SISTEMAS DINÁMICOS FINITOS BOOLEANOS MONOMIALES AFINES

Por
Leonid Brehsner Sepúlveda Avendaño

Tesis sometida en cumplimiento parcial de los requerimientos para el grado de:

MAESTRÍA EN CIENCIAS
en
MATEMÁTICAS PURAS

Universidad de Puerto Rico
Recinto Universitario de Mayagüez
2007

Aprobado Por:

Dr. Omar Colón Reyes Presidente, Comité Graduado	Fecha
Dr. Luis F. Cáceres Duque Miembro, Comité Graduado	Fecha
Dr. Gabriele Castellini Miembro, Comité Graduado	Fecha
Dr. Edusmildo Orozco S. Representante de Estudios Graduados	Fecha
Dr. Julio C. Quintana Díaz Director de Departamento de Ciencias Matemáticas	Fecha

Resumen

En este trabajo presentamos dos métodos para el estudio de la dinámica de algunos sistemas discretos. Un método envuelve el estudio del comportamiento cíclico de la dinámica del sistema discreto lineal. El otro método presenta una nueva herramienta para el estudio de sistemas dinámicos discretos monomiales, usando la transformada discreta de fourier sobre $\mathbb{F}_q$. La transformada discreta de fourier nos permite convertir un sistema multidimensional a uno unidimensional. Al final se resuelven dos problemas: determinar una cota superior para el número de soluciones de $f(x) =\in$ de un sistema monomial booleano afín f y también contar el número de ciertas involuciones sobre un cuerpo finito en términos de los residuos cuadráticos.

Abstract

In this work we present two methods to study the dynamics of some finite dynamical systems. One method concerns the study of the cyclic behavior of the dynamics of a linear finite dynamical system. The other method concerns a way to transform a finite dynamical system, from a multidimensional to a unidimensional one. This last method is known as the discrete fourier transform over $\mathbb{F}_q$. At the end, we solve two problems: we determine an upper bound for the number of solutions of $f(x) =\in$ where f is an affine boolean monomial system, and we count the number of certain involutions over a finite field in terms of quadratic residues.

Dedicatoria

A mis hijos Yeidy, Andrew y Santiago
A mi esposa Arcenia
A mi padre y hermanos
Al profesor Guztavo Loaiza: Dios lo tenga en la gloria

.

Agradecimientos

Quiero Agradecer:

En mi declinable afecto: al Dr. Omar Colón-Reyes.

Por el apoyo a la academia: al Dr. Pedro Vásquez Urbano, al Dr. Luís Fernando Cáceres Duque y al Dr. Julio César Quintana.

A los valores personales: al amigo Gabriel Darío Uribe Guerra.

Al acompañamiento fraternal: los amigos Rafael Aparicio Cuello y a Julián Rodríguez y Gabriel Uribe.

Por mi formación académica: al Dr. Omar Colón-Reyes, al Dr. Julio Barety, al Dr. Hector Salas, al Dr. Luís F. Cáceres....

Por su colaboración en la redacción de la tesis: la señorita Carmen Saldaña y el caballero Luís Pérez y José Bermejo.

Por su compañerismo: todos los antes mencionados y los estudiantes graduados, Luís Fuentes, los esposos Flores, Wanda Ortíz, Catalina Rúia y Sindy Díaz...

Por su humildad: al Dr. Wieslaw Dziobiak.

A una persona que se merece un afecto especial: Jonathan Ho.
Y todos aquellos que de alguna manera me enriquecieron culturalmente y socialmente.

Índice de figuras

1.1. Espacio Fase de un Sistema Dinámico Finito Lineal 4
1.2. Espacio Fase de un Sistema Dinámico Finito de Punto Fijo 4

2.1. Espacio Fase de f 7
2.2. Órbita de x 8
2.3. Transient t 8
2.4. Diagrama de f-invariante 9
2.5. Gráfica del Ejemplo 24 19
2.6. Espacio Fase S_{f_Ψ} 22
2.7. Espacio Fase de S_{f_χ} 22
2.8. Espacio Fase de S_{f_ζ} 23
2.9. Parte Nilpotente N y Parte Invertible I 24
2.10. Producto entre la Parte N y la Parte I. 26
2.11. Espacio Fase y Grafo Dependiente 27
2.12. Ejemplo de un Espacio Fase y Grafo Dependiente 28

3.1. Espacio Fase 31
3.2. Diagrama Conmutativo 33
3.3. Sistemas Dinámicos Finitos no Equivalentes 33
3.4. Subgrafos Isomorfos 34
3.5. Isomorfismo de Espacios Fase Bajo Fourier 37

4.1. Sistema Dinámico Finito Booleano Monomial y Afín 43
4.2. Dos Grafos de Dependencia 44
4.3. Grafos Simétricos Completos 46
4.4. Espacio Fase de g 47
4.5. Grafo simétrico de orden 3 basado en cubo 49
4.6. Distribución de RC y NRC para $p = 13$ 52

Índice general

1. Introducción **3**

2. Trabajos Previos **6**
2.1. Conceptos Básicos 6
2.2. Trabajos Importantes sobre Sistemas Dinámicos Finitos lineales y No-lineales 15
2.2.1. "The Theory A. of Linear Sequential Networks" 15
2.2.2. "The B. of Affine Boolean Sequential Networks" 20
2.2.3. "Linear Finite Dynamical Systems" 23
2.2.4. "Boolean Monomial Fixed Point Systems" 26

3. Transformada Discreta de Fourier Aplicada a SDF **30**
3.1. Preliminares 30
3.2. Método de la Transformada Discreta de Fourier sobre Cuerpos Finitos 35

4. SDF Booleanos Monomiales Afines y Temas Relacionados **42**
4.1. Resultados Relacionados a Sistemas Dinámicos Finitos Booleanos Monomiales Afines 42
4.2. Tópicos Relacionados y Problemas de Investigación 50

5. Conclusiones y Trabajos Futuros **58**
5.1. Conclusiones 58
5.2. Trabajos Futuros 58

Capítulo 1

Introducción

Los sistemas dinámicos finitos (SDF) sobre un cuerpo finito pueden clasificarse de dos tipos: lineales y no lineales. Varios autores están interesados en el estudio de los SDF procurando hallar una descripción completa de la dinámica de estos sistemas y, para nuestro interés, establecer condiciones necesarias y suficientes para que un SDF no lineal tenga una dinámica de punto fijo. Este trabajo de investigación se ha enfocado en el último problema, y en particular, sobre cuerpos finitos de característica dos, relacionada con la teoría booleana. En especial, trabajamos sobre los llamados sistemas dinámicos finitos booleanos monomiales afines. Para el caso de los SDF lineales sobre un cuerpo finito se tiene una descripción completa de la dinámica de estos sistemas (ver [13, 14]), donde la dinámica se encuentra codificada en el polinomio característico de la matriz que induce dicho sistema. En cambio, para el caso no lineal, no se tiene establecido una relación similar para su dinámica y, mas bien, se han presentado condiciones suficientes, como por ejemplo, para que un SDF monomial sea de punto fijo (ver [8]), y en específico, las condiciones suficientes y necesarias para que un SDF booleano monomial sea de punto fijo (ver [5, 7]). Bajo estos mismos objetivos, la investigación muestra una herramienta que puede ser aplicable a un SDF booleano monomial afín de punto fijo aprovechando un SDF polinomial equivalente y algunos aportes relacionados a la estructura algebraica de un caso especial de este último sistema. Para eso se presenta brevemente una reseña histórica de los trabajos relacionados con los SDF y la teoría matemática para el estudio de los SDF booleanos monomiales afines.

El SDF sobre un cuerpo finito tiene en la aplicación varios resultados importantes, por ejemplo, en áreas como redes secuenciales autónomas, teoría de autómatas, ciencia de la computación, simulación de computadores, redes bioquímicas, biología computacional y modelos matemáticos (ver [3, 9, 13]). Sin duda, a primera vista, los SDF pretenden relacionarse directamente con las ecuaciones diferenciales y estos sistemas (los SDF sobre un cuerpo finito) ahora aparecen como una nueva herramienta a la aplicación. Básicamente se aplica el álgebra, combinatoria, teoría de grafos y análisis de fourier discreto sobre grupos abelianos

finitos, (ver [17, 22]). A pesar de que muchas de estas áreas tienen un amplio cuerpo teórico, todavía no se halla en el medio bibliográfico un desarrollo fuerte del tema y en eso nuestra investigación quiere dejar varias contribuciones y preguntas abiertas que en algún momento fueron estudiadas (ver capítulo 5).

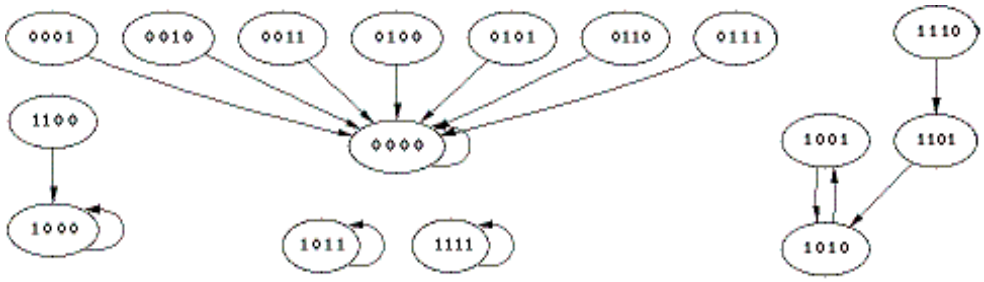


Figura 1.1: Espacio Fase de un Sistema Dinámico Finito Lineal

A continuación, en un breve resumen, explicaremos algunos conceptos mencionados previamente y presentamos el contenido que se encuentra incluido en varios capítulos para una buena ilustración. Cada vez que a un SDF se le quiere expresar su dinámica, la estaremos entendiendo por las órbitas del SDF (ó las iteraciones del sistema) y por su representación un grafo dirigido (llamado el espacio fase o espacio de iteración del SDF). Precisamente el diagrama del espacio fase va a enseñarnos el comportamiento dinámico del SDF (ver figura 1.1[1]); un caso especial, aquel cuyo espacio fase esta representado por sólo ciclos de longitud 1 (llamados ciclos triviales);es decir, un espacio fase con este diagrama se conoce como la

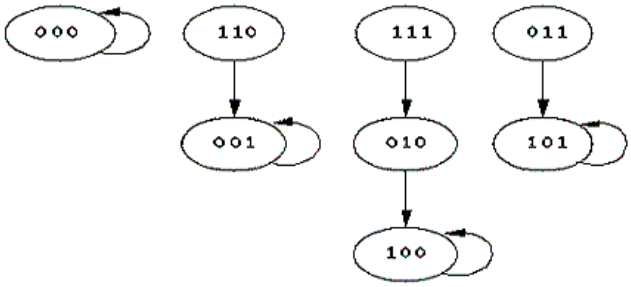


Figura 1.2: Espacio Fase de un Sistema Dinámico Finito de Punto Fijo

representación de un SDF de punto fijo que es equivalente a que el sistema tiene dinámica de quietud a partir de cierto momento en adelante (ver figura 1.2). Formalmente, un sistema dinámico finito es una función:

[1]La figura fué tomada y realizada la página http://dvd.vbi.vt.edu/visualizer/new_dvd11.pl. También muchas de las gráficas posteriores son realizadas por el mismo sistema.

$$f: \ \mathbb{X} \rightarrow \ \mathbb{X}$$

donde $\mathbb{X}$ es un conjunto finito y las iteraciones ó órbitas de f representan su dinámica. Un ejemplo concreto de un sistema dinámico finito sobre $\mathbb{F}_2^3$ donde $\mathbb{F}_2 = \{0, 1\}$ el cuerpo con dos elementos es:

$$\begin{array}{rccc} f: & \mathbb{F}_2^3 & \longrightarrow & \mathbb{F}_2^3 \\ & (x,y,z) & \rightarrow & f(x,y,z) = \ (x+y, xyz, xy+z) \end{array}$$

Para representar la dinámica de estos sistemas emplearemos un diagrama de flechas conocido como el espacio fase, denotado por S_f que consiste de un grafo dirigido donde el conjunto de vértices es $\mathbb{X}$ y cada vértice tiene una sola flecha de salida; es decir, el espacio fase S_f es un grafo dirigido cuyo conjunto de vértices es $\mathbb{X}$ donde un lado dirigido del vértice α al vértice β se representa por $\alpha \rightarrow \beta$, siempre y cuando $f(\alpha) = \beta$. Para el caso del ejemplo anterior el espacio fase está dado por la figura 1.2.

Dividiremos este trabajo en cinco capítulos. En el capitulo 1 una introducción del contenido y en el capítulo 2 se quiere presentar algunos de los resultados más importantes de los principales trabajos previos a esta investigación,

- "The Theory of Autonomous Linear Sequential Networks" por Bernard Elspas.
- "The Behavior of Affine Boolean Sequential Networks" por D. K. Milligan y M. J. D. Wilson.
- "Linear Finite Dynamical Systems" por Rene H. Toledo.
- "Boolean Monomial Dynamical Systems" por Omar Colón-Reyes, R. Laubenbacher y B. Pareigis.

En el capítulo 3 vamos a emplear una herramienta nueva que nos permite ver como un SDF sobre un espacio de dimensión finita tiene propiedades similares (la dinámica) a un SDF sobre un cuerpo finitos de una dimensión. Utilizando el análisis discreto de fourier sobre cuerpos finitos, estos dos sistemas son equivalentes en el sentido que su dinámica es la misma. Además, presentamos ejemplos que ilustran como dos SDF tienen el mismo comportamiento dinámico. En el capítulo 4 mostraremos dos importantes resultados que se obtuvieron, el primero sobre los SDF monomiales afines, y el segundo, sobre SDF polinomiales sobre $\mathbb{Z}_p$. Por último se presenta las conclusiones del trabajo de investigación y el trabajo a seguir en capítulo 5.

Capítulo 2

Trabajos Previos

Este capítulo esta dividido en dos secciones: la primera sección recoge la terminología general y conceptos fundamentales de álgebra lineal y campos finitos. La segunda sección es una recopilación de varios artículos importantes previos a este trabajo sobre sistemas dinámicos finitos lineales y no-lineales. También se presentan muchos ejemplos que ilustran algunos teoremas y proposiciones de suma importancia y que motivan en primera instancia el desarrollo de los demás capítulos. Los artículos de B. Elspas, H. Toledo, Milligan y Wilson (ver [13, 14, 18]) han sido importantes en la investigación, que desde un principio, se ha querido establecer como objetivo el "Estado del Arte" de los sistemas dinámicos lineales sobre un cuerpo finito, pero sólo presentamos lo que puede ser, en principio, una base teórica de estos sistemas lineales. En cambio el estudio de los sistemas dinámicos discretos no lineales dirigido a los monomiales, es nuevo, y un aporte inicial a esto aparece en el artículo de O. Colón, R. Laubenbacher y B. Paregis (ver [8]) enfocado hacia los sistemas dinámicos de punto fijo.

2.1. Conceptos Básicos

Esta sección básicamente esta dedicada en gran parte a los preliminares para el desarrollo de los capítulos.

Definición 1 *Una función de conjunto $f : X \to X$ donde X es un conjunto finito, se llama sistema dinámico finito sobre X.*

Utilizaremos la notación SDF para Sistema Dinámico Finito y SDFL para Sistema Dinámico Finito Lineal. Recordemos que si X es un espacio vectorial de dimensión n sobre un cuerpo E, el SDF f se puede escribir de la forma $f = (f_1, f_2, \ldots, f_n)$, donde cada $f_i : X \to E$ es llamada la función coordenada de f. Cuando $X = \mathbb{F}_q^n$ un espacio vectorial sobre $\mathbb{F}_q$ (cuerpo finito de característica prima), las funciones coordenadas f_i pueden ser representados por polinomios en

$\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ (ver [16]). En particular, cuando $X = \mathbb{F}_2^n$ el SDF es booleano y lo abreviamos por SDFB.

La siguiente definición muestra una componente gráfica de un SDF determinado por un grafo dirigido. Este grafo representa una herramienta práctica para ilustrar la dinámica de f.

Definición 2 (Espacio Fase) *El espacio fase de un SDF f sobre X, es un grafo dirigido tal que:*

- El conjunto de vértices es X.
- Dados $\mu, \beta \in X$, existe un eje dirigido o lado dirigido $\mu \xrightarrow{f} \beta$ si y sólo si $f(\mu) = \beta$.
- El espacio fase de un SDF f lo denotamos por $S(f)$ ó S_f.

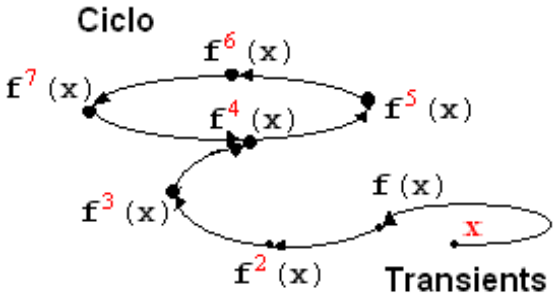


Figura 2.1: Espacio Fase de f

En la figura 2.1 podemos observar las iteraciones de f consigo misma, basado en x, y esto permite reconstruir el espacio fase de f por intermedio de los ciclos y los "Transients" (más adelante se definirá el "Transient"). Las iteraciones de un SDF se definirán a continuación y se conoce como la órbita de x (ver figura 2.2).

Definición 3 *El conjunto $\mathcal{O}_f(x) = \{f^n(x) : n \geq 0\}$ con $n \in \mathbb{Z}$, se define como la órbita de $x \in X$ relativo a f.*

El espacio fase de un SDF no biyectivo aparecen dos componentes importantes, una componente cíclica y otra la componente "Transient" y se procura a definirse.

Definición 4 *En las órbitas de $x \in X$, $\mathcal{O}_f(x)$ existen enteros $k \geq 1$ y $n \geq 0$ tal que, $f^{n+k}(x) = f^n(x)$. Si tomamos los valores de n y k minimales entonces se define lo siguiente:*

Ciclo Si $f^k(a) = f^0(a) = a$, para algún $a \in X$, entonces se tiene que $\mathcal{O}_f(x)$ es un ciclo de longitud k, basado en a.

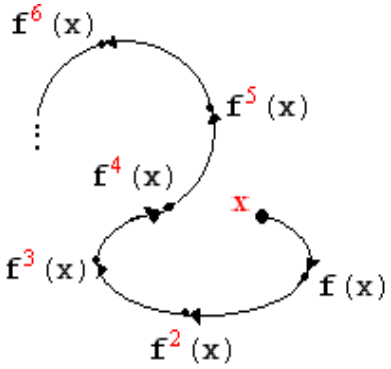


Figura 2.2: Órbita de x

Punto Fijo En el caso anterior, cuando $k = 1$, $(f(a) = a)$, a se llama punto fijo.

Parte "Transient" En el caso que $n \geq 0$, la parte correspondiente de la órbita x, $f(x)$, $f^2(x), \ldots, f^k(x)$ con k el valor mínimo que satisface $f^k(x) = f^{k+l}(x)$ y $f^k(x) \neq f(x)$, es llamada la parte "Transient" de la órbita de x. También es llamado el "Transient" t si hay un ciclo basado en $f^t(x)$ (ver figura 2.3).

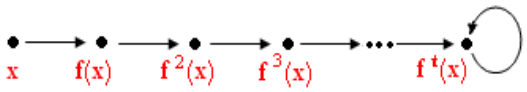


Figura 2.3: Transient t

Definición 5 (Dinámica de un SDF) *La dinámica de un SDF se conoce como el comportamiento de todas las órbitas o iteraciones del sistema, es decir, la cantidad de ciclos, árboles, "Transients" y la longitud de ellos.*

Si $f : X \to X$ es un SDFL y X un espacio vectorial de dimensión finita, entonces podemos escribir a X como la suma directa de dos subespacios invariantes bajo f; es decir, existen subespacios $\mathbb{W}_i \subseteq X$, tal que $f(\mathbb{W}_i) \subseteq X$ y $X = W_1 \oplus W_2$. Por consiguiente, el estudio de la dinámica de un SDFL se obtiene como consecuencia del estudio de la dinámica de cada subespacio invariante del sistema (ver [13, 14]). Asumiremos a X un espacio Vectorial.

Definición 6 (Subespacio Invariante) *Sea f un SDFL sobre X. Un subespacio $\mathbb{W} \subseteq X$ se llama un subespacio invariante relativo a f (o simplemente $f-$invariante), si $f(\mathbb{W}) \subseteq \mathbb{W}$.*

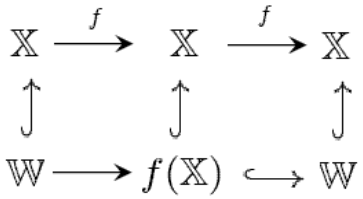


Figura 2.4: Diagrama de f-invariante

Recordemos que $X = \mathbb{F}_q^n = \overbrace{\mathbb{F}_q \oplus \mathbb{F}_q \oplus \cdots \oplus \mathbb{F}_q}^{n-veces}$ representa el producto de n copias directas de $\mathbb{F}_q$ donde $n \geq 1$ y $\mathbb{F}_q$ es un cuerpo finito con q elementos, y la suma de transformaciones lineales es de nuevo una transformación lineal sobre $\mathbb{F}_q^n$. En las siguientes dos proposiciones se muestra la descomposición de $\mathbb{F}_q^n$ como suma directa de subespacios invariantes, para ello se usa el concepto de polinomio minimal de f (respectivamente M_f) y lo denotamos por $m_f(x)$ (respectivamente $m_{M_f}(x)$). El polinomio minimal de f es el polinomio mónico de menor grado sobre $\mathbb{F}_q$ que al ser evaluado por la matriz representación de f, esta resulta ser la matriz cero. También el determinante de $M_f - Ix$ donde I es la matriz identidad se conoce como el polinomio característico del SDFL f o de la matriz M_f y lo denotamos por $\varphi_f(x)$.

