_{n-k}(t-1)$
–Concurrent form: $r_t = \&_{i=0}^{n-k} r_{t-1}(i) \bigoplus [(D(k) \bigoplus r_{t-1}(n-k)) \bigotimes g(i)]$
$Next_i; Next_j; Next_k;$

The expression has been re-dimensioned concurrently [8], [15] by replacing the temporal dimension with a fractal spatial dimension. It is

important to note that optimizations in a field can be extrapolated to the extended field. The description of the optimized model [20-22], in which the temporal analysis was performed and the behavior of the LFSR was interpreted to obtain the equations of a concurrent architecture, can be supported under a Holographic Principle approach, of coexistence in the sequential results space. In which you can identify: self-organizing architecture of the n-LFSR, coefficients, weights or adaptive gains, Feedback of partial ring terms, combination of space-temporal terms and dimensional projection on fractal equations. Each finite field that belongs to a set has embedded the composition of the preceding field for operation.

4. Conclusion

The recognition of similarity between the structure of the GF_{mult} operations and automorphism has allowed defining a simplification on extended field, with the advantages of a generalized mathematical treatment for applications of this function. The equations developed in this research represent a contribution to the optimization of computation in applications of error correction codes, cryptography and for the design of complex systems, with feedback, being of special interest in multidimensional systems such as $2D - RS$ codes [10], scientific advance on fractal models [23-24]. This has advantages in the circuit of operations over finite fields, in the areas of mathematics and engineering.

(i) LFSR-Fractal ANN Model in extended finite fields.

(ii) Field generation polynomials with involution properties to simplify decoding over the extended field: $G(G(D(x)) = D(X)$.

(iii) Technique for the generation of structures for the parallel implementation of modular arithmetic [6], over finite field, where the number of component operations and their ordering is simplified and minimized.

(iv) Iterative algorithms for partial operations over extended finite fields, for hardware description for energy optimization [21].

(v) Expressions of energy balance, for Hybrid-Renewable Energy Systems [25, 26, 27, 28], with residual feedback inspired by modular LFSR reduction and circular operations with adaptive coefficients, in dynamic polynomial systems over finite fields.

References

[1] C. Carstensen, B. Fine, and G. Rosenberger, *Abstract algebra: applications to Galois theory, algebraic geometry and cryptography*. Berlin: de Gruyter, 2011.

[2] T. W. Hungerford, “Fields and Galois theory”, in *Algebra*, New York, NY: Springer, 1974, pp. 230–310, doi: 10.1007/978-1-4612-6101-8_6

[3] A. M. de Viola-Prioli, and J. E. Viola-Prioli, *Teoría de grupos y teoría de Galois*. Barcelona: Reverté, 2006.

[4] E. Arohuata, "Una clasificación completa de los campos finitos", Tesis de Licenciatura en Ciencias Físico Matemáticas, Universidad Nacional del Altiplano - Puno, 2017. [On line]. Available: https://bit.ly/3y7mbth

[5] C. E. Sandoval-Ruiz, “Modelo de estructuras reconfigurables con registro desplazamiento, para lenguaje descriptor de hardware VHDL”, *Revista de la Facultad de Ingeniería*, vol. 31, no. 3, pp. 63-72, 2016. [On line]. Available: https://bit.ly/2R5aEdA

[6] L. A. Cortés Vega, “A general method for to decompose modular multiplicative inverse operators on Group of units”, *Proyecciones (Antofagasta)*, vol. 37, no. 2, pp. 265-293, 2018. doi: 10.4067/S0716-09172018000200265

[7] J. Avila, “Partial actions and quotient rings”, *Proyecciones (Antofagasta)*, vol. 30, no. 2, pp. 201-212, 2011, doi: 10.4067/S0716-09172011000200006

[8] C. E. Sandoval-Ruiz, “Codificador RS (n,k) basado en LFCS: caso de estudio RS (7,3)”, *Revista Facultad de Ingeniería Universidad de Antioquia*, no. 64, pp. 68-78, 2012. [On line]. Available: https://bit.ly/2SKbVqT

[9] G. Reed and I. S. Solomon, “Polynomial codes on certain finite fields”, *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300-304, 1960, doi: 10.1137/0108018

[10] C. E. Sandoval-Ruiz, “Logical-mathematical model of encoder 2DRS for hardware description in VHDL”, *Revista ingeniería UC*, vol. 24, no. 1, pp. 28-39, 2017. [On line]. Available: https://bit.ly/3uFgtN3

[11] C. E. Sandoval Ruiz, “Multiplicador paralelo en campos finitos de Galois GF (2m) aplicado a códigos Reed Solomon con longitud ajustable sobre FPGA”, in *Memorias VII Congreso Nacional y 1er Congreso Internacional de Investigación de la Universidad de Carabobo. La Investigación en el Siglo XXI: Oportunidades y Retos*, vol. 2, Universidad de Carabobo and Consejo de Desarrollo Científico y Humanístico, Eds. Valencia: Universidad de Carabobo, 2010, pp. 1707–1711. [On line]. Available: https://bit.ly/3y2cE6X

