ESTABILIDAD DE SISTEMAS DINAMICOS MONOMIALES SOBRE CUERPOS FINITOS

Por

Germán Gómez Angarita

Tesis presentada en cumplimiento parcial de los requisitos para el grado de:

MAESTRÍA EN CIENCIAS

en

MATEMÁTICA PURA

UNIVERSIDAD DE PUERTO RICO
RECINTO UNIVERSITARIO DE MAYAGÜEZ

Noviembre, 2016

Aprobada por:

Julio Barety, Ph.D Miembro, Comité Graduado	Fecha
Gabriele Castellini, Ph.D Miembro, Comité Graduado	Fecha
Victor Ocasio, Ph.D Presidente, Comité Graduado	Fecha
Mauricio Cabrera, Ph.D Representante de Estudios Graduados	Fecha
Olgamary Rivera, Ph.D Director(a) del Departamento	Fecha

Abstract of Dissertation Presented to the Graduate School
of the University of Puerto Rico in Partial Fulfillment of the
Requirements for the Degree of Master of Sciences

STABILITY OF MONOMIAL DYNAMICAL SYSTEMS OVER FINITE FIELD

By

Germán Gómez Angarita

November 2016

Chair: Victor Ocasio
Major Department: Mathematical Sciences

In 2005, Colón and others [3] gave necessary and sufficient conditions for a monomial dynamical system over a finite field to be a fixed point system, that is, all cycles are of length one. Moreover, in 2009, Ocasio, Colón and others [8] gave necessary and sufficient stabilization conditions for a boolean monomial dynamical system. We make use of such criteria to study the concept of stability over n-tuple cartesian product of the field $\mathbb{F}_q$, where $n = 2$ and $q = 2^r + 1$ prime with $r \geq 1$. This work contains necessary and sufficient conditions to determine when a monomial dynamic control system with a unique control variable over $\mathbb{F}_{2^r+1}^2$ is stabilizable.

Resumen de Disertación Presentado a Escuela Graduada
de la Universidad de Puerto Rico como requisito parcial de los
Requerimientos para el grado de Maestría en Ciencias

ESTABILIDAD DE SISTEMAS DINAMICOS MONOMIALES SOBRE CUERPOS FINITOS

Por

Germán Gómez Angarita

Noviembre 2016

Consejero: Victor Ocasio
Departamento: Ciencias Matemáticas

En 2005, Colón y otros [3] dieron condiciones suficientes y necesarias para que un sistema dinámico monomial sobre un cuerpo finito sea un sistema de punto fijo, esto es, todos los ciclos son de longitud uno. Más aún, en 2009 Ocasio, Colón y otros [8] dieron condiciones suficientes y necesarias para que un sistema dinámico booleano sea estabilizable. Utilizaremos éstos para estudiar un concepto de estabilidad sobre la n-tupla del producto cartesiano del cuerpo $\mathbb{F}_q$, donde $n = 2$ y $q = 2^r + 1$ primo con $r \geq 1$. Este trabajo contiene condiciones necesarias y suficientes para determinar cuando un sistema dinámico monomial de control con una única variable de control sobre $\mathbb{F}_{2^r+1}^2$ es estabilizable.

Dedico este trabajo a mis padres, hermanos por todo el apoyo y compresión que me han brindado.

AGRADECIMIENTOS

Quiero agradecer a Victor Ocasio, mi consejero, por toda su ayuda y guianza. También a mi comité por su estricta pero bien intencionadas revisiones y consejos.

Quiero reconocer y agradecer a todos mis compañeros y amigos que me han acompañado durante este tiempo.

Índice general

página

Índice de cuadros

Índice de figuras

Figura página

LISTA DE ABREVIATURAS

SDMC	Sistema Dinámico Monomial de Control.
SDMB	Sistema Dinámico Monomial Booleano.
spf	Sistema de Punto Fijo.
CCF	Componente Conectada Fuertemente.

LISTA DE SÍMBOLOS

$\hat{f}$	Sistema Dinámico Monomial sin variables de control.
$T(f)$	Sistema Monomial Booleano de f.
$L(f)$	Sistema lineal de f sobre el anillo $\mathbb{Z}_{q-1}$

Capítulo 1
INTRODUCCIÓN

Un sistema dinámico finito es una función $f : X \longrightarrow X$, donde X es un conjunto finito [8]. Estamos interesados en el caso $X = \mathbb{F}_q^n$, donde $\mathbb{F}_q$ es un cuerpo finito y q es primo. La dinámica de f es generada por iteraciones de f y se codifica en su *espacio fase* $S(f)$, que es un grafo dirigido. Los vértices de $S(f)$ son los elementos de X. Existe una arista dirigida $a \longrightarrow b$ en $S(f)$ si $f(a) = b$. En particular, una arista dirigida de un vértice a sí mismo es admisible [4]. Decimos que el espacio fase de f, $S(f)$ contiene un ciclo de longitud $t > 0$ si existe $a \in \mathbb{F}_q^n$ tal que $f^t(a) = a$ y no existe un t' más pequeño tal que $f^{t'}(a) = a$. Cada componente conexa del grafo de $S(f)$ consiste de un ciclo dirigido. Decimos que f es un *sistema de punto fijo*(spf) si todos los ciclos de f tienen longitud 1 [3]. Por simpleza consideramos $f = (f_1, \ldots, f_n) : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ tal que es un sistema polinomial, con cada f_i un monomial, esto es, $f_i = x_1^{a_{i1}} x_2^{a_{i2}} \cdots x_n^{a_{in}}$, con a_{ij} un entero no negativo, y por lo menos un $a_{ij} \neq 0$. Asociamos con f un Sistema Dinámico Monomial Booleano(SDMB) $T(f) : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ y un sistema lineal $L(f)$ sobre el anillo $R = \mathbb{Z}_{q-1}$ [4]. En [2], Colón y otros, hablan acerca de la importancia de esos sistemas en modelación genética y su capacidad para modelar la dinámica de la expresión de genes y relaciones entre genes. Por ejemplo, supongamos que tenemos unas series de tiempos $\{s_1, s_2, \ldots, s_t\}$, donde cada s_i es un vector de longitud n, con valores en $\mathbb{Z}_2$; es decir, $s_i = (s_{i1}, s_{i2}, \ldots, s_{in})$, $s_{ij} \in \{0, 1\}$. Podemos interpretar estos datos como una sucesión de lecturas de ARNm durante la infección de un organismo. El índice i puede ser interpretado como el tiempo en que la medida fue tomada y s_{ij} como el estado

en el que el gen j estuvo en el tiempo i, en nuestro caso 0 ó 1, ó "apagado"ó "encendido", ver [1]. Podemos obtener una función $f : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^n$, tal que $f(s_i) = s_{i+1}$. Esto significa que podemos obtener una función que modela el comportamiento de los genes durante la infección en un intervalo de tiempo. De igual manera, Sistemas dinámicos sobre el cuerpo con dos elementos pueden ser usados para modelar redes booleanas que tienen aplicaciones en la autómata celular y la biología computacional, ver [5]. Elspas menciona en [7] aplicaciones de sistemas dinámicos lineales en circuito de control por ordenador y sistemas de comunicaciones.

Un Sistema Dinámico de Control(SDC) sobre un cuerpo finito es una función $f : \mathbb{F}_q^n \times \mathbb{F}_q^m \longrightarrow \mathbb{F}_q^n$, donde q es primo y $n, m \in \mathbb{N}$. Note que $f = (f_1, f_2, \ldots, f_n)$, $f_i \in \mathbb{F}_q^n[x_1, x_2, \ldots, x_n, u_1, \ldots, u_m]$. Llamamos $\{x_1, x_2, \ldots, x_n\}$ el conjunto de *variables estado* y $\{u_1, u_2, \ldots, u_m\}$ el conjunto de *variables control* [1], [8]. Un SDC es llamado *estabilizable* si existe una función $g : \mathbb{F}_q^n \hookrightarrow \mathbb{F}_q^n \times \mathbb{F}_q^m$, $g = (u_1, \ldots, u_m)$ y cada

$u_i = x_1^{a_{i1}} x_2^{a_{i2}} \cdots x_n^{a_{in}}$ con a_{ij} un entero no negativo, llamada *controlador de realimentación*, tal que la composición $f \circ g : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ es un sistema de punto fijo [8]. Para el caso booleano, criterios para determinar si un SDC es estabilizable han sido encontrados [1], [8]. Criterios para determinar cuando un sistema dinamico finito, $f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$, es un spf, son escasos. En 2005, Colón, ver [3], da criterios para que un sistema dinámico monomial sobre un cuerpo finito sea un spf. Tal criterio depende en determinar cuando una matriz n-dimensional $L(f)$ sobre el anillo $\mathbb{Z}_{q-1}$ es un spf también. En [9] se dan condiciones suficientes y necesarias para que los sistemas dinámicos lineales sean un sistema de punto fijo, pero el autor no considera el papel que estos criterios juegan en la estabilización de un SDC. Además, los resultados son algebraicos y no prácticos desde un punto de vista computacional. Nuestro propósito

es clasificar los Sistemas Dinámicos Monomiales de Control (SDMC) que son estabilizables. Si es posible, dado un SDMC estabilizable hallar una función controladora de realimentación. Trabajaremos con $f : \mathbb{F}_{2^r+1}^n \longrightarrow \mathbb{F}_{2^r+1}^n$, siempre que $2^r + 1$ sea un número primo, con r un número positivo y $n = 2$.

En el Capítulo 2, discutiremos resultados previos que establecen criterios para que un sistema dinámico finito sea un spf. Primero daremos criterios para que un sistema dinámico Booleano $T(f)$ sea un spf. Tambien discutiremos un criterio para que un sistema dinámico sobre un cuerpo finito sea un spf, que nos dice que f es un spf si y sólo si $T(f)$ y $L(f)$ ambos son un spf [3]. Además, definiremos la Forma Normal Smith(FNS) de una matriz y un resultado importante de [6]. Ese resultado será la herramienta básica para obtener las condiciones necesarias y suficientes para que un sistema dinámico de control sobre el cuerpo $\mathbb{F}_{2^r+1}$ sea estabilizable. En el Capítulo 3, definimos lo que es *marcar* una fila de $L(f)$. Definiremos formalmente lo que es un Sistema Dinámico Monomial de Control y encontramos criterios para que un Sistema Dinámico Monomial de Control(SDMC) sobre el cuerpo $\mathbb{F}_{2^r+1}$ sea estabilizable.

Capítulo 2
PRELIMINARES SOBRE SISTEMAS DINÁMICOS

Los resultados que vamos a presentar en este capítulo ya han sido publicados en [3], [8], [4], [5], [6].

Recuerde que un sistema dinámico monomial finito(SDM) es una función f de X a sí mismo, $f : X \longrightarrow X$, donde $X = \mathbb{F}_q^n$, con q un número primo. Consideraremos $f = (f_1, \ldots, f_n)$ con cada f_i un *monomial*, esto es, $f_i = x_1^{a_{i1}} x_2^{a_{i2}} \ldots x_n^{a_{in}}$, con a_{ij} entero no negativo y por lo menos un $a_{ij} \neq 0$. Estamos interesados en sistemas de punto fijo (spf), esto es, en sistemas dinámicos finitos en el que todos los ciclos tienen longitud 1. Asociamos con f un sistema monomial Booleano $T(f)$ y un sistema lineal $L(f)$ sobre el anillo $\mathbb{Z}_{q-1}$, los cuales definiremos formalmente más adelante. Mostraremos que $T(f)$ es un sistema de punto fijo si y sólo si cada componente conectada fuertemente del grafo de dependencia de $T(f)$ tiene

número ciclo 1. También discutiremos un resultado importante en [3] que dice que f es un spf si y sólo si $T(f)$ y $L(f)$ son ambos un spf.

Comenzaremos la discusión de sistemas dinámicos discutiendo algunos conceptos de grafos dirigidos. Para una exposición más a fondo sobre la relación entre grafos dirigidos y SDM veáse [3], [8].

Definición 2.1 (Definición 2.2.1, [8]). *Un camino p de longitud r en un grafo es una sucesión de vértices $(v_1, v_2, \ldots, v_r)$ donde cada (v_j, v_{j+1}) es conectado por una arista. Denotamos el camino p por $p : v_j \longrightarrow v_i$ y la longitud de p por $r = |p|$. Si un camino comienza y termina sobre el mismo vértice entonces es llamado un camino*

cerrado.

La idea del soporte de un vector es lo que nos permite asociar un SDM con un grafo dirigido de una manera natural.

Definición 2.2 (Definición 2.1,[5]). *Para $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$, definimos soporte de a, denotado por $supp(a) = (b_1, \ldots, b_n)$, donde*

$$b_i = \begin{cases} 1 & si\ a_i \neq 0; \\ 0 & si\ a_i = 0. \end{cases}$$

El sistema monomial $f = (f_1, \ldots, f_n)$ induce un sistema monomial Booleano $T(f) = (g_1, \ldots, g_n)$ sobre $\mathbb{F}_2^n$ con $g_i = x_1^{b_{i1}} \cdots x_n^{b_{in}}$ y para todo i, $(b_{i1}, \ldots, b_{in}) = supp(a_{i1}, \ldots, a_{in})$.

Note que si f es un SDM con $f_i \in \mathbb{F}_q^n[x_1, \ldots, x_n]$ entonces $T(f) \in \mathbb{F}_q^n[x_1, \ldots, x_n]$ es un SDMB.

Definición 2.3 (Definición 2.1.1, [3]). *Sea f un SDM, definimos el grafo de dependencia de f, como el digrafo que consiste de un conjunto de vértices $V = \{v_1, \ldots, v_n\}$ tal que existe una arista dirigida de v_i a v_j, es decir, $v_i \longrightarrow v_j$ si x_j es un factor de f_i.*

Aristas $v_i \longrightarrow v_i$ estan permitidas. Tales aristas ocurren si f_i tiene el factor x_i. Note que el sistema monomial $T(f)$ es completamente codificado por el grafo de dependencia $\mathcal{X}$.

Ejemplo 2.4. *Supongamos un $f = (x_2^3x_3^5, x_1^2x_2^4, x_1^2x_3^5) : \mathbb{F}_7^3 \longrightarrow \mathbb{F}_7^3$. Entonces, $T(f) = (x_2x_3, x_1x_2, x_1x_3)$. El grafo de dependencia $\mathcal{X}$ es:*

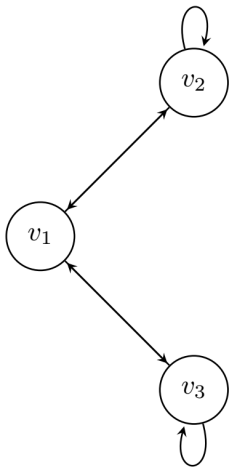

Figura 2–1: Grafo de Dependencia

Ahora definiremos una relación de equivalencia en el grafo de dependencia en el cual dos vértices a y b son equivalentes si y sólo si a y b están en una componente conectada fuertemente.