Definición 7 *Sea $\psi(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{F}_q[x]$ y sea $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ un SDFL entonces f puede ser representada por una matriz, llamada M_f y $\psi(f) = a_0 \cdot 1 + a_1f + \cdots + a_nf^n$ es un SDFL donde 1 es el SDF identidad sobre $\mathbb{F}_q^n$, también se puede definir $\psi(M_f) = a_0 \cdot I + a_1M_f + \cdots + a_nM_f^n$ donde I es la matriz identidad (ver [10]).*

Para el polinomio minimal se tiene la siguiente propiedad de Caley-Hamilton (ver [10, 11, 16]):

- Si $m_f(x) \neq 0$ en $\mathbb{F}_q[x]$ entonces $m_f(f) = 0$ (respectivamente $m_f(M_f) = 0$) .
- Si $g(x) \in \mathbb{F}_q[x]$ tal que $g(f) = 0$ entonces $m_f(x) \mid g(x)$ en $\mathbb{F}_q[x]$.

Note que $\varphi_f(f) = 0$ ($\varphi_f(x)$ es el polinomio característico del SDFL f) entonces por la propiedad de Caley-Hamilton $m_f(x) \mid \varphi_f(x)$, es más, $\varphi_f(x) \mid m_f(x)^n$ para algún entero positivo n (ver [11], pag. 478]). Si f es un SDFL sobre $\mathbb{F}_q^n$ y su polinomio minimal es irreducible, entonces $m_f(x) \mid \varphi_f(x)$ y $\varphi_f(x) \mid m_f(x)$; en otras palabras, el polinomio minimal de f es igual al polinomio característico, es decir,

$$\varphi_f(x) = m_f(x)$$

Las siguientes dos proposiciones se requieren para la próxima sección (ver [10]) y muestra como descomponer a $\mathbb{F}_q^n$ como suma directa de subespacios invariantes. Los SDFL como transformaciones lineales tienen muchas propiedades comunes que se tendrán en consideración y adicional a eso resaltamos una sobre espacios invariantes: dice que el comportamiento cíclico está compuesto por producto de ciclos entre espacios invariantes.

Proposición 8 (Espacio Nulo) *Sea f un SDFL sobre $\mathbb{F}_q^n$ y $\phi(x) \in \mathbb{F}_q[x]$, entonces el conjunto*

$$N(\phi(f)) = \left\{v \in \mathbb{F}_q^n : \phi(f)(v) = 0\right\}$$

es un $f-$ invariante.
Prueba. *Dado que f es un SDFL sobre $\mathbb{F}_q^n$ entonces $\phi(f)$ también lo es. Además $\phi(f)(f) = f(\phi(f))$. Probemos que $N(\phi(f))$ es un $f-$ invariante, es decir, si $z \in N(\phi(f))$ entonces $f(z) \in N(\phi(f))$. En efecto,*

$$\phi(f)(f(z)) = (\phi(f)f)(z) = (f\phi(f))(z) = f(\phi(f)(z)) = f(0) = 0$$

por tanto $f(z) \in N(\phi(f))$ ■

Proposición 9 (Descomposición Primaria de $\mathbb{F}_q^n$) *Sea f un SDFL sobre $\mathbb{F}_q^n$ y sea $m_f(x) = \prod_{i=1}^{k} p_i(x)^{e_i}$ el polinomio mínimo de f, donde cada $p_i(x)$ son factores irreducibles distintos en $\mathbb{F}_q[x]$. Entonces para cada $i \in \{1, 2, \ldots, k\}$, se define:*

$$N(\ p_i^{e_i}(f)) = \left\{v \in \mathbb{F}_q^n \ : \ p_i^{e_i}(f)(v) = 0\right\}$$

es un f-invariante de $\mathbb{F}_q^n$ y

$$\mathbb{F}_q^n = \bigoplus_{i=1}^{k} N(p_i^{e_i}(f))$$

donde el polinomio minimal de $f\ |_{N(p_i^{e_i}(f))}$ es $p_i^{e_i}(f)$.
Prueba. *Sea $q_i(x) = \frac{m_f(x)}{p_i^{e_i}(f)}$ con $1 \leq i \leq k$ son polinomios que no tienen factores comunes irreducibles entre si, ya que cada factor irreducibles de algún $q_i(x)$ no aparece en algún $q_j(x)$, por tanto existen $f_i(x) \in \mathbb{F}_q[x]$ con $1 \leq i \leq k$ tal que*

$$1 = \sum_{i=1}^{k} q_i(x) f_i(x)$$

reemplazando a x por f en esta ecuación se tiene que

$$1 = \sum_{i=1}^{k} q_i(f) f_i(f)$$

luego para cada $z \in \mathbb{F}_q^n$ *podemos representar a* z *por la siguiente suma*

$$z = \sum_{i=1}^{k} \left(q_i(f) f_i(f)\right)(z)$$

donde $\left(q_i(f) \cdot f_i(f)\right)(z) \in N(p_i^{e_i}(f))$*, ya que*

$$\begin{aligned} p_i^{e_i}(f)\left(q_i(f) f_i(f)\right)(z) &= \left(p_i^{e_i}(f)\frac{m_f(f)}{p_i^{e_i}(f)}\right)\left(f_i(f)(z)\right) \\ &= \left(m_f(f) f_i(f)\right)(z) = \left(0 f_i(f)\right)(z) = 0 \end{aligned}$$

Ahora probemos que esta representación es única. Es suficiente probar que dado

$$v_1 + v_2 + \cdots + v_k = 0 \text{ con } \; v_i \in N(p_i^{e_i}(f))$$

entonces para todo i*,* $v_i = 0$*.*
En efecto, primero se cumple por definición que $p_i^{e_i}(f) v_i = 0$ *y segundo para* $i \neq j$ *se tiene*

$$\begin{aligned} q_i(f) v_j &= p_1^{e_1}(f) \cdots p_j^{e_j}(f) \cdots p_k^{e_k}(f) v_j \;\; \text{donde } p_i^{e_i}(f) \text{ no aparece} \\ &= \left(p_1^{e_1}(f) \cdots p_{j-1}^{e_{j-1}}(f) p_{j+1}^{e_{j+1}}(f) \cdots p_k^{e_k}(f)\right) p_j^{e_j}(f)(v_j) \\ &= \left(p_1^{e_1}(f) \cdots p_{j-1}^{e_{j-1}}(f) p_{j+1}^{e_{j+1}}(f) \cdots p_k^{e_k}(f)\right)(0) \\ &= 0 \end{aligned} \tag{2.1}$$

como $p_i(x)^{e_i}$ *y* $q_i(x)$ *son polinomios primos relativos sobre* $\mathbb{F}_q$ *entonces existen* $f(x)$*,* $b(x) \in \mathbb{F}_q[x]$ *tales que*

$$1 = f(x) p_i^{e_i}(f) + b(x) q_i(x)$$

luego

$$1 = f(f) p_i^{e_i}(f) + b(f) q_i(f)$$

por tanto, empleando la ecuación 2.1

$$\begin{aligned} v_i &= 1 \cdot v_i \\ &= \left(f(f) p_i^{e_i}(f) + b(f) q_i(f)\right) v_i \\ &= \left(f(f) p_i^{e_i}(f)\right)(v_i) + \left(b(f) q_i(f)\right)(v_i) \\ &= f(f)0 + b(f) q_i(f)\left(-(v_1 + \cdots + v_{i-1} + v_{i+1} + \cdots + v_k)\right) \\ &= 0 - b(f) q_i(f)(v_1) - \cdots - b(f) q_i(f)(v_{i-1}) - b(f) q_i(f)(v_{i+1}) - \cdots - b(f) q_i(f)(v_k) \\ &= 0 \end{aligned}$$

por tanto $v_i = 0$
se concluye por definición de suma directa que

$$\mathbb{F}_q^n = N(p_1^{e_1}(f)) \oplus N(p_2^{e_2}(f)) \oplus \cdots \oplus N(p_k^{e_k}(f))$$

por último, tomemos $f_i = f\,|_{N(p_i^{e_i}(f))}$ *y por definición de la función restricción de* f *se cumple* $p_i^{e_i}(f) = 0$ *y por la propiedad de Caley-Hamilton su polinomio minimal* $m_f(x)$ *cumple* $m_f(x) \mid p_i^{e_i}(f)$ *por tanto, esto sólo es cierto si* $m_f(x) = p_i^{e_i}(f)$*.* ■

Ahora, introducimos el concepto de divisores elementales de un SDFL f y el concepto de subespacio $f-$cíclico sobre el espacio vectorial $\mathbb{F}_q^n$.

Definición 10 (Subespacio $f-$cíclico) *Sea f un SDFL sobre $\mathbb{F}_q^n$. Un subespacio $\mathbb{W}$ de $\mathbb{F}_q^n$ es $f-$cíclico, si existe un vector $w \in \mathbb{W}$ para los cuales el conjunto $\{w,\ f(w)\ ,\ldots,\ f^{m-1}(w)\}$ es una base para $\mathbb{W}$ sobre $\mathbb{F}_q$, donde m es la dimensión de $\mathbb{W}$.*

Observación 11 *La descomposición primaria de $\mathbb{F}_q^n$ se puede aplicar a cada espacio nulo $N(\,p_i^{e_\mathbf{i}}(f))$ (proposición 9 y ver[20]), donde $N(\,p_i^{e_\mathbf{i}}(f))$ puede escribirse como suma directa de subespacios $f-$cíclicos*

$$N(p_i^{e_\mathbf{i}}(f)) = \bigoplus_{j=1}^{k} N(p_j^{e_\mathbf{j}}(f))$$

donde el polinomio mínimo de $f\mid_{N(p_\mathbf{i}^{\mathbf{e_{i_j}}}(x))}$ es $p_\mathbf{i}^{\mathbf{e_{i_j}}}(x)$ con

$$e_i = e_{\mathbf{i}_1} \geq e_{\mathbf{i}_2} \geq \cdots \geq e_{\mathbf{i}_{\mathbf{k}_\mathbf{i}}}\ \ y\ \ e_{\mathbf{i}_1} + e_{\mathbf{i}_2} + \cdots + e_{\mathbf{i}_{\mathbf{k}_i}} = e_i$$

Los polinomios $p_\mathbf{i}^{\mathbf{e_{i_j}}}(x)$ se llaman los divisores elementales de f determinados de manera única.

Definición 12 (Divisores Elementales) *Los polinomios $p_\mathbf{i}^{\mathbf{e_{i_j}}}(x)$ de la observación anterior se llaman los divisores elementales de f.*

El concepto de divisores elementales de un SDFL es de suma importancia y se relaciona directamente con el polinomio minimal y el polinomio característico de un SDFL. Sin entrar en detalles la forma equivalente del polinomio minimal (denotado por $m_f(x)$) es el producto de todos los divisores elementales de f de mayor grado y el polinomio característico (denotado por $\varphi_f(x)$) es el producto de todos los divisores elementales de f (ver [11]). Las proposiciones siguientes y el teorema 15 son fundamentales para SDFL y se encuentran en [14].

Definición 13 (Polinomio Aniquilador) *El polinomio aniquilador $p(x)$ de un SDFL f, si $p(f) = 0$.*

Observación 14 *La existencia de un polinomio aniquilador de cualquier mapa lineal esta garantizado por la propiedad de Caley-Hamilton (ver* [11]*).*

El siguiente teorema se encuentra en el artículo de Toledo (ver [14]).

Teorema 15 *Sea p un polinomio aniquilador del SDFL f sobre X (espacio finito dimensional). Sea $p(x) = p_1(x)p_2(x)$ donde $p_1(x)$ y $p_2(x)$ son polinomios relativamente primos. Entonces,*

$$X = F_1 \oplus F_2$$

donde F_1 y F_2 son subespacios $f-$ invariantes y $p_i(x)$ es el polinomio aniquilador para la restricción de f sobre F_i ($f_i = f\mid_{F_i}$). Para el caso donde $p(x) = \phi_f(x)$ es el polinomio característico del SDFL f entonces $p_i(x)$ es el polinomio característico de f_i.
Prueba. *Usando el hecho de que $p_i(x)$ es el polinomio aniquilador de f_i, se tiene $p_i^{e_i}(f)(v) = 0 \Leftrightarrow v \in N(p_i(f))$, por tanto, tomando $F_i = N(p_i(f))$ y aplicando el teorema anterior se tiene que*

$$X = F_1 \oplus F_2$$

donde $p_i(x)$ también es el polinomio característico de $f_i = f\mid_{F_i}$ ■

Para denotar el producto directo entre dos SDFL, por ejemplo, f_1 y f_2 sobre F_1 y F_2 respectivamente, se empleará $(f_1, F_1) \times (f_2, F_2)$. En la próxima proposición se aplica esta notación a dos subespacios invariantes.

Proposición 16 *Sea f un SDFL sobre X y supongamos que*

$$X = F_1 \oplus F_2$$

donde F_1 y F_2 son subespacios $f-$ invariantes. Sea f_i la restricción de f sobre F_i. Entonces f es un SDFL sobre F_i y $(f, X) = (f_1, F_1) \times (f_2, F_2)$.
Prueba. *Se tiene que $X = F_1 \oplus F_2 \cong F_1 \times F_2$. Ahora por la linealidad de f y la representación única, para todo $x \in X$, existe $x_i \in F_i$ tal que $x = x_1 + x_2$ entonces*

$$f(x) = f(x_1 + x_2) = f(x_1) + f(x_2) = f_1(x_1) + f_2(x_2)$$

por tanto $f = f_1 \times f_2$. ■

En la proposición anterior se representó a X como el producto directo entre los espacios vectoriales F_1 y F_2, por ende el estudio de la dinámica del SDFL f puede limitarse al estudio de la dinámica de los SDFL f_1 y f_2 (ver sección siguiente). Mostraremos un ejemplo que enseña este comportamiento a continuación.

Ejemplo 17 *Consideremos el siguiente SDFL*

$$\begin{array}{rccc} f: & \mathbb{F}_3^3 & \longrightarrow & \mathbb{F}_3^3 \\ & (x,y,z) & \mapsto & (2x, 2x+y+z, x+y) \end{array}$$

entonces su polinomio característico esta dado por $\phi_{M_f}(x) = (x+1)(x^2+2x+2)$, *donde*

$$M_f = \begin{pmatrix} 2 & 0 & 0 \\ 2 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

$y\ \phi_{f_1}(x) = x+1\ \ y\ \ \phi_{f_2}(x) = x^2+2x+2$. *Por la proposición 16*

$$\mathbb{F}_3^3 = \mathbb{F}_3 \oplus \mathbb{F}_3^2 \quad \Longleftrightarrow \quad (f, \mathbb{F}_3^3) = (f_1, \mathbb{F}_3) \times (f_2, \mathbb{F}_3^2)$$

donde $f_1 = f\mid_{\mathbb{F}_3}$ y $f_2 = f\mid_{\mathbb{F}_3^2}$, *además sus polinomios característicos son* $\phi_{f_1}(x)$ $y\ \ \phi_{f_2}(x)$.

Si f es un SDFL sobre X (espacio vectorial de dimensión n sobre $\mathbb{F}$) entonces las iteraciones v, $f(v)$, $f^2(v), \ldots,$ $f^{n-1}(v)$ con $v \neq 0$ forma un conjunto linealmente independiente, entonces podemos escribir:

$$f^n(v) = -a_0 - a_1 f(v) - a_2 f^2(v) - \cdots - a_{n-1} f^{n-1}(v)$$

donde $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}$. Así, el polinomio

$$m_{v,f}(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$$

es mónico y único llamado el polinomio minimal de v con respecto a f. Como $m_{v,f}(f) = 0$ y cualquier otro polinomio $P(x)$ que cumpla $P(f)(v) = 0$ entonces $m_{v,f}(x) \mid P(x)$. En particular, $m_{v,f}(x) \mid m_f(x)$ y $m_{v,f}(x) \mid \phi_f(x)$. Además, si $m_f(x)$ es irreducible entonces $m_{v,f}(x) = m_f(x)$.

Se definirá el concepto de orden o periodo de un polinomio respectivamente para describir completamente el comportamiento cíclico de un SDFL biyectivo (caso especial).

Definición 18 (Orden o Periodo de un Polinomio) *El orden de un polinomio* $g(x) \in \mathbb{F}[x]$ *es el menor entero* k *tal que* $g(x) \mid x^k - 1$. *Al orden de* $g(x)$ *lo denotamos por* $ord(g(x))$. *El orden de un elemento* $v \in X$ *con respecto a* f *es el menor entero positivo* k *que satisface* $f^k(v) = v$ *y lo denotamos por* $ord_f(v)$. *También el orden de un polinomio se conoce como el Periodo de un polinomio .*

Una de las propiedades que motivaron la investigación de este trabajo se encuentra, el de establecer condiciones para que un SDF booleano sea de punto fijo, es decir, donde todas las órbitas son triviales (sólo ciclos triviales). Por eso, el concepto de orden de un elemento y el orden de un polinomio nos permitir estudiar el comportamiento cíclico de cualquier SDF, en especial, para SDFL (SDF lineal) está determinado completamente estudiando el polinomio característico (próxima sección). El hecho que un polinomio $g(x) \mid x^k - 1$, es importante,

ya que para el caso de un SDFL f su polinomio característico $\phi_f(x) \mid x^k - 1$, y la matriz representación M_f del sistema f satisface que $\phi_f(M_f) = 0$, luego $0 = \phi_f(M_f)h(M_f) = M_f^k - M_f$ para algún $h(x) \in \mathbb{F}[x]$, es decir, $M_f^k = M_f$. Esto último permite establecer el comportamiento dinámico completo de un SDFL a partir de la factorización prima del polinomio característico de f (ver [13, 14]) y algo similar se desearía para un SDF no-lineal.

Proposición 19 *Sea f un SDFL biyectivo sobre X (X un espacio vectorial sobre un cuerpo finito). Entonces*

$$ord_f(v) = ord(m_{v,f}(f))$$

donde $ord_f(v)$ es el orden de v con respecto a f.
Prueba. *Sea $k = ord_f(v)$, entonces $f^k(v) = v$ donde k es el menor entero positivo que satisface esta propiedad pero esto es equivalente a $(f^k - 1)(v) = 0$. Tomando $P(x) = x^k - 1$ se tiene $P(f)(v) = 0$, luego $m_{v,f}(x) \mid P(x) = x^k - 1$ donde k es el menor entero positivo, por consiguiente $ord(m_{v,f}(f)) = k = ord_f(v)$.* ■

Ejemplo 20 *Del ejemplo 17 se tiene:*

1. *El orden de $\phi_{M_{f_1}}(x)$ es 2, donde $x^2 - 1 = \phi_{f_1}(x)(x - 1)$.*
2. *El orden de $\phi_{M_{f_2}}(x)$ es 8, donde $x^8 - 1 = \phi_{f_2}(x)(x+1)(x+2)(x^2+1)(x^2 + x + 2)$.*

2.2. Trabajos Importantes sobre Sistemas Dinámicos Finitos lineales y No-lineales

2.2.1. "The Theory A. of Linear Sequential Networks"

El interés en el estudio de este artículo esta orientado a los SDFL sobre cuerpos finitos, por ejemplo, "Network Logical Structure" y "Autonomous Linear Sequential Networks", las dos aplicaciones del ejemplo anterior son equivalentes a los SDFL, y a los resultados principales y la manera como se determina la estructura cíclica de estos sistemas. Él Dr. Elspas establece en este artículo un análisis matemático para SDFL sobre un cuerpo finito (visto como espacios vectoriales) empleando propiedades de los divisores elementales de la matriz transformación, los cuales ya fueron definidas en la sección anterior. De una manera formal pero sin ninguna demostración rigurosa se establecen dos resultados de importancia relacionados con el comportamiento dinámico de un SDFL y su estructura cíclica con las justificaciones respectivas. Por último antes de entrar al contenido,

se quiere resaltar que la descripción inicial de los sistemas modulares lineales (SML), es atribuido al Dr. B. Elspas (ver [16, 18]), donde los SML son SDFL sobre cuerpos finitos. Recordemos que un SDFL sobre un cuerpo finito es una transformación lineal sobre el mismo cuerpo.

Sea f un SDFL sobre un cuerpo finito de característica p (p primo) con matriz transformación M_f y polinomio característico $\phi_{M_\mathbf{f}}(x)$. Dado que el cuerpo finito es un dominio de factorización única, podemos escribir a

$$\phi_{M_\mathbf{f}}(x) = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_s(x)^{e_\mathbf{s}}$$

donde $p_j(x)$ es un polinomio irreducible y el polinomio $\phi_{M_\mathbf{f}}(x)$ se puede definir completamente por el siguiente conjunto de divisores elementales de M_f

$$E_{M_\mathbf{f}} = \{p_i(x)^{e_{\mathbf{i}_1}}, p_i(x)^{e_{\mathbf{i_2}}}, \ldots, p_i(x)^{e_{\mathbf{i_{r_i}}}} : \ i = 1, 2, \ldots, s\}$$

donde cada $p_i(x)$ es un factor irreducible de $\phi_{M_\mathbf{f}}(x)$, con $e_{\mathbf{i}_1} \geq e_{\mathbf{i}_2} \geq \cdots \geq e_{\mathbf{i}_{\mathbf{r}_i}}$ y $e_{\mathbf{i}_1} + e_{\mathbf{i}_2} + \cdots + e_{\mathbf{i}_{\mathbf{r}_i}} = e_i$. En otras palabras, $\phi_{M_\mathbf{f}}(x)$ es el producto de todos los divisores elementales de M_f y el polinomio minimal $m_f(x)$ es el producto de todos divisores elementales de mayor grado (ver [11]). Así, la matriz M_f está completamente caracterizada por el conjunto $E_{M_\mathbf{f}}$ (es decir, caracterizada por los divisores elementales).

