Complejidad de arreglos periódicos multidimensionales

Jeffry M. Matos

I. Rubio

1. Resumen

Para obtener arreglos que puedan tener aplicaciones en sistemas que utilizan marcas de agua digitales, criptografía o señales de radar multi-blanco, los mismos deben poseer buenas propiedades de correlación y complejidad [5]. Por esto es imperativo el poder tener una medida de la complejidad de un arreglo multidimensional que no presente limitaciones. Las bases de Gröbner [3] son conjuntos de polinomios que poseen propiedades algorítmicas muy ricas. Al utilizarlas, es posible generalizar la definición de la medida de la complejidad lineal de una sucesión a un arreglo. Si calculamos alguna base de Gröebner que genere los polinomios asociados al arreglo periódico multidimensional, entonces podremos examinar la complejidad del arreglo porque esto permite obtener un conjunto delta $\Delta_{Val(A)}$ cuyo tamaño define la complejidad lineal del arreglo. En este trabajo se estudian algunas propiedades de arreglos construidos utilizando un método propuesto por Moreno y Tirkel [7]. Se utilizó el algoritmo de Rubio-Sweedler [9] para computar las bases de Gröbner del arreglo y con las mismas examinar la complejidad de arreglos periódicos multidimensionales obtenidos con construcciones en [7], comparar con la complejidad de los arreglos vistos como multisucesiones [8], formular conjeturas y obtener resultados.

Palabras Clave: bases de Gröbner, ideales, arreglos multidimensionales, arreglos periódicos, marcas de agua digitales.

2. Introducción

Cuando hablamos de un arreglo multidimensional nos referimos a un arreglo donde un elemento puede ser identificado mediante un vector de índices. Por ejemplo, un arreglo de dos dimensiones (una tabla rectangular) requeriría dos índices para localizar cada elemento (uno para la fila y otro para la columna). Si deseamos obtener arreglos multidimensionales que puedan ser utilizados en mensajes ocultos en imágenes [7] (marcas de agua digitales), criptografía y/o señales de radar multi-blanco, éstos deben poseer buenas propiedades de correlación y complejidad [5]; por lo que existe una necesidad de obtener una medida de la complejidad de los mismos. De esta manera podemos construir arreglos que sean resistentes a ataques y mantener la información segura. Trabajo previo [7] permite examinar la complejidad lineal de un arreglo utilizando el Teorema Chino del Residuo (CRT) y el algoritmo de Berlekamp-Massey [6] pero limita las dimensiones del arreglo a ser relativamente primas. Por lo que se busca una nueva definición de la complejidad lineal que extienda las posibilidades para los arreglos. Otra medida para la complejidad lineal de un arreglo se obtiene interpretando el arreglo como una multisucesión.

Comenzaremos introduciendo los conceptos para arreglos de una dimensión: sucesiones. Considere una sucesión $S = (s_i) = (s_0, s_1, ..., s_n, ...)$ con período n. Esto quiere decir que s_{i+nk}=s_i, $\forall\ i, k \in N$, indicando que existe una relación de recurrencia donde $s_{i+nk} - s_i = 0$, $\forall\ i, k \in Z$. Esta relación de recurrencia se puede representar usando un polinomio $x^n - 1$.

Definición 1: Sea $N_0 = \{0, 1, 2, ...\}$, el polinomio $C(x) = \sum c_i x^i$ define una **relación de recurrencia lineal** para la sucesión S si la ecuación:

$$\sum c_\alpha s_{\alpha+\beta} = 0$$

se cumple $\forall\ \beta \in N_0$, donde la suma es sobre los términos de $C(x)$. También se dice que $C(x)$ es **válido** en S. Un polinomio $C(x)$ válido en una sucesión también genera la misma. Podemos ver que el polinomio $x^n - 1$ siempre generará la sucesión S con período n ya que la periodicidad garantiza la existencia de coeficientes $c_n = 1, c_0 = -1$ tal que $c_n s_{n+\beta} + c_0 s_\beta = s_{n+\beta} - s_\beta = 0$, $\forall\ \beta \in N_0$. Esto implica que $s_{n+\beta} = s_\beta$; obteniendo así los términos de S a

partir de unos términos iniciales. Pero la sucesión también puede tener otros polimomios generadores con grado $m < n$.