Definición 2.5 (Definición 2.2.1, [5]). *Supongamos $\mathcal{X}$ es el grafo de dependencia de f, SDM.*

1. *Para vértices $a, b \in \mathcal{X}$, decimos que a y b estan conectados fuertemente, y escribimos $a \backsim b$, si y sólo si existe un camino $p : a \longrightarrow b$ y un camino $q : b \longrightarrow a$. Observe que siempre existe un camino de longitud cero (el camino vacío) de $b \longrightarrow b$.*
2. *La clase de equivalencia de $a \in \mathcal{X}$ bajo $\backsim$ es llamada una componente conectada fuertemente(CCF).*

Definición 2.6 (Definición 2.3.1, [3]). *Supongamos que $\mathcal{X}$ el grafo de dependencia de f y donde f es un SDM. El número ciclo de $b \in \mathcal{X}$, $\mathcal{L}(b)$, es el mínimo de todos los números $t \geq 1$ con $t = |q| - |p|$ para todos los caminos cerrados $p, q : b \longrightarrow b$. Si no existen caminos cerrados de b a b entonces el número ciclo es cero.*

El siguiente Lema, nos dice que para $a, b \in \mathcal{X}$, el número ciclo es invariante, $\mathcal{L}(a) = \mathcal{L}(b)$, si $\mathcal{X}$ es una CCF.

Lema 2.6.1 (Lema 2.3.3, [3]). *El número ciclo es constante sobre cualquier CCF, por lo que el número ciclo de una CCF es un número bien definido.*

El siguiente lema establece una relación entre el número ciclo y las longitudes de los caminos en $\mathcal{X}$.

Lema 2.6.2 (Lema 2.3.4, [3]). *Supongamos que el número ciclo de $\mathcal{X}$ es t. Supongamos $p' : b_i \longrightarrow b_j$ y $q' : b_i \longrightarrow b_j$ son caminos. Entonces $|p'| - |q'| \in (t) \subseteq \mathbb{Z}$, donde (t) es el ideal generado por t.*

Resultados que se encuentran en [4] establecen la relación entre el espacio fase de f y su grafo de dependencia. La idea es asociar la CCF de un grafo de dependencia con el espacio fase de un t-gono dirigido. El espacio fase de este t-gono es isomorfo a una acción sobre un hipercubo en $\mathbb{F}_2^t$. Estos resultados producen como consecuencia el Teorema 2.7 y el Teorema 2.8.

Teorema 2.7 (Corolario 2.3.17, [3]). *Supongamos $\mathcal{X}$ es una CCF y es el grafo de dependencia de f. El sistema $T(f)$ es un sistema de punto fijo si y sólo si el número ciclo de $\mathcal{X}$ es 1.*

Teorema 2.8 (Teorema 2.2.13, [8]). *Supongamos que $\mathcal{X}$ es el grafo de dependencia de f.*

$T(f)$ es un sistema de punto fijo si y sólo si el número ciclo de cada CCF de $\mathcal{X}$ es 1.

Aunque el sistema $T(f)$ y el grafo de dependencia proveen una idea sobre el comportamiento de un sistema dinámico monomial finito, f, no son suficientes para determinar cuando es de punto fijo. Por ejemplo, considere $f = (x_1^3x_2, x_1^4x_2) : \mathbb{F}_5^2 \longrightarrow \mathbb{F}_5^2$, Su $T(f) = (x_1x_2, x_1x_2)$ es un spf ya que por el Teorema 2.7, la CCF tiene número ciclo 1. Pero f no es un spf, ya que en el espacio fase se encuentra el ciclo $(1,2) \to (2,2) \to (1,2)$. Por lo tanto definiremos un sistema lineal n-dimensional, $L(f)$, sobre un anillo finito, para analizar el comportamiento de f.

Definición 2.9 (Definición 3.1.1, [3]). *Dado un cuerpo finito $\mathbb{F}_q^n$, y una función $f = (f_1, \ldots, f_n) : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$, donde $f_i \in \mathbb{F}_q^n[x_1, \ldots, x_n]$, $f_i = x_1^{a_{i1}} x_2^{a_{i2}} \cdots x_n^{a_{in}}$. Definimos $g_i = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n$ en $\mathbb{Z}_{q-1}[x_1, \ldots, x_n]$ y defina $L(f) : \mathbb{Z}_{q-1}^n \longrightarrow \mathbb{Z}_{q-1}^n$ como $L(f)(\vec{x}) := (g_1(\vec{x}), g_2(\vec{x}), \ldots, g_n(\vec{x}))$. Llamamos $L(f)$ el log de f.*

Note que la representación matricial de $L(f)$ puede ser escrita como:

$$A_L = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

Abusamos de la notación y de ahora en adelante consideraremos $L(f)$ como la representación matricial A_L.

Ejemplo 2.10. *Consideremos $f = (x_1^2, x_1^2 x_2) : \mathbb{F}_3^2 \longrightarrow \mathbb{F}_3^2$. Entonces $L(f) = \begin{pmatrix} 2 & 0 \\ 2 & 1 \end{pmatrix}$*

Ahora, mencionaremos un resultado importante de [3], que da condiciones suficientes y necesarias para que un SDM sea un spf.

Criterios para que un sistema dinámico monomial booleano sea un spf fueron establecidos. Omar Colón en [3] da condiciones suficientes y necesarias para que el sistema lineal dinámico $L(f)$ sea spf. Con estas teorías podemos dar el siguiente Teorema que es una caracterización para que un sistema dinámico monomial sobre cualquier cuerpo finito de cualquier dimensión sea un spf.

Teorema 2.11 (Corolario 3.1.14, [3]). *Supongamos $f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ es un SDM. Entonces f es un spf si y sólo si $T(f)$ y $L(f)$ son spf.*

La siguiente definición nos dará una herramienta eficaz para determinar cuando un sistema lineal sea un spf.

Definición 2.12 (Definición 3.2, [6]). *Supongamos R es un anillo de ideal principal y $A \in R^{n\times n}$. Existen matrices invertibles $U, V \in R^{n\times n}$ tales que*

$$FNS(A) = UAV = \begin{pmatrix} s_1 & & & & & \\ & \ddots & & & & \\ & & s_m & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

donde $s_i \mid s_{i+1}$ para $1 \leq i \leq m-1$. $FNS(A)$ es llamado la Forma Normal de Smith(FNS) de A. Las entradas diagonales s_i son llamados los factores invariantes de A que son únicos módulo multiplicación por una unidad. Supongamos que M es un ideal propio de R y ψ es una función canónica de R en $\frac{R}{M}$. Los elementos $\psi(s_i)$ en $\frac{R}{M}$ son llamados los factores invariantes de A sobre $\frac{R}{M}$.

En la definición anterior nosotros vamos a tomar $R = \mathbb{Z}$, al calcular la FNS de un sistema lineal sobre $\mathbb{Z}$ obtenemos los factores invariantes s_i y despues utilizamos la función $\psi(s_i)$ en $\mathbb{Z}_n$ para analizar la imagen de los factores invariantes.

Al calcular la FNS de una matriz $A \in \mathbb{Z}^{2\times 2}$, para encontrar las matrices invertibles U y V como en la definición anterior, no es tarea fácil y por lo tanto la siguiente Proposición nos provee un algoritmo para calcular la FNS de la matriz $A \in \mathbb{Z}^{2\times 2}$.

Lema 2.12.1. *Supongamos* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2\times 2}$ *y* $gcd(a,b,c,d) = 1$. *Entonces* $FNS(A) = \begin{pmatrix} 1 & 0 \\ 0 & ad-bc \end{pmatrix}$.

Demostración. *Supongamos únicamente que* $gcd(a,b) = 1$, *entonces existen* x_1, x_2 *enteros tales que,* $1 = ax_1 + bx_2$. *Entonces,*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 & -b \\ x_2 & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \underbrace{cx_1 + dx_2}_{u_1} & ad-bc \end{pmatrix}$$

Note que:

$$\begin{pmatrix} x_1 & -b \\ x_2 & a \end{pmatrix}^{-1} = \tfrac{1}{(ax_1+bx_2)} \times \begin{pmatrix} a & b \\ -x_2 & x_1 \end{pmatrix} = \begin{pmatrix} a & b \\ -x_2 & x_1 \end{pmatrix}.$$

Por lo tanto, $\begin{pmatrix} x_1 & -b \\ x_2 & a \end{pmatrix}$, *es invertible.*

Por tanto, $\begin{pmatrix} 1 & 0 \\ -u_1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ u_1 & ad-bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & ad-bc \end{pmatrix}$

Similarmente, si únicamente $gcd(c,d) = 1$, *simplemente,*

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$, *volvemos al caso anterior y por tanto* $FNS(A) = \begin{pmatrix} 1 & 0 \\ 0 & ad-bc \end{pmatrix}$.

Ahora, supongamos que únicamente $gcd(a,c) = 1$, *entonces existen* x_3, x_4 *enteros tales que,* $1 = ax_3 + cx_4$. *Por tanto,* $\begin{pmatrix} x_3 & x_4 \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & \overbrace{bx_3 + dx_4}^{v_1} \\ 0 & ad-bc \end{pmatrix}$

$$\begin{pmatrix} 1 & v_1 \\ 0 & ad-bc \end{pmatrix} \begin{pmatrix} 1 & -v_1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & ad-bc \end{pmatrix}.$$

Similarmente, si únicamente $gcd(b,d) = 1$, *simplemente* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & a \\ d & c \end{pmatrix}$, *volvemos al caso anterior y por tanto* $FNS(A) = \begin{pmatrix} 1 & 0 \\ 0 & ad-bc \end{pmatrix}$.

Supongamos que únicamente $gcd(a,d) = 1$. *Por tanto, para* $e = gcd(a,c)$ *existen* y_1, y_2 *enteros tales que,* $e = gcd(a,c) = ay_1 + cy_2$. *Por lo tanto,*

$$\begin{pmatrix} y_1 & y_2 \\ \frac{-c}{e} & \frac{a}{e} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} e & \overbrace{by_1 + dy_2}^{u} \\ 0 & \frac{ad-bc}{e} \end{pmatrix}.$$

Ahora supongamos que $e_1 = gcd(e,u) = ey_3 + uy_4$, *con* y_3, y_4 *enteros.*

Además, note que $e_1 \mid e \iff (e) \subseteq (e_1)$, *donde* (e) *es el ideal generado por* $e \in \mathbb{Z}$.

Por tanto,

$$\begin{pmatrix} e & u \\ 0 & \frac{ad-bc}{e_1} \end{pmatrix} \begin{pmatrix} y_3 & \frac{-u}{e_1} \\ y_4 & \frac{e}{e_1} \end{pmatrix} = \begin{pmatrix} e_1 & 0 \\ \frac{ad-bc}{e}y_4 & \frac{ad-bc}{e}\frac{e}{e_1} \end{pmatrix} = \begin{pmatrix} e_1 & 0 \\ \frac{ad-bc}{e}y_4 & \frac{ad-bc}{e_1} \end{pmatrix}.$$

Además, dado que $e_1 \mid e$, *entonces* $\frac{ad-bc}{e} \mid \frac{ad-bc}{e_1}$. *Por tanto,* $gcd(\frac{ad-bc}{e}y_4, \frac{ad-bc}{e_1}) \neq 1$. *Si* $gcd(e_1, \frac{ad-bc}{e}y_4) \neq 1$, *entonces escogemos* $e_2 = gcd(e_1, \frac{ad-bc}{e}y_4)$, *note que* $e_1 \mid e_2$, *por lo tanto, continuando este proceso entre la primera fila y la primera columna, tendremos una sucesión de elementos* e, e_1, e_2, $\cdots$. *En términos de ideales, esto quiere decir que* $(e) \subseteq (e_1) \subseteq (e_2) \subseteq \cdots$.

Dado que cualquier sucesión creciente en un dominio de ideal principal se estabiliza, entonces existe $k \in \mathbb{Z}$ *tal que* $\forall\ n \geq k$ *y* $(e_n) = (gcd(a,d)) = (1) = \mathbb{Z}$. *Por lo tanto, volvemos a los casos anteriores y así:*

$$FNS(A) = \begin{pmatrix} 1 & 0 \\ 0 & ad-bc \end{pmatrix}.$$

Similarmente si únicamente $gcd(b,c) = 1$, *simplemente*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & a \\ d & c \end{pmatrix},$$ *volvemos al caso anterior y por tanto* $FNS(A) = \begin{pmatrix} 1 & 0 \\ 0 & ad-bc \end{pmatrix}$. □

Proposición 2.13. *Supongamos* $A \in \mathbb{Z}^{n\times n}$. *Entonces para cada,* $k \in \mathbb{Z}$, $FNS(k \cdot A) = k \cdot FNS(A)$.

Demostración. *Por la definición anterior, existen* $U, V \in \mathbb{Z}^{n\times n}$ *tales que* $FNS(A) = UAV$. *Supongamos que los factores invariantes son* s_1, s_2, *donde* $s_1 \mid s_2$. *Entonces,* $k \cdot FNS(A) = k(UAV) = U(k \cdot A)V$, *note que* $(k \cdot s_i) \mid (k \cdot s_{i+1})$. *Por tanto,* $FNS(k \cdot A) = k \cdot FNS(A)$.

La siguiente Proposición es el algoritmo que estaremos usando para calcular la FNS de una matriz $A \in \mathbb{Z}^{2\times 2}$.

Proposición 2.14. *Supongamos que* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2\times 2}$, *y además que* $gcd(a,b,c,d) = e$. *Entonces,* $FNS(A) = \begin{pmatrix} e & 0 \\ 0 & \frac{ad-bc}{e} \end{pmatrix}$.

Demostración. *Sea* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Entonces, $\frac{1}{e}A = \begin{pmatrix} \frac{a}{e} & \frac{b}{e} \\ \frac{c}{e} & \frac{d}{e} \end{pmatrix}$.

Por lo tanto, dado que $gcd(\frac{a}{e}, \frac{b}{e}, \frac{c}{e}, \frac{d}{e}) = 1$, *entonces por el lema 2.12.1,*

$$FNS(\tfrac{1}{e}A) = \begin{pmatrix} 1 & 0 \\ 0 & \frac{a}{e}\frac{d}{e} - \frac{b}{e}\frac{c}{e} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{ad}{e^2} - \frac{bc}{e^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{ad-bc}{e^2} \end{pmatrix}$$

Entonces, por la Proposición 2.13,

$$FNS(A) = e \cdot FNS(\tfrac{1}{e}A) = \begin{pmatrix} e & 0 \\ 0 & e \times \frac{ad-bc}{e^2} \end{pmatrix} = \begin{pmatrix} e & 0 \\ 0 & \frac{ad-bc}{e} \end{pmatrix}.$$

Por lo tanto, $FNS(A) = \begin{pmatrix} e & 0 \\ 0 & \frac{ad-bc}{e} \end{pmatrix}$.