Más adelante se justificará el conjunto de ciclos de M_f que está determinado por el producto de los conjuntos de ciclos de cada uno de los divisores elementales $p_i(x)^{e_{\mathbf{ij}}}$, es decir, cada ciclo del SDFL f es el producto de ciclos de los SDFL restringidos $f_i = f\,|_{N(p_\mathbf{i}(x)^{\mathbf{e_{ij}}})}$ (ver teorema 15 y proposición 16 respectivamente). En resumen, si se quiere estudiar los ciclos de un SDFL en general, basta con estudiar cada uno de los factores irreducibles de su propio polinomio característico. Así que mostraremos en detalle, el estudio del conjunto de ciclos para un cierto SDFL h cuyo polinomio característico de M_h es $\phi_{M_\mathbf{h}}(x) = p(x)^e$ con $p(x)$ irreducible y e un entero positivo (en este caso $\phi_{M_\mathbf{h}}(x) = m_h(x)$ o $m_h(x) \mid \phi_{M_\mathbf{h}}(x)$). En el ejemplo 24 se justifica esta afirmación.

Para tal efecto, el estudio de la dinámica del SDFL esta básicamente formalizado bajo la estructura cíclica de un SDFL f donde $\phi_{M_\mathbf{f}}(x) = p(x)^e$. Para el caso del ejemplo 17, la estructura cíclica de f se necesitó estudiar primero la estructura cíclica de cada uno de los polinomios característicos $\phi_{f_\mathbf{1}}(x)$ y $\phi_{f_\mathbf{2}}(x)$.

Supongamos que SDFL f tiene como polinomio característico a $\phi_{M_\mathbf{f}}(x) = p_i(x)^e$ donde M_f es su matriz transformación. El espacio nulo $N_e = N(p_i(f)^e)$ y por la propiedad de Caley-Halmiton $p_i(M_f)^e = 0$. La estructura cíclica de f esta determinada por el grado del polinomio $p_i(x)$ (llamado n), su periodo t y el valor de e, (ver más adelante ecuación ([*]) y por el conjunto de ciclos (ciclos canónicos) denotado por:

$$S_{i_\mathbf{k}} = \left\{1, \mu_{\mathbf{i}_1}(l_{\mathbf{i}_1}), \mu_{\mathbf{i}_2}(l_{\mathbf{i}_2}), \ldots, \mu_{\mathbf{i}_k}(l_{\mathbf{i}_k})\right\}$$

donde los valores l representan largos de los ciclos y las μ las multiplicidades de los ciclos de un largo específico y 1 representa el ciclo trivial en el vector cero. Se entiende por espacio nulo anidado a los espacios nulos

$$N_{i_\mathbf{k}} = \left\{ v \in \mathbb{F}_q^n : p_i(M_f)^k v = 0 \right\}$$

con $0 \leq k \leq e$ que satisfacen $N_{i_\mathbf{k}} \subseteq N_{i_{\mathbf{k+1}}}$. Cada uno de estos espacios nulos es un $f-$invariante (ver [9]), y el espacio nulo N_0 por definición sólo contiene el origen o el vector cero cuyo ciclo es de largo 1 (ciclo trivial en el vector cero) y N_e es el espacio completo. En particular, el conjunto de ciclos del espacio nulo $N_{i_\mathbf{k}}$ contiene el conjunto completo de ciclos de $N_{i_{\mathbf{k-1}}}$ más $\mu_{\mathbf{i_k}}$ ciclos de largo $l_{\mathbf{i_k}}$, es decir, $N_{i_\mathbf{k}}$ tienen el número de ciclos de $N_{i_{\mathbf{k-1}}}$ ($N_{i_\mathbf{k}}$ son anidados), además el número de ciclos de longitud $l_{\mathbf{i_k}}$ con multiplicidad $\mu_{\mathbf{i_k}}$ en $N_{i_\mathbf{k}} - N_{i_{\mathbf{k-1}}}$ es $\mu_{\mathbf{i_k}}(l_{\mathbf{i_k}})$. En otras palabras, a medida que se toman valores para k, aparece un número de ciclos de largo $l_{\mathbf{i_k}}$ que es denotado $\mu_{\mathbf{i_k}}(l_{\mathbf{i_k}})$. Para determinar estos valores de μ y l se necesita el siguiente lema y sólo se describirá el proceso de hallarlos sin justificaciones rigurosas.

Lema 21 *El periodo del polinomio $p^j(x) = 0$ es $tp^{r_\mathbf{j}}$, donde t es el periodo de $p(x) = 0$ y r_j es el mas pequeño entero que satisface $p^{r_\mathbf{j}} \geq j$.*

El lema anterior aparece explícitamente en el artículo de Elspas aplicado al espacio $N_{i_\mathbf{k}} - N_{i_{\mathbf{k-1}}}$, donde todos sus vértices se encuentran sobre los ciclos de longitud $l_{\mathbf{i_k}}$ y cuyo número de vértices es $p^{kn} - p^{(k-1)n}$, es decir, los ciclos en $N_{i_\mathbf{k}} - N_{i_{\mathbf{k-1}}}$ son de longitud $tp^{r_\mathbf{k}}$ y existen $p^{nk} - p^{n(k-1)} = p^{n(k-1)}(p^n - 1)$. Por tanto, los valores de μ y l están dados por:

$$\mu_{\mathbf{i_j}} = \frac{p^{n(j-1)}(p^n - 1)}{tp^{r_\mathbf{j}}} \text{ y } l_{\mathbf{i_j}} = tp^{r_\mathbf{j}} \qquad ([*])$$

donde $r_{i_\mathbf{j}}$ es el más pequeño entero positivo tal que $p^{r_\mathbf{j}} \geq j$.

Una vez establecido el conjunto de ciclos canónicos de los espacios nulos a partir de cada uno de los divisores elementales de f (en el caso anterior los divisores elementales de f son $p_i(x)^{e_\mathbf{k}}$, con $e = e_\mathbf{1} \geq e_2 \geq \cdots \geq e_\mathbf{s}$y $e_1 + e_2 + \ldots + e_s = e$), la estructura cíclica completa del SDFL f en general se obtiene del producto de estos conjuntos de ciclos canónicos, en este caso, teniendo en cuenta la fórmula siguiente:

$$\mu_{\mathbf{i_j}}(l_{\mathbf{i_j}})\mu_{\mathbf{i_k}}(l_{\mathbf{i_k}}) = \gcd(l_{\mathbf{i_j}}, l_{\mathbf{i_k}})\ \mu_{\mathrm{lcm}(l_{\mathbf{i_j}}, l_{\mathbf{i_k}})} \text{ y } \mu_{\mathbf{i_j}}(l) + \mu_{\mathbf{i_k}}(l) = (\mu_{\mathbf{i_j}} + \mu_{\mathbf{i_k}})(l) \qquad (2.2)$$

donde $\mu_{\mathbf{i_k}}$ es la multiplicidad del ciclo de longitud $l_{\mathbf{i_k}}$ y cuando aparece μ_l representa un sólo ciclo de longitud l. Se ve con el ejemplo 24 la aplicación del método de hallar ciclos de un SDFL arbitrario.

En resumen, lo anterior se recopila en dos teorema importantes y resaltan el trabajo de Elspas en los artículos de Hernández Toledo y "Milligan and Wilson". Los teoremas los presentamos tales como se encuentran presentado explícitamente en el propio artículo de Toledo (ver [14]).

Teorema 22 *Sea $f : X \to X$ un SDFL biyectivo, donde X es un espacio vectorial n dimensional sobre el cuerpo finito E cuyo polinomio característico de la matriz transformación es $\phi_M(x) = p_1^{e_1}(x)p_2^{e_2}(x)\cdots p_s^{e_s}(x)$ donde $p_i(x)$ son polinomios irreducibles sobre E, entonces S_f es el producto de los espacios fases asociados con cada $p_i(x)^{e_i}$. Para cada i se tiene una descomposición cíclica por medio de los divisores elementales.*

El siguiente teorema permite hallar la estructura cíclica de un SDFL biyectivo.

Teorema 23 *Sea $f : X \to X$ un SDFL biyectivo donde X es un espacio vectorial n dimensional sobre un cuerpo E de característica p (p primo) y con q elementos. Supongamos que el polinomio minimal de f es $m_{\mathbf{f}}(x) = p(x)^e$, donde $p(x)$ es un polinomio irreducible de grado n sobre E. Entonces la estructura cíclica del S_f está dado por:*

$$G_f = 1 + \sum_{k=1}^{e} \frac{q^{nk} - q^{n(k-1)}}{l_{\mathbf{i_k}}} \mu_{\mathbf{i}_k}(l_{\mathbf{i}_k})$$

donde 1 es el ciclo cero, $\mu_{\mathbf{i}_k}(l_{\mathbf{i}_k})$ es un ciclo de longitud $l_{\mathbf{i}_k}$ con multiplicidad $\mu_{\mathbf{i}_k}$ y $l_{\mathbf{i}_k} = ord(p(x)^k)$.

Prueba. Ver [14]. ■

Ejemplo 24 *Continuando con el ejemplo 17. Aplicando el teorema 23 y el producto entre ciclos, buscar la estructura cíclica de $\phi_{M_{f_1}}(x)$, $\phi_{M_{f_2}}(x)$ y $\phi_{M_f}(x)$.*

- $\boxed{\boldsymbol{\phi_{\mathbf{M_{f_1}}}(\mathbf{x})}}$: La estructura cíclica de f_1

  1. $q = 3$.
  2. $n = grad\ (\phi_{M_{\mathbf{f_1}}}(x)) = 1$.
  3. $r_i = 0$ es el mínimo que cumple $3^{r_1} \geq 1$..
  4. $l_{\mathbf{i_1}} = 2$ y $e = 1$.

Por tanto,

$$\begin{aligned} G_{f_1} &= 1 + \sum_{k=1}^{1} \frac{3^{nk} - 3^{n(k-1)}}{l_{\mathbf{i_k}}} \mu^*_{\mathbf{i}_k}(l_{\mathbf{i}_k}) \\ &= 1 + \frac{3^1 - 3^0}{l_{\mathbf{i_1}}} \mu^*_{\mathbf{i_1}}(l_{\mathbf{i_1}}) \\ &= 1 + \tfrac{2}{2}\mu^*_{\mathbf{i}_1}(2) \\ &= 1 + \mu^*_{\mathbf{i}_1}(2) \end{aligned}$$

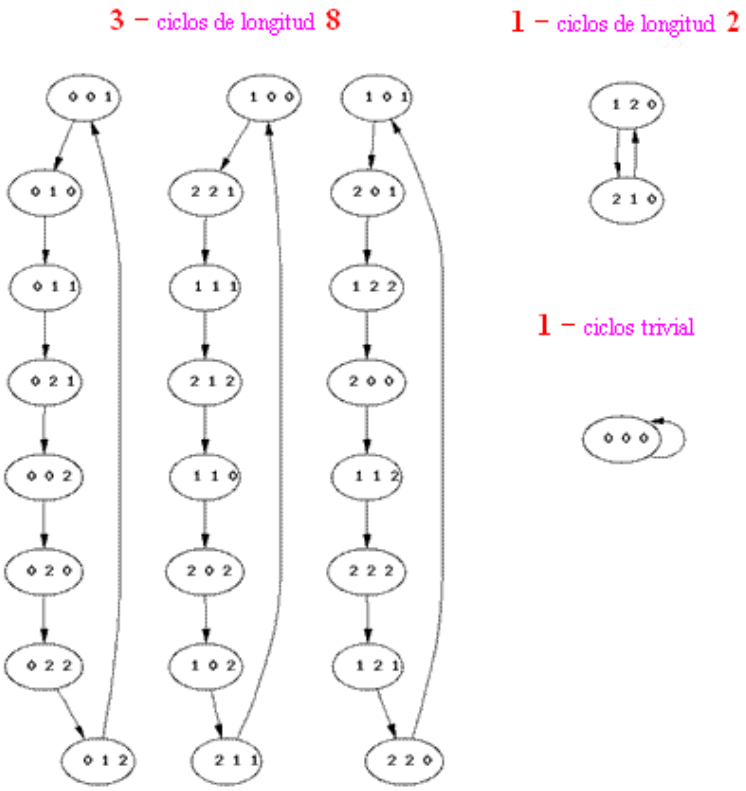


Figura 2.5: Gráfica del Ejemplo 24

- $\boxed{\phi_{\mathbf{M_{f_2}}}(\mathbf{x})}$: La estructura cíclica de f_2.

  1. $q = 3^2$.
  2. $n = grad\ (\phi_{M_{f_1}}(x)) = 2$.
  3. $r_i = 0$ es el mínimo que cumple $3^{r_1} \geq 1$.
  4. $l_{\mathbf{i_1}} = 8$ y $e = 1$.

Por tanto,

$$\begin{aligned} G_{f_2} &= 1 + \sum_{k=1}^{1} \frac{(3^2)^{\mathbf{nk}} - (3^2)^{\mathbf{n(k-1)}}}{l_{\mathbf{i_k}}} \mu_{\mathbf{i}_k}(l_{\mathbf{i}_k}) \\ &= 1 + \tfrac{9-1}{l_{\mathbf{i_1}}} \mu_{\mathbf{i_1}}(l_{\mathbf{i_1}}) \\ &= 1 + \tfrac{8}{8} \mu_{\mathbf{i_1}}(8) \\ &= 1 + \mu_{\mathbf{i_1}}(8) \end{aligned}$$

- $\boxed{\phi_{\mathbf{M_f}}(\mathbf{x})}$: La estructura cíclica de f es el producto de los ciclos de f_1y f_2.

$$\begin{aligned} G_{f_2} &= \left(1+\mu^*_{\mathbf{i}_1}(2)\right)\left(1+\mu_{\mathbf{i}_1}(8)\right) \\ &= 1+\mu^*_{\mathbf{i}_1}(2)+\mu_{\mathbf{i}_1}(8)+\mu^*_{\mathbf{i}_1}(2)\mu_{\mathbf{i}_1}(8) \\ &= 1+\mu_2+\mu_8+\gcd(2,8)\mu_{\mathrm{lcm}(2,8)} \\ &= 1+\mu_2+\mu_8+2\mu_8 \\ &= 1+\mu_2+3\mu_8. \end{aligned}$$

  donde μ_2 y μ_8 denotan un sólo ciclo de longitud 2 y 8 respectivamente, $\mu^*_{\mathbf{i}_1}=1$ y $\mu_{\mathbf{i}_1}=1$. Concluimos que el SDF f de 27 vértices tiene 5 ciclos disjuntos, uno trivial, uno de longitud 2 y tres de longitud 8.

2.2.2. "The B. of Affine Boolean Sequential Networks"

Los SDF afines considerados en este trabajo se encuentran publicado en el artículo escrito por Milligan y Wilson (ver [18]). El artículo determina el comportamiento dinámico de ciertas redes secuenciales lineales booleanas, empleando SDFL para aplicarlo a las redes booleanas afines. Se entenderá por redes secuenciales booleanas lineales los SDFL booleanos y por redes booleanas afines los SDF booleanos afines, esto con el objetivo de seguir utilizando las definiciones y los conceptos asumidos en la investigación. Milligan y Wilson concluyeron que los SDF booleanos afines considerados conservan la misma estructura de los "Transients" y la estructura cíclica de un SDFL booleano. También emplearon de manera introductoria la teoría de los sistemas modulares lineales (SML) (ver [13]), como SDFL (atribuidos a Dr. Elspas (1959) quien dio una descripción inicial de los SDFL). Milligan y Wilson dirigieron la atención hacia el comportamiento dinámico de un SDFL booleano, cuando éste se extienda de manera especial para formar un SDF booleano afín.

A continuación presentará un modelo lineal que tiene las propiedades dinámicas de un SDF booleano afín usando la descripción de Elspas sobre $\mathbb{F}_2^n$. Sea f un SDFL sobre $\mathbb{F}_2^n$ que tiene a M_f como su matriz de transformación, S_f su espacio fase e identificamos el conjunto como Ψ (llamado espacio lineal booleano) tal que cumple:

$$M_f x = y \tag{2.3}$$

donde x y y son vectores en $\mathbb{F}_2^n$. El objetivo del modelo es extender el SDFL booleano f a un SDF booleano afín, definiendo el concepto de suma de " Inverters" como el cambio en el vector x en una de sus componentes adicionándole como suma un 1 (la componente de x es x_i cambiarla por x_i+1) para generar un espacio afín resultante que identificamos con χ (llamado espacio boleano afín), su SDF booleano afín por f_χ y al espacio fase por S_{f_χ}. Este sistema satisface la siguiente ecuación:

$$M_f x + b = \tilde{y} \tag{2.4}$$

donde b es un vector distinto de cero en $\mathbb{F}_2^n$ y para alguna componente b_i es 1 ($b_i = 1$ representa el "inverters" de la componente i-ésima de b).

Para hallar la relación entre los ciclos de los espacios fases S_f y S_{f_χ}, es necesario emplear un nuevo SDFL f_ζ definido por el espacio compuesto ζ entre los espacios Ψ y χ. El espacio fase determinado ζ esta subdividido en dos partes, uno por el espacio fase S_f de Ψ y el otro espacio fase S_{f_χ} de χ. El nuevo SDFL booleano f_ζ se representa por la matriz transformación C de bloques de orden $(n+1)\times(n+1)$ sobre $\mathbb{F}_2^n$ obtenida de la siguiente manera:

$$x^* = \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ y } C = \left(\begin{array}{c|c} 1 & 0 \\ \hline b & M_f \end{array}\right)$$

que satisface la ecuación $Cx^* = y^*$. La equivalencia algebraicamente esta dada por:

$$M_f x + b x_0 = \tilde{y}$$

donde:

- Si $x_0 = 0$, entonces $M_f x = \tilde{y}$, (ver ecuación 2.3) representa el SDFL booleano del espacio identificado por Ψ.
- Si $x_0 = 1$, entonces $M_f x + b = \tilde{y}$, (ver ecuación 2.4) representa el SDF booleano afín del espacio identificado por χ .

En el siguiente ejemplo se quiere construir un SDFL booleano afín a partir de un SDFL booleano y que comparte propiedades dinámicas similares a otro SDFL booleano.

Ejemplo 25 *Consideremos el SDFB,*

$$\begin{array}{rccc} f_\Psi : & \mathbb{F}_2^2 & \longrightarrow & \mathbb{F}_2^2 \\ & (x_1, x_2) & \to & (x_1 + x_2, x_2) \end{array}$$

y su espacio fase S_{f_Ψ} esta dado por la figura 2.6, donde Ψ identifica el espacio completo, es decir, es representado tanto por el espacio fase S_{f_Ψ} como por el SDFL f_Ψ.
La matriz transformación del SDFL f_Ψ está dada por $M_{f_\Psi} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ tal que,

$$M_{f_\Psi} x = y \iff \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ x_2 \end{pmatrix}$$

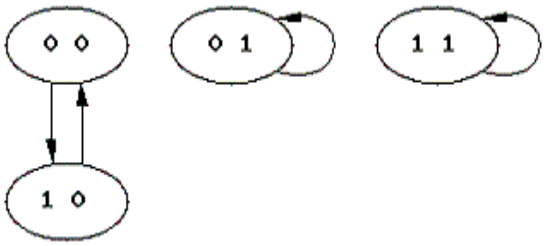


Figura 2.6: Espacio Fase S_{f_Ψ}

donde $x = \binom{x_1}{x_2} \in \mathbb{F}_2^2$. *Ahora se aplica un "Inverters" al sistema* Ψ *en la variable* x_1*, es decir, cambiamos a* x_1 *por* $x_1 + 1$*, entonces*

$$M_{f_\Psi}\begin{pmatrix} x_1+1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1+x_2+1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1+x_2 \\ x_2 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix} = M_{f_\Psi}x + b$$

donde $b = \binom{1}{0}$*. O sea, se construye un SDFB afín* f_χ *determinado por la siguiente ecuación*

$$M_{f_\Psi}x + bx_0 = \tilde{y}$$

y el espacio fase S_{f_χ} *de* χ *está dado por:*

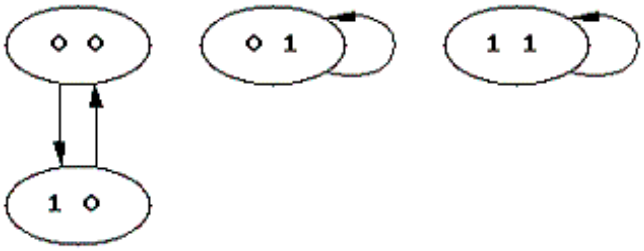


Figura 2.7: Espacio Fase de S_{f_χ}

Ahora el SDFB afín construido satisface que:

$$C = \left(\begin{array}{c|c} 1 & 0 \\ \hline b & M_{f_\Psi} \end{array}\right) = \left(\begin{array}{c|c} 1 & 0 \\ \hline \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \end{array}\right) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

tal que

$$Cx^* = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_0 \\ x_0+x_1+x_2 \\ x_2 \end{pmatrix}$$

y el espacio fase de ς *esta dado por la figura 2.8.*

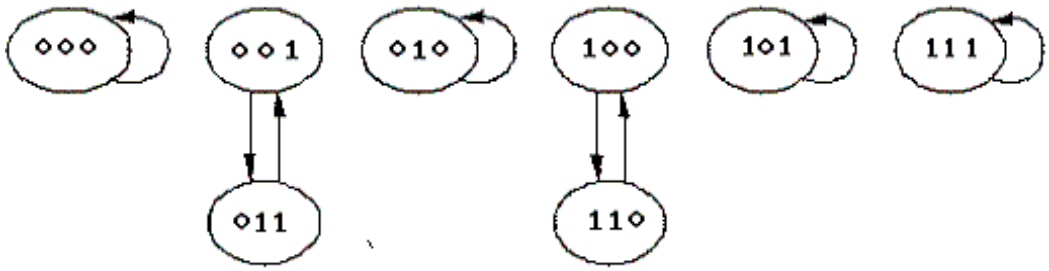


Figura 2.8: Espacio Fase de S_{f_ς}

Por último, se enuncian tres teoremas que aparecen en el artículo de Milligan y Wilson (ver [18]) y se encuentran explicados completamente por el modelo anterior y por los divisores elementales de las matrices M_f y C (éstos corresponden a los mismos divisores elementales de sus respectivos SDFL). El primero y segundo teorema establecen la preservación de la estructura cíclica entre el SDF booleano afín del espacio χ y el SDFL booleano extendido del espacio ς, y el último teorema dice que la estructura de los " Transients" es totalmente el mismo en los dos espacios.