Definición 2: La **complejidad lineal** de una sucesión periódica S es el grado del polinomio de grado mínimo que genera la misma [4].

Podemos interpretar un arreglo infinito **a** de dos dimensiones como una sucesión de sucesiones A=$(S_0, S_1, ..., S_m, ...)$ donde S_i es una sucesión. El mismo podemos ilustrarlo de la siguiente manera:

$$A = (a_{i,j}) = \begin{array}{|c|c|c|c|c|} \hline & & \vdots & & \\ \hline a_{0,3} & a_{1,3} & a_{2,3} & a_{3,3} & \\ \hline a_{0,2} & a_{1,2} & a_{2,2} & a_{3,2} & \\ \hline a_{0,1} & a_{1,1} & a_{2,1} & a_{3,1} & \cdots \\ \hline a_{0,0} & a_{1,0} & a_{2,0} & a_{3,0} & \\ \hline S_0 & S_1 & S_2 & S_3 & \cdots \\ \hline \end{array}$$

donde cada columna i de A está dada por cada sucesión S_i. El arreglo se dice ser *2-dimensional periódico* si existe un vector de período $n = (n_1, n_2) \in N_0^2$ tal que $a_{i+n_1,j+n_2}$=$a_{i,j}$, $\forall\ (i, j) \in N_0^2$. Esto indica que cualquier término $a_{i,j}$ se repite cada n_1 entradas horizontales y n_2 entradas verticales.

Definición 3: Sea $\alpha = (\alpha_1, \alpha_2)$ y $\mathbf{x}^\alpha = x^{\alpha_1} y^{\alpha_2}$, el polinomio $C(x, y) = \sum_{(\alpha_1,\alpha_2)} c_\alpha \mathbf{x}^\alpha$ define una **relación de recurrencia lineal** para el arreglo A si la ecuación:

$$\sum c_\alpha a_{\alpha+\beta} = 0$$

se cumple $\forall\ \beta \in N_0^2$, donde la suma es sobre los términos de $C(x, y)$. Si el polinomio $C(x, y)$ cumple con la Definición 3 es llamado un **polinomio válido** para el arreglo.

Llamamos $Val(A)$ a el conjunto de todos los polinomios válidos en el arreglo A. Este conjunto forma un ideal y es generado por un subconjunto de sus polinomios. La complejidad lineal, entonces, es una medida de resistencia a encontrar un conjunto mínimo generador de $Val(A)$. Algunos de estos conjuntos mínimos forman una base de Gröbner. El concepto de bases de

Gröbner fue introducido por Bruno Buchberger en 1965 [2] junto a un algoritmo para computarlas.

Definición 4: Sea $G = \{g_0, g_1, ..., g_l\} \subset I$, donde I es un ideal en $F[x_1, ..., x_n]$. Se dice que G es una **base de Gröbner** para I con respecto a un orden monomial $<_T$ si $\langle LM(g_0), LM(g_1), ..., LM(g_l)\rangle = \langle LM(I)\rangle$ (donde $LM(g_i)$ se refiere al monomio líder del polinomio g_i) [3].

El conjunto de polinomios que forma la base de Gröbner del ideal I respecto a $<_T$ genera I. Un concepto clave para definir la complejidad lineal de un arreglo periódico es el conjunto delta.

Lema 1: Sean $\Delta, \Gamma \subset N_0$. Los siguientes son equivalentes:

1. Para $\beta \in \Delta, \alpha \in N_0$, si $\alpha \leq \beta$ entonces $\alpha \in \Delta$.

2. Para $\alpha \in \Gamma, \beta \in N_0$, si $\alpha \leq \beta$ entonces $\beta \in \Gamma$.

El conjunto de exponentes de los monomios líderes en el ideal satisfacen (2) del Lema 1 ya que el ideal es cerrado bajo multiplicación de polinomios. Entonces, el conjunto de exponentes de los monomios que no sean monomios líderes en el ideal forman el **conjunto delta** ($\Delta_I = N_0^n \setminus LE(I)$).