El siguiente Teorema es la base de nuestros resultados, nos provee condiciones suficientes y necesarias para que un sistema lineal sea un spf.

Teorema 2.15 (Teorema 5.2,[6]). *Supongamos* $r > 1$, p *un número primo y* L *es sistema dinámico lineal.*

$(\mathbb{Z}_{p^r}^n, L)$ *es un spf si y sólo si* $(\mathbb{Z}_p^n, L)$ *es un spf y cada factor invariante de* $L - I$ *sobre* $\mathbb{Z}_{p^r}$ *es unidad ó* 0.

Para nuestros propósitos vamos a enfocarnos en los casos donde $p = 2$ y $n = 2$. Recuerde que los ceros sobre $\mathbb{Z}_{2^r}$ son de la forma $x = 2^r k$ con $k \in \mathbb{Z}$.

Note que en $\mathbb{Z}_{2^r}$ cada elemento distinto de cero es unidad ó es divisor de cero. Por tanto, $x \in \mathbb{Z}_{2^r}$ es un divisor de cero $\Leftrightarrow$ x es par.

Definición 2.16. *Decimos que* $(\mathbb{Z}_{2^r}^2, B)$*,* B *es sistema dinámico lineal, satisface la Propiedad de la Forma Normal de Smith(PFNS) si cada factor invariante de* $B - I$ *sobre* $\mathbb{Z}_{2^r}$ *es unidad ó* 0*.*

Capítulo 3
SISTEMA DE CONTROL DINÁMICO FINITO

Dado un cuerpo finito $\mathbb{F}_q$, $q = 2^r + 1$ con $r \geq 1$ y una función $f : \mathbb{F}_q^2 \times \mathbb{F}_q \longrightarrow \mathbb{F}_q^2$, tal que $f = (f_1, f_2)$ con $f_i \in \mathbb{F}_q[x_1, x_2, u]$, para $i = 1, 2$. Nos hacemos la siguiente pregunta, ¿cualquier sistema dinámico sobre un cuerpo $\mathbb{F}_q^n$, donde $n = 2$ y $q = 2^r + 1$ primo con $r \geq 1$ puede ser manipulado para que sea un sistema de punto fijo? [8]. La respuesta es no, y en este capítulo desarrollaremos condiciones suficientes y necesarias para que f sea estabilizable.

Definición 3.1 (Definición 3.1.1,[8]). *Un Sistema Dinámico Monomial de Control(SDMC) es una función $f : \mathbb{F}_q^n \times \mathbb{F}_q^m \longrightarrow \mathbb{F}_q^n$, con q un número primo. Note que $f = (f_1, \ldots, f_n)$, y $\forall i$ $f_i \in \mathbb{F}_q[x_1, \ldots, x_n, u_1, \ldots, u_m]$ y f_i es un monomial.*
Asumiremos que $\forall i$, $f_i \not\equiv 1$. Decimos que $\{x_1, \ldots, x_n\}$, es el conjunto de variables de estado y $\{u_1, \ldots, u_m\}$, el conjunto de variables de control.

Definición 3.2 (Definición 3.1.3,[8]). *Supongamos que $f = (f_1, \ldots, f_n) : \mathbb{F}_q^n \times \mathbb{F}_q^m \longrightarrow \mathbb{F}_q^n$ es un SDMC. Decimos que f es estabilizable si existe una función $g : \mathbb{F}_q^n \hookrightarrow \mathbb{F}_q^n \times \mathbb{F}_q^m$, llamado controlador de realimentación, tal que $h := f \circ g : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ es un sistema de punto fijo.*

En ocasiones, queremos ver el comportamiento del sistema dinámico antes de intervenir y hallar el controlador de realimentación. Podemos observar este comportamiento asignando $u_i \equiv 1$ para todo $1 \leq i \leq m$.

Definición 3.3. *Supongamos que* $f : \mathbb{F}_q^n \times \mathbb{F}_q^m \longrightarrow \mathbb{F}_q^n$ *es un SDMC. Definamos* $\imath : \mathbb{F}_q^n \hookrightarrow \mathbb{F}_q^n \times \mathbb{F}_q^m$ *tal que* $\imath(x_1, \ldots, x_n) = (x_1, \ldots, x_n, \overbrace{1, \ldots, 1}^{m-veces})$*, denotaremos* $\hat{f} = f \circ \imath$.

Recordamos la Definición 2.2, donde definimos a $T(f)$ como la booleanización de f. Utilizaremos las siguientes observaciones y lemas para proveer una clasificación de los SDMC que son estabilizables para el caso más simple descrito en el Teorema 3.6.

Una manipulación de símbolos sencilla es suficiente para demostrar la observación a continuación.

Observación 1. *Supongamos que* $f : \mathbb{F}_q^n \times \mathbb{F}_q^m \longrightarrow \mathbb{F}_q^n$ *es un SDMC. Entonces* $\widehat{T(f)} = T(\hat{f})$.

La Observación 2, nos dice que si $T(\hat{f})$ es un spf, para cualquier función de realimentación g, si componemos el SDMC $T(f)$ con esa función g, sigue siendo un spf.

Observación 2. *Supongamos que* $f : \mathbb{F}_{2^r+1}^2 \times \mathbb{F}_{2^r+1}^m \longrightarrow \mathbb{F}_{2^r+1}^2$ *es un SDMC. Si* $T(\hat{f})$ *es un spf entonces para cualquier función* $g : \mathbb{F}_{2^r+1}^2 \hookrightarrow \mathbb{F}_{2^r+1}^2 \times \mathbb{F}_{2^r+1}^m$*, se tiene que* $T(f \circ g)$ *es un spf.*

Demostración. *Dado que* $T(\hat{f})$ *es un spf. Entonces tenemos lo siguiente:*

Supongamos que el grafo de dependencia de $T(\hat{f})$ *tiene únicamente una componente conectada fuertemente(CCF). Entonces por Teorema 2.7, el número ciclo de esa CCF es 1. Entonces cualquier valor que adquiera* u_i *únicamente estaría posiblemente agregando aristas en el grafo de dependencia de* $T(\hat{f})$*, lo cuál no cambiaría el número ciclo, que es 1. Por Teorema 2.7,* $T(f \circ g)$ *es un spf.*

Por otro lado, supongamos que el grafo de dependencia tiene dos CCF. Entonces la función g tiene las siguientes posibilidades:

(i) convertir las dos CCF en una única CCF

(ii) hace que permanezcan las dos CCF

Si se cumple la posibilidad (i)*, entonces las dos CCF se convierte en una única CCF. Como* $T(\hat{f})$ *es un spf entonces el número ciclo de la CCF es 1, ya que, el Lema 2.6.1, nos dice que el número ciclo es invariante sobre CCF. Por Teorema 2.7 entonces* $T(f \circ g)$ *es un spf.*

Por otro lado si se cumple la posibilidad (ii) *entonces dado que cada CCF tiene número ciclo 1, por Teorema 2.8 entonces* $T(f \circ g)$ *es un spf.* □

Definición 3.4. *Supongamos que* $f = (f_1, \ldots, f_n), f_i \in \mathbb{F}_q[x_1, \ldots, x_n]$ *y* $g = (g_1, \ldots, g_n)$, $g_i \in \mathbb{F}_q[x_1, \ldots, x_n]$*. Decimos que "*$f$ *divide a* g*",* $f \mid g \Longleftrightarrow \forall_i f_i \mid g_i$*.*

Dado un SDMC f, es en teoría más fácil determinar si $T(f)$ es estabilizable ya que existen criterios generales ver [8]. Ademas, para demostrar que f es estabilizable debemos hallar una función de realimentación g que estabilice simultáneamente a $T(f)$ y a $L(f)$[ver Definición 2.9]. La siguiente observación nos permite hallar una función g para f que pudiera servir para estabilizar a f si ya sabemos de antemano que $T(f)$ es estabilizable.

Observación 3. *Supongamos que* $f : \mathbb{F}_{2^r+1}^2 \times \mathbb{F}_{2^r+1}^m \longrightarrow \mathbb{F}_{2^r+1}^2$ *es un SDMC.*

$T(f) : \mathbb{F}_2^2 \times \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^2$ *es estabilizable si y sólo si existe* $g : \mathbb{F}_{2^r+1}^2 \hookrightarrow \mathbb{F}_{2^r+1}^2 \times \mathbb{F}_{2^r+1}^m$ *tal que* $T(f \circ g)$ *es un spf.*

Demostración. *Si suponemos que* $T(\hat{f})$ *es un spf, entonces por la observación 1 y 2 no hay nada que probar.*

Supongamos que $T(\hat{f})$ *no es un spf. Entonces note que* $T(\hat{f}) = (x_2, x_1)$*.*

$(\Rightarrow)$ *Dado que* $T(f)$ *es estabilizable entonces existe* $\tilde{g} : \mathbb{F}_2^2 \hookrightarrow \mathbb{F}_2^2 \times \mathbb{F}_2^m$ *tal que* $T(f) \circ \tilde{g}$ *es un spf.*

Entonces la función $\tilde{g}$ *agrega una arista* $a_{i_0} \longrightarrow a_{i_0}$ *en el grafo de dependencia de* $T(\hat{f})$*.*

Definamos $g : \mathbb{F}_{2^r+1}^2 \hookrightarrow \mathbb{F}_{2^r+1}^2 \times \mathbb{F}_{2^r+1}^m$*, tal que* $x_i^{\alpha_i} \mid \tilde{g} \longleftrightarrow x_i^{\alpha_i} \mid g$*. Entonces, el*

número ciclo de la CCF es 1, ya que g agrega una arista $a_{i_0} \longrightarrow a_{i_0}$ en el grafo de dependencia de $T(\hat{f})$, y por Teorema 2.8, $T(f \circ g)$ es un spf.

($\Leftarrow$) Por hipótesis existe $g : \mathbb{F}_{2^r+1}^2 \hookrightarrow \mathbb{F}_{2^r+1}^2 \times \mathbb{F}_{2^r+1}^m$ tal que $T(f \circ g)$ es un spf. Entonces la función g agrega una arista $a_{i_0} \longrightarrow a_{i_0}$ en el grafo de dependencia de $T(\hat{f})$.

Note que $T(g) : \mathbb{F}_2^2 \hookrightarrow \mathbb{F}_2^2 \times \mathbb{F}_2^m$, entonces $T(f) \circ T(g)$ es un spf, ya que $T(g)$ agrega una arista $a_{i_0} \longrightarrow a_{i_0}$ en el grafo de dependencia de $T(\hat{f})$, entonces en el número ciclo de la CCF es 1, y por Teorema 2.8, $T(f)$ es estabilizable. □

Recordamos la Definición 2.9, que nos define el mapa lineal $L(f)$.

Definición 3.5. *Sea u una variable de control de SDMC f. Decimos que u "marca" la i-ésima fila de $L(f)$ si $u \mid f_i$.*

El siguiente Lema nos ayudará a verificar si un sistema lineal sobre $\mathbb{Z}_2^2$ es un sistema de punto fijo. Además, nos servirá de base para utilizar el Teorema 2.15 el cuál es una herramienta esencial en nuestros resultados.

Lema 3.5.1. *Supongamos que $A \in \mathbb{Z}_2^{2\times 2}$. A no es invertible ó $A = I$ si y sólo si A es un sistema lineal de punto fijo.*

Demostración. *($\Rightarrow$) Supongamos que $A = I$, entonces A es un spf, ya que todos los ciclos límites en el espacio fase $S(A)$ son de longitud 1.*

Supongamos que A no es invertible. Entonces $det(A) = 0$. Supongamos que,

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

Entonces $a_{11}a_{22} - a_{21}a_{22} = det(A) = 0$, es decir, $a_{11}a_{22} = a_{21}a_{22}$.

Las posibilidades son:

1. $a_{11} = a_{21} = 0$
2. $a_{11} = a_{12} = 0$
3. $a_{22} = a_{21} = 0$
4. $a_{22} = a_{12} = 0$
5. $a_{11} = a_{22} = a_{12} = a_{21}$
6. $a_{22} = a_{12} = a_{21} = 0$
7. $a_{11} = a_{12} = a_{21} = 0$
8. $a_{11} = a_{22} = a_{12} = 0$
9. $a_{11} = a_{22} = a_{21} = 0$

Por tanto las posibilidades para la matriz A son:

$$\begin{pmatrix} 0 & a_{12} \\ 0 & a_{22} \end{pmatrix} \quad \begin{pmatrix} 0 & 0 \\ a_{21} & a_{22} \end{pmatrix} \quad \begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} a_{11} & 0 \\ a_{21} & 0 \end{pmatrix} \quad \begin{pmatrix} a_{11} & a_{11} \\ a_{11} & a_{11} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & 0 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 \\ 0 & a_{22} \end{pmatrix} \quad \begin{pmatrix} 0 & 0 \\ a_{21} & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & a_{12} \\ 0 & 0 \end{pmatrix}$$

Asignándole valores a $a_{ij} \in \{0, 1\}$ *para cada* i, j *tenemos que:*

$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Observando su espacio estado concluimos que cada uno de ellos es un sistema de punto fijo.

($\Leftarrow$) *Supongamos que* $A \in \mathbb{Z}_2^{2\times 2}$ *es un sistema de punto fijo. Supongamos que* A *es invertible y* $A \neq I$*. Lleguemos a una contradicción.*

Entonces, $0 \neq det(A) = a_{11}a_{22} - a_{12}a_{21}$*. Entonces las posibilidades son:*

1. $a_{12} = a_{21} = a_{22} = 1$, $a_{11} = 0$
2. $a_{11} = a_{21} = a_{22} = 1$, $a_{12} = 0$
3. $a_{11} = a_{12} = a_{22} = 1$, $a_{21} = 0$
4. $a_{11} = a_{12} = a_{21} = 1$, $a_{22} = 0$
5. $a_{11} = a_{22} = 0$, $a_{12} = a_{21} = 1$

Por lo tanto las posibilidades para la matriz A *son:*

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Observando el espacio estado de cada uno de ellos tenemos que, ninguno de ellos es un sistema de punto fijo. Por lo tanto contradice que A *es un sistema de punto fijo. Por lo tanto, lo que habíamos afirmado no puede ser cierto, esto es,* A *no es invertible ó* $A = I$*.* $\square$

Con todas las piezas necesarias, analizamos el caso $r = 1$, con $q = 2^r + 1$ primo, y proveemos condiciones suficientes y necesarias para un SDMC sea estabilizable en el caso más simple.