Teorema 26 *Todo SDF booleano afín extendido por un SDFL booleano dados por los espacios χ y ς respectivamente, preserva la misma estructura cíclica.*

Teorema 27 *Todo SDF booleano afín extendido por un SDFL booleano dados por los espacios χ y ς respectivamente, deja los largos de los ciclos incambiable o el resultado de los largos de los ciclos, los cuales son un subconjunto de los ciclos de los largos originales, que son múltiplos de una potencia de dos.*

Teorema 28 *Todo SDF booleano afín extendido por un SDFL booleano dado por los espacios χ y ς respectivamente, tiene la misma estructura de los "Transients".*

2.2.3. "Linear Finite Dynamical Systems"

El trabajo realizado por el Dr. Hernández Toledo (ver [14]), se orientó únicamente a SDFL sobre un cuerpo finito y determina herramientas algebraicas para el comportamiento dinámico de un SDFL por medio de ciclos y árboles (ver sección 3 del artículo de Toledo). Hernández Toledo caracterizó completamente estos sistemas estableciendo una descripción de la dinámica de un SDFL y el comportamiento de las órbitas como una descomposición de dos componentes: una componente biyectiva (mapa lineal biyectivo, sección 6) y otra la componente nilpotente (mapa nilpotente, sección 5). El resultado principal establece que todo espacio fase o espacio de iteración está compuesto por la union disjunta de ciclos-árboles (donde en cada vértice de un ciclo esta pegado el mismo árbol),

o sea el espacio fase de un SDFL consiste de la suma de ciclos-árboles, con una copia del mismo árbol pegado cada vértice del ciclo, por tanto, el espacio fase está configurado de la siguiente manera: una parte es un árbol dado para la parte nilpotente y la otra son ciclos dado para la parte biyectiva, (ver teorema 30). También el autor presenta una descripción nueva de la dinámica de la parte nilpotente del mapa lineal.

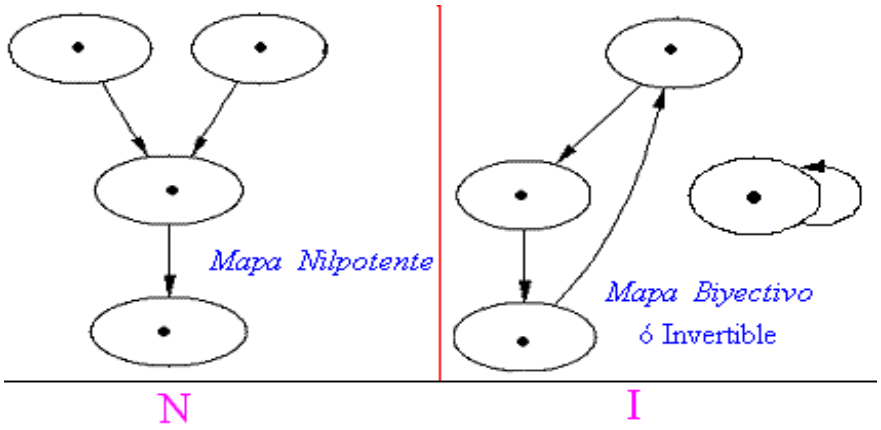


Figura 2.9: Parte Nilpotente N y Parte Invertible I

Para la descripción completa de la dinámica de un SDFL se utilizan grafos para construir SDFL, definiendo a partir de la suma y producto de dos SDFL, en especial, el producto de SDFL. A continuación desglosamos un estudio global de los SDFL que Toledo presentó en su artículo:

Producto de ciclos El producto entre ciclos es o son ciclos de la misma longitud y que en principio Elspas dio propiedades de su estructura. Ver ejemplo 24.

Producto de mapas biyectivos La estructura cíclica entre mapas biyectivo no es más que el producto entre ciclos.

Productos de árboles Es un árbol cuya profundidad (largo) es el máximo de las profundidades y cuyo punto terminal esta formado por los puntos terminales de ambos árboles.

Producto entre un ciclo y un árbol Es un ciclo-árbol o un grafo que esta formado por el mismo ciclo y por el mismo árbol "Transients" donde en cada vértice del ciclo existe una copia del árbol.

Definición 29 (Mapa Nilpotente) *Un mapa $g : X \to X$ es nilpotente puro, si existe un natural n tal que $g^n = 0$.*

Un mapa biyectivo es precisamente un SDF biyectivo cuyo espacio fase consiste de sólo ciclos. Usando las propiedades de los espacios vectoriales X sobre un cuerpo finito, la dinámica de un SDFL f en general, se limita al estudio de la dinámica de los SDF definidos sobre subespacios $f-$invariantes de X (ver proposiciones 8, 9 y 16) como espacio vectorial de dimensión n sobre un cuerpo finito de característica p. La matriz transformación M_f del SDFL tiene polinomio característico

$$\varphi_{M_f}(x) = x^s\psi(x), \quad x \neq 0 \ \text{ y } \ \psi(0) \neq 0$$

donde x^s es el polinomio característico del mapa nilpotente de f y $\psi(x)$ es el polinomio característico del mapa biyectivo de f. De esta manera se resume lo presentado por Toledo en el artículo. A continuación presentamos dos teoremas de los resultados principales de su artículo.

Teorema 30 *Sea $g : X \to X$ un mapa nilpotente puro (SDF) donde X es un espacio vectorial de dimensión n sobre E y $|E| = q$, entonces su espacio fase es un árbol q-ario completo con altura n, excepto el vértice raíz (raíz del árbol) tiene sólo $q-1$ preimagenes.*

Teorema 31 *El SDFL es el producto de un SDFL nilpotente y un SDFL biyectivo.*

Prueba. Ver [14]. ■

Ejemplo 32 *Sea el SDFL*

$$\begin{array}{rccl} f: & \mathbb{F}_2^4 & \longrightarrow & \mathbb{F}_2^4 \\ & (x_1,x_2,x_3,x_4) & \to & f(x_1,x_2,x_3,x_4) \quad = (x_1{+}x_2{+}x_3, x_1{+}x_2{+}x_3, x_1{+}x_3, x_1) \end{array}$$

con espacio fase con matriz transformación

$$M_f = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

con polinomio característico

$$\phi_f(f) = x^4 - 3x^3 + x^2 = x^2(x^2 - 3x + 1)$$

donde $p(x) = x^2$ es el polinomio característico del mapa nilpotente con espacio fase representado por un árbol $2-$ario de longitud 2 y $\psi(x) = x^2 - 3x + 1$; $x \neq 0$ y $\psi(0) \neq 0$ es el polinomio característico del mapa biyectivo con espacio fase representado por ciclos de longitud 1 y 3. Así, el espacio fase del SDFL

$$f(x_1,x_2,x_3,x_4) = (x_1{+}x_2{+}x_3, x_1{+}x_2{+}x_3, x_1{+}x_3, x_1)$$

está dado por la figura 2.10 (ver página siguiente).

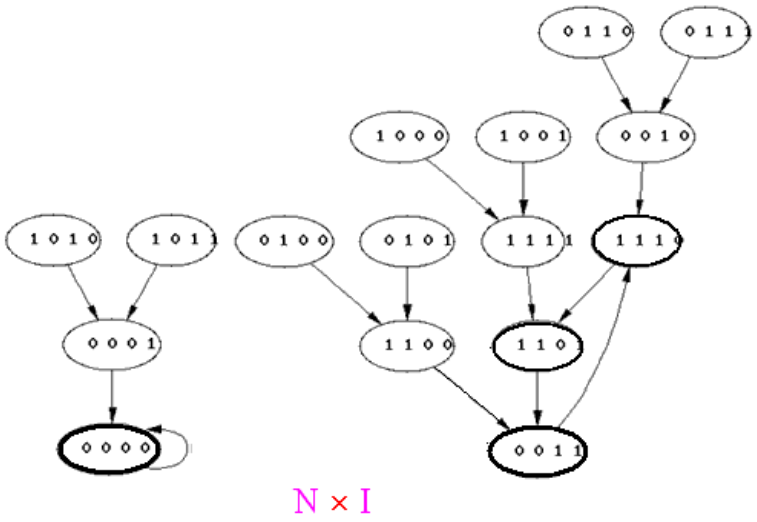


Figura 2.10: Producto entre la Parte N y la Parte I.

De lo anterior el espacio fase de un SDFL consiste de la unión disjunta de ciclos con el mismo árbol pegado a cada uno de los vértices de los ciclos.

2.2.4. "Boolean Monomial Fixed Point Systems"

En resumen, el artículo presenta lo siguiente: una familia de SDF sobre $\mathbb{F}_2^n$ que se define más adelante por sistemas dinámicos finitos booleanos monomiales y por el cual presenta condiciones suficientes para que un sistema monomial tenga sólo puntos fijos como ciclos límites. En otras palabras, estas condiciones dependen de la estructura cíclica del grafo dependencia del sistema. Unas de las preguntas fundamentales que son común en la aplicación es analizar la dinámica del sistema sin enumerar todos los vértices, donde la enumeración es del orden exponencial o la complejidad es exponencial en número de variables modelos. Una respuesta a esta pregunta se da en este documento para una familia de sistemas dinámicos monomiales, donde la información de la dinámica de estos sistemas se obtiene a partir de la estructura del sistema, es decir, la dinámica se encuentra codificada por medio del grafo dependencia y este grafo es un grafo dirigido determinado por las funciones coordenadas que representa el sistema. También el espacio fase del sistema consiste de grafos componentes conectados donde cada uno consiste de un ciclo límite con un árbol dirigido pegado a cada vértice del ciclo, llamado "Transients". Por tanto, la dinámica representado por el espacio fase del sistema puede ser determinado por el grafo dependencia, grafo que se obtiene de las funciones componentes del sistema.

Se presenta a continuación los resultados de interés del trabajo Dr. Omar Colon-Reyes que serán resaltados para el caso booleano (ver [8]).

Definición 33 (SDFBM) *Un sistema*

$$f = (f_1, f_2, \ldots, f_n) : \mathbb{F}_2^n \to \mathbb{F}_2^n$$

es un sistema dinámico finito booleano monomial, si cada uno de los f_i es de la forma

$$f_i = \alpha_i x_1^{\in_{\mathbf{i1}}}, x_2^{\in_{\mathbf{i2}}}, \ldots, x_n^{\in_{\mathbf{in}}}$$

donde $\in_{ij}, \alpha_i \in \{0,1\}$. Si $\alpha_i = 0$ entonces todos los $\in_{ij}= 0$. La composición n-veces del mapa f con el mismo denotado por $f^m = (f_1^m, f_2^m, \ldots, f_n^m)$ donde cada $f_{\mathbf{i}}^m = \alpha_i (f_1^{m-1})^{\in_{\mathbf{1i}}} (f_2^m)^{\in_{\mathbf{2i}}} \cdots (f_n^m)^{\in_{\mathbf{ni}}}$.

Definición 34 (Grafo Dependencia) *Al sistema f le asociamos un digrafo χ, llamado grafo dependencia, con conjunto de vértices $\{a_1, a_2, \ldots, a_n, \in\}$. Existe un lado dirigido desde a_i hacia a_j, si $\alpha_i = 1$ y x_j es una factor en f_i (es decir, $\in_{ij}= 1$). Existe un lado dirigido desde a_i hacia $\in$ si $\alpha_i = 0$ (es decir, $f_i = 0$).*

Ejemplo 35 *Sea el SDFBM*

$$\begin{array}{rccl} f: & \mathbb{F}_2^3 & \to & \mathbb{F}_2^3 \\ & (x_1, x_2, x_3) & \to & f(x_1, x_2, x_3) \quad = (x_1 x_2, x_3, x_1 x_3) \end{array}$$

cuyo espacio fase y grafo dependencia están dados por las siguientes gráficas.

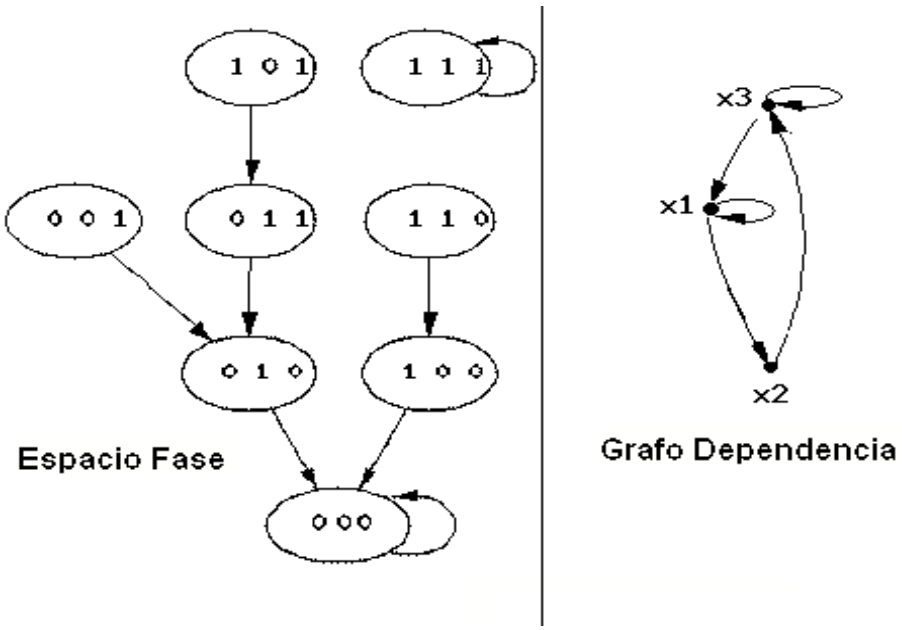


Figura 2.11: Espacio Fase y Grafo Dependiente

Para nuestro interés, destacamos los siguientes resultados y que sólo requieren de conceptos comunes de grafo y cuya prueba se remite al artículo (ver [8]).

Teorema 36 *Sea χ un digrafo de $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Lo siguiente es equivalente:*

1. El sistema $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ es un sistema de punto fijo.
2. Para cada vértice $a \in \chi$ de lo siguiente se verifica,
   - *a)* a permite dos caminos cerrados $p, q : a \to a$ de longitud $|q| = p + 1$,
   - *b)* a esta conectado con un camino al cero, o
   - *c)* Existe un camino de longitud ≥ 1 desde a hacia a.

Definición 37 *Un sistema*

$$f = (f_1, f_2, \ldots, f_n) : \mathbb{F}_2^n \to \mathbb{F}_2^n$$

es un sistema triangular, si cada uno de los f_i es de la forma

$$f_i = \alpha_i x_1^{\in_{i1}} x_2^{\in_{i2}} \cdots x_i^{\in_{in}}$$

donde $\in_{ij}$, $\alpha_i \in \{0, 1\}$.

Corolario 38 *Todo sistema triangular es de punto fijo.*

Ejemplo 39 *Sea el SDFBM triangular*

$$\begin{array}{rccl} f: & \mathbb{F}_2^3 & \to & \mathbb{F}_2^3 \\ & (x_1, x_2, x_3) & \to & f(x_1, x_2, x_3) \quad = (x_1, x_1, x_1 x_3) \end{array}$$

cuyo espacio fase y grafo dependencia están dados por las siguientes gráficas.

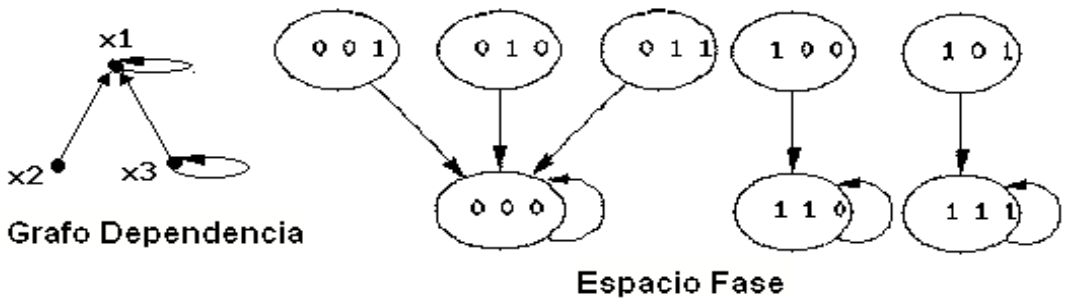


Figura 2.12: Ejemplo de un Espacio Fase y Grafo Dependiente

Corolario 40 *Sea f un sistema con grafo de dependencia χ. Entonces f es un sistema de punto fijo si y sólo si toda componente conectada fuertemente de χ corresponde a un sistema de punto o conectada por caminos hacia el cero en χ.*

Teorema 41 *Sea χ un digrafo de un sistema de punto fijo $f = (f_1, f_2, \ldots, f_n)$. Si no existe ningún camino desde a_i hacia a_j o a_j tiene un camino de longitud ≥ 1 hacia el mismo, entonces $g = (f_1, \ldots x_i f_j, \ldots, f_n)$ es un sistema de punto fijo.*

Corolario 42 *$f = (f_1, f_2, \ldots, f_n)$ un sistema de punto fijo y m un monomial. Entonces $mf = (mf_1, mf_2, \ldots, mf_n)$ es un sistema de punto fijo (no importa la hipótesis siempre es cierto.*

Se resalta las nuevas herramientas usadas en este artículo para determinar que un SDF monomial booleano sea de punto fijo y fue sólo una orientación a este trabajo; ya que todavía se encuentra en investigación.

Capítulo 3

Transformada Discreta de Fourier Aplicada a SDF

Este capítulo presenta el método para transformar cualquier SDF sobre $\mathbb{F}_q^n$ (de dimensión n) en un SDF polinomial sobre $\mathbb{F}_{q^n}$ (una dimensión) utilizando la matriz representación de la transformada discreta de fourier sobre cuerpos finitos. Este método puede ser encontrado en el artículo de los doctores Bollman, Colón-Reyes y Orozco (ver [3]) y permite obtener SDF equivalentes unidimensional de un SDF dado, es decir, se puede encontrar SDF polinomiales cuya estructura dinámica son los mismos o sus espacios fases son isomórficos. Se sabe que la dinámica de un SDF esta codificada por el espacio fase, así que este método de fourier transmite la información de un SDF a otro y abre una nueva herramienta a la investigación para SDF arbitrarios. Para la ejecución de este capítulo se divide en dos secciones: la primera, enfocada a los preliminares, y la segunda, dedicada al método de la transformada discreta de fourier sobre cualquier cuerpo finito.

3.1. Preliminares

Introduciremos dos nuevos conceptos: SDF equivalentes y isomorfismos entre grafos dirigidos (o espacios fases).

Definición 43 (SDF sobre $\mathbb{F}_q^n$) *un sistema dinámico finito (SDF) sobre $\mathbb{F}_q^n$ es una función $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ donde $n \geq 1$, $\mathbb{F}_q$ es el cuerpo finito con q elementos y $\mathbb{F}_q^n$ el producto directo de n copias de $\mathbb{F}_q$.*

Definición 44 (El espacio fase) *El espacio fase de un SDF f (denotado por S_f), es un grafo dirigido que cumple:*

- El conjunto de vértices es $\mathbb{F}_q^n$.
- Dados $\mu, \beta \in \mathbb{F}_q^n$, existe un eje dirigido $\mu \xrightarrow{f} \beta$ si y sólo si $f(\mu) = \beta$.

El siguiente ejemplo es un SDFB de punto fijo y se quiere mostrar inicialmente como su dinámica la desarrollamos bajo unos puntos cardinales representados por los vértices de un cubo. La idea es motivar y mostrar la dinámica de estos SDFB dentro un cubo, para el caso tres dimensiones.

Ejemplo 45 *Sea* $f = (xz+1, x+1, xy+1)$ *un SDFB sobre* $\mathbb{Z}_2^3$. *Por la definición anterior* $\mathbb{Z}_2^3$ *es el conjunto de vértices del espacio fase* S_f *donde el conjunto de flechas representa la dinámica del sistema. Ver figura 3.1 del espacio fase de* f.

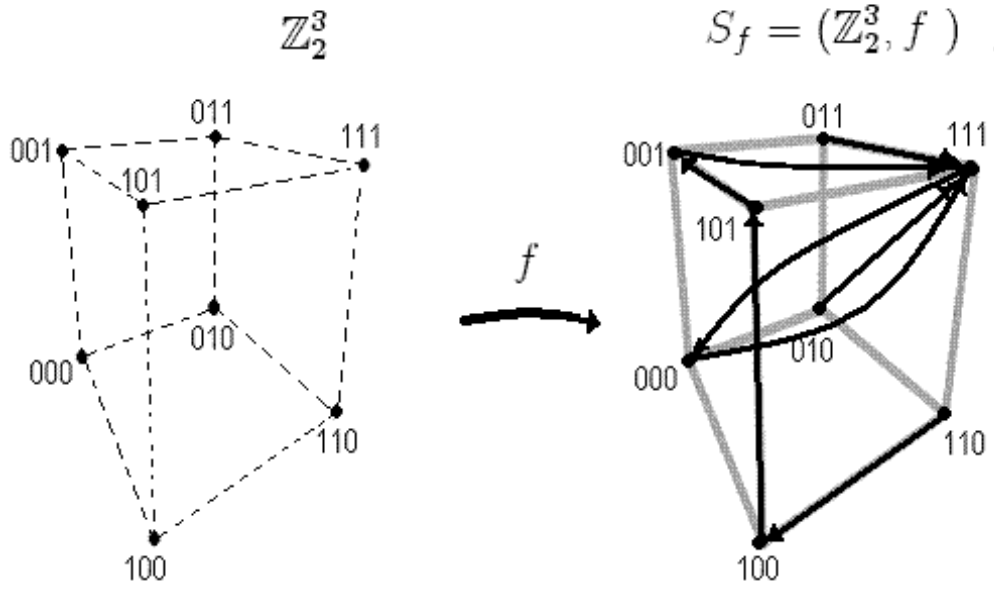


Figura 3.1: Espacio Fase

Se conoce que todo SDF f lo podemos expresar de la forma $f = (f_1, f_2, \ldots, f_n)$, donde cada $f_i : \mathbb{F}_q^n \to \mathbb{F}_q$ es una función coordenada y sin prueba alguna se describió que toda función coordenada f_i se representa por medio de una función polinomial. Ahora se quiere mostrar formalmente este hecho en el siguiente enunciado.