[12] C. E. Sandoval-Ruiz, "VHDL optimized model of a multiplier in finite fields", *Ingeniería y universidad*, vol. 21, no. 2, pp. 195-211, 2017, doi: 10.11144/Javeriana.iyu21-2.vhdl

[13] G. C. Ahlquist, B. Nelson, and M. Rice, "Optimal finite field multipliers for FPGAs", in *Field programmable logic and applications*, P. Lysaght, J. Irvine, and R. Hartenstein, Eds. Berlin: Springer, 1999, pp. 51–60, doi: 10.1007/978-3-540-48302-1_6

[14] L. Cerda-Romero, and C. Martnez-Ranero, "The diophantine problem for addition and divisibility for subrings of rational functions over finite fields", *Proyecciones (Antofagasta)*, vol. 39, no. 3, pp. 721-735, 2020, doi: 10.22199/issn.0717-6279-2020-03-0045

[15] C. E. Sandoval-Ruiz, "Modelo optimizado del codificador Reed-Solomon (255,k) en VHDL a través de un LFSR paralelizado", Tesis de Doctorado, Universidad de Carabobo, Venezuela, 2013. [On line]. Available: https://bit.ly/3uFXfak

[16] J. Großschädl and E. Savaş, "Instruction set extensions for fast arithmetic in finite fields GF (p) and GF (2m)", in *Cryptographic hardware and embedded systems - CHES 2004*, M. Joye and J. Quisquater. Eds. Berlin: Springer, 2004, pp. 133-147, doi: 10.1007/978-3-540- 28632-5_10

[17] Z. Liu, H. Seo, J. Großschädl, and H. Kim, "Reverse product-scanning multiplication and squaring on 8-bit AVR processors", in *Information and communications security*, L. C. K. Hui, S. H. Qing, E. Shi, and S. M. Yiu, Eds. Cham: Springer, 2014, pp. 158-175, doi: 10.1007/978-3-319-21966-0_12

[18] C. E. Sandoval-Ruiz, "Operador matemático LFC(n,k) en campos finitos basado en concatenación fractal para GF (2m)Extendido". *Ciencia e ingeniería (Mérida)*, vol. 41, no. 2, pp. 197-204, 2020. [On line]. Available: https://bit.ly/3hhTKmD

[19] S. H. Weintraub, "Field theory and Galois theory" in *Galois theory*, 2nd Ed. New York, NY: Springer, 2009, pp. 7-44, doi: 10.1007/978-0-387-87575-0_2

[20] C. E. Sandoval-Ruiz and A. Fedón-Rovira, "Efficient RS (255,k) encoder on reconfigurable systems", *Revista técnica de la Facultad de Ingeniería. Universidad del Zulia*, vol. 37, no. 2, pp. 151-159, 2014. [On line]. Available: https://bit.ly/2QcBbVO

[21] C. E. Sandoval Ruiz, "Power consumption optimization in Reed Solomon encoders on FPGA", *Latin American applied research (Online)*, vol. 44, no. 1, pp. 81-85, 2014, doi: 10.52292/j.laar.2014.422

[22] C. E. Sandoval-Ruiz, "Métodos numéricos en diferencias finitas para la estimación de recursos de hardware FPGA en arquitecturas LFSR(n,k) fractales", *Ingeniería, investigación y tecnología (electrónica)*, vol. 20, no. 03, pp. 1-10, 2019, doi: 10.22201/fi.25940732e.2019.20n3.032

[23] C. E. Sandoval-Ruiz, "Análisis de circuitos fractales y modelado a través de sistema de funciones iteradas para VHDL", C*iencia e ingeniería (Mérida)*, vol. 38, no. 1, pp. 3-16, 2017. [On line]. Available: https://bit.ly/3w2jQOm

[24] C. E. Sandoval-Ruiz, C., "LFSR-fractal ANN model applied in R-IEDs for smart energy", *IEEE Latin America transactions*, vol. 18, no. 04, pp. 677-686, 2020, doi: 10.1109/tla.2020.9082210

[25] C. E. Sandoval-Ruiz, "Arreglos fotovoltaicos inteligentes con modelo LFSR-reconfigurable", *Ingeniera*, vol. 30, no. 2, pp. 32-61, 2020, doi: 10.15517/ri.v30i2.39484

[26] C. E. Sandoval-Ruiz, "Arreglo inteligente de concentración solar FV para MPPT usando tecnología FPGA", *Revista Técnica de la Facultad de Ingeniería*, vol. 43, no. 3, pp. 122-133, 2020, doi: 10.22209/rt.v43n3a02

[27] C. E. Sandoval-Ruiz, "Tecnología R-IEDs para ERNC, teletrabajo y mitigación de impacto ambiental", *Industrial data*, vol. 23, no. 2, pp. 151-167, 2020, doi: 10.15381/idata.v23i2.18633

[28] C. E. Sandoval-Ruiz, "Laboratorio móvil para optimización de sistemas de energías renovables y aplicaciones ambientales". *Ciencia e ingeniería (Mérida)*, vol. 42, no. 2, 169-178, 2021. [On line]. Available: https://bit.ly/33OCihL