Teorema 3.6. *Supongamos* $f : \mathbb{F}_3^2 \times \mathbb{F}_3^m \longrightarrow \mathbb{F}_3^2$ *es un SDMC. Entonces,*

f *es estabilizable* $\Longleftrightarrow$ $T(f)$ *es estabilizable.*

Demostración. ($\Rightarrow$) *Supongamos que* f *es estabilizable, entonces existe* $g : \mathbb{F}_3^2 \hookrightarrow \mathbb{F}_3^2 \times \mathbb{F}_3^m$ *tal que* $f \circ g$ *es un spf. Por Teorema 2.11, entonces* $T(f \circ g)$ *y* $L(f \circ g)$ *ambos son un spf. Entonces* $T(f \circ g)$ *es un spf y por la observacion 3,* $T(f)$ *es estabilizable.*

($\Leftarrow$) *Dado que* $T(f) : \mathbb{F}_2^2 \times \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^2$ *es estabilizable, por la observación 3, existe* $h : \mathbb{F}_3^2 \hookrightarrow \mathbb{F}_3^2 \times \mathbb{F}_3^m$ *tal que* $T(f \circ h) : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$ *es un spf.*

Definimos $F : \mathbb{F}_3^2 \times \mathbb{F}_3^m \longrightarrow \mathbb{F}_3^2$ *un SDMC, tal que* $u_i \mid f_j \longleftrightarrow u_i \mid F_j$ *y* $x_i^{\alpha_i} \mid (f \circ h)_j \longleftrightarrow x_i^{\alpha_i} \mid F_j$. *Note que,* $T(\hat{F})$ *es un spf.*

Consideremos $L(\hat{F}) = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$.

Por lema 3.5.1, debemos encontrar $\tilde{g} : \mathbb{F}_3^2 \hookrightarrow \mathbb{F}_3^2 \times \mathbb{F}_3$ *tal que* $L(F \circ \tilde{g}) = I$ *ó* $det(L(F \circ \tilde{g})) = 0$.

Si $L(\hat{F}) = I$ *ó* $det(L(\hat{F})) = 0$, *definimos* $\tilde{g} \equiv 1$, *ya que* $\hat{F} = F \circ \tilde{g} = f \circ h$ *y así* f *sería estabilizable por lema 3.5.1.*

Si $L(\hat{F}) \neq I$ *y* $det(L(\hat{F})) \neq 0$, *tenemos dos casos:*

Caso 1

$L(\hat{F}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Se tienen las siguientes posibilidades:

(1) Si u_i marca únicamente la primera fila, defina $u_i = x_2$ y $\forall j \neq i$, $u_j = 1$ ó

(2) Si u_i marca únicamente la segunda fila, defina $u_i = x_1$ y $\forall j \neq i$, $u_j = 1$ ó

(3) Si u_i marca ambas filas, defina $u_i = x_1$ y $\forall j \neq i$, $u_j = 1$.

Note que en cada uno de ellos el $det(L(F \circ \tilde{g})) = 0$, y por lema 3.5.1, $L(F \circ \tilde{g})$ es un spf.

Caso 2

$L(\hat{F})$ es triangular. Es decir, supongamos que únicamente $a_{ij} = 0$.

Se tienen las siguientes posibilidades:

(1) Si u_s marca únicamente la fila que contiene el 0, defina $u_s = x_j$ y $\forall l \neq s$ $u_l = 1$ ó

(2) Si u_s marca únicamente la fila que no contiene el 0, defina $u_s = x_j$ y $\forall l \neq s$ $u_l = 1$ ó

(3) Si u_s marca ambas filas. Supongamos que $i \neq j$, definimos $u_s = x_i$, y $\forall l \neq s$, $u_l = 1$. Si $a_{11} = 0$, entonces definimos $u_s = x_2$ y $\forall l \neq s$, $u_l = 1$. Si $a_{22} = 0$, entonces definimos $u_s = x_1$ y $\forall l \neq s$, $u_l = 1$.

Note que en cada subcaso el $det(L(F \circ \tilde{g})) = 0$, y por lema 3.5.1, $L(F \circ \tilde{g})$ es un spf.

Sea $g : \mathbb{F}_3^2 \hookrightarrow \mathbb{F}_3^2 \times \mathbb{F}_3^m$ tal que $x_i^{\alpha_i} \mid g_j$ con $\alpha_i = max\{\alpha : x_i^{\alpha_i} \mid h_j$ ó $x_i^{\alpha_i} \mid \tilde{g}_j\}$.

Note que $f \circ g = F \circ \tilde{g}$, ya que $h \mid g$ y $\tilde{g} \mid g$.

Entonces $T(f \circ g) = T(F \circ \tilde{g})$ es un spf, por la observación 2.

Además, $L(f \circ g) = L(F \circ \tilde{g})$ *es un spf. Por lo tanto,* $f \circ g$ *es un spf y así* f *es estabilizable.* □

Ejemplo 3.7. *Supongamos* $f : \mathbb{F}_3^2 \times \mathbb{F}_3 \longrightarrow \mathbb{F}_3^2$ *es un SDMC y* $f = (x_2u, x_1)$*. Note que* $T(f) = (x_2u, x_1)$*. Si hacemos* $u = x_1$*, entonces* $T(f \circ g) = (x_1x_2, x_1)$ *que es un spf y por la Observación 3,* $T(f)$ *es estabilizable. Por Teorema 3.6,* f *también es estabilizable.*

Nota. *Denotaremos* $Bool(L(f \circ g))$*, la boolanización de* $L(f \circ g)$*, es decir,* $L(f \circ g) \in \mathbb{Z}_2^{2\times 2}$.

El Teorema 3.6, simplica el cómputo para verificar la estabilidad de un SDMC $f : \mathbb{F}_3^2 \times \mathbb{F}_3^m \longrightarrow \mathbb{F}_3^2$, ya que simplemente lo que tendríamos que verificar es si su sistema booleano $T(f)$, es estabilizable. De ahora en adelante estaremos trabajando con una única variable de control, a diferencia con el Teorema 3.6 que permite una cantidad arbitraria de variables de control. Sin embargo, note que aunque los resultados obtenidos utilizan una única variable de control, las condiciones suficientes para que f sea estabilizable con una variable de control también es suficiente para estabilizar un f con una cantidad arbitraria de variables de control.

Ahora, nos enfocaremos en el caso con $r > 1$, que es más complejo ya que el mapa lineal $L(f)$ estaría sobre el anillo $\mathbb{Z}_{2^r}$.

Asumiremos de ahora en adelante los exponentes $0 \leq a, b, c, d \leq 2^r$ de las variables de estado de f son valores en $\mathbb{Z}_{2^r}$, ya que recordamos que el mapa lineal $L(f) : \mathbb{Z}_{2^r} \longrightarrow \mathbb{Z}_{2^r}$. Además, dado que estamos en el cuerpo $\mathbb{F}_{2^r+1}$, para cada $x \in \mathbb{F}_{2^r+1}$ se tiene que $x^{2^r+1} = x$. Por tanto al estabilizar la función f no importa que tan grandes sean los exponentes α y β que estabilicen la función, siempre se pueden escoger de tal forma que se encuentren entre 0 y 2^r. Es necesario que recordemos

las definiciones 2.12 y 2.16, que definen la Forma Normal de Smith y otras cosas relacionadas, que utilizaremos de ahora en adelante en cada una de las pruebas de los Teoremas. También en cada prueba usaremos el Lema 3.5.1 y el Teorema 2.15 junto con la Proposición 2.14, que son los que nos permiten verificar si un mapa lineal es un spf. Por último, proveemos ejemplos para que el lector se familiarice con los Teoremas.

Antes de la demostraciones de los Teoremas 3.8, 3.11 recordamos el Teorema de la ecuación diofantina, bastante conocido en algebra abstracta.

La ecuación diofantina $ax+by = m$ tiene solución si y solamente si $gcd(a, b) \mid m$.

Si (x_0, y_0) es solución, también lo és:

$$x = x_0 - \frac{b}{gcd(a,b)}k$$

$$y = y_0 + \frac{a}{gcd(a,b)}k, \text{ con } k \in \mathbb{Z}.$$

Teorema 3.8. *Supongamos que* $f : \mathbb{F}_{2^r+1}^2 \times \mathbb{F}_{2^r+1} \longrightarrow \mathbb{F}_{2^r+1}^2$ *sea un SDMC con* $r > 1$. *Supongamos* $f = (x_1^a u^{\epsilon_1}, x_2^d u^{\epsilon_2})$ *con* $0 < a, d \leq 2^r$ *y* $\forall i$ $\epsilon_i \in \{0, 1\}$. *Tenemos varios casos:*

(1) Si $\epsilon_1 = 1$ *y* $\epsilon_2 = 0$. *Entonces* f *es estabilizable* $\iff d = 1$ *ó* d *es par.*

(2) Si $\epsilon_1 = 0$ *y* $\epsilon_2 = 1$. *Entonces* f *es estabilizable* $\iff a = 1$ *ó* a *es par.*

(3) Si $\epsilon_1 = 1$ *y* $\epsilon_2 = 1$. *Entonces:*

f *no es estabilizable* $\iff a - 1 = 2^n\gamma_1$, $d - 1 = 2^s\gamma_2$ *con* $0 < n, s < r$ *y* $\gamma_1, \gamma_2 \in \mathbb{Z}$ *impares y* $n = s$.

Demostración. *Dado que* $T(\hat{f}) = (x_1, x_2)$ *es un spf, por la Observación 2, solamente nos interesa encontrar una función* g *tal que* $L(f \circ g)$ *sea spf.*

$$\text{Si } L(\hat{f}) = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}.$$

$$L(\hat{f}) - I = \begin{pmatrix} a-1 & 0 \\ 0 & d-1 \end{pmatrix}.$$

$$FNS(L(\hat{f}) - I) = \begin{pmatrix} gcd(a-1, d-1) & 0 \\ 0 & \dfrac{(a-1)(d-1)}{gcd(a-1, d-1)} \end{pmatrix}.$$

Si $a-1$ *y* $d-1$ *son impares, es decir,* a *es par y* d *es par, entonces* $(L(\hat{f}), \mathbb{Z}_{2^r}^2)$ *es un spf, ya que* $gcd(a-1, d-1)$ *es impar y* $\dfrac{(a-1)(d-1)}{gcd(a-1, d-1)}$ *es impar, por tanto satisface la PFNS y además* $Bool(L(\hat{f})) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, *que es un spf, por lema 3.5.1.*

Por lo tanto es suficiente considerar los casos en que a *ó* d *sean impares.*

Prueba caso (1). *Supongamos que* $\epsilon_1 = 1$ *y* $\epsilon_2 = 0$.

($\Leftarrow$) *Supongamos que* d *es par y* a *es impar. Simplemente escogemos* $u = x_1$, *y tendríamos que ambos exponentes son pares, que anteriormente se mostró que es estabilizable.*

Supongamos que $d = 1$.

- *Si* a *es impar, simplemente* $u = x_1$, *ya que* $L(f \circ g) = \begin{pmatrix} a+1 & 0 \\ 0 & 1 \end{pmatrix}$.

$FNS(L(f\circ g)-I)=\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, *satisface la PFNS.*

Además, $Bool(L(f\circ g))=\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, *que es un spf por lema 3.5.1.*

Por lo tanto $L(f\circ g)$ *es un spf y* $T(f\circ g)$ *también lo és. Por tanto* f *es estabilizable.*

- *Si* a *es par, simplemente escogemos* $g\equiv 1$, *ya que* $L(f\circ g)=L(\hat{f})$ *y también* $FNS(L(\hat{f})-I)=\begin{pmatrix} a-1 & 0 \\ 0 & 0 \end{pmatrix}$, *satisface la PFNS.*

Además, $Bool(L(\hat{f}))=\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, *que es un spf por lema 3.5.1.*

Por lo tanto $L(f\circ g)$ *es un spf y* $T(f\circ g)$ *también lo és. Por tanto* f *es estabilizable.*

($\Rightarrow$) *Supongamos que* $d\neq 1$ *y* d *es impar. Probemos que* f *no es estabilizable. Para ello supongamos que* $u=x_1^{\alpha}x_2^{\beta}$, $L(f\circ g)=\begin{pmatrix} a+\alpha & \beta \\ 0 & d \end{pmatrix}$,

$$L(f\circ g)-I=\begin{pmatrix} a+\alpha-1 & \beta \\ 0 & d-1 \end{pmatrix}.$$

$$FNS(L(f\circ g)-I)=\begin{pmatrix} gcd(d-1,\beta,a+\alpha-1) & 0 \\ 0 & \dfrac{(d-1)(a+\alpha-1)}{gcd(d-1,\beta,a+\alpha-1)} \end{pmatrix}.$$

Note que, $(d-1)(a+\alpha-1)$ *es par, ya que,* d *es impar. Entonces consideremos lo siguiente:*

(i) Si β *es par y* $a+\alpha$ *es impar.*

(ii) Si β *y* $a+\alpha$ *ambos impares.*

(iii) Si β es de paridad arbitraria y $a+\alpha$ par.

Si (i) se cumple entonces $gcd(d-1, \beta, a+\alpha-1)$ sería un divisor de cero en $\mathbb{Z}_{2^r}$, por lo que no satisface la PFNS.

Si (ii) se cumple entonces,

$Bool(L(f \circ g)) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, no es un spf por lema 3.5.1.

Por tanto la única posibilidad es que se cumpla (iii). Dado que $(d-1)(a+\alpha-1)$ es par, para que satisfaga la PFNS, entonces $(d-1)(a+\alpha-1) = 2^r k$, para algún $k \in \mathbb{Z}$.

Entonces:

$$\begin{aligned} a+\alpha &= \frac{2^r}{d-1}k+1 \\ &= \frac{2^r}{2^s\gamma_2}k+1 \\ &= 2^{r-s}\frac{k}{\gamma_2}+1 \end{aligned}$$

donde $d-1 = 2^s\gamma_2$, con $0 < s < r$ y $\gamma_2 \in \mathbb{Z}$ impar.

Note que $a+\alpha$ es impar, lo cual es absurdo. Por lo tanto (iii) no puede cumplirse. Entonces no hay posibilidad que permita que f sea estabilizable, y así f no es estabilizable.

Prueba caso (2). *Supongamos que $\epsilon_1 = 0$ y $\epsilon_2 = 1$. De una forma análoga al caso (1), se concluye que:*

f es estabilizable $\iff a = 1$ ó a es par.