Proposición 46 *Toda función* $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q$ *se puede escribir como un polinomio único en* $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$.

Prueba. (Ver [16], pag. 369). La idea principal se encuentra utilizando el hecho de que existe una única representación de la forma

$$\gamma(x) = \sum_{(c_1,c_2,\ldots,c_n)\in\mathbb{F}_q^n} \varphi(c_1,c_2,\ldots,c_n)(1\text{-}(x_1\text{-}c_1)^{q-1})(1\text{-}(x_2\text{-}c_2)^{q-1})\cdots(1\text{-}(x_n\text{-}c_n)^{q-1})$$

tales que $\varphi(x) = \gamma(x)$ para todo $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ para probar el enunciado. ■

Una vez expresado φ como polinomio sobre $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$, cada variable del polinomio aparece a lo mas de grado q. En otras palabras, cualquier φ dado por la proposición 46, y usando el algoritmo de la división, existe un único

$$\gamma \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]/\langle x_i^q - x_i; i = 1, 2, \ldots, n\rangle$$

de grado $< q$ tal que $\varphi(a) = \gamma(a)$ para todo $a \in \mathbb{F}_q^n$ (ver [16], pp. 371). Luego, un SDFB puede ser representado por un SDF polinomial cuyos términos son solo monomiales en $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$.

Ejemplo 47 *Considere $f(x, y, z) : \mathbb{Z}_2^3 \to \mathbb{Z}_2$ un SDFB tal que la función esta dada por $f(0,0,0)$=1, $f(1,0,0)$=0, $f(0,1,0)$=1, $f(0,0,1)$=1, $f(1,1,0)$=0, $f(1,0,1)$=0, $f(0,1,1)$=1, $f(1,1,1)$=0. Empleando la fórmula de Interpolación de Lagrange Multivariado sobre cuerpos finitos (ver [16])*

$$\varphi(x,y,z) = \sum_{(c_1,c_2,c_3)\in\mathbb{Z}_2^3} f(c_1,c_2,c_3)(1-(x-c_1)^{2-1})(1-(y-c_2)^{2-1})(1-(z-c_3)^{2-1})$$

y extendiendo esta expresión se tiene que:

$$\begin{aligned}\boldsymbol{\varphi}(\mathbf{x},\mathbf{y},\mathbf{z}) = \;& f(0,0,0)(1\text{-}x)(1\text{-}y)(1\text{-}z)+f(1,0,0)x(1\text{-}y)(1\text{-}z)+f(0,1,0)y(1\text{-}x)(1\text{-}z)+\\ & f(0,0,1)z(1\text{-}x)(1\text{-}y)+f(1,1,0)xy(1\text{-}z)+f(1,0,1)xz(1\text{-}y)+\\ & f(0,1,1)yz(1\text{-}x)+ f(1,1,1)xyz\end{aligned}$$

simplificando

$$\varphi(x,y,z) = (1-x)(1-y)(1-z)-(1-x)y(1-z)-(1-x)(1-y)z+(1-x)yz = x+1$$

así, esta función coordenada se puede representar por el polinomio

$$\varphi(x, y, z) = x + 1$$

sobre $\mathbb{Z}_2$.

Ahora recordemos lo siguiente: dos grafos dirigidos son isomórficos $G_1 \cong G_2$ si existe una función χ desde el conjunto de vértices G_1 al conjunto de vértices G_2 tal que:

- χ es una función biyectiva.
- $\chi(v)$ es adyacente a $\chi(w)$ en G_2 si y solo si v es adyacente a w en G_1.

Se quiere motivar este concepto a dos SDF, por ejemplo a f y g por medio de una función ϕ biyectiva que preserve ejes (función puente, ver más abajo) y cuyos espacios fase tienen como conjuntos de vértices a espacios vectoriales finitos del mismo cardinal (en este caso decimos que los sistemas f y g son equivalentes). Para el caso de dos SDFL equivalentes, esto mismo equivalente a decir que sus matrices representación son similares.

$$\begin{array}{ccccc} & & f & & \\ & \mathbb{F} & \longrightarrow & \mathbb{F} & \\ \phi & \downarrow & & \downarrow & \phi \\ & \mathbb{E} & \longrightarrow & \mathbb{E} & \\ & & g & & \end{array}$$

Figura 3.2: Diagrama Conmutativo

Definición 48 (SDF Equivalentes) *Decimos que los SDF* $f : \mathbb{F} \to \mathbb{F}$ *y* $g : \mathbb{E} \to \mathbb{E}$ *son equivalentes, si existe una función biyectiva* $\phi : \mathbb{F} \to \mathbb{E}$ *tal que* $\phi \circ f = g \circ \phi$.

La definición anterior se ve por intermedio del diagrama conmutativo de la figura 3.2 donde f y g son equivalentes y ϕ una función biyectiva, que llamaremos función puente, es decir, el diagrama satisface $\phi \circ f = g \circ \phi$.

$$\begin{array}{ccc} Z_4 & \xrightarrow{f(x) = x} & Z_4 \\ \phi(x) = \overline{x} \downarrow & & \downarrow \phi(x) = \overline{x} \\ Z_2 & \xrightarrow[g(x) = x]{} & Z_2 \end{array}$$

Figura 3.3: Sistemas Dinámicos Finitos no Equivalentes

Observemos que en la anterior definición, si $\mathbb{F}$ y $\mathbb{E}$ son espacios de igual dimensión solo basta que ϕ sea sobreyectiva (ϕ sería también inyectiva), si ϕ es solo un epimorfismo y $|\mathbb{F}| \leq |\mathbb{E}|$ entonces $|\mathbb{F}| = |\mathbb{E}|$. Ya que por el principio del palomar al menos dos elementos de $\mathbb{E}$ están relacionados con un elemento de $\mathbb{F}$ y por la sobreyectividad ϕ no sería función. Y si $|\mathbb{F}| \geq |\mathbb{E}|$ entonces S_f sería isomorfismo a un subgrafo dirigido de S_g, por ejemplo, el siguiente diagrama conmuta y ϕ es un epimorfismo donde $\overline{x}$ es el residuo módulo 2 y por tanto el espacio fase S_g es isomórfico a un subgrafo del espacio fase S_f (ver gráfica 3.4).

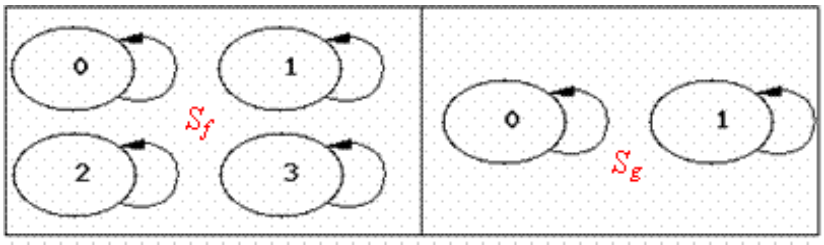


Figura 3.4: Subgrafos Isomorfos

El único teorema de esta sección establece condiciones para que dos espacios fases sean isomórficas.

Teorema 49 *Sean $f : \mathbb{F} \to \mathbb{F}$ y $g : \mathbb{E} \to \mathbb{E}$ dos SDF. f y g son dos SDF equivalentes si y solo si $S_f \cong S_g$.*

Prueba. ($\to$) Supongamos que f y g son SDF equivalentes, entonces existe $\phi : \mathbb{F} \to \mathbb{E}$ biyectiva tal que $\phi \circ f = g \circ \phi$. Como S_f y S_g son grafos dirigidos, por la propiedad entre isomorfismo de grafos dirigidos falta probar que ϕ y ϕ^{-1} preserven ejes, es decir, $\mu \xrightarrow{f} \beta$ entonces $\phi(\mu) \xrightarrow{g} \phi(\beta)$ para todo $\mu, \beta \in \mathbb{F}$ y $a \xrightarrow{g} b$ entonces $\phi^{-1}(a) \xrightarrow{f} \phi^{-1}(b)$ para todo $a, b \in \mathbb{E}$. En efecto, $g(\phi(\mu)) = (g \circ \phi)(\mu) = (\phi \circ f)(\mu) = \phi(f(\mu)) = \phi(\beta)$, la última ecuación se sustituyó $f(\mu)$ por β, por tanto $\phi(\mu) \xrightarrow{g} \phi(\beta)$. Lo segundo se cumple por hipótesis, ϕ es biyectiva, por tanto $g = \phi \circ f \circ \phi^{-1}$ ó $\phi^{-1} \circ g = f \circ \phi^{-1}$. Supongamos que $a \xrightarrow{g} b$, es decir, $g(a) = b$ entonces

$$\phi^{-1}(b) = \phi^{-1}(g(a)) = (\phi^{-1} \circ g)(a) = (f \circ \phi^{-1})(a) = f(\phi^{-1}(a))$$

por tanto $\phi^{-1}(a) \xrightarrow{f} \phi^{-1}(b)$. Por consiguiente $S_f \cong S_g$.

($\leftarrow$) Supongamos que $S_f \cong S_g$, entonces existe $\phi : \mathbb{F} \to \mathbb{E}$ biyectiva tal que ϕ preserva sus ejes, es decir, dados $\mu, \beta \in \mathbb{F}$ tal que $\mu \xrightarrow{f} \beta$ entonces $\phi(\mu) \xrightarrow{g} \phi(\beta)$. Definamos $\varphi : \mathbb{F} \to \mathbb{E}$ por $\varphi(\mu) = \phi(\mu)$ para todo $\mu \in \mathbb{F}$. es obvio que φ es biyectiva, falta probar $\varphi \circ f = g \circ \varphi$. En efecto, sea $\mu \in \mathbb{F}$ entonces

$(g \circ \varphi)(\mu) = g(\varphi(\mu)) = g(\phi(\mu)) = \phi(\beta) = \varphi(\beta) = \varphi(f(u)) = (\varphi \circ f)(u)$ esto último por hipótesis y $f(u) = \beta$. Como μ es arbitrario entonces $g \circ \varphi = \varphi \circ f$ y por consiguiente f y g son SDF equivalentes. ■

3.2. Método de la Transformada Discreta de Fourier sobre Cuerpos Finitos

Una reseña histórica sobre la transformada de fourier discreta rápida sobre cuerpos finitos, "es atribuida directamente a Cooley y Tukey en 1965, sin embargo, Heidermann en 1984 observa que el algoritmo de Cooley y Tukey fue esencialmente conocido por Carl Friedrich Gauss en 1805, dos años después Fourier y 160 años después Cooley y Tukey"(ver [22]). Esta importante herramienta tiene sus inicios desde Gauss y permite construir SDF polinomiales unidimensionales a partir de la transformada discreta de fourier sobre cuerpos finitos aplicada a un SDF finito dimensional. Por eso, esta sección muestra las condiciones necesarias para obtener este SDF polinomial sobre un cuerpo finito.

Definición 50 (TDF (ver [3])) *Sea* $p(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in \mathbb{F}[x]$ *y* $\omega \in \mathbb{F}$ *un elemento primitivo, es decir,* ω *es un generador del grupo multiplicativo* $\mathbb{F} - \{0\}$ *, entonces la expresión*

$$\hat{p} = p(\omega^0) + p(\omega^1)x + \cdots + p(\omega^{n-1})x^{n-1} := \hat{a}_0 + \hat{a}_1 x + \cdots + \hat{a}_{n-1}x^{n-1}$$

se llama la transformada discreta de fourier (TDF) de p *y los* $\hat{a}_i$ *son los coeficientes de fourier de* p*.*

Al polinomio $p(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ se representa por $p := (a_0, a_1, \ldots, a_{n-1})$ tal que,

$$p(x) = (x^0, x^1, \ldots, x^{n-1}) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}$$

donde esta operación es un producto escalar entre $n - duplas$. Por tanto, la trasformada de fourier discreta (TDF) es una secuencia de n puntos constituidos de la evaluación del polinomio $p(x)$ con coeficientes $(a_0, a_1, \ldots, a_{n-1})$ en los puntos $\{\omega^0, \omega^1, \ldots, \omega^{n-1}\}$, es decir, cada coeficiente de la transformada fourier esta determinado por la evaluación

$$\hat{a}_i = p(\omega^i) = (\omega^{i0}, \omega^i, \ldots, \omega^{i(n-1)}) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \tag{3.1}$$

donde ω es una raíz n-ésima primitiva de la unidad. En resumen, la transformada de fourier discreta esta representado por:

$$\begin{pmatrix} \hat{a}_0 \\ \hat{a}_1 \\ \vdots \\ \hat{a}_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)(n-1)} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \mathrm{T}_{q,\omega} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \quad (1,2)$$

La expresión $T_{q,\omega}$ la definimos a continuación sobre un cuerpo finito con q^n elementos y es motivada para el resto del capítulo.

Definición 51 *$T_{q,\omega}$ es llamada la matriz transformada de fourier discreta sobre $\mathbb{F}_{q^n}$ (TDF), donde*

$$T_{q,\omega} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{q^n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{q^n-2} & \omega^{2(q^n-2)} & \cdots & \omega^{(q^n-2)(q^n-2)} \end{pmatrix} = \left(\omega^{ij}\right)_{0 \le i,j \le q^n-2}$$

y su inversa esta dada por $T_{q,\omega}^{-1} = (q^n-1)^{-1} T_{q,\omega^{-1}} = -T_{q,\omega^{-1}}$

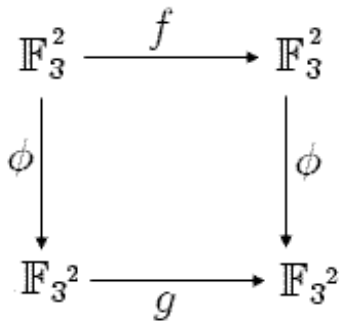
También esta definición se encuentra motivada en general para cualquier cuerpo (ver [3]). Usando las propiedades de campos finitos $\mathbb{F}_q[x]/\langle p(x)\rangle \cong \mathbb{F}_q(\omega)$ donde $p(x)$ es un polinomio irreducible sobre $\mathbb{F}_q$ de grado n tal que $p(\omega) = 0$, ω satisface la condición de raíz primitiva q^n-ésima de la unidad sobre $\mathbb{F}_q$ (es un generador del grupo multiplicativo $\mathbb{F}_{q^n} - \{0\}$), es decir, $\mathbb{F}_{q^n} = \left\{0, 1, \omega, \omega^2, \ldots, \omega^{q^n-2}\right\}$ donde $\omega^{q^n-1} = 1$. Más aún ω^k también es una raíz primitiva si y solo si $mcd(k, q^n-1) = 1$ (mcd significa máximo común divisor).

A continuación se presenta un ejemplo ilustrativo donde dos SDF tienen espacios fases isomórficos. Más adelante, después del método de la TDF (dos SDF distintos algebraicamente sean equivalentes y preserven los espacios fases bajo isomorfismos y fourier en el sentido de la transformada discreta), se mostrará un ejemplo donde uno de los sistemas es construido a partir de la TDF.

Ejemplo 52 *Considere*

$$\begin{array}{rccc} f: & \mathbb{F}_3^2 & \to & \mathbb{F}_3^2 \\ & (x,y) & \to & (xy, xy) \end{array}$$

un SDF cuyo espacio fase está dado por la figura 3.5. Ahora tomemos el polinomio $g(x) = \alpha^2 x^2 + \alpha^7 x^4 + x^6 \in \mathbb{F}_3(\alpha)[x]$ donde $\mathbb{F}_3(\alpha) = \{0, \alpha, \alpha^2, \ldots, \alpha^8\} = \mathbb{F}_9$ y α satisface el polinomio irreducible $x^2 + x + 2$ de grado 2 sobre $\mathbb{F}_3$ tal que $\mathbb{F}_3[x]/\langle x^2 + x + 2\rangle \cong \mathbb{F}_3(\alpha)$. Ahora los SDF f y g son equivalentes bajo la transformada de fourier, es decir, el siguiente diagrama conmuta $\phi \circ f = g \circ \phi$



y ϕ es la correspondencia natural (ϕ estará dado por la notación 53 , una correspondencia natural entre $\mathbb{F}_3^2$ y $\mathbb{F}_{3^2}$). Así por el teorema 49 los espacios fases de f y g son isomorfos (ver figura 3.5).

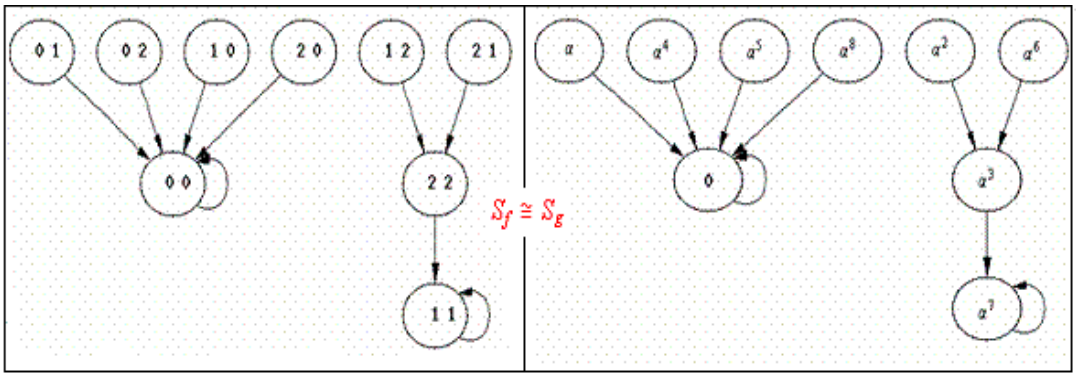


Figura 3.5: Isomorfismo de Espacios Fase Bajo Fourier

El método Discreto de Fourier sobre cuerpos finitos es un caso particular del análisis de fourier discreto sobre grupos finitos (ver [22, 16]). La conexión entre los SDF y el análisis de fourier discreta es nuevo y se encuentra una aplicación al área reguladora de redes genéticas (ver [3]). El método de TDF permite buscar SDF equivalentes de una dimensión a partir de un SDF finito dimensional sobre cualquier cuerpo. Las condiciones necesarias para estudiar SDF por el método de TDF deben satisfacer lo siguiente: dados $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$, $\phi : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$ biyectiva y definir una función $g : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ tal que $\phi \circ f = g \circ \phi$, con esto sus espacios fases serán isórmoficos $S_f \cong S_g$. A continuación se detallará más este método.