Definición 5: Sea A un arreglo periódico multidimensional y $Val(A)$ el ideal de polinomios válidos en él, se define la **complejidad lineal** de A como la cantidad de elementos en el conjunto $\Delta_{Val(A)}$. Esto es, $\mathcal{L}(A) = |\Delta_{Val(A)}|$ [5].

Definición 6: Sea A un arreglo periódico 2-dimensional y (n_1, n_2) su vector de periodo. Se define la **complejidad lineal normalizada** $\mathcal{L}_n(A)$ del arreglo A como $\mathcal{L}_n(A) = \mathcal{L}(A)/n_1 n_2$ [1].

El concepto de complejidad lineal para sucesiones ha sido muy utilizado durante muchos años [4]. El algoritmo estándar para calcularla es el algoritmo de Berlekamp-Massey (BM) [6, 4]. Sin embargo, no existía un concepto de complejidad lineal para arreglos. En trabajos anteriores [7] la complejidad lineal de un arreglo se calculaba transformando el arreglo a una sucesión utilizando el teorema chino del residuo (TCR), y luego calculando la complejidad lineal de la sucesión utilizando el algoritmo de Berlekamp-Massey. Este método tenía la limitación de que, para poder utilizar el TCR las dimensiones del arreglo debían ser relativamente primas.

La definición de complejidad lineal introducida en [5] Definición 5 en este trabajo) permite calcular la complejidad lineal de arreglos de cualquier dimensión. La definición es consistente con el método TCR-BM ya que el cambio de un arreglo a una sucesión está estableciendo un orden de monomios y el cómputo de una base de Gröbner es una generalización del algoritmo de Berlekamp-Massey. Durante el resto de este trabajo F_q representa el cuerpo finito con q elementos.

3. Multisucesiones

El ótro método que ha sido utilizado para calcular la complejidad lineal de un arreglo es el de multisucesiones. En este método se interpreta el arreglo como una sucesión de columnas en donde cada columna representa alguna sucesión.

Definición 7: Para un entero arbitrario m, una **multisucesión** "m-folded" sobre F_q es una sucesión de m sucesiones paralelas sobre F_q, $S_1, ..., S_m$ [8].

Sean $f_1, ..., f_m \in F_q[x]$ polinomios mónicos arbitrarios con $grado(f_i) \geq 1$, $1 \leq i \leq m$. El conjunto $M_q(f_1, ..., f_m)$ es definido como el **conjunto de multisucesiones "m-folded"** $(S_1, ..., S_m)$ sobre F_q tal que para cada $1 \leq i \leq m$, S_i es una sucesion de recurrencia lineal con polinomio característico f_i.

Definición 8: El **polinomio conjunto mínimo** de una multisucesión "m-folded" $S \in M_q(f_1, ..., f_m)$ es el único polinomio mónico $M \in F_q[x]$ de grado mínimo que es un polinomio característico de S_i para todo $1 \leq i \leq m$. La **complejidad lineal conjunta** de S, $\mathcal{LM}(S)$, es el grado del polinomio con-

junto mínimo M [8].

Definición 9: El **conjunto de multisucesiones m-folded** n-periódicas es $M_q(f_1, ..., f_m)$ con $f_1 = ... = f_m = x^n - 1$. La complejidad lineal conjunta de una multisucesión también puede ser definida como el largo de la relación de recurrencia más corta que las m sucesiones paralelas satisfacen simultaneamente [8].

El siguiente teorema provee un método para calcular la complejidad lineal conjunta.

Teorema 1 [8]: La complejidad lineal conjunta de una multisucesión "m-folded" n-periódica $S = (S_1, ..., S_m)$ está dada por:

$$\mathcal{L}(S) = n - deg\left(\gcd\left(x^n - 1, S_0(x), S_1(x), ..., S_m(x)\right)\right).$$

Definición 10: Sea S una multisucesión "m-folded" con período n y $\mathcal{LM}(S)$ la complejidad lineal conjunta de S. Se define la **complejidad lineal conjunta normalizada** de S como $\mathcal{L}_n\mathcal{M}(S) = \mathcal{LM}(S)/n$ [8].