Prueba caso (3). *Supongamos que $\epsilon_1 = 1$ y $\epsilon_2 = 1$.*

($\Rightarrow$) *Para la prueba de esta implicación la haremos por contrapositivo. Supongamos que* a *es impar y* d *es par. Escogemos,* $u = x_1$.

$$L(f \circ g) = \begin{pmatrix} a+1 & 0 \\ 1 & d \end{pmatrix}, \text{ y}$$

$$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & a(d-1) \end{pmatrix}, \text{ que satisface la PFNS, ya que } a(d-1)$$

es impar. Además,

$$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \text{ que es un spf, por el lema 3.5.1. Por lo tanto } f \text{ es}$$

estabilizable.

De una manera similar, suponiendo que d *es impar y* a *es par. Escogemos,* $u = x_2$, *y tenemos que* f *es estabilizable.*

Ahora supongamos que $a = 1$. *Entonces,*

- *Si* d *es par, simplemente escogemos* $g \equiv 1$. *Entonces,*

$$L(f \circ g) = L(\hat{f}) = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}, \text{ y}$$

$$FNS(L(\hat{f}) - I) = \begin{pmatrix} d-1 & 0 \\ 0 & 0 \end{pmatrix}, \text{ que satisface la PFNS, ya que } d-1 \text{ es impar.}$$

Además,

$Bool(L(\hat{f})) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, *que es un spf por el lema 3.5.1. Por lo tanto* f *es estabilizable.*

- *Si* d *es impar, simplemente hacemos* $u = x_2$. *Entonces* $L(f \circ g) = \begin{pmatrix} 1 & 1 \\ 0 & d+1 \end{pmatrix}$, *y*

$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, *que satisface la PFNS. Además,*

$Bool(L(f \circ g)) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$, *que es un spf, por lema 3.5.1. Por lo tanto* f *es estabilizable.*

Análogamente, supongamos que $d = 1$. *Entonces,*

- *Si* a *es par, simplemente hacemos* $g \equiv 1$. *Entonces,*

$L(f \circ g) = L(\hat{f}) = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, *y*

$FNS(L(\hat{f}) - I) = \begin{pmatrix} a-1 & 0 \\ 0 & 0 \end{pmatrix}$, *que satisface la PFNS, ya que* $a - 1$ *es impar. Además,*

$Bool(L(\hat{f})) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, *que es un spf, por lema 3.5.1. Por lo tanto* f *es estabilizable.*

- *Si a es impar, simplemente hacemos $u = x_1$. Entonces,*

$L(f \circ g) = \begin{pmatrix} a+1 & 0 \\ 1 & 1 \end{pmatrix}$, *y*

$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, *que satisface la PFNS. Además,*

$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$, *que es un spf, por el lema 3.5.1. Por lo tanto f es estabilizable.*

Supongamos, $a - 1 = 2^n\gamma_1$, $d - 1 = 2^s\gamma_2$, con $\gamma_1, \gamma_2 \in \mathbb{Z}^+$ impares y $0 < n > s < r$. Sin perdida de generalidad suponemos ahora mismo que $n > s$ ó viceversa. Entonces $a \neq 1$ y $d \neq 1$.

Supongamos, $u = x_1^\alpha x_2^\beta$. Entonces:

$$L(f \circ g) = \begin{pmatrix} a+\alpha & \beta \\ \alpha & d+\beta \end{pmatrix}$$

$$FNS(L(f \circ g) - I) = \begin{pmatrix} gcd(a+\alpha-1, \alpha, \beta, d+\beta-1) & 0 \\ 0 & \dfrac{(a+\alpha-1)(d+\beta-1) - \alpha\beta}{gcd(a+\alpha-1, \alpha, \beta, d+\beta-1)} \end{pmatrix}.$$

Dado que $gcd(a+\alpha-1, \alpha, \beta, d+\beta-1) = gcd(gcd(a-1, \alpha), gcd(d-1, \beta)) \leq gcd(a-1, \alpha)$ y $gcd(a-1, \alpha) \leq a - 1 < 2^r$. Para que la PFNS se cumpla, $gcd(a+\alpha-1, \alpha, \beta, d+\beta-1)$ debe ser impar. Para ello debemos escoger α impar ó β impar. Pero si α y β son impares. Entonces,

$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, *que no es un spf por el lema 3.5.1.*

Por lo tanto debemos escoger α y β de distinta paridad. Al escoger los α y β note que $(a+\alpha-1)(d+\beta-1) - \alpha\beta$ es par. Para que satisfaga la PFNS debemos

hallar α *y* β *tales que* $(a+\alpha-1)(d+\beta-1)-\alpha\beta = 2^r k$, $k \in \mathbb{Z}$.

Entonces, $(a-1)(d-1)+(d-1)\alpha+(a-1)\beta = 2^r k$. *Por lo tanto:*
Para $k \in \mathbb{Z}$,

$$\alpha = \frac{2^r k}{d-1} - \beta\frac{a-1}{d-1} - (a-1)$$

ó

$$\beta = \frac{2^r k}{a-1} - \alpha\frac{d-1}{a-1} - (d-1)$$

Como $n > s$, *entonces escogemos,* $\beta = \gamma_2$. *Note que* β *es impar. Por tanto,*

$$\alpha = \frac{2^r}{d-1}k - \beta\frac{a-1}{d-1} - (a-1) = \frac{2^r}{d-1}k - 2^{n-s}\gamma_1 - (a-1).$$

Note que existe $k \in \mathbb{Z}$ *tal que* $\alpha \in \mathbb{Z}^+$ *con* $d-1 \mid k$ *y además*
$gcd(\alpha-1, \beta-1, a+\alpha, b+\beta) \mid d-1$, *entonces* $gcd(\alpha-1, \beta-1, a+\alpha, b+\beta) \mid k$.
Además, note que α *es par. También,*
$Bool(L(f\circ g)) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$, *que es un spf por el lema 3.5.1. Así* $(L(f\circ g), \mathbb{Z}_{2^r}^2)$ *es un spf. Entonces* f *sería estabilizable.*

($\Leftarrow$) *Supongamos que* $n = s < r$. *Entonces veamos que* f *no es estabilizable.*

Supongamos que, $a-1 = 2^n\gamma_1$, $d-1 = 2^s\gamma_2$, *con* γ_1, γ_2 *impares.*

$$\begin{aligned}\alpha &= \frac{2^r}{d-1}k - \beta\frac{a-1}{d-1} - (a-1) \\ &= \frac{2^{r-s}}{\gamma_2}k - \beta\frac{\gamma_1}{\gamma_2} - 2^n\gamma_1 \\ &= \frac{2^{r-s}k - \beta\gamma_1}{\gamma_2} - 2^n\gamma_1\end{aligned}$$

ó

$$\begin{aligned}\beta &= \frac{2^r}{a-1}k - \alpha\frac{d-1}{a-1} - (d-1)\\ &= \frac{2^{r-n}}{\gamma_1}k - \alpha\frac{\gamma_2}{\gamma_1} - 2^s\gamma_2\\ &= \frac{2^{r-n}k - \alpha\gamma_2}{\gamma_1} - 2^s\gamma_2\end{aligned}$$

Recuerde que para que f sea estabilizable en este caso, α y β deben tener paridades distintas. Hallemos la solución de la siguiente ecuación:
$2^{r-n}k - \alpha\gamma_2 = l\gamma_1$, *la cuál tiene solución, ya que,* $gcd(2^{r-n}, \gamma_2) = 1 \mid l\gamma_1$. *Además existen λ y η enteros tales que* $2^{r-n}\lambda - \eta\gamma_2 = gcd(2^{r-n}, \gamma_2) = 1$, *entonces η debe ser impar, ya que γ_2 es impar. Note que,* $k_0 = l\lambda\gamma_1$, $\alpha_0 = l\eta\gamma_1$ *son soluciones.*

Entonces las soluciones generales son:
Para $\lambda_1 \in \mathbb{Z}$,
$k = l\lambda\gamma_1 + \lambda_1\gamma_2$
$\alpha = l\eta\gamma_1 + 2^{r-n}\lambda_1$.
Por lo tanto,

$$\begin{aligned}\beta &= \frac{2^{r-n}k - \alpha\gamma_2}{\gamma_1} - 2^s\gamma_2\\ &= \frac{2^{r-n}(l\lambda\gamma_1 + \lambda_1\gamma_2) - (l\eta\gamma_1 + \lambda_1 2^{r-n})\gamma_2}{\gamma_1} - 2^s\gamma_2\\ &= \frac{2^{r-n}l\lambda\gamma_1 + 2^{r-n}\lambda_1\gamma_2 - l\eta\gamma_1\gamma_2 - \lambda_1 2^{r-n}\gamma_2}{\gamma_1} - 2^s\gamma_2\\ &= 2^{r-n}l\lambda - l\eta\gamma_2 - 2^s\gamma_2\\ &= (2^{r-n}l\lambda - 2^s\gamma_2) - l\eta\gamma_2\end{aligned}$$

Dado que, $\alpha = l\eta\gamma_1 + 2^{r-n}\lambda_1$.
Si $\lambda_1 = 0$, *entonces* $\alpha = l\eta\gamma_1$, *note que α depende de la paridad de l, ya que η y γ_1*

son impares.

Si l es par, α es par y β también es par, ya que η y γ_2 son impares.
Si l es impar, α es impar y β también es impar, ya que η y γ_2 son impares.
Por lo tanto, α y β tienen la misma paridad.

Si $\lambda_1 \neq 0$ entonces no importa la paridad que sea λ_1, siempre $2^{r-n}\lambda_1$ es par. Por lo tanto α otra vez depende de la paridad de l y así volvemos al caso cuando $\lambda_1 = 0$, y por tanto α y β tienen la misma paridad. Análogamente, si hallamos la solución de $2^{r-s}k - \beta\gamma_1 = l\gamma_2$, también α y β tienen la misma paridad.
Por lo tanto, f no es estabilizable. □

Veamos los siguientes ejemplos del Teorema 3.8. Mostraremos un SDMC que no es estabilizable y otro que sí lo es. Pero antes que todo haremos la siguiente observación:

Observación 4. *Sea $f = (x_1^{\alpha_1}x_2^{\alpha_2}, x^{\alpha_3}x_2^{\alpha_4})$ un SDM sobre $\mathbb{F}_{2^r+1}$ con α_1, α_2, α_3, α_4 enteros positivos. Entonces existen elementos α_1', α_2', α_3', α_4' de $\mathbb{Z}_{2^r}$ tal que $f \equiv (x_1^{\alpha_1'}x_2^{\alpha_2'}, x^{\alpha_3'}x_2^{\alpha_4'})$ y además α_i', α_i tienen la misma paridad para todo i.*

Demostración. *Supongamos sin pérdida de generalidad que $\alpha_1 \geq 2^r + 1$. Por el algoritmo de la división para α_1 y $2^r + 1$ existen enteros únicos q, r_0 tales que $\alpha_1 = q(2^r + 1) + r_0$, con $0 \leq r_0 < 2^r + 1$. Entonces*

$$\alpha_1 - 2^r q = q + r_0 \tag{3.1}$$

Dado que $x \in \mathbb{F}_{2^r+1}$, $x^{2^r+1} = x$. Entonces,
$x^{\alpha_1} = x^{q(2^r+1)+r} = (x^{2^r+1})^q x^{r_0} = x^q x^{r_0} = x^{q+r_0}$.
Si α_1 es par entonces por la fórmula 3.1, $q + r_0$ también es par.

Si α_1 es impar entonces por la fórmula 3.1, $q + r_0$ también es impar.

Note que podemos utilizar las veces que sea necesario el algoritmo de la división para encontrar un $\alpha_1' < 2^r + 1$ con $\alpha_1' \in \mathbb{Z}^+$ y con la misma paridad de α_1. De una manera similar podemos hacer lo mismo para los otros exponentes. □

Ejemplo 3.9. *Supongamos $f = (x_1^{15}u, x_2^9u)$ un SDMC sobre $\mathbb{F}_{17}^2$. Por Teorema 3.8, parte (3), f es estabilizable. Además, $\frac{8}{14} = \frac{4}{7}$, escogemos $\alpha = 7$, entonces $\beta = \frac{16}{14}k - 7 \times \frac{4}{7} - 8$. Por lo tanto, para $k = 14$,*
$\beta = \frac{16\times14}{14} - \frac{7\times8}{14} - 8 = 16 - 12 = 4$. Definamos a $u = x_1^7x_2^4$. Obtenemos,
$f \circ g = (x_1^{22}x_2^4, x_1^7x_2^{13}) = (x_1^6x_2^4, x_1^7x_2^{13})$ que es un spf.

Ejemplo 3.10. *Supongamos $f = (x_1^{13}u, x_2^3)$ un SDMC sobre $\mathbb{F}_{17}^2$. Uitilicemos la estrategia del Teorema 3.8, de la parte (1), para probar que f no es estabilizable. Supongamos que $u = x_1^\alpha x_2^\beta$. Entonces $f \circ g = (x_1^{13+\alpha}x_2^\beta, x_2^3)$. Por tanto,*
$L(f \circ g) = \begin{pmatrix} 13+\alpha & \beta \\ 0 & 3 \end{pmatrix}$.

Si β es par y α es par entonces $gcd(2, \beta, 12 + \alpha) = 2$ es un divisor de cero en $\mathbb{Z}_{16}$, que no satisface la PFNS.

Si β es impar y α es par entonces $Bool(L(f \circ g)) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, que no es un spf por Lema 3.5.1.

Por tanto la única posibilidad es que β sea de paridad arbitraria y α sea impar. Pero para que se satisfaga la PFNS, $2(12 + \alpha) = 16k$, para algún $k \in \mathbb{Z}$. Por tanto, $\alpha = 8k - 12$ es par, pero esto es una contradicción, ya que α es impar.

Por lo tanto f no es estabilizable.

El siguiente Teorema provee condiciones suficientes y necesarias para que un SDMC con dos exponentes a, d tales que $a = d = 0$ sea estabilizable.

Teorema 3.11. *Supongamos que* $f : \mathbb{F}_{2^r+1}^2 \times \mathbb{F}_{2^r+1} \longrightarrow \mathbb{F}_{2^r+1}^2$ *sea un SDMC con* $r > 1$. *Supongamos* $f = (x_2^b u^{\epsilon_1}, x_1^c u^{\epsilon_2})$ *con* $0 < b, c \leq 2^r$ *y* $\forall i\ \epsilon_i \in \{0, 1\}$. *Tenemos varios casos:*

(1) Si $\epsilon_1 = 1$ *y* $\epsilon_2 = 0$.. *Entonces* f *es estabilizable.*

(2) Si $\epsilon_1 = 0$ *y* $\epsilon_2 = 1$. *Entonces* f *es estabilizable.*

(3) Si $\epsilon_1 = 1$ *y* $\epsilon_2 = 1$. *Entonces:* f *no es estabilizable* $\iff b + 1 = 2^n\gamma_1$, $c + 1 = 2^s\gamma_2$ *con* $0 < n, s < r$ *y* $\gamma_1, \gamma_2 \in \mathbb{Z}$ *impares y* $n = s$.