Notación 53 *Sea $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ un SDF. Se define la correspondencia natural entre $\mathbb{F}_q^n$ y $\mathbb{F}_{q^n}$ por:*

$$\begin{array}{rccc} \phi_\omega : & \mathbb{F}_q^n & \to & \mathbb{F}_{q^n} \\ & x = (x_0, x_1, \ldots, x_{n-1}) & \to & \phi_\omega(x) = x_0 + x_1\omega + \cdots + x_{n-1}\omega^{n-1} \end{array}$$

donde $x = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_q^n$, $\mathbb{F}_q[x]/\langle p(x)\rangle \cong \mathbb{F}_{q^n}(\omega)$ *con* $p(x)$ *un polinomio irreducible sobre* $\mathbb{F}_q$ *de grado* n *y* $p(\omega) = 0$ *. No es difícil ver que* ϕ_ω *es biyectiva, ya que* ϕ_ω *se escribe como combinación lineal de la base de* $\mathbb{F}_q(\omega)$ *y además única, entonces para cada* $a_y \in \mathbb{F}_{q^n}$ *existe un único* $y = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_q^n$ *tal que* $\phi_\omega(y) = a_y$.
Se define

$$\begin{array}{rccl} g: & \mathbb{F}_{q^n} & \to & \mathbb{F}_{q^n} \\ & a & \to & g(a) = \ (\phi_\omega \circ f)(y) \end{array}$$

y por la biyección de ϕ_ω*, también se cumple que para cada* $x \in \mathbb{F}_q^n$ *existe un único* $a_x \in \mathbb{F}_{q^n}$ *tal que:*

$$(g \circ \phi_\omega)(x) = g(\phi_\omega(x)) = g(a_x) = (\phi_\omega \circ f)(x)$$

y como x *es arbitrario, entonces* $g \circ \phi_\omega = \phi_\omega \circ f$*. Luego por la definición 48 los SDF* f *y* g *son equivalentes. Apliquemos esta notación en el siguiente teorema que se encuentra en el artículo [3] de la bibliografía..*

Teorema 54 (TFD) *Se asume la notación anterior. Para cada* $i = 1, 2, \cdots q^n - 1$*, se define*

$$\begin{aligned} B_0 &= (\phi_\omega \circ f)(0, 0, \ldots, 0) \\ B_i &= (\phi_\omega \circ f)(a_{i,0}, a_{i,1}, \ldots, a_{i,n-1}) \end{aligned}$$

donde ω es una raíz de un polinomio irreducible sobre $\mathbb{F}_q$ de grado n y

$$\omega^{i-1} = a_{i,0} + a_{i,1}\omega + \cdots + a_{i,n-1}\omega^{n-1}$$

entonces $g(x) = b_0 + b_1 x + \cdots + b_{q^n-1}x^{q^n-1}$donde $B_0 = b_0$ y

$$\begin{pmatrix} b_{q^n-1} \\ \\ b_1 \end{pmatrix} = -T_{q,\omega} \begin{pmatrix} B_1 - b_0 \\ \\ B_{q^n-1} - b_0 \end{pmatrix}$$

Prueba. Para cada $i = 1, 2, .., q^n - 1$ y ω un elemento primitivo de $\mathbb{F}_{q^n}$ ($\omega^{q^n-1} =$

1) entonces

$$\begin{aligned} B_i &= (\phi_\omega \circ f)(a_{i,0}, a_{i,1}, \ldots, a_{i,n-1}) \\ &= \phi_\omega(f(a_{i,0}, a_{i,1}, \ldots, a_{i,n-1})) \\ &= g(\phi_\omega(a_{i,0}, a_{i,1}, \ldots, a_{i,n-1})) \\ &= g(a_{i,0} + a_{i,1}\omega + \cdots + a_{i,n-1}\omega^{n-1}) \\ &= g(\omega^{i-1}) \end{aligned}$$

ahora por la proposición 46, $g(x) = b_0 + b_1 x + \cdots + b_{q^n-1}x^{q^n-1}$ (se representa por un polinomio de grado a lo mas $q^n - 1$). Así que

$$g(\omega^{i-1}) = b_0 + b_1\omega^{i-1} + \cdots + b_{q^n-1}\left(\omega^{i-1}\right)^{q^n-1}$$

luego

$$\begin{aligned} B_i - b_0 &= g(\omega^{i-1}) - b_0 = b_1\omega^{i-1} + \cdots + b_{q^n-1}\left(\omega^{i-1}\right)^{q^n-1} \\ &= b_{q^n-1} + b_{q^n-2}\left(\omega^{i-1}\right)^{q^n-2} + \cdots + b_1\omega^{i-1} \end{aligned}$$

y por la ecuación (3.1)

$$B_i - b_0 = \begin{pmatrix} 1 & \omega^{(i-1)(q^n-2)} & \cdots & \omega^{i-1} \end{pmatrix} \begin{pmatrix} b_{q^n-1} \\ \vdots \\ b_1 \end{pmatrix}$$

también para cualquier entero k,

$$\left(\omega^{i-1}\right)^{q^n-(k+1)} = \left(\omega^{i-1}\right)^{-k} = \left(\omega^{-1}\right)^{(i-1)k}$$

Ahora por la ecuación (3.2)

$$\begin{pmatrix} B_1 - b_0 \\ B_2 - b_0 \\ \vdots \\ B_{q^n-1} - b_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega^{q^n-2} & \omega^{q^n-3} & \cdots & \omega \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{(q^n-2)(q^n-2)} & \omega^{(q^n-3)(q^n-2)} & \cdots & \omega^{q^n-2} \end{pmatrix} \begin{pmatrix} b_{q^n-1} \\ \vdots \\ b_1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & \left(\omega^{-1}\right)^2 & \cdots & \left(\omega^{-1}\right)^{q^n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \left(\omega^{-1}\right)^{q^n-2} & \left(\omega^{-1}\right)^{2(q^n-2)} & \cdots & \left(\omega^{-1}\right)^{(q^n-2)(q^n-2)} \end{pmatrix} \begin{pmatrix} b_{q^n-1} \\ \vdots \\ \\ b_1 \end{pmatrix}$$

$$= T_{q,\omega^{-1}} \begin{pmatrix} b_{q^n-1} \\ \vdots \\ b_1 \end{pmatrix}$$

y como la transformada de fourier tiene inversa entonces

$$\begin{pmatrix} b_{q^n-1} \\ \vdots \\ b_1 \end{pmatrix} = (T_{q,\omega^{-1}})^{-1} \begin{pmatrix} B_1 - b_0 \\ B_2 - b_0 \\ \vdots \\ B_{q^n-1} - b_0 \end{pmatrix}$$

$$= -T_{q,(\omega^{-1})^{-1}} \begin{pmatrix} B_1 - b_0 \\ B_2 - b_0 \\ \vdots \\ B_{q^n-1} - b_0 \end{pmatrix}$$

$$= -T_{q,\omega} \begin{pmatrix} B_1 - b_0 \\ B_2 - b_0 \\ \vdots \\ B_{q^n-1} - b_0 \end{pmatrix}$$

por tanto queda demostrado. ■
En el último ejemplo se estudio el SDF $g(x) = \omega^2 x^2 + \omega^7 x^4 + x^6 \in \mathbb{F}_{3^2}[\omega]$. Ahora mostraremos por medio TDF como se obtuvo este SDF.

Ejemplo 55 *Apliquemos el teorema 54 para un sistema dinámico finito tridimensional. Sea*

$$\begin{array}{rccc} f: & \mathbb{F}_3^2 & \to & \mathbb{F}_3^2 \\ & (x,y) & \to & (xy, xy) \end{array}$$

el SDF del ejemplo 52 y mostraremos que el SDF polinomial g de este ejemplo fue encontrado por la TDF. Sea $p(x) = x^2 + x + 2$ irreducible sobre $\mathbb{F}_3$, por tanto una raíz ω de p es un elemento primitivo de $\mathbb{F}_{3^2}$, es decir, $p(\omega) = 0$ ó $\omega^2 = 2\omega + 1$ y cualquier potencia de ω se puede escribir como combinación lineal de $\{1, \omega\}$ sobre $\mathbb{F}_3$. A continuación se describe brevemente los pasos del método.
PASO 1. *Determinar las potencias $\omega^{i-1} = a_{i,0} + a_{i,1}\omega$ para $i = 1, 2, .., 8$ y el caso trivial $0 \in \mathbb{F}_{3^2}$*

$(w^i \bmod (w^2 + w + 2)) \bmod 3$	$= a_{i,0} + a_{i,1}\omega$	$(a_{i,0}, a_{i,1})$
0	$= 0$	$(0,0)$
w^0	$= 1$	$(1,0)$
w^1	$= w$	$(0,1)$
w^2	$= 2w + 1$	$(1,2)$
w^3	$= 2w + 2$	$(2,2)$
w^4	$= 2$	$(2,0)$
w^5	$= 2w$	$(0,2)$
w^6	$= w + 2$	$(2,1)$
w^7	$= w + 1$	$(1,1)$

PASO 2. *Calcular*

$$\begin{aligned} B_0 &= (\phi_\omega \circ f)(0,0) \\ B_i &= (\phi_\omega \circ f)(a_{i,0}, a_{i,1}) \end{aligned}$$

donde $\phi_\omega(x_0, x_1) = x_0 + x_1\omega$

i		$\phi_\omega(f(a_{i,1}, a_{i,0}))$	$= B_i$
0	$\phi_\omega(f(0,0))$	$= \phi_\omega((0,0))$	$= 0$
1	$\phi_\omega(f(a_{0,0}, a_{0,1}))$	$= \phi_\omega((0,0))$	$= 0$
2	$\phi_\omega(f(a_{1,0}, a_{1,1}))$	$= \phi_\omega((0,0))$	$= 0$
3	$\phi_\omega(f(a_{2,0}, a_{2,1}))$	$= \phi_\omega((2,2))$	$= 2 + 2\omega = \omega^3$
4	$\phi_\omega(f(a_{3,0}, a_{3,1}))$	$= \phi_\omega((1,1))$	$= 1 + \omega = \omega^7$
5	$\phi_\omega(f(a_{4,0}, a_{5,1}))$	$= \phi_\omega((0,0))$	$= 0$
6	$\phi_\omega(f(a_{5,0}, a_{5,1}))$	$= \phi_\omega((0,0))$	$= 0$
7	$\phi_\omega(f(a_{6,0}, a_{6,1}))$	$= \phi_\omega((2,2))$	$= 2 + 2\omega = \omega^3$
8	$\phi_\omega(f(a_{7,0}, a_{8,1}))$	$= \phi_\omega((1,1))$	$= 1 + \omega = \omega^7$

PASO 3. *Calcular los coeficientes de g por intermedio de la matriz transformada de fourier discreta* $T_{q,\omega}$.

$$\begin{pmatrix} b_8 \\ b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \end{pmatrix} = - \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 & \omega^{10} & \omega^{12} & \omega^{14} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} & \omega^{15} & \omega^{18} & \omega^{21} \\ 1 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} & \omega^{20} & \omega^{24} & \omega^{28} \\ 1 & \omega^5 & \omega^{10} & \omega^{15} & \omega^{20} & \omega^{25} & \omega^{30} & \omega^{35} \\ 1 & \omega^6 & \omega^{12} & \omega^{18} & \omega^{24} & \omega^{30} & \omega^{36} & \omega^{42} \\ 1 & \omega^7 & \omega^{14} & \omega^{21} & \omega^{30} & \omega^{35} & \omega^{42} & \omega^{49} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ \omega^3 \\ \omega^7 \\ 0 \\ 0 \\ \omega^3 \\ \omega^7 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \omega + 1 = \omega^7 \\ 0 \\ 2\omega + 1 = \omega^2 \\ 0 \end{pmatrix}$$

PASO 4. *Encontrar* $g(x) : \mathbb{F}_{3^2} \to \mathbb{F}_{3^2}$*: Los coeficientes del polinomio g son:* $b_8 = 0, b_7 = 0, b_6 = 1, b_5 = 0, b_4 = \omega^7, b_3 = 0, b_2 = \omega^2, b_1 = 0$,$b_0 = 0$ *por tanto el polinomio g esta dado por*

$$g(x) = \omega^2 x^2 + \omega^7 x^4 + x^6$$

Básicamente este método nos permite establecer un polinomio unidimensional sobre un cuerpo finito a partir de un SDF multidimensional cuyas propiedades dinámicas se trasmiten sin cambio alguno. La ventaja que se puede tener con respecto al segundo sistema es que los campos finitos son una herramienta más común que los mismos campos de Galois multidimensional. Es un tema de continuo estudio y según nuestra investigación la respuesta es afirmativa.

Capítulo 4

SDF Booleanos Monomiales Afines y Temas Relacionados

4.1. Resultados Relacionados a Sistemas Dinámicos Finitos Booleanos Monomiales Afines

Esta sección esta dedicada principalmente al trabajo investigado sobre SDF monomiales afines, en particular, los booleanos. Varios resultados presentados son extendidos a cualquier campo finito y después se aplica a los booleanos. El contenido de esta sección responde a varios problemas hasta ahora abiertos y en gran parte sobre los SDFB monomiales afines (ver [7]). Aspectos combinatorios referentes a SDF también serán presentados, como por ejemplo, una cota inferior para el conjunto B_ϵ; conjunto de puntos que tienen contacto con el nodo $\in$ para; un sistema monomial afín, y para un caso especial, el corolario 65 establece que ese contacto es $B_\epsilon = 2^n - 1$. También se determinó: que la unión de todos los espacios fases de los sistemas dinámicos finitos booleanos monomiales afines forman el grafo simétrico de orden 2^n, si el grafo de dependencia del sistema es un grafo simétrico completo de orden n. Adicional a la investigación se establece el número de ciertos polinomios que son involuciones en $\mathbb{Z}_p$ y básicamente este conteo utiliza el número ternas consecutivas de residuos cuadráticos y no residuos cuadráticos.

A continuación se presentan dos definiciones fundamentales para el caso booleano. Primero el concepto de SDFB monomial por un SDF de la forma

$$f = (f_1, f_2, \ldots, f_n) : \mathbb{F}_2^n \to \mathbb{F}_2^n$$

donde $f_i = \alpha_i x_1^{\delta_{\mathbf{1i}}} x_2^{\delta_{\mathbf{2i}}} \cdots x_n^{\delta_{\mathbf{ni}}}$ con $\alpha_i, \delta_{ji} \in \{0, 1\}$. Si $\alpha_i = 0$ el conjunto de todos los $\delta_{ji} = 0$. El segundo el concepto de un SDF monomial afín sobre $\mathbb{F}_q^n$. La siguiente definición es de interés principal y varios de los resultados se extendieron a campos arbitrarios usando el concepto de SDFB monomial afín.

Definición 56 (SDFB Monomial Afín) *Se define el SDFB monomial afín sobre* $\mathbb{F}_2^n$ *por la función* $g = f + \epsilon$, *donde* $0 \neq \epsilon \in F_2^n$ *y* $f = (f_1, f_2, \ldots, f_n)$ *un SDFB monomial sobre* $\mathbb{F}_2^n$.

Para el caso donde $0 \neq \epsilon \in F_q^n$ y f es un SDF monomial sobre F_q^n (donde $\alpha_i, \delta_{ji} \in \{0, 1, \ldots, q-1\}$. Si $\alpha_i = 0$ el conjunto de todos los $\delta_{ji} = 0$), se dice que g es un SDF monomial afín sobre F_q^n cuyo espacio fase se denota por $S_g(f)$.

Ejemplo 57 *Consideremos el SDFB monomial* $f = (x_1, x_1x_2x_3, x_1x_2)$ *sobre* $\mathbb{Z}_2^3$ *y el SDFB monomial afín* $g = (x_1, x_1x_2x_3, x_1x_2) + (1, 0, 0)$ *sobre* $\mathbb{Z}_2^3$. *La siguiente gráfica muestra sus espacios fases donde* $\epsilon = (1, 0, 0) \in \mathbb{Z}_2^3$.

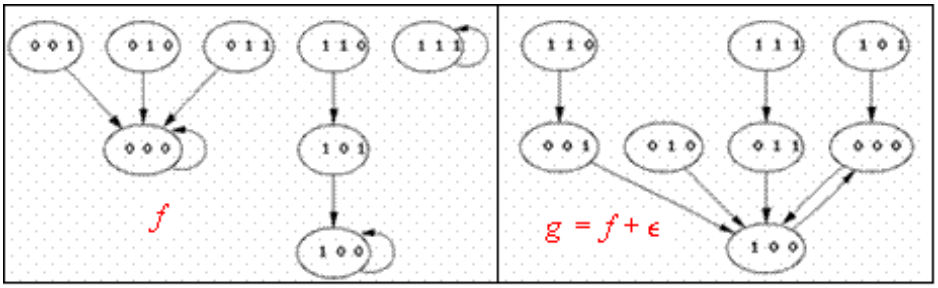


Figura 4.1: Sistema Dinámico Finito Booleano Monomial y Afín

La siguiente definición permite relacionar las funciones f_i por medio de un grafo dirigido. Una de las preguntas abiertas importantes formuladas sobre SDF sobre cuerpos finitos es: ¿de qué manera el estudio de los f_i me permiten dar información completa del comportamiento dinámico de la función f (ver [7])?.

Definición 58 (Grafo de Dependencia) *Sea* f *un SDF sobre* $\mathbb{F}_2$. *Asociamos a* f *un digrafo* X_f *llamado grafo de dependencia, con vértices* $\{x_1, x_2, \ldots, x_n, \epsilon_0\}$. *Existe un eje dirigido de* x_i *a* x_j $(x_i \to x_j)$, *si* $\alpha_i = 1$ *y* $x_j \mid f_i$. *Existe un lado dirigido de* x_i *a* ϵ_0 $(x_i \to \epsilon_0)$, *si* $\alpha_i = 0$.

Veamos a continuación un ejemplo gráfico de la definición anterior.

Ejemplo 59 *Consideremos los SDFB monomiales* $f_1 = (x_1, x_1x_2, x_1x_4, x_1)$ *y* $f_2 = (x_1x_2, x_2x_3, 0)$ *con sus respectivos grafos dependencia (ver gráfica 4.2).*

Observación 60 *Se denotarán el conjunto* $\{1, 2, \ldots, n\}$ *por* $[n]$, *las n-duplas* $(1, 1, \ldots, 1) = \bar{1}$ *y* $(0, 0, \ldots 0) = \bar{0}$

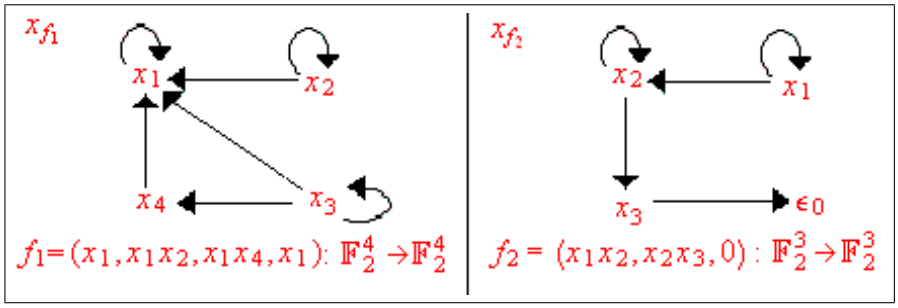


Figura 4.2: Dos Grafos de Dependencia

Los siguientes dos teoremas nos permiten obtener dos cotas inferiores para todo $g = f + \epsilon$ que satisface $g(x) = \epsilon$ y f un SDF monomial cuyo grafo de dependencia es X_f. En otras palabras, nos permite establecer una cota inferior para el conjunto $B_\epsilon = \{x \in F_q^n : g(x) = \epsilon\}$, y para eso, contaremos cuantas posibles soluciones satisfacen $f(x) = 0$; puesto $f(x) = 0$ implica $g(x) = \epsilon$. Las ideas del primer resultado (cota mala) son usadas para el segundo y mejora bastante el primero. Se tendrán en cuenta los dos teoremas por que en esencia los conteos son diferentes. Para el caso, $q = 2$ y X_f completo los dos teoremas son óptimos (ver corolario 65).

Teorema 61 *Sea $g = f + \epsilon$ un SDF monomial afín sobre F_q^n. Definamos el conjunto $A_f = \{j \in [n] : x_j \mid f_i;\ \forall i \in [n]\}$ y $B_\epsilon = \{x \in F_q^n : g(x) = \epsilon\}$ entonces*

$$|B_\epsilon| \geq (q-1)^{n-|A_{\mathbf{f}}|}\left[q^{|A_{\mathbf{f}}|} - (q-1)^{|A_{\mathbf{f}}|}\right]$$

Prueba. *Sea f un SDF Monomial. Sí $|A_{\mathbf{f}}| = 0$ entonces $|B_\epsilon| \geq 0$ (se verifica la desigualdad con la cota más trivial). Si $|A_{\mathbf{f}}| \neq 0$, sea $S_k \subset A_{\mathbf{f}}$ con $k = |S_k|$ entre 1 y $|A_{\mathbf{f}}|$. Definamos la siguiente propiedad: Tomemos $\widetilde{x} = (x_1x_2, \ldots, x_n) \in F_q^n$ tal que*

$$x_m \quad = \left\{ \begin{array}{l} 0,\ si\ m \in S_k \\ c,\ si\ m \notin S_k\ y\ c \in F_q^* \end{array} \right\}.$$

Los elementos $\widetilde{x}$ que satisfacen esta propiedad cumplen que $f(\widetilde{x}) = 0$, ya que para cada $\widetilde{x}$ existe $j \in S_k$ tal que $x_j = 0$ ($|S_k| \geq 1$) y como $S_k \subset A_{\mathbf{f}}$ entonces $x_j \mid f_i$; $\forall i \in [n]$, por tanto, $f_i(\widetilde{x}) = 0$, $\forall i \in [n]$, es decir, $f(\widetilde{x}) = (f_1(\widetilde{x}), f_2(\widetilde{x}), \ldots, f_n(\widetilde{x})) = \overline{0}$. Ahora para contar cuántos $\widetilde{x} \in F_q^n$ satisfacen esta propiedad, digamos que ese número es N_f, basta contar el número de subconjuntos con k elementos de $A_{\mathbf{f}}$ que determinan a $\widetilde{x}$ con k componentes ceros, o sea, el número de ceros que tiene las componentes de $\widetilde{x}$ son k ceros y que es igual al número de elementos de un subconjunto de $A_{\mathbf{f}}$, que en total son $\binom{|A_{\mathbf{f}}|}{k}$, por $(n-k)$ componentes de $\widetilde{x}$ que son distintas de cero y en total son $\left((q-1)^{n-k}\right)$,

por tanto existen $(q-1)^{n-k}\binom{|A_{\mathbf{f}}|}{k}$ *elementos* $\widetilde{x}$ *para colocarle en* k *componentes un cero y las demás componentes,* $(q-1)$ *elementos distintos de cero, donde* $1 \leq k \leq |A_{\mathbf{f}}|$*, así, en sumatoria sobre* k *se tiene*

$$N_f = (q-1)^{n-1}\binom{|A_{\mathbf{f}}|}{1} + (q-1)^{n-2}\binom{|A_{\mathbf{f}}|}{2} + \cdots + (q-1)^{n-|A_{\mathbf{f}}|}\binom{|A_{\mathbf{f}}|}{|A_{\mathbf{f}}|}$$

elementos que satisfacen $f(\widetilde{x}) = 0$*, y simplificando*

$$\begin{aligned} N_f &= (q-1)^{n-|A_{\mathbf{f}}|}\left[(q-1)^{n-1-n+|A_{\mathbf{f}}|}\binom{|A_{\mathbf{f}}|}{1} + (q-1)^{n-2-n+|A_{\mathbf{f}}|}\binom{|A_{\mathbf{f}}|}{2} + \cdots + \right. \\ &\quad \left. (q-1)^{n-|A_{\mathbf{f}}|-n+|A_{\mathbf{f}}|}\binom{|A_{\mathbf{f}}|}{|A_{\mathbf{f}}|}\right] \\ &= (q-1)^{n-|A_{\mathbf{f}}|}\left[\binom{|A_{\mathbf{f}}|}{1}(q-1)^{|A_{\mathbf{f}}|-1} + \binom{|A_{\mathbf{f}}|}{2}(q-1)^{|A_{\mathbf{f}}|-2} + \cdots + \binom{|A_{\mathbf{f}}|}{|A_{\mathbf{f}}|}\right] \\ &= (q-1)^{n-|A_{\mathbf{f}}|}\left[(q-1+1)^{|A_{\mathbf{f}}|} - \binom{|A_{\mathbf{f}}|}{0}(q-1)^{|A_{\mathbf{f}}|}\right] \\ &= (q-1)^{n-|A_{\mathbf{f}}|}\left[(q)^{|A_{\mathbf{f}}|} - (q-1)^{|A_{\mathbf{f}}|}\right] \end{aligned}$$