4. Construcciones de Moreno-Tirkel

En 2011 Moreno y Tirkel presentaron una construcción de arreglos de dos dimensiones $A = (a_{i,j})$ considerando dos sucesiones, una con buena buena complejidad y otra con buenas propiedades de correlación [7]. Construyendo, entonces, un arreglo de dos dimensiones desplazando la sucesión con buena complejidad en cada columna. El desplazamiento está dado por la sucesión con buenas propiedades de correlación. Esto es, si (s_i) es una sucesión con buena complejidad lineal y (t_i) es una sucesión con buena correlación, entonces $(a_{i,j})$ se define por $a_{i,j} = s_{j-t_i}$.

Por ejemplo, una sucesión con buena complejidad es la sucesión de Legendre y una sucesión con buenas propiedades de correlación es la sucesión de Costas.

Ejemplo 1: Sea $S = (s_j)$ una sucesión de Legendre respecto a 7, $S = (0, 1, 1, 0, 1, 0, 0, \ldots)$ definida por:

$$s_j = \begin{cases} \frac{1+\left(\frac{j}{7}\right)}{2}, & \text{if } j \neq 0 \ (mod\ 7) \\ 0, \text{ en otros casos} \end{cases},$$

y (t_i) la sucesión de Costas definida por $t_i = 3^i \pmod 7$. Se construye un arreglo colocando en la columna i la sucesión de Legendre desplazada t_i unidades hacia arriba (*Figuras 1, 2, 3*).

$S =$

6	0
5	0
4	1
3	0
2	1
1	1
0	0

Figura 1. Sucesión de Legendre S

$T =$

1	3	2	6	4	5
0	**1**	**2**	**3**	**4**	**5**

Figura 2. Sucesión de Costas T

6				$*$		
5						$*$
4					$*$	
3		$*$				
2			$*$			
1	$*$					
0						
	0	**1**	**2**	**3**	**4**	**5**

Figura 3. Inicio de los desplazamientos de S.

$$A = a_{(i,j)} = \begin{array}{|c|c|c|c|c|c|c|}\hline \mathbf{6} & 1 & 1 & 0 & \mathbf{0} & 0 & 0 \\ \hline \mathbf{5} & 0 & 0 & 1 & 1 & 0 & \mathbf{0} \\ \hline \mathbf{4} & 1 & 0 & 0 & 1 & \mathbf{0} & 1 \\ \hline \mathbf{3} & 0 & \mathbf{0} & 0 & 0 & 1 & 1 \\ \hline \mathbf{2} & 0 & 1 & \mathbf{0} & 1 & 1 & 0 \\ \hline \mathbf{1} & \mathbf{0} & 1 & 1 & 0 & 0 & 1 \\ \hline \mathbf{0} & 1 & 0 & 1 & 0 & 1 & 0 \\ \hline & \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} \\ \hline \end{array}$$

Figura 4. Arreglo con desplazamientos de S.

Las construcciones de Moreno-Tirkel pueden interpretarse desde la perspectiva de arreglo y como multisucesión. Si calculamos alguna base de Gröbner para los polinomios válidos en los arreglos construidos, entonces podremos examinar su complejidad hallando el conjunto delta $\Delta_{Val(A)}$ y la Definición 5. Queremos comparar esta definición de complejidad lineal con la definición de complejidad lineal del arreglo interpretado como multisucesión.

5. Metodología

1. Se computó la complejidad lineal de un arreglo periódico multidimensional A de dimensión 7×6 utilizando la Definición 5. El arreglo fue construido con el método Moreno-Tirkel utilizando una sucesión de Legendre sobre 7 y una sucesión de Costas

I. Se escogió el orden monomial $<_T$ grado lexicográfico $grlex$ y $(x > y)$.

II. Se calculó la base de Gröbner para $Val(A)$ con respecto a $<_T$ y

$x > y$ utilizando el algoritmo Rubio-Sweedler [9].

2. Se analizó la estructura y complejidad de las sucesiones que componían el arreglo.

3. Se computó la complejidad lineal conjunta dada por la Definición 9 y también utilizando el Teorema 1.

4. Se comparó la complejidad lineal del arreglo A de la Definición 5 y la complejidad lineal conjunta para la multisucesión A de la Definición 10.