Demostración. ***Prueba caso*** (1) *Supongamos que* $\epsilon_1 = 1$ *y* $\epsilon_2 = 0$. *Supongamos que* $b, c \in \mathbb{Z}$, *con* $0 < b, c \leq 2^r$. *Escogemos* $u = x_1 x_2^{2^r - b}$. *Note que,*
$T(f \circ g) = (x_1 x_2, x_1)$ *es un spf. Además,*

$$L(f \circ g) = \begin{pmatrix} 1 & 2^r \\ c & 0 \end{pmatrix},$$

$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 2^r c \end{pmatrix}$, *que satisface la PFNS, ya que* $2^r c$, *es cero sobre* $\mathbb{Z}_{2^r}$. *Además,*

$$Bool(L(f \circ g)) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$ *con* c *par y,*

$Bool(L(f \circ g)) = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$, *con* c *impar. Ambos por el lema 3.5.1, son un spf. Por lo tanto* $L(f \circ g)$*, es un spf y así* f *es estabilizable.*

Prueba caso (2) *Supongamos que* $\epsilon_1 = 0$ *y* $\epsilon_2 = 1$*. Supongamos que* $b, c \in \mathbb{Z}$*, con* $0 < b, c \leq 2^r$*. Escogemos* $u = x_1^{2^r - c} x_2$*. Note que* $T(f \circ g) = (x_2, x_1 x_2)$ *es un spf. Además,*

$$L(f \circ g) = \begin{pmatrix} 0 & b \\ 2^r & 1 \end{pmatrix},$$

$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 2^r b \end{pmatrix}$, *que satisface la PFNS, ya que* $2^r b$*, es cero sobre* $\mathbb{Z}_{2^r}$*. Además,*

$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, *con* b *par y,*

$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$, *con* b *impar. Ambos por el lema 3.5.1, son un spf. Por lo tanto* $L(f \circ g)$*, es un spf y así* f *es estabilizable.*

Prueba caso (3) *Supongamos que* $\epsilon_1 = 1$ *y* $\epsilon_2 = 1$*.*

($\Rightarrow$) *La prueba de esta implicación lo haremos por contrapositivo. Asumamos que* $u = x_1^{\alpha} x_2^{\beta}$*. Note que si* $\alpha \neq 0$ *ó* $\beta \neq 0$ *para que* $T(f \circ g)$ *es un spf. Por tanto, nos enfocaremos en encontrar una función* g*, tal que* $L(f \circ g)$ *sea un spf.*

$$L(f \circ g) = \begin{pmatrix} \alpha & b + \beta \\ c + \alpha & \beta \end{pmatrix},$$

$$FNS(L(f\circ g)-I) = \begin{pmatrix} gcd(\alpha-1,\beta-1,c+\alpha,b+\beta) & 0 \\ 0 & \dfrac{(\alpha-1)(\beta-1)-(c+\alpha)(b+\beta)}{gcd(\alpha-1,\beta-1,a+\alpha,b+\beta)} \end{pmatrix}.$$

Note que $gcd(\alpha-1,\beta-1,c+\alpha,b+\beta) = gcd(gcd(c+1,c+\alpha),gcd(b+1,b+\beta)) = gcd(gcd(c+1,\alpha-1),gcd(b+1,\beta-1))$. *Además, dado que* $gcd(c+1,c+\alpha) \leq c+1$ *y* $gcd(b+1,b+\beta) \leq b+1$. *Entonces,*
$gcd(\alpha-1,\beta-1,a+\alpha,b+\beta) \leq gcd(c+1,c+\alpha) \leq c+1$, *y también* $\leq b+1$.

• *Supongamos que* b *ó* c *ambos son pares. Entonces veamos que* f *es estabilizable. En efecto,*

Supongamos que b *y* c *ambos son pares. Entonces veamos que* f *es estabilizable. Escogemos* $u = x_1x_2$. *Además,*

$$L(f\circ g) = \begin{pmatrix} 1 & b+1 \\ c+1 & 1 \end{pmatrix},$$

$$FNS(L(f\circ g)-I) = \begin{pmatrix} gcd(b+1,c+1) & 0 \\ 0 & \dfrac{(b+1)(c+1)}{gcd(b+1,c+1)} \end{pmatrix},$$ *que satisface la PFNS, ya que,* $(c+1)(b+1)$ *es impar. Además,*

$$Bool(L(f\circ g)) = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix},$$ *que es un spf por el lema 3.5.1. Por tanto* $L(f\circ g)$ *es un spf y así* f *es estabilizable.*

Supongamos que b *es par y* c *es impar. Entonces veamos que* f *es estabilizable.*

Escogemos $u = x_2^2$, *para que* $Bool(L(f\circ g))$ *sea un spf. Además,*

$$L(f \circ g) = \begin{pmatrix} 0 & b+2 \\ c & 2 \end{pmatrix},$$

$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & (b+2)c+1 \end{pmatrix}$, *que satisface la PFNS, ya que* $(b+2)c+1$, *es impar. Además,*

$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, *que es un spf por el lema 3.5.1. Por tanto* $L(f \circ g)$ *es un spf y así* f *es estabilizable.*

Análogamente, si b *es impar y* c *es par, escogemos* $u = x_1^2$ *entonces* f *es estabilizable.*

- *Supongamos que* $b = 2^r - 1$ *ó* $c = 2^r - 1$. *Entonces, veamos que* f *es estabilizable.*

Si $b = 2^r - 1$ *entonces escogemos* $u = x_2$. *Además,*

$$L(f \circ g) = \begin{pmatrix} 0 & 2^r \\ c & 1 \end{pmatrix},$$

$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 2^r c \end{pmatrix}$, *que satisface la PFNS y además*

Si c *es par, entonces:*

$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, *que es un spf por el lema 3.5.1*

Si c *es impar, entonces:*

$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$, *que es un spf por el lema 3.5.1*

Por lo tanto f es estabilizable.

Análogamente, si $c = 2^r - 1$, escogemos $u = x_1$ para que f sea estabilizable.

- *Supongamos que $b + 1 = 2^n\gamma_1$, $c + 1 = 2^s\gamma_2$ con $\gamma_1, \gamma_2 \in \mathbb{Z}^+$ impares y $0 < n > s < r$. Sin perída de generalidad suponemos ahora mismo que $n > s$ ó viceversa.*

Recordamos que si suponemos $u = x_1^\alpha x_2^\beta$.

$$FNS(L(f\circ g)-I) = \begin{pmatrix} gcd(\alpha-1, \beta-1, c+\alpha, b+\beta) & 0 \\ 0 & \dfrac{(\alpha-1)(\beta-1)-(c+\alpha)(b+\beta)}{gcd(\alpha-1, \beta-1, c+\alpha, b+\beta)} \end{pmatrix}.$$

Note que $b \neq 2^r - 1$ y $c \neq 2^r - 1$. Entonces:
$gcd(\alpha-1, \beta-1, c+\alpha, b+\beta) \leq b+1, c+1 < 2^r$. Entonces para que la PFNS se cumpla $gcd(\alpha-1, \beta-1, c+\alpha, b+\beta)$ debe ser impar. Para ello debemos escoger α par ó β par.

Pero si α es par y β es par. Entonces:
$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, *que no es un spf, por el lema 3.5.1.*
Por lo tanto esos α y β deben ser de paridad distinta.

Al escoger los α y β note que $(\alpha-1)(\beta-1)-(c+\alpha)(b+\beta)$ es par, para que satisfaga la PFNS, debemos hallar α y β tales que $(\alpha-1)(\beta-1)-(c+\alpha)(b+\beta) = 2^r k$, para algún $k \in \mathbb{Z}$. Entonces,

$$\alpha = -\frac{2^r}{b+1}k - (\beta-1)\frac{c+1}{b+1} - c$$

ó

$$\beta = -\frac{2^r}{c+1}k - (\alpha-1)\frac{b+1}{c+1} - b$$

Como $n > s$ entonces, escogemos $\alpha = \gamma_2 + 1$, que sería par y $\beta = -\frac{2^r}{c+1}k - 2^{n-s}\gamma_1 - b$, *que sería impar, ya que b es impar. Note que existe $k \in \mathbb{Z}$ tal que $\alpha \in \mathbb{Z}^+$ con $b+1 \mid k$ y además $gcd(\alpha-1, \beta-1, a+\alpha, b+\beta) \mid b+1$, entonces $gcd(\alpha-1, \beta-1, a+\alpha, b+\beta) \mid k$. Por lo tanto f es estabilizable.*

($\Leftarrow$) *Supongamos que $n = s < r$. Entonces veamos que f no es estabilizable.*

Supongamos que, $b+1 = 2^n\gamma_1$, $c+1 = 2^s\gamma_2$.

$$\begin{aligned}\alpha &= -\frac{2^r}{b+1}k - (\beta-1)\frac{c+1}{b+1} - c \\ &= -\frac{2^{r-n}}{\gamma_1}k - (\beta-1)\frac{\gamma_2}{\gamma_1} - 2^s\gamma_2 + 1 \\ &= -\frac{2^{r-n}k + (\beta-1)\gamma_2}{\gamma_1} - 2^s\gamma_2 + 1\end{aligned}$$

ó

$$\begin{aligned}\beta &= -\frac{2^r}{c+1}k - (\alpha-1)\frac{b+1}{c+1} - b \\ &= -\frac{2^{r-s}}{\gamma_2}k - (\alpha-1)\frac{\gamma_1}{\gamma_2} - 2^n\gamma_1 + 1 \\ &= -\frac{2^{r-s}k + (\alpha-1)\gamma_1}{\gamma_2} - 2^n\gamma_1 + 1\end{aligned}$$

Recuerde que para que f sea estabilizable en este caso, α y β deben tener paridadades distintas. Hallemos la solución de la siguiente ecuación: $2^{r-n}k + (\beta-1)\gamma_2 = l\gamma_1$, *la cuál tiene solución, ya que, $gcd(2^{r-n}, \gamma_2) = 1 \mid l\gamma_1$. Además, existen λ y η enteros tales que* $2^{r-n}\lambda + \eta\gamma_2 = gcd(2^{r-n}, \gamma_2) = 1$, *entonces η debe ser impar, ya que γ_2 es impar. Note que, $k_0 = l\lambda\gamma_1$, $(\beta-1)_0 = l\eta\gamma_1$ son soluciones.*

Entonces las soluciones generales son:

Para $\lambda_1 \in \mathbb{Z}$,

$k = l\lambda\gamma_1 - \lambda_1\gamma_2$

$\beta - 1 = l\eta\gamma_1 + 2^{r-n}\lambda_1$

Por lo tanto,

$$\begin{aligned}
\alpha &= -\frac{2^{r-n}k + (\beta-1)\gamma_2}{\gamma_1} - 2^s\gamma_2 + 1 \\
&= -\frac{2^{r-n}(l\lambda\gamma_1 - \lambda_1\gamma_2) + (l\eta\gamma_1 + \lambda_1 2^{r-m})\gamma_2}{\gamma_1} - 2^s\gamma_2 + 1 \\
&= -\frac{2^{r-n}l\lambda\gamma_1 - 2^{r-n}\lambda_1\gamma_2 + l\eta\gamma_1\gamma_2 + \lambda_1 2^{r-n}\gamma_2}{\gamma_1} - 2^s\gamma_2 + 1 \\
&= -(2^{r-n}l\lambda + l\eta\gamma_2) - 2^s\gamma_2 + 1 \\
&= -(2^{r-n}l\lambda + 2^s\gamma_2) - l\eta\gamma_2 + 1
\end{aligned}$$

Dado que, $\beta = l\eta\gamma_1 + 2^{r-n}\lambda_1 + 1$.

Si $\lambda_1 = 0$, *entonces* $\beta = l\eta\gamma_1 + 1$, *note que* β *depende de la paridad de* l, *ya que* η *y* γ_1 *son impares.*

Si l *es par,* β *es impar y* α *también es impar, ya que* η *y* γ_2 *son impares*

Si l *es impar,* β *es par y* α *también es par, ya que* η *y* γ_2 *son impares*

Por lo tanto, α *y* β *tienen la misma paridad.*

Si $\lambda_1 \neq 0$ *entonces no importa la paridad que sea* λ_1, *siempre* $2^{r-n}\lambda_1$ *es par. Por lo tanto* β *otra vez depende de la paridad de* l *y así volvemos al caso cuando* $\lambda_1 = 0$, *y por tanto* α *y* β *tienen la misma paridad. Análogamente, si hallamos la solución de* $2^{r-s}k + (\alpha-1)\gamma_1 = l\gamma_2$, *también* α *y* β *tienen la misma paridad. Por lo tanto,* f *no es estabilizable.*□

Veamos los siguientes ejemplos del Teorema 3.11. Que nos mostrará SDMC que no son estabilizables y otros que sí lo son.

Ejemplo 3.12. *Supongamos* $f = (x_2^9 u, x_1^{13} u)$ *un SDMC sobre* $\mathbb{F}_{17}^2$. *Asumimos,* $b+1 = 10 = 2 \times 5$, $c+1 = 14 = 2 \times 7$, *note que* $n = s = 1$. *Por Teorema 3.11, parte* (3), f *no es estabilizable.*

Ejemplo 3.13. *Supongamos* $f = (x_2^{12}, x_1^6 u)$ *un SDMC sobre* $\mathbb{F}_{17}^2$. *Entonces en la prueba del Teorema 3.11, parte* (2), *escogemos* $u = x_1^{10} x_2$, *no es difícil comprobar que* $f \circ g = (x_2^{12}, x_1^{16} x_2)$ *es un spf.*

El siguiente Teorema provee condiciones suficientes y necesarias para que un SDMC con dos exponentes b, d tales que $b = d = 0$ sea estabilizable.

Teorema 3.14. *Supongamos que* $f : \mathbb{F}_{2^r+1}^2 \times \mathbb{F}_{2^r+1} \longrightarrow \mathbb{F}_{2^r+1}^2$ *un SDMC. Supongamos* $f = (x_1^a u^{\epsilon_1}, x_1^c u^{\epsilon_2})$ *con* $0 < a, c \leq 2^r$ *y* $\forall i \ \epsilon_i \in \{0, 1\}$. *Tenemos varios casos:*

(1) Si $\epsilon_1 = 1$ *y* $\epsilon_2 = 0$. *Entonces* f *es estabilizable.*

(2) Si $\epsilon_1 = 0$ *y* $\epsilon_2 = 1$. *Entonces* f *es estabilizable* $\iff a = 1$ *ó* a *es par.*

(3) Si $\epsilon_1 = 1$ *y* $\epsilon_2 = 1$. *Entonces* f *es estabilizable.*

Demostración. *Dado que* $T(f) = (x_1, x_1)$ *es un spf, por la observación 2, solamente nos interesa encontrar una función* g *tal que* $L(f \circ g)$ *sea un spf.*

Además,

$$L(\hat{f}) = \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix},$$

Entonces,

$$L(\hat{f}) - I = \begin{pmatrix} a-1 & 0 \\ c & -1 \end{pmatrix},$$

$$FNS(L(\hat{f}) - I) = \begin{pmatrix} 1 & 0 \\ 0 & a-1 \end{pmatrix}$$

Para que la PFNS satisfaga, $a-1$ *debe ser impar, es decir,* a *debe ser par.*

Además, note que si a *es par, entonces*

$Bool(L(\hat{f})) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, *con* c *par ó*

$Bool(L(\hat{f})) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, *con* c *impar, los cuales son un spf, por lema 3.5.1.*

Por lo tanto, $\hat{f}$ *es un spf siempre que* a *sea par. Por lo tanto, nos interesa estabilizar* f *cuando* a *sea impar.*

Además, si $a = 1$. *Entonces,*

$$L(\hat{f}) = \begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix},$$

Entonces,

$$L(\hat{f}) - I = \begin{pmatrix} 0 & 0 \\ c & -1 \end{pmatrix},$$

Entonces,

$FNS(L(\hat{f}) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, *que satisface la PFNS.*

$Bool(L(\hat{f})) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, *con* c *par ó*

$Bool(L(\hat{f})) = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$, *con* c *impar, los cuales son un spf, por lema 3.5.1.*

Así, $\hat{f}$ es un spf con $a = 1$. Por lo tanto, nos interesa estabilizar f cuando $a \neq 1$ sea impar.

Prueba caso (1).

Supongamos que $\epsilon_1 = 1$ y $\epsilon_2 = 0$. Entonces simplemente escogemos $u = x_1$, por lo tanto $a + 1$ sería par y por la parte anterior,
f es estabilizable.

Prueba caso (2)

Supongamos que $\epsilon_1 = 0$ y $\epsilon_2 = 1$. Supongamos que $u = x_1^{\alpha} x_2^{\beta}$. Entonces,

$$L(f \circ g) = \begin{pmatrix} a & 0 \\ \alpha + c & \beta \end{pmatrix},$$

Entonces,

$$L(f \circ g) - I = \begin{pmatrix} a-1 & 0 \\ \alpha + c & \beta - 1 \end{pmatrix},$$

$$FNS(L(f \circ g) - I) = \begin{pmatrix} gcd(a-1, \alpha + c, \beta - 1) & 0 \\ 0 & \dfrac{(a-1)(\beta-1)}{gcd(a-1, \alpha + c, \beta - 1)} \end{pmatrix},$$

Note que $gcd(a-1, \alpha + c, \beta - 1) \leq a - 1 < 2^r$.

Además, $(a-1)(\beta-1)$ es par, ya que a es impar, por lo tanto queremos que $(a-1)(\beta-1) = 2^r k$, para algún entero k. Es decir, $\beta = \dfrac{2^r}{a-1} k + 1$, β sería impar, ya que $a - 1 = 2^s \gamma_1$, con $\gamma_1, s \in \mathbb{Z}$, $2^{s+1} \nmid a - 1$ y $0 < s < r$. Por lo tanto, pongámosle condiciones a $\alpha + c$.

(i) Si $\alpha + c$ es par, entonces $gcd(a-1, \alpha+c, \beta-1)$ sería par, y por lo tanto $gcd(a-1, \alpha+c, \beta-1)$ sería un divisor de cero, que no satisface la PFNS.

(ii) Si $\alpha + c$ es impar, entonces,

$Bool(L(f \circ g)) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, *que no es un spf, por lema 3.5.1.*

Por lo tanto, f no es estabilizable.

Por lo tanto, si a es par ó $a = 1 \Longrightarrow f$ es estabilizable y si a es impar y $a \neq 1 \Longrightarrow f$ no es estabilizable. Esto es equivalente a decir que, f es estabilizable $\Longleftrightarrow a$ es par ó $a = 1$.

Prueba caso (3)

Supongamos que $\epsilon_1 = 1$ y $\epsilon_2 = 1$. Entonces, escogemos $u = x_1$. Entonces,

$$L(f \circ g) = \begin{pmatrix} a+1 & 0 \\ c+1 & 0 \end{pmatrix},$$

$$L(f \circ g) - I = \begin{pmatrix} a & 0 \\ c+1 & -1 \end{pmatrix},$$

$$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}.$$

Como a es impar, satisface la PFNS y además,

$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, *si c es par y*

$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, *si c es impar, los cuales son un spf, por el lema 3.5.1.*

Así $f \circ g$ es un spf, es decir, f es estabilizable. $\square$

En los ejemplos siguientes hacemos uso del Teorema 3.14. Veremos SDMC que no son estabilizables y otros que sí lo son.

Ejemplo 3.15. *Supongamos $f = (x_1^7, x_1^8 u)$ un SDMC sobre $\mathbb{F}_{17}^2$. Por Teorema 3.14, parte (2), f no es estabilizable.*

Ejemplo 3.16. *Supongamos $f = (x_1^{10}, x_1^9 u)$ un SDMC sobre $\mathbb{F}_{17}^2$. Por Teorema 3.14, parte (2), f es estabilizable, basta escoger $u = 1$, ya que $\hat{f}$ es un spf.*

El siguiente Teorema provee condiciones suficientes y necesarias para que un SDMC con dos exponentes a, c tales que $a = c = 0$ sea estabilizable.

Teorema 3.17. *Supongamos que $f : \mathbb{F}_{2^r+1}^2 \times \mathbb{F}_{2^r+1} \longrightarrow \mathbb{F}_{2^r+1}^2$ sea un SDMC. Supongamos $f = (x_2^b u^{\epsilon_1}, x_2^d u^{\epsilon_2})$ con $0 < b, d \leq 2^r$ y $\forall i\ \epsilon_i \in \{0, 1\}$. Tenemos varios casos:*

(1) Si $\epsilon_1 = 1$ y $\epsilon_2 = 0$. Entonces f es estabilizable $\iff d = 1$ ó d es par.

(2) Si $\epsilon_1 = 0$ y $\epsilon_2 = 1$. Entonces f es estabilizable .

(3) Si $\epsilon_1 = 1$ y $\epsilon_2 = 1$. Entonces f es estabilizable.

Demostración. *Dado que $T(f) = (x_2, x_2)$ es un spf, por la observación 2, solamente nos interesa encontrar una función g tal que $L(f \circ g)$ sea un spf.*

$$L(\hat{f}) = \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix},$$

$$L(\hat{f}) - I = \begin{pmatrix} -1 & b \\ 0 & d-1 \end{pmatrix},$$

Entonces,

$$FNS(L(\hat{f}) - I) = \begin{pmatrix} 1 & 0 \\ 0 & d-1 \end{pmatrix}$$

Para que la PFNS satisfaga, $d-1$ *debe ser impar, es decir,* d *debe ser par.*

Además, note que si d *es par, entonces*

$Bool(L(\hat{f})) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, *con* b *par ó*

$Bool(L(f)) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, *con* b *impar, los cuales son un spf, por lema 3.5.1.*

Por lo tanto, $\hat{f}$ *es un spf siempre que* d *sea par. Por lo tanto, nos interesa estabilizar* f *cuando* d *sea impar.*

Además, si $d = 1$. *Entonces,*

$$L(f) = \begin{pmatrix} 0 & b \\ 0 & 1 \end{pmatrix},$$

$$L(f) - I = \begin{pmatrix} -1 & b \\ 0 & 0 \end{pmatrix},$$

Entonces,

$FNS(L(f) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, *que satisface la PFNS.*

$Bool(L(\hat{f})) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, *con* b *par ó*

$Bool(L(f)) = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$, *con* b *impar, los cuales son un spf, por lema 3.5.1.*

Así, $\hat{f}$ es un spf con $d = 1$. Por lo tanto, nos interesa estabilizar f cuando $d \neq 1$ sea impar.

Prueba caso (1).

Supongamos que $\epsilon_1 = 1$ y $\epsilon_2 = 0$. Supongamos que $u = x_1^{\alpha} x_2^{\beta}$. Entonces,

$$L(f \circ g) = \begin{pmatrix} \alpha & b+\beta \\ 0 & d \end{pmatrix},$$

$$L(f \circ g) - I = \begin{pmatrix} \alpha - 1 & b+\beta \\ 0 & d-1 \end{pmatrix},$$

Entonces,

$$FNS(L(f \circ g) - I) = \begin{pmatrix} gcd(d-1, \alpha-1, \beta+b) & 0 \\ 0 & \dfrac{(d-1)(\alpha-1)}{gcd(d-1, \alpha-1, \beta+b)} \end{pmatrix},$$

Note que, $gcd(d-1, \alpha-1, \beta+b) \leq d-1 < 2^r$.

Además, $(d-1)(\alpha-1)$ es par, ya que d es impar, por lo tanto queremos que $(d-1)(\alpha-1) = 2^r k$, para algún entero k. Es decir, $\alpha = \dfrac{2^r}{d-1}k + 1$, α sería impar, ya que $d-1 = 2^s \gamma_2$, con $\gamma_2, s \in \mathbb{Z}$, $2^{s+1} \nmid d-1$ y $0 < s < r$. Por lo tanto, pongámosle condiciones a $\beta + b$.

(i) Si $\beta + b$ es par, entonces $gcd(d-1, \alpha-1, \beta+b)$ sería par, y por lo tanto $gcd(d-1, \alpha-1, \beta+b)$ sería un divisor de cero, que no satisface la PFNS.

(ii) Si $\beta + b$ es impar, entonces,

$Bool(L(f \circ g)) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, *que no es un spf, por lema 3.5.1.*

Por lo tanto, f *no es estabilizable.*

Por lo tanto,

si d *es par ó* $d = 1 \implies f$ *es estabilizable y si* d *es impar y* $d \neq 1 \implies f$ *no es estabilizable. Esto es equivalente a decir que,*

f *es estabilizable* $\iff d$ *es par ó* $d = 1$.

Prueba caso (2).

Supongamos que $\epsilon_1 = 0$ *y* $\epsilon_2 = 1$. *Entonces simplemente escogemos* $u = x_2$, *por lo tanto* $d + 1$ *sería par y por la parte anterior,* f *es estabilizable.*

Prueba caso (3).

Supongamos que $\epsilon_1 = 1$ *y* $\epsilon_2 = 1$. *Entonces, escogemos* $u = x_2$. *Entonces,*

$$L(f \circ g) = \begin{pmatrix} 0 & b+1 \\ 0 & d+1 \end{pmatrix},$$

$$L(f \circ g) - I = \begin{pmatrix} -1 & b+1 \\ 0 & d \end{pmatrix},$$

$$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}.$$

Como d *es impar, satisface la PFNS y además,*

$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, *si* b *es par y*

$Bool(L(f\circ g)) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, *si* b *es impar, los cuales son un spf, por el lema 3.5.1.*

Así $f \circ g$ *es un spf, es decir,* f *es estabilizable* $\square$.

Veamos los siguientes ejemplos del Teorema 3.17. Veremos SDMC que son ó no son estabilizables.

Ejemplo 3.18. *Supongamos* $f = (x_2^8 u, x_2^7)$ *un SDMC sobre* $\mathbb{F}_{17}^2$. *Por Teorema 3.17, parte* (1), f *no es estabilizable.*

Ejemplo 3.19. *Supongamos* $f = (x_2^9 u, x_2^5)$ *un SDMC sobre* $\mathbb{F}_{17}^2$. *Por Teorema 3.17, parte* (1), f *es estabilizable, basta escoger* $u = 1$, *ya que* $\hat{f}$ *es un spf.*

De los Teoremas anteriores, el Teorema 3.11 el $T(f)$ no es un spf, por lo tanto había que estabilizar el $T(f)$ y también la $L(f)$, así la manera en que hicimos la demostración difiere de los Teoremas 3.8, 3.14, 3.17, exceptuando que utilizamos la FNS, el Teorema 2.15, y la Proposición 2.14.

El próximo Teorema es un caso más general que los anteriores, sin embargo veremos que las estrategias que utilizamos para resolver los teoremas anteriores son aplicables. La mayor diferencia en el enunciado de este teorema con el de los anteriores es que en los teoremas anteriores la estabilidad de f dependia de comparar si dos exponentes tenian las mismas potencias de 2. Aqui necesitamos que necesariamente sean diferentes ó iguales dependiendo donde se encuentre la variable de control.

El Teorema provee condiciones suficientes y necesarias para que un SDMC con cuatro exponentes a, b, c, d con a lo más uno de ellos sea cero, sea estabilizable.

Teorema 3.20. *Supongamos que* $f : \mathbb{F}_{2^r+1}^2 \times \mathbb{F}_{2^r+1} \longrightarrow \mathbb{F}_{2^r+1}^2$ *un SDMC con* $r > 1$. *Supongamos* $f = (x_1^a x_2^b u^{\epsilon_1}, x_1^c x_2^d u^{\epsilon_2})$ *con* $0 \leq a, b, c, d \leq 2^r$ *y* $\forall i$ $\epsilon_i \in \{0, 1\}$ *y a lo*

sumo uno de los exponentes a, b, c, d es cero. Tenemos varios casos:

(1) Si $\epsilon_1 = 1$ y $\epsilon_2 = 0$. Entonces, f no es estabilizable $\iff c = 2^{s_3}\gamma_3$, $d - 1 = 2^{s_4}\gamma_4$, con γ_3, γ_4 impares y $s_3 > s_4$.

(2) Si $\epsilon_1 = 0$ y $\epsilon_2 = 1$. Entonces, f no es estabilizable $\iff a - 1 = 2^{s_1}\gamma_1$, $b = 2^{s_2}\gamma_2$, con γ_1, γ_2 impares y $s_2 > s_1$.

(3) Si $\epsilon_1 = 1$ y $\epsilon_2 = 1$. Entonces, f no es estabilizable $\iff a - c - 1 = 2^{s_1}\gamma_1$, $d - b - 1 = 2^{s_2}\gamma_2$, con γ_1, γ_2 impares y $s_1 = s_2$.