Ahora, si $|A_{\mathbf{f}}| \neq n$*, entonces* $x = \overline{0}$ *no satisface la propiedad anterior pero satisface* $f(x) = 0$*, por tanto,*

$$|B_\epsilon| \geq (q-1)^{n-|A_{\mathbf{f}}|}\left[q^{|A_{\mathbf{f}}|} - (q-1)^{|A_{\mathbf{f}}|}\right] + 1 > (q-1)^{n-|A_{\mathbf{f}}|}\left[q^{|A_{\mathbf{f}}|} - (q-1)^{|A_{\mathbf{f}}|}\right]$$

y para $|A_{\mathbf{f}}| = n$ *(equivalente a* X_f *es completo) el* $x = \overline{0}$ *también satisface la propiedad, por consiguiente,*

$$|B_\epsilon| \geq (q-1)^{n-|A_{\mathbf{f}}|}\left[q^{|A_{\mathbf{f}}|} - (q-1)^{|A_{\mathbf{f}}|}\right]$$

por tanto queda demostrado. ■

Teorema 62 *Sea* $g = f + \epsilon$ *un SDF monomial afín sobre* F_q^n *con* A_f *como en el teorema 61 entonces*

$$|B_\epsilon| \geq q^{n-|A_{\mathbf{f}}|}\left[q^{|A_{\mathbf{f}}|} - (q-1)^{|A_{\mathbf{f}}|}\right]$$

Prueba. *Sea* f *un SDF monomial. Sí* $|A_{\mathbf{f}}| = 0$ *entonces* $|B_\epsilon| \geq 0$ *(se verifica la desigualdad con la cota más trivial). Si* $|A_{\mathbf{f}}| \neq 0$ *sea* $A_{\mathbf{f}} = \left\{j_1, j_2, \ldots, j_{|A_{\mathbf{f}}|}\right\} \subset [n]$ *con* $j_1 \leq j_2 \leq \ldots \leq j_m$*. Definamos la siguiente propiedad: Tomemos* $\widetilde{x} = (x_1 x_2, \ldots, x_n) \in F_q^n$ *tal que para cada* $j_k \in A_{\mathbf{f}}$ *hacemos* $x_{j_r} \neq 0$ *para* $1 \leq r \leq k-1$ *y* $x_{j_k} = 0$*, para las demás componentes cualquier valor de* F_q*. Los elementos* $\widetilde{x}$ *que satisfacen esta propiedad cumplen que* $f(\widetilde{x}) = 0$*, ya que para cada uno de estos* $\widetilde{x}$ *existe* $j \in A_{\mathbf{f}}$ *tal que* $x_j = 0$ *y como* $x_j \mid f_i$*;* $\forall i \in [n]$*, entonces* $f_i(\widetilde{x}) = 0$*,* $\forall i \in [n]$*, es decir,* $f(\widetilde{x}) = (f_1(\widetilde{x}), f_2(\widetilde{x}), \ldots, f_n(\widetilde{x})) = \overline{0}$*. Ahora para contar cuántos* $\widetilde{x} \in F_q^n$ *satisfacen la propiedad anterior, digamos que ese número es* N_f *basta contar los* $(k-1)$ *componentes que son distintos de cero, que en total es* $(q-1)^{k-1}$*, más la*

componente j_k igual a cero (uno solo) y los demás $(n-k)$ componentes se coloca cualquier valor de F_q^n, que en total son q^{n-k}. Así en sumatoria o sumando sobre k se tiene que

$$N_f = \sum_{k=1}^{|A_{\mathbf{f}}|} q^{n-k}\,(q-1)^{k-1} = q^{n-1} + q^{n-2}\,(q-1) + \cdots + q^{n-|A_{\mathbf{f}}|}\,(q-1)^{|A_{\mathbf{f}}|-1}$$

transformando la expresión

$$\begin{aligned} N_f &= \left[q^{n-1-n+|A_{\mathbf{f}}|} + q^{n-2-n+|A_{\mathbf{f}}|}\,(q-1) + \cdots + q^{n-|A_{\mathbf{f}}|+1-n+|A_{\mathbf{f}}|}\,(q-1)^{|A_{\mathbf{f}}|-2}\right] \\ &\quad + \cdots + \left[(q-1)^{|A_{\mathbf{f}}|-1}\right]] \times q^{n-|A_{\mathbf{f}}|} \\ &= q^{n-|A_{\mathbf{f}}|}[\left[q^{|A_{\mathbf{f}}|-1} + q^{|A_{\mathbf{f}}|-2}\,(q-1) + \cdots + q\,(q-1)^{|A_{\mathbf{f}}|-2} + (q-1)^{|A_{\mathbf{f}}|-1}\right] \end{aligned}$$

pero

$$q^{|A_{\mathbf{f}}|} - (q-1)^{|A_{\mathbf{f}}|} = \left[q^{|A_{\mathbf{f}}|-1} + q^{|A_{\mathbf{f}}|-2}\,(q-1) + \cdots + q\,(q-1)^{|A_{\mathbf{f}}|-2} + (q-1)^{|A_{\mathbf{f}}|-1}\right]$$

por tanto

$$N_f = q^{n-|A_{\mathbf{f}}|}\left[q^{|A_{\mathbf{f}}|} - (q-1)^{|A_{\mathbf{f}}|}\right]$$

se concluye que

$$|B_\epsilon| \geq N_f.$$

por tanto queda demostrado. ■

Definición 63 *Un grafo dirigido G es simétrico completo de orden n con V el conjunto de n vértices, si para dos vértices distintos $\mu, \nu \in V$ de G, los ejes (μ, ν) y (ν, μ) están presente en G. Denotamos al grafo G por K_n^*, el conjunto de vértices por $V_{K_n^*}$ y el conjunto de ejes por $E_{K_n^*}$ (ver [12]).*

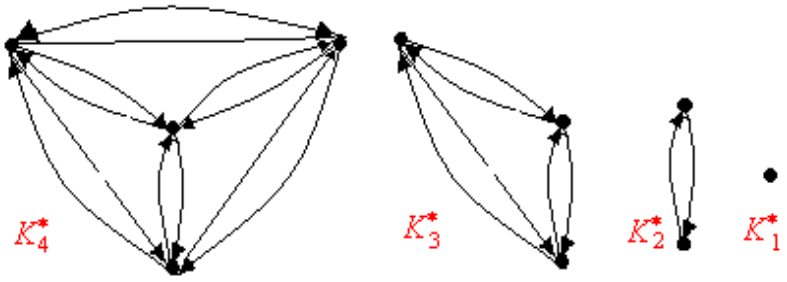


Figura 4.3: Grafos Simétricos Completos

Ejemplo 64 *Sea* $g = (x_1x_2x_3, x_1x_2x_3, x_1x_2x_3) + (1,1,0) = (\bar{x}+1, \bar{x}+1, \bar{x})$ *un SDFB monomial afín sobre* $\mathbb{Z}_2^3$ *donde* $\bar{x} = x_1x_2x_3$ *y con* $|A_{\mathbf{f}}| = 3$*, entonces*

$$B_{(1,1,0)} = \{(0,0,0),(1,0,0),(0,1,0),(0,0,1),(1,1,0),(1,0,1),(0,1,1)\}$$

donde $\left|B_{(1,1,0)}\right| = 2^3 - 1 = 7$*. También desde su espacio fase se verifica, ver figura 4.4, Además su grafo de dependencia es* K_3^**.*

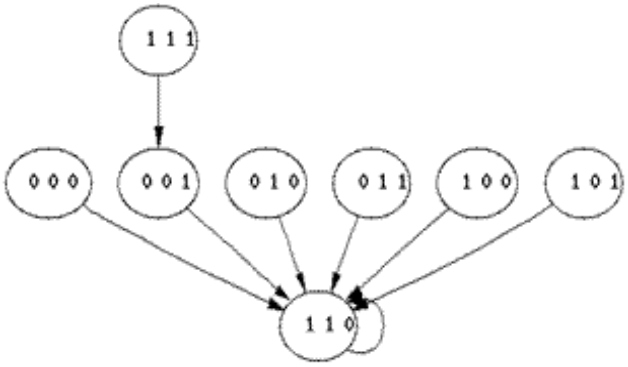


Figura 4.4: Espacio Fase de g

Cuando $|A_f| = n$ y X_f es un grafo simétrico completo de orden n, estas dos expresiones son equivalentes y nos permite ver el grafo de dependencia desde estos dos puntos de vista. El siguiente corolario es una consecuencia óptima de los dos teorema anteriores para cuando $|A_f| = n$.

Corolario 65 *Sea* $g = f + \epsilon$ *un SDFB monomial afín sobre* $\mathbb{F}_2^n$ *entonces*

1. $|B_\epsilon| > 2^{n-|A_{\mathbf{f}}|}\left[2^{|A_{\mathbf{f}}|} - 1\right]$*, siempre que* $|A_{\mathbf{f}}| \neq n$*.*
2. *Sí* $X_f = K_n^*$ *entonces* $|B_\epsilon| = 2^n - 1$*.*

Prueba.

1. *Si* $|A_{\mathbf{f}}| \neq n$ *y* $q = 2$*. El punto* $x = \overline{0}$ *no satisface la propiedad del teorema 62 y sumarle uno más a la cota inferior, por consiguiente*

$$|B_\epsilon| \geq 2^{n-|A_{\mathbf{f}}|}\left[2^{|A_{\mathbf{f}}|} - 1\right] + 1 > 2^{n-|A_{\mathbf{f}}|}\left[2^{|A_{\mathbf{f}}|} - 1\right].$$

2. *Para* $|A_{\mathbf{f}}| = n$ *el* $x = \overline{0}$ *satisface la propiedad del teorema 61, así que* $\overline{0}$ *está contado y* $2^n > |B_\epsilon| \geq 2^n - 1$*, ya que* $g(\overline{1}) = \overline{1} + \epsilon \neq \epsilon$*, por consiguiente* $|B_\epsilon| = 2^n - 1$*.*

Por tanto queda demostrado. ■

Se denotó el espacio fase $S_g(f)$ del espacio afín formado por el SDFB f y se denota un eje dirigido de x a y por (x, y) ó $x \to y$.

Lema 66 *Si g y $\widetilde{h}$ son dos SDF monomiales afines sobre $\mathbb{F}_2^n$ entonces*

$$S_g(f) \cap S_{\widetilde{h}}(f) = \phi.$$

Prueba. *Sean $g = f+\epsilon$ y $\widetilde{h} = f+\widetilde{\epsilon}$ con $\widetilde{\epsilon} \neq \epsilon$. Supongamos que $S_g(f) \cap S_{\widetilde{h}}(f) \neq \phi$, entonces existe un lado dirigido (x, y) en $S_g(f) \cap S_{\widetilde{h}}(f)$ tal que $x \xrightarrow{g} y$ y $x \xrightarrow{\widetilde{h}} y$ son lados del espacio fase $S_g(f)$ y $S_{\widetilde{h}}(f)$ respectivamente, es decir, $g(x) = y$ y $\widetilde{h}(x) = y$ pero g y $\widetilde{h}$ son SDF monomiales afines, entonces*

$$f(x) + \epsilon = g(x) = y = \widetilde{h}(x) = f(x) + \widetilde{\epsilon}$$

luego $\epsilon = \widetilde{\epsilon}$ absurdo, por tanto $S_g(f) \cap S_{\widetilde{h}}(f) = \phi$. ■

Se presentará a continuación un resultado que permite ver el grafo dirigido simétrico completo de 2^n vértices por medio de uniones disjuntas de grafos dirigidos determinados por los espacios fases de los SDFB monomiales afines. Más detalles se muestran en el siguiente corolario.

Corolario 67 *Sea $g_i = f + \epsilon_i$ con $i \in \{1, 2, \ldots, 2^n\}$ un SDFB monomial afín sobre $\mathbb{F}_2^n$ y $X_f = K_n^*$, entonces la unión disjunta de todos los espacios fases $S_{g_i}(f)$ es el grafo simétrico completo $K_{2^n}^*$.*

Prueba. *Basta probar $\overset{\circ}{\bigcup} S_{g_i}(f) = K_{2^n}$, es decir,*

1. *Comparten el mismo conjunto de vértices, es decir, $\bigvee_{\overset{\circ}{\cup} S_{g_i}(f)} = \bigvee_{K_{2^n}}$*
2. *Comparten el mismo conjunto de lados, es decir, $E_{\overset{\circ}{\cup} S_{g_i}(f)} = E_{K_{2^n}}$*

   En efecto, para el primer caso etiquetamos los vértices de K_{2^n} con cada elemento de $\mathbb{F}_2^n$ tal que $\bigvee_{K_{2^n}} = \mathbb{F}_2^n$. Por definición de espacio fase de un SDFB $\bigvee_{S_{g_i}(f)} = \mathbb{F}_2^n$ y como $\bigvee_{S_{g_i}(f)} = \bigvee_{\overset{\circ}{\cup} S_{g_i}(f)} = \mathbb{F}_2^n$ por consiguiente $\bigvee_{\overset{\circ}{\cup} S_{g_i}(f)} = \bigvee_{K_{2^n}}$.

   Para el segundo caso: es fácil ver que $E_{\overset{\circ}{\cup} S_{g_i}(f)} \subset E_{K_{2^n}}$, ya que todo lado de $\overset{\circ}{\bigcup} S_{g_i}(f)$ esta sobre $\mathbb{F}_2^n$ que es un lado del grafo dirigido K_{2^n}. veamos que $E_{K_{2^n}} \subset E_{\overset{\circ}{\cup} S_{g_i}(f)}$, en efecto, sea $(\widetilde{\epsilon}, \epsilon) \in E_{K_{2^n}}$ entonces $\widetilde{\epsilon} \to \epsilon$. Definamos lo siguiente:

   - *Si $\widetilde{\epsilon} \neq \bar{1}$ definimos $g = f+\epsilon$ con $\epsilon = (\epsilon_1, \epsilon_2, \ldots, \epsilon_n)$ y $\widetilde{\epsilon} = (\widetilde{\epsilon}_1, \widetilde{\epsilon}_2, \ldots, \widetilde{\epsilon}_n)$*

- *Si* $\widetilde{\epsilon} = \bar{1}$ *definimos* $g = f + \epsilon^{\perp}$ *con* $\epsilon^{\perp} = (\epsilon_1^{\perp}, \epsilon_2^{\perp}, \ldots, \epsilon_n^{\perp})$ *con* $\epsilon_k^{\perp} = \epsilon_k + 1$ *para todo* $k \in [n]$

Sea $\widetilde{\epsilon} \neq \bar{1}$ *, luego existe un* $j \in [n]$ *tal que* $\widetilde{\epsilon}_j = 0$ *y como* X_f *es completo entonces* $f(\widetilde{\epsilon}) = 0$*, sustituyendo* $\widetilde{\epsilon}$ *en* g*,* $g(\widetilde{\epsilon}) = f(\widetilde{\epsilon}) + \epsilon = 0 + \epsilon = \epsilon$*, es decir,* $\widetilde{\epsilon} \xrightarrow{g} \epsilon$*, por consiguiente* $(\widetilde{\epsilon}, \epsilon) \in E_{S_g(f)} \subset E^{\circ}_{\cup_{S_{g_i}(f)}}$*. Si* $\widetilde{\epsilon} = \bar{1}$ *entonces*

$$\begin{aligned} g(\widetilde{\epsilon}) &= f(\widetilde{\epsilon}) + \epsilon^{\perp} \\ &= f(\bar{1}) + \epsilon^{\perp} \\ &= \bar{1} + (\epsilon_1^{\perp}, \epsilon_2^{\perp}, \ldots, \epsilon_n^{\perp}) \\ &= (1 + \epsilon_1^{\perp}, 1 + \epsilon_2^{\perp}, \ldots, 1 + \epsilon_n^{\perp}) \end{aligned}$$

pero por definición de $\epsilon^{\perp}$*,* $(1 + \epsilon_1^{\perp}, 1 + \epsilon_2^{\perp}, \ldots, 1 + \epsilon_n^{\perp}) = (\epsilon_1, \epsilon_2, \ldots, \epsilon_n) = \epsilon$ *por tanto,* $\widetilde{\epsilon} \xrightarrow{g} \epsilon$*, es decir,* $(\widetilde{\epsilon}, \epsilon) \in E_{S_g(f)} \subset E^{\circ}_{\cup_{S_{g_i}(f)}}$*. De los dos casos anteriores se tiene que* $E^{\circ}_{\cup_{S_{g_i}(f)}} = E_{K_{2^n}}$
Concluimos que

$$\overset{\circ}{\bigcup} S_{g_i}(f) = K_{2^n}$$

por tanto queda demostrado. ■

Un ejemplo de este teorema, se encuentra sobre $\mathbb{F}_2^3$ basado sobre el cubo (ver figura 4.5).

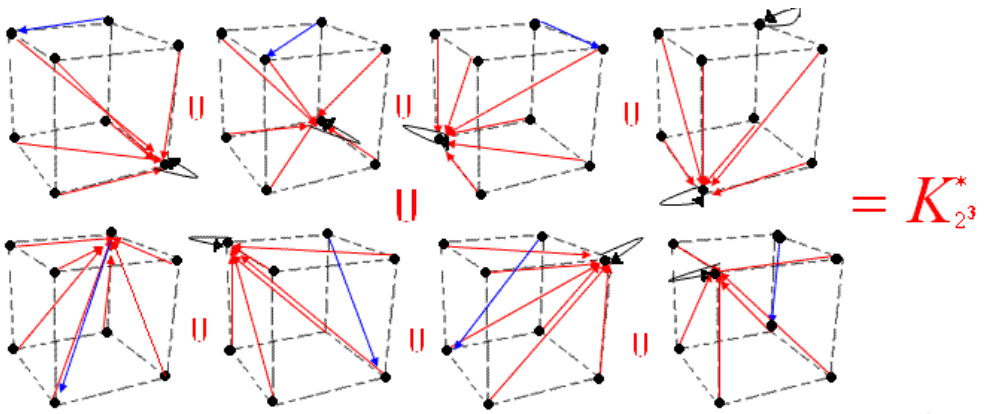


Figura 4.5: Grafo simétrico de orden 3 basado en cubo

Corolario 68 *Sea* $f = (f_1, f_2, \cdots, f_n)$ *un SDFB monomial sobre* $\mathbb{F}_2^n$ *con* $X_f = K_n^*$ *. Consideremos* $g = f + \epsilon$ *; con* $\epsilon \neq \bar{1}$*,*
entonces

1. *g es un SDFB monomial de punto fijo.*

2. *f es un SDFB monomial afín de punto fijo*

Prueba.

1. *Por hipótesis X_f es completo y $\epsilon \neq \bar{1}$. así que por definición $A_f = n$ y por el corolario 65 $|B_\epsilon| = 2^n - 1$, en otras palabras, $B_\epsilon = \mathbb{F}_2^n - \{\bar{1}\}$ y $g(x) = \epsilon$ para todo $x \epsilon B_\epsilon$,en particular $g(\epsilon) = \epsilon$, es un punto fijo. Veamos que $g^m(x) \neq x$ para todo $m > 1$ y $x \in \mathbb{F}_2^n$. Primero sea $x \in \mathbb{F}_2^n - \{\bar{1}, \epsilon\}$ y supongamos que existe $m > 1$ que satisface $g^m(x) = x$, entonces*
$$\begin{aligned} x = g^m(x) &= g^{m-1}(g(x)) \\ &= g(x) \qquad\qquad \text{ya que } g(\epsilon) = \epsilon \\ &= \epsilon \end{aligned}$$
así que $x = \epsilon$ absurdo, por tanto, no existe un ciclo de longitud mayor que 1. Por último, supongamos que si existe $m > 1$ que satisface $g^m(\bar{1}) = \bar{1}$.
$$\begin{aligned} \bar{1} = g^m(\bar{1}) &= g^{m-1}(g(\bar{1})) \\ &= g^{m-1}(f(\bar{1}) + \epsilon) \\ &= g^{m-1}(\bar{1} + \epsilon) \\ &= \epsilon \qquad\qquad\qquad g(x) = \epsilon,\ \forall x \epsilon B_\epsilon \text{ o } g(\bar{1} + \epsilon) = \epsilon \neq \bar{1} \end{aligned}$$
así que $\epsilon = \bar{1}$ absurdo, por hipótesis. Concluimos que para todo $x \epsilon \mathbb{F}_2^n$, g no tiene ciclos de longitud mayor que 1, por tanto g es un SDFB monomial afín de punto fijo.

2. *Basta tomar $g = f + \bar{0} = f$, y por la parte anterior f es un SDFB monomial de punto fijo.*

por tanto queda demostrado. ■

4.2. Tópicos Relacionados y Problemas de Investigación

Mostraremos en esta sección la relación existente entre el número de ternas consecutivas de residuos cuadráticos y no residuos cuadráticos sobre $\mathbb{Z}_p$ y el número de SDF de la forma $f(x) = x^{p-2} + \beta x^{\frac{p-3}{2}}$ que no son de punto fijo sobre $\mathbb{Z}_p$. El interés inicial surge del estudio de un trabajo de investigación hecho por los doctores Omar Colón y Alberto Cáceres sobre polinomios de permutación sobre $\mathbb{Z}_p$ (ver [6]). Para tal efecto, recordaremos algunos conceptos de Teoría de Números y en adelante emplearemos la siguiente terminología: sea a un entero y p un primo impar, se define el símbolo de Legendre $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$ y cada vez

que el símbolo de Legendre $\left(\frac{a}{p}\right) = 1$ decimos que a es un Residuo Cuadrático (RC) y si $\left(\frac{a}{p}\right) = -1$ decimos que a es No Residuo Cuadrático (NRC). También se denota a $N(\alpha_1, \alpha_2, \alpha_3)$ por el número de enteros a tales que $1 \leq a \leq p-3$ satisfacen

$$\alpha_1 = \left(\frac{a}{p}\right), \alpha_2 = \left(\frac{a+1}{p}\right), \alpha_3 = \left(\frac{a+2}{p}\right)$$

en otras palabras, el número de ternas consecutivas de RC o NRC sobre $\mathbb{Z}_p$. La siguiente proposición muestra una identidad que relaciona implícitamente $N(\alpha_1, \alpha_2, \alpha_3)$ con el Símbolo de Legendre y sobre ternas consecutivos de RC o NRC. La misma fórmula implícita cumple de igual manera para k enteros consecutivos en RC o NRC (ver [21]). La prueba se presenta para $k = 3$ y es idéntica para todo k. También presentaremos algunos resultados relacionados con los SDF sobre cuerpos finitos que fueron resueltos en paralelo con esta investigación.