5. Se formuló y probó la Proposición 1 relacionada al polinomio generador de sucesiones periódicas desplazadas.

6. Se formuló la Conjetura 1 que relaciona la compleijdad lineal normalizada y la complejidad lineal conjunta normalizada.

6. Resultados y análisis

Comparamos la complejidad lineal de un arreglo de dos dimensiones obtenida utilizando la Definición 5 con la complejidad lineal conjunta del arreglo interpretado como multisucesión (Definición 9).

6.1. Complejidad lineal conjunta de multisucesión

Trabajamos interpretando el arreglo del Ejemplo 1 como multisucesión. En este ejemplo, el período de las sucesiones es $n = 7$. Se puede verificar que el polinomio mínimo para la sucesión correspondiente a cada una de las columnas es:

$$P(x) = x^4 + x^2 + x + 1.$$

Esto implica que el polinomio mínimo de la multisucesión es:

$$P(x) = x^4 + x^2 + x + 1,$$

y, por lo tanto, la complejidad lineal conjunta de la multisucesión es 4. También podemos calcular la complejidad lineal conjunta utilizando el Teorema 1.

Escribiendo cada sucesión en su representación como polinomio tenemos:

$$\begin{aligned} S_0(x) &= x^6 + x^4 + 1 \\ S_1(x) &= x^6 + x^2 + x \\ S_2(x) &= x^5 + x + 1 \\ S_3(x) &= x^5 + x^4 + x^2 \\ S_4(x) &= x^3 + x^2 + 1 \\ S_5(x) &= x^4 + x^3 + x \\ S_f(x) &= x^7 - 1. \end{aligned}$$

Calculamos el divisor mayor común (GCD) de $\{S_f, S_0, S_1, S_2, S_3, S_4, S_5\}$, obteniendo $x^3 + x + 1$. Utilizando el Teorema 1, obtenemos que la complejidad lineal conjunta del arreglo es:

$$\mathcal{LM}(S) = n - deg\left(\gcd\left\{S_f, S_0, S_1, S_2, S_3, S_4, S_5\right\}\right) = 7 - 3 = 4.$$

La complejidad normalizada de la multisucesión es

$$\mathcal{L}_n\mathcal{M}(A) = \frac{4}{7} \approx 0.57.$$

El algoritmo propuesto por Berlekamp-Massey [6] para computar la complejidad lineal de una sucesión periódica dada en la Definición 2 permitió analizar cada sucesión individual que conformaba el arreglo construido con el método de Moreno-Tirkel [7]. Los resultados presentados permitieron formular la siguiente proposición.

Proposición 1: Sea $S = (s_i)$ una sucesión con período n y $S' = (s'_i)$, $s'_i = s_{i-t}$ la sucesión con desplazamiento circular hacia arriba de t entradas de S donde $i - t$ es reducido módulo n. Si $C(y)$ es un polinomio válido en S, entonces $C(y)$ es un polinomio válido en S'.

Demostración:

Suponga que $C(y)$ $\in$Val(S).*Entonces*

$$\sum c_i s_{i+\beta} = 0, \ \forall \ \beta \in N_0.$$

Debemos demostrar que $C(y) \in Val(S')$

$$\sum c_i s'_{i+\alpha} = \sum c_i s_{i-t+\alpha)}$$

$$= \sum c_i s_{i-t+\alpha+nk} = \sum c_i s_{i+\beta} = 0$$

donde $\beta = -t + \alpha + nk$, escogiendo nk de modo que β sea no negativo. La segunda ecuación resulta de la periodicidad de la sucesión, ya que S tiene período n.

6.2. Complejidad lineal del arreglo

Ahora interpretamos A como arreglo y calculamos la base de Gröbner reducida para $Val(A)$ con respecto al grado lexicográfico con $x > y$ utilizando una implementación del algoritmo Rubio-Sweedler en [9] hecha por Lillian González. Conseguimos que la base de Gröbner reducida para $Val(A)$ con respecto al orden monomial grado lexicográfico y $x > y$ es:

$$\left\{x^6 - 1, y^4 + y^2 + y + 1, xy^3 + xy^2 + x + y^3 + y^2 + 1\right\}$$

De aquí podemos obtener los monomios que no son monomios líderes de ningún polinomio en $Val(A)$. Estos polinomios forman el conjunto

$$\Delta_{Val(A)} = \Big\{1, y, x, y^2, xy, x^2, y^3, xy^2, x^2y, x^3,$$
$$x^2y^2, x^3y, x^4, x^3y^2, x^4y, x^5, x^4y^2, x^5y, x^5y^2\Big\},$$

obteniendo que $\left|\Delta_{Val(A)}\right| = 19$.