Demostración. *Supongamos que a lo sumo uno de los exponentes a, b, c, d es cero. Note que la única manera para que $T(\hat{f})$ no sea un spf es que $T(\hat{f}) = (x_2, x_1)$. En nuestro caso $T(\hat{f})$ siempre es un spf. Por lo tanto, sólo nos interesa encontrar una función g tal que $L(f \circ g)$ sea un spf.*

Prueba Caso (1)

($\Rightarrow$) *Para esta implicación haremos la prueba por contrapositivo. Supongamos que $\epsilon_1 = 1$ y $\epsilon_2 = 0$. Entonces tenemos las siguientes condiciones:*

(i) a, b, c son pares y d es impar.

(ii) a, c son pares y b, d son impares.

(iii) a, d son impares y b, c son pares.

(iv) a, b, d son impares y c es par.

No es difícil ver que bajo cualquier otra condición la función f es estabilizable. (ver apéndice A).

Note que la condición (i) y la condición (ii) difieren únicamente de la paridad de b. Análogamente, note que la condición (iii) y la condición (iv) difieren únicamente

de la paridad de b.

Supongamos que $u = x_1^{\alpha} x_2^{\beta}$,

$$L(f \circ g) = \begin{pmatrix} a+\alpha & b+\beta \\ c & d \end{pmatrix},$$

$$L(f \circ g) - I = \begin{pmatrix} a-1+\alpha & b+\beta \\ c & d-1 \end{pmatrix},$$

$$FNS(L(f \circ g) - I) = \begin{pmatrix} gcd(a-1+\alpha, b+\beta, c, d-1) & 0 \\ 0 & \dfrac{(a-1+\alpha)(d-1) - c(b+\beta)}{gcd(a-1+\alpha, b+\beta, c, d-1)} \end{pmatrix}.$$

Note que si la condición (i) *se cumple, entonces dado que* $gcd(a-1+\alpha, b+\beta, c, d-1) < 2^r$, *para que la PFNS se cumpla,* $gcd(a-1+\alpha, b+\beta, c, d-1)$ *debe ser impar. Para ello debemos escoger* α *par ó* β *impar, pero si* α *es impar y* β *es impar entonces,* $Bool(L(f \circ g)) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, *que no es un spf por lema 3.5.1. Por lo tanto, esos* α *y* β *deben ser:* α *par y* β *impar ó* α *par y* β *par. Es decir, para que la función* f *pueda ser estabilizable esos* α *y* β *deben ser* α *es par y* β *es de paridad arbitraria.*

De un análisis similar, para que la función f *pueda ser estabilizable debemos escoger a esos* α *y* β *de la siguiente manera:*
Si la condición (ii) *se cumple entonces* α *es par y* β *es de paridad arbitraria.*
Si la condición (iii) *se cumple entonces* α *es impar y* β *es de paridad arbitraria y si la condición* (iv) *se cumple entonces* α *es impar y* β *es de paridad arbitraria.*

Al escoger los α *y* β *que correspondan a cada una de las cuatro condiciones, note que* $(a-1+\alpha)(d-1) - c(b+\beta)$ *es par, por lo tanto queremos hallar* α *y* β *enteros positivos tales que* $(a-1+\alpha)(d-1) - c(b+\beta) = 2^r k$, $k \in \mathbb{Z}$.
Entonces, para $k \in \mathbb{Z}$

$$\alpha = \frac{2^r}{d-1}k + (\beta + b)\frac{c}{d-1} - (a-1)$$

ó

$$\beta = -\frac{2^r k}{c} + (a - 1 + \alpha)\frac{(d-1)}{c} - b$$

Note que en las cuatro condiciones c es par y d es impar. Supongamos que $d = 1$. Entonces veamos que f es estabilizable para cada una de las cuatro condiciones. En efecto, para las condiciones (i) y (ii) escogemos $\alpha = 0$ y $\beta = 2^r - b$. No es díficil ver que $f \circ g$ es un spf. Por lo tanto, f es estabilizable.

Similarmente, para las condiciones (iii) y (iv) escogemos $\alpha = 1$ y $\beta = 2^r - b$. No es difiícil ver que $f \circ g$ es un spf. Por lo tanto, f es estabilizable.

Supongamos que $c = 0$ y $d \neq 1$ impar. Entonces veamos que f no es estabilizable, en cada una de las cuatro condiciones. En efecto, supongamos que $d - 1 = 2^{s_4}\gamma_4$ con $\gamma_4 \in \mathbb{Z}$ es impar y $0 < s_4 < r$, $s_4 \in \mathbb{Z}$. Entonces,

$$\alpha = \frac{2^r}{d-1}k - (a-1) = 2^{r-s_4}\frac{k}{\gamma_4} - (a-1)$$

Si la condición (i) ó (ii) se cumplen entonces note que α debe ser par y β puede ser de cualquier paridad, para que f sea estabilizable. Note que, $\alpha = \dfrac{2^{r-s_4}k - (a-1)\gamma_4}{\gamma_4}$. Además, dado que a es par en las condiciones (i) y (ii), por tanto $\alpha = \dfrac{\overbrace{2^{r-s_4}k}^{par} - \overbrace{(a-1)\gamma_4}^{impar}}{\underbrace{\gamma_4}_{impar}}$. Entonces, α es impar, con $\alpha \in \mathbb{Z}$. Por lo tanto f no es estabilizable.

Ahora, si la condición (iii) ó (iv) se cumplen entonces note que α debe ser impar y β puede ser de cualquier paridad, para que f sea estabilizable. Note que, $\alpha = \dfrac{2^{r-s_4}k - (a-1)\gamma_4}{\gamma_4}$.

Además, dado que a es impar en las condiciones (iii) y (iv), por tanto

$\alpha = \dfrac{\overbrace{2^{r-s_4}k}^{par} - \overbrace{(a-1)\gamma_4}^{par}}{\underbrace{\gamma_4}_{impar}}$. *Entonces,* α *es par, con* $\alpha \in \mathbb{Z}$. *Por lo tanto* f *no es estabilizable.*

Supongamos que $d \neq 1$, d *es impar y* $c \neq 0$ *es par. Además, supongamos que* $c = 2^{s_3}\gamma_3$, $d-1 = 2^{s_4}\gamma_4$, *tales que* γ_3, γ_4 *son impares con* $\gamma_3, \gamma_4 \in \mathbb{Z}$ *y además* $0 < s_3 < r$, $0 < s_4 < r$ *con* $s_3, s_4 \in \mathbb{Z}$.

Supongamos que $s_4 \geq s_3$. *Entonces veamos que* f *es estabilizable para cada una de las cuatro condiciones. Para* $l_1 \in \mathbb{Z}$,

$$\alpha = \frac{2^r k}{d-1} + l_1 - (a-1) = 2^{r-s_4}\frac{k}{\gamma_4} + l_1 - (a-1)$$

$$\beta = l_1\frac{(d-1)}{c} - b = 2^{s_4-s_3}l_1\frac{\gamma_4}{\gamma_3} - b$$

Escogemos $l_1 \in \mathbb{Z}$ *impar tal que* $\beta \in \mathbb{Z}^+$. *También escogemos* $k \in \mathbb{Z}$ *tal que* $\alpha \in \mathbb{Z}^+$.

Supongamos que se cumple la condición (i) *ó la condición* (ii). *Si se cumple la condicion* (i), *entonces* α *es par ya que* a *es par y* l_1 *es impar, y además no importa la paridad de* β, *ya que su paridad es arbitraria. Por lo tanto* f *es estabilizable.*

Análogamente, si se cumple la condición (ii), *dado que la condición* (ii) *y la condición* (i) *difieren únicamente de la paridad de* b, *entonces* α *es par ya que* a *es par y* l_1 *es impar y además no importa la paridad de* β, *ya que su paridad es arbitraria. Así* f *es estabilizable.*

Supongamos que se cumple la condición (iii) *ó la condición* (iv). *Si se cumple la condición* (iii) *entonces* α *es impar ya que* a *es impar y* l_1 *es impar. No importa la paridad de* β, *ya que su paridad es arbitraria. Así* f *es estabilizable.*

Análogamente, si se cumple la condición (iv), *dado que la condición* (iv) *y la condición* (iii) *difieren únicamente de la paridad de* b, *entonces* α *es impar ya que* a *es*

impar y l_1 es impar. No importa la paridad de β, ya que su paridad es arbitraria. Por lo tanto f es estabilizable.

($\Leftarrow$) *Supongamos que $s_3 > s_4$. Entonces veamos que f no es estabilizable en cada una de las cuatro condiciones. En efecto, recordamos que $c = 2^{s_3}\gamma_3$, $d-1 = 2^{s_4}\gamma_4$. Entonces,*

$$\begin{aligned}\alpha &= \frac{2^r k}{d-1} - (\beta+b)\frac{c}{d-1} - (a-1)\\ &= 2^{r-s_4}\frac{k}{\gamma_4} + 2^{s_3-s_4}(\beta+b)\frac{\gamma_3}{\gamma_4} - (a-1)\\ &= \frac{2^{r-s_4}k + 2^{s_3-s_4}(\beta+b)\gamma_3 - (a-1)\gamma_4}{\gamma_4}\end{aligned}$$

No importa la paridad de β ya que paridad es arbitraria en cada una de las cuatro condiciones. Si la condición (i) ó (ii) se cumplen entonces note que α debe ser par para que f sea estabilizable. Además, note que a es par en las condiciones (i) y (ii). Por lo tanto,

$$\alpha = \frac{\overbrace{2^{r-s_4}k}^{par} + \overbrace{2^{s_3-s_4}(\beta+b)\gamma_3}^{par} - \overbrace{(a-1)\gamma_4}^{impar}}{\underbrace{\gamma_4}_{impar}}$$

Entonces, α es impar, con $\alpha \in \mathbb{Z}$. Así, f no es estabilizable.

Si la condición (iii) ó (iv) se cumplen entonces note que α debe ser impar para que f sea estabilizable. Además, a es impar en las condiciones (iii) y (iv). Por lo tanto,

$$\alpha = \frac{\overbrace{2^{r-s_4}k}^{par} + \overbrace{2^{s_3-s_4}(\beta+b)\gamma_3}^{par} - \overbrace{(a-1)\gamma_4}^{par}}{\underbrace{\gamma_4}_{impar}}$$

Entonces α es par, con $\alpha \in \mathbb{Z}$. Así, f no es estabilizable.

Prueba Caso (2)

($\Rightarrow$) *Para esta implicación haremos la prueba por contrapositivo. Supongamos que*

$\epsilon_1 = 0$ *y* $\epsilon_2 = 1$. *Entonces tenemos las siguientes condiciones:*

(i) a *es impar y* a, b, c *son pares*

(ii) a, d *son impares y* b, c *son pares.*

(iii) a, c *son impares y* b, d *son pares.*

(iv) a, c *son impares y* b *es par.*

No es difícil ver que bajo cualquier otra condición la función f *es estabilizable. (ver apéndice A).*

Note que la condición (i) *y la condición* (iii) *difieren únicamente de la paridad de* c. *Análogamente, note que la condición* (ii) *y la condición* (iv) *difieren únicamente de la paridad de* c.

Supongamos que $u = x_1^{\alpha} x_2^{\beta}$,

$$L(f \circ g) = \begin{pmatrix} a & b \\ c+\alpha & d+\beta \end{pmatrix},$$

$$L(f \circ g) - I = \begin{pmatrix} a-1 & b \\ c+\alpha & d-1+\beta \end{pmatrix},$$

$$FNS(L(f \circ g) - I) = \begin{pmatrix} gcd(a-1, b, c+\alpha, d-1+\beta) & 0 \\ 0 & \dfrac{(a-1)(d-1+\beta) - b(c+\alpha)}{gcd(a-1, b, c+\alpha, d-1+\beta)} \end{pmatrix}.$$

Note que si la condición (i) *se cumple, entonces dado que* $gcd(a-1, b, c+\alpha, d-1+\beta) < 2^r$, *para que la PFNS se cumpla,* $gcd(a-1, b, c+\alpha, d-1+\beta)$ *debe ser impar. Para ello debemos escoger* α *impar ó* β *par, pero si* α *es impar y* β *es impar entonces,* $Bool(L(f \circ g)) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, *que no es un spf por lema 3.5.1. Por lo tanto, esos* α *y* β *deben ser:* α *impar y* β *par ó* α *par y* β *par. Es decir, para que la función* f *pueda ser estabilizable esos* α *y* β *deben ser* α *es de paridad arbitraria y* β *es par.*

De un análisis similar, para que la función f *pueda ser estabilizable debemos escoger*

a esos α y β de la siguiente manera:

Si la condición (ii) se cumple entonces α es de paridad arbitraria y β es impar.

Si la condición (iii) se cumple entonces α es paridad arbitraria y β es par y si la condición (iv) se cumple entonces α es de paridad arbitraria y β es impar. Al escoger los α y β que correspondan a cada una de las cuatro condiciones, note que $(a-1)(d-1+\beta)-b(c+\alpha)$ es par, por lo tanto queremos hallar α y β enteros positivos tales que $(a-1)(d-1+\beta)-b(c+\alpha)=2^r k$, $k\in\mathbb{Z}$.

Entonces, para $k\in\mathbb{Z}$

$$\alpha=-\frac{2^r}{a-1}k+(d-1+\beta)\frac{(a-1)}{b}-c$$

ó

$$\beta=-\frac{2^r k}{a-1}+(c+\alpha)\frac{b}{a-1}-(d-1)$$

Note que en las cuatro condiciones a es impar y b es par. Supongamos que $a=1$. Entonces veamos que f es estabilizable para cada una de las cuatro condiciones. En efecto, para las condiciones (i) y (ii) escogemos $\alpha=2^r-c$ y $\beta=0$. No es díficil ver que $f\circ g$ es un spf. Por lo tanto, f es estabilizable.

Similarmente, para las condiciones (iii) y (iv) escogemos $\alpha=2^r-c$ y $\beta=1$. No es difiícil ver que $f\circ g$ es un spf. Por lo tanto, f es estabilizable.

Supongamos que $b=0$ y $a\neq 1$ impar. Entonces veamos que f no es estabilizable, en cada una de las cuatro condiciones. En efecto, supongamos que $a-1=2^{s_1}\gamma_1$ con $\gamma_1\in\mathbb{Z}$ es impar y $0<s_1<r$, $s_1\in\mathbb{Z}$. Entonces,

$$\beta=\frac{2^r}{a-1}k-(d-1)=2^{r-s_1}\frac{k}{\gamma_1}-(d-1)$$

No importa la paridad de α ya que su paridad en cada una de las cuatro condiciones es arbitraria.

Si la condición (i) ó (iii) se cumplen entonces note que β debe ser par, para que f sea estabilizable. Note que, $\beta = \dfrac{2^{r-s_1}k-(d-1)\gamma_1}{\gamma_1}$.

Además, dado que d es par en las condiciones (i) y (iii), por tanto $\beta = \dfrac