Proposición 69 *Dados $\alpha_1, \alpha_2, \alpha_3$ con $\alpha_j = -1, 1$ para todo j entonces*

$$8N(\alpha_1, \alpha_2, \alpha_3) = \sum_{a=1}^{p-3} \left(1 + \alpha_1\left(\frac{a}{p}\right)\right)\left(1 + \alpha_2\left(\frac{a+1}{p}\right)\right)\left(1 + \alpha_3\left(\frac{a+2}{p}\right)\right)$$

donde p es un primo impar.

Prueba. *Primero fijemos los valores*

$$\alpha_1 = \left(\frac{a}{p}\right), \alpha_2 = \left(\frac{a+1}{p}\right), \alpha_3 = \left(\frac{a+2}{p}\right)$$

y esta condición determina el conjunto

$$\eta = \left\{x \in \{1, 2, ..., p-3\} : \alpha_1 = \left(\frac{x}{p}\right), \alpha_2 = \left(\frac{x+1}{p}\right), \alpha_3 = \left(\frac{x+2}{p}\right)\right\}$$

de donde $|\eta| = N(\alpha_1, \alpha_2, \alpha_3)$. En adelante denotamos

$$\gamma_a = \left(1 + \alpha_1\left(\frac{a}{p}\right)\right)\left(1 + \alpha_2\left(\frac{a+1}{p}\right)\right)\left(1 + \alpha_3\left(\frac{a+2}{p}\right)\right)$$

luego

$$\sum_{a=1}^{p-3} \gamma_a = \sum_{a \in \eta} \gamma_a + \sum_{a \notin \eta} \gamma_a$$

Probemos que la segunda sumatoria es cero; en efecto, para cada $a \notin \eta$ existe un $j \in \{1, 2, ..., p-3\}$ tal que $\alpha_j \neq \left(\frac{a+j-1}{p}\right)$, así que

$$\left[\alpha_j = 1 \ y \ \left(\frac{a+j}{p}\right) = -1\right] o \left[\alpha_j = -1 \ y \ \left(\frac{a+j}{p}\right) = 1\right]$$

luego $\alpha_j\left(\frac{a+j}{p}\right) = -1$, *osea* $\alpha_j\left(\frac{a+j}{p}\right) + 1 = 0$ *por tanto*

$$\begin{aligned}\sum_{a\notin\eta}\gamma_a &= \sum_{a\notin\eta}\left(1+\alpha_1\left(\tfrac{a}{p}\right)\right).....\underset{\text{posición } j}{\left(1+\alpha_j\left(\tfrac{a+j}{p}\right)\right)}.....\left(1+\alpha_2\left(\tfrac{a+2}{p}\right)\right)\\ &= \sum_{a\notin\eta}(1+\alpha_1\left(\tfrac{a}{p}\right))...\ (0)\ ...(1+\alpha_k\left(\tfrac{a+2}{p}\right))\\ &= \sum_{a\notin\eta}0\\ &= 0\end{aligned}$$

Ahora en la primera sumatoria se tiene que para todo $a \in \eta$ *se cumple que*

$$\alpha_1 = \left(\frac{a}{p}\right), \alpha_2 = \left(\frac{a+1}{p}\right), \alpha_2 = \left(\frac{a+2}{p}\right)$$

así que $\alpha_j\left(\frac{a+j}{p}\right) = 1$ *para cada* $j = 1, 2, 3$ *por tanto*

$$\begin{aligned}\sum_{a\in\eta}\gamma_i &= \sum_{a\in\eta}(1+\alpha_1\left(\tfrac{a}{p}\right))...(1+\alpha_j\left(\tfrac{a+j}{p}\right))...(1+\alpha_k\left(\tfrac{a+2}{p}\right))\\ &= \sum_{a\in\eta}(1+1)^{3-\overset{veces}{\cdots}}(1+1)\\ &= \sum_{\in\eta}2*2*2\\ &= \sum_{a\in\eta}2^3\\ &= 2^3\sum_{a\in\eta}1\\ &= 2^3*|\eta|\end{aligned}$$

por consiguiente

$$\begin{aligned}\sum_{a=1}^{p-3}\gamma_a &= \sum_{a\in\eta}\gamma_a + \sum_{a\notin\eta}\gamma_a\\ &= 2^3*|\eta| + 0\\ &= 2^3*|\eta|\end{aligned}$$

y como $|\eta| = N(\alpha_1, \alpha_2, \alpha_3)$ *se tiene que*

$$8N(\alpha_1,\alpha_2,\alpha_3) = \sum_{a=1}^{p-3}\left(1+\alpha_1\left(\frac{a}{p}\right)\right)\left(1+\alpha_2\left(\frac{a+1}{p}\right)\right)\left(1+\alpha_3\left(\frac{a+2}{p}\right)\right)$$

por tanto queda demostrado. ■

Ejemplo 70 *Sea* $p = 13$ *y a continuación presentamos un gráfico circular que identifica los residuos cuadráticos y no residuos cuadráticos.*

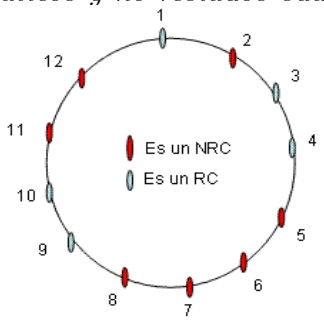


Figura 4.6: Distribución de RC y NRC para $p = 13$

$$2^3N(-1,-1,-1) = \sum_{a=1}^{10}(1-\left(\frac{a}{13}\right))(1-\left(\frac{a+1}{13}\right))(1-\left(\frac{a+2}{13}\right))$$

es igual

$$\begin{aligned}
&= (1\text{-}\left(\tfrac{1}{13}\right))(1\text{-}\left(\tfrac{2}{13}\right))(1\text{-}\left(\tfrac{3}{13}\right)) + (1\text{-}\left(\tfrac{2}{13}\right))(1\text{-}\left(\tfrac{3}{13}\right))(1\text{-}\left(\tfrac{4}{13}\right)) \\
&+(1\text{-}\left(\tfrac{3}{13}\right))(1\text{-}\left(\tfrac{4}{13}\right))(1\text{-}\left(\tfrac{5}{13}\right)) + (1\text{-}\left(\tfrac{4}{13}\right))(1\text{-}\left(\tfrac{5}{13}\right))(1\text{-}\left(\tfrac{6}{13}\right)) \\
&+(1\text{-}\left(\tfrac{5}{13}\right))(1\text{-}\left(\tfrac{6}{13}\right))(1\text{-}\left(\tfrac{7}{13}\right)) + (1\text{-}\left(\tfrac{6}{13}\right))(1\text{-}\left(\tfrac{7}{13}\right))(1\text{-}\left(\tfrac{8}{13}\right)) \\
&+(1\text{-}\left(\tfrac{7}{13}\right))(1\text{-}\left(\tfrac{8}{13}\right))(1\text{-}\left(\tfrac{9}{13}\right)) + (1\text{-}\left(\tfrac{8}{13}\right))(1\text{-}\left(\tfrac{9}{13}\right))(1\text{-}\left(\tfrac{10}{13}\right)) \\
&+(1\text{-}\left(\tfrac{9}{13}\right))(1\text{-}\left(\tfrac{10}{13}\right))(1\text{-}\left(\tfrac{11}{13}\right)) + (1\text{-}\left(\tfrac{10}{13}\right))(1\text{-}\left(\tfrac{11}{13}\right))(1\text{-}\left(\tfrac{12}{13}\right))
\end{aligned}$$

y simplicando $2^3N(\text{-}1,\text{-}1,\text{-}1) = 16$, *por tanto* $N(\text{-}1,\text{-}1,\text{-}1) = 2$.

Ahora presentamos un teorema que aparece en el texto de George Andrew probado en 1971 pero Monzingo probó estos resultados en 1985 usando otra herramienta y se remite su prueba al texto o al artículo (ver [1, 19]).

Teorema 71 *Dado p un primo impar entonces*

$$\begin{aligned}
8N(\alpha,\beta,\gamma) \quad &= (p-3) - (\beta+\gamma+\alpha\beta+\alpha\gamma+\beta\gamma)\text{-}(\alpha+\beta+\alpha\gamma)_1\left(\tfrac{-1}{p}\right) - \alpha\left(\tfrac{-2}{p}\right) \\
&-(\gamma+\alpha\beta+\beta\gamma)\left(\tfrac{2}{p}\right) + \alpha\beta\gamma\sum_{a=1}^{p-3}\left(\tfrac{a}{p}\right)\left(\tfrac{a+1}{p}\right)\left(\tfrac{a+2}{p}\right)
\end{aligned}$$

Prueba. *(ver [19, 1]).* ■

El siguiente corolario es presentado explícitamente en Monzingo (ver [19]).

Corolario 72 *Sea p un primo entonces*

1. *Si* $p \equiv 3 \bmod 8$, *entonces*

$$8N(\alpha,\beta,\gamma) = p-3$$

.

2. *Si* $p \equiv 7 \bmod 8$, *entonces*

$$8N(\alpha,\beta,\gamma) = p-3-2[\alpha(\beta-1)+\gamma(1+\beta)]$$

.

3. Si $p \equiv 5 \bmod 8$, *entonces*

$$8N(\alpha,\beta,\gamma) = p - 3 - 2(\beta + \alpha\gamma) + \alpha\beta\gamma \sum_{a=1}^{p-3} \left(\frac{a}{p}\right)\left(\frac{a+1}{p}\right)\left(\frac{a+2}{p}\right)$$

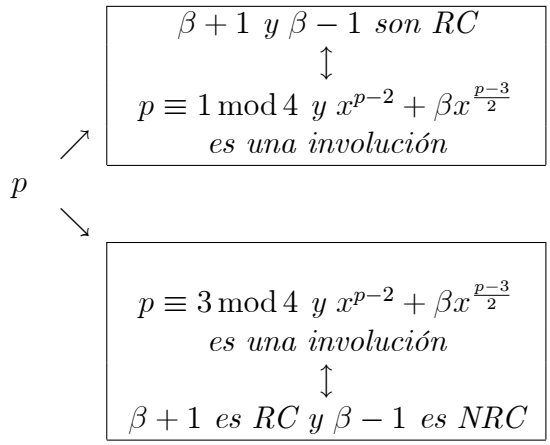
.

4. Si $p \equiv 1 \bmod 8$, *entonces*
$8N(\alpha,\beta,\gamma) = p - 3 - 2\left[\alpha\,(1+\beta) + \beta\,(1+\gamma) + \gamma\,(1+\alpha)\right] + \alpha\beta\gamma \sum_{a=1}^{p-3} \left(\frac{a}{p}\right)\left(\frac{a+1}{p}\right)\left(\frac{a+2}{p}\right)$.

Prueba. *(Ver [19]).* ■

Recordemos que unos de los objetivos de esta sección, se debió al estudio del conteo de polinomios de permutación o SDF de la forma $f(x) = x^{p-2} + \beta x^{\frac{p-3}{2}}$ que no son de punto fijo sobre $\mathbb{Z}_p$. Para el caso de SDF f invertibles sobre $\mathbb{Z}_p$ (si existe el SDF f^{-1}), estos no son de punto fijo, es decir, el SDF f contiene ciclos de longitud mayor que 1. Aún más, se dice que f es una involución, si $f = f^{-1}$. El siguiente teorema muestra la relación sobre la distribución de ternas consecutivas de RC y NRC con estos sistemas. Iniciemos con una conexión importante establecidad por Colón-Cáceres (ver [6]).

Teorema 73 (Colón-Cáceres) *Sea* p *un primo impar* $f(x) = x^{p-2} + \beta x^{\frac{p-3}{2}}$ *entonces*



El corolario 72 y el teorema de Colón-Cáceres permiten buscar el conteo de estas involuciones usando el número ternas consecutivas de RC o NRC sin importar el valor del símbolo de Legendre del medio de tres símbolos de legendre consecutivos para un primo impar. Este conteo se determinó durante la investigación y se estableció lo siguiente:

Teorema 74 *Sea* p *un primo entonces*

$p \equiv 1 \bmod 4$	$\nearrow$	$p \equiv 1 \bmod 8$	$N(1,\lambda,1) = \frac{P-9}{4}$
	$\searrow$	$p \equiv 5 \bmod 8$	$N(1,\lambda,1) = \frac{P-5}{4}$
$p \equiv 3 \bmod 4$	$\nearrow$	$p \equiv 3 \bmod 8$	$N(-1,\lambda,1) = \frac{P-3}{4}$
	$\searrow$	$p \equiv 7 \bmod 8$	$N(-1,\lambda,1) = \frac{P-7}{4}$

Prueba. Tomemos $p \equiv 1 \bmod 4$, y por el teorema de Colón-Cáceres $\beta+1$ y $\beta-1$ son RC y β RC o NRC, es decir,

$$\left(\frac{\beta-1}{p}\right) = 1,\ \lambda = \left(\frac{\beta}{p}\right), \left(\frac{\beta+1}{p}\right) = 1$$

por el corolario 72 se divide en los siguientes dos casos: cuando $p \equiv 1 \bmod 8$,

$$8N(1,1,1) = p - 15 + \sum_{a=1}^{p-3} \left(\frac{a}{p}\right)\left(\frac{a+1}{p}\right)\left(\frac{a+2}{p}\right)$$

y

$$8N(1,-1,1) = p - 3 - \sum_{a=1}^{p-3} \left(\frac{a}{p}\right)\left(\frac{a+1}{p}\right)\left(\frac{a+2}{p}\right)$$

y sumamos estas dos ecuaciones se tiene

$$8N(1,\lambda,1) = 8\left[N(1,1,1) + N(1,-1,1)\right] = 2p - 18$$

por tanto $N(1,\lambda,1) = \frac{p-9}{4}$, similarmente cuando $p \equiv 5 \bmod 8$ entonces $N(1,\lambda,1) = \frac{P-5}{4}$. Ahora si tomamos el caso cuando $p \equiv 3 \bmod 4$, y por el teorema de Colón.Cáceres $\beta+1$ es RC, $\beta-1$ es NRC y β RC o NRC, es decir,

$$\left(\frac{\beta-1}{p}\right) = -1, \lambda = \left(\frac{\beta}{p}\right), \left(\frac{\beta+1}{p}\right) = 1$$

por el corolario 72 se divide en los siguientes dos casos: cuando $p \equiv 3 \bmod 8$,

$$8N(-1,1,1) = p - 3 \text{ y } 8N(-1,-1,1) = p - 3$$

y sumamos estas dos expresiones se tiene

$$8N(-1,\lambda,1) = 8\left[N(-1,1,1) + N(-1,-1,1)\right] = 2p-6$$

por tanto $N(-1,\lambda,1) = \frac{p-3}{4}$, similarmente cuando $p \equiv 7 \bmod 8$ entonces

$$N(-1,\lambda,1) = \frac{p-7}{4}$$

por tanto queda demostrado. ■
Precisamente los teoremas 73 y 74 permiten contar el número de SDF de la forma $x^{p-2} + \beta x^{\frac{p-3}{2}}$ convolutivos, es decir, son SDF que tienen ciclos no triviales. Este conteo se presenta en la siguiente proposición.

Proposición 75 *El número de involuciones de la forma* $f(x) = x^{p-2} + \beta x^{\frac{p-3}{2}}$ *para p primo impar esta dado:*

1. *Si* $p \equiv 1 \bmod 8$, $N(1,\beta,1) = \frac{P-9}{4}$
2. *Si* $p \equiv 5 \bmod 8$, $N(1,\beta,1) = \frac{P-5}{4}$.
3. *Si* $p \equiv 3 \bmod 8$, $N(-1,\beta,1) = \frac{P-3}{4}$.
4. *Si* $p \equiv 7 \bmod 8$, $N(-1,\beta,1) = \frac{P-7}{4}$.

1. Para $p = 13$, el número de involuciones de la forma $x^{p-2} + \beta x^{\frac{p-3}{2}}$ son 2, verificando con la siguiente tabla

a	1	2	3	4	5	6	7	8	9	10	11	12
$\left(\frac{a}{13}\right)$	1	−1	1	1	−1	−1	−1	−1	1	1	−1	1

se tiene que $13 \equiv 5 \bmod 8$ y $N(1,\beta,1) = \frac{13-5}{4} = \frac{8}{4} = 2$.

2. Para $p = 23$, el número de involuciones de la forma $x^{p-2} + \beta x^{\frac{p-3}{2}}$ son 4, verificando con la siguiente tabla

a	1	2	3	4	5	6	7	8	9	10	11
$\left(\frac{a}{23}\right)$	1	1	1	1	−1	1	−1	1	1	−1	−1
a	12	13	14	15	16	17	18	19	20	21	22
$\left(\frac{a}{23}\right)$	1	1	−1	−1	1	−1	1	−1	−1	−1	−1

se tiene que $23 \equiv 7 \bmod 8$ y $N(-1, \beta, 1) = \frac{23-7}{4} = \frac{16}{4} = 4$.

Por consiguiente, se ha determinado cotas inferiores para el número de soluciones para un cierto SDF booleano monomial afín y se determinó por medio de la proposición 75 el número de involuciones usando la distribución de ternas consecutivas en residuos cuadrático o no residuos cuadráticos módulo un primo impar.

Capítulo 5

Conclusiones y Trabajos Futuros

5.1. Conclusiones

1. Se expone el método para transformar sistemas dinámicos finitos multidimensionales en sistemas dinámicos de una dimensión para campos finitos.

2. Se determinó una cota inferior para B_ϵ, conjunto de puntos que tiene contacto con el nodo $\in$. Para un caso particular de booleanos $B_\epsilon = 2^n - 1$.

3. Se determinó: La unión de todos los espacios fases de los sistemas dinámicos finitos booleanos monomiales afines forman el grafo simétrico de orden 2^n.

4. Se determinó el número de involuciones de la forma $x^{p-2} + \beta x^{\frac{p-3}{2}}$.

5.2. Trabajos Futuros

1. Caracterizar los SDF monomiales afines a partir de su grafo de dependencia.

2. Establecer condiciones para que el valor del cardinal de $B_\in$ sea cerrado o óptimo.

3. Establecer condiciones necesarias y suficientes para que un SDF monomial afín en general sea de punto fijo.

Bibliografía

[1] Andrews, George E. Number Theory, Dover Publications, Inc. New York, 1971.

[2] Apostol, Tom, Introduction to Analytic Number Theory, Springer; May 28, 1998.

[3] Bollman D., O. Colón-Reyes, y O. Edusmildo, Fixed Point in Discret Models for Regulatory Genetic Networks, EURASIP Journal on Bioinformatics and Systems Biology, Vol. 2007 (2007), Article ID 97356, 8 pages.

[4] Burton, David, Elementary Number Theory, McGraw-Hill Companies; 4th edition, August 1,

1997.

[5] Colón-Reyes, Monomial Dynamical Systems over Finite Fields, ProQuest / UMI , Marzo 18, 2006. ISBN: 0496983520.

[6] Colón-Reyes, A. Cáceres, Some permutation polynomials, preprint, 2001.

[7] Colón-Reyes, R. Laubenbacher, A. Jarrah, and B. Sturmfelds, Monomial Dynamical Systems over Finite Fields, Complex Systems 16, 2006, 333-342.

[8] Colón-Reyes, R. Laubenbacher and B. Pareigis, Boolean Monomial Dynamical Systems. Annals of Combinatorics 8, 2004, 425-439.

[9] Cull, P., Linear analysis of switching net, kybernetik 8, 1971, 31-39.

[10] Curtis, C. W., Linear Algebra, New York Springer Verlag, 1991.

[11] Doomit, David y Foote, Richard, Abstract Algebra, Jhon Wiley and Sons, Inc. 2004.

[12] Chartrand, Gary y Lensniak, Linda, Graphs and Digraphs, The wadsworth and Brook/Cole. Mathematics Series. ED 2, 1986.

[13] Elspas, Bernard, The Theory of Autonomous Linear Sequential Networks, IRE Transactions on the Circuit Theory, CT-6, 1959, 45-60.

[14] Hernández Toledo, Rene A, Linear Finite Dynamical Systems, Communications in Algebra 33, 2005, 2977-2989.

[15] Hungeford, Algebra,New York Springer Verlag, 1974.

[16] Lidl, R., and Niederreiter, H., Finite Fields, Encyclopedia of Math and its Appl. 20, Cambridge University press, London, 1997.

[17] Lidl, R., and Pilz, G., Applied Abstract Algebra. Springer Verlag, New York. 1998.

[18] Milligan, D.K., and Wilson, M.J.D., The Behavior of Affine Sequential Boolean Networks, Connection science 5, 1993, 153-167.

[19] Monzingo, M. G., On Distribution of Consecutive Triples of Quadratic and Quadratic NonResidues And Related Topic.The Fibonacci Quartely, vol 23, 1985, 133-138.

[20] Roman Steven, Advanced Linear Algebra. Springer Verlag. 1992.

[21] Sepúlveda Leonid, Tópicos sobre Duplas y Ternas Consecutivas en Residuos Cuadráticos y No Residuos Cuadráticos módulo un primo, preprint, 2003.

[22] Terras, Audrey, Fourier Analysis on Finite Groups and Applications, London Mathematical Society Student.