La complejidad normalizada del arreglo es

$$\mathcal{L}_n(A) = \frac{19}{42} \approx \ 0.45.$$

6.3. Comparación de las definiciones de complejidad

Utilizando los resultados obtenidos al computar la complejidad lineal y la complejidad lineal conjunta se formuló la Conjetura 1 que compara la complejidad normalizada con la complejidad lineal conjunta normalizada.

Conjetura 1 Sea A un arreglo, $\mathcal{L}_n(A)$ la complejidad lineal normalizada utilizando la Definición 3 y sea $\mathcal{L}_n\mathcal{M}(A)$ la complejidad lineal conjunta normalizada utilizando la Definición 4. Entonces,

$$\mathcal{L}_n(A) \leq \mathcal{L}_n\mathcal{M}(A). \tag{1}$$

Computar una base de Gröbner para el arreglo permitió comparar la complejidad del arreglo visto desde la perspectiva de multisucesión y la complejidad utilizando la Definición 5; obteniendo que estas no son iguales (Figura 5). Más aún, $\mathcal{L}_nM(A) = \mathcal{L}_n(S)$ debido a que el polinomio característico de la

multisucesión [8] captura las relaciones entre entradas en la misma columna pero no relaciona entradas en distintas columnas. Por lo tanto la complejidad propiesta por la Definición 10 enfoque en multisuceciones se reduce, utilizando el Teorema 1, a:

$$\mathcal{LM}(a) = n_2 - deg(gcd(y^{n_2} - 1, s^{n_2}(y)...)) = \mathcal{L}(S). \tag{2}$$

Esto implica que es óptimo observar las construcciones desde la perspectiva de arreglo y analizar su complejidad utilizando la Definición 5 ya que ésta definición captura relaciones de recurrencia que la Definición 10 no captura. Por lo tanto, la medida de complejidad que propone la Definición 5 provee una herramienta más eficiente para el análisis de complejidad de las construcciones.

Referencias

[1] R. Arce, F. Castro, O. Moreno, J. Ortiz, I. Rubio (2016), Construction and analysis of multidimensional periodic arrays, draft.

[2] B. Buchberger (1965). An algorithm for Finding a Basis for the Residue Class Ring of a Zero-dimensional Polynomial Ideal", Ph.D. Thesis, Univ. Of Innsbruck (Austria), Math. Inst., 1965.

[3] D. Cox, J. Little, D'OShea (2007). Ideals, Varieties and algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, Third Edition, Springer.

[4] C. Ding, T. Helleseth, W. Shan (1998). "On the linear complexity of Legendre Sequences", *IEEE Transactions on Information Theory*, Vol. 44, No. 3, (pp. 1276-1278).

[5] D. Gómez, T. Høholdt, O. Moreno, I. Rubio (2015). Linear Complexity for multidimensional arrays- a numerical invariant. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2015), (pp. 2697-2701).

[6] J. Massey (1969). Shift-Register Synthesis and BHC Decoding, , *IEEE Transactions on Information Theory*, Vol. IT-15, (pp.122-127).

[7] Moreno, O., Tirkel, A. (2011). Multidimensional periodic arrays for watermarking, Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on, (pp. 2691-2695).

[8] Mullen, G. L., Panario, D. (2013). Handbook of finite fields. London, NY: CRC Press.

[9] I. Rubio, M. Sweedler, C. Heegard (2016). Finding a Gröbner Basis for the ideal of recurrence relations on m-dimensional periodic arrays, Contemporary Developments in Finite Fields and Their Applications (accepted).

[10] S. Sakata (1989). Extension of the berlekamp-Massey Algorithm to n Dimensions, Inform. And Computation, vol. 84, (pp. 207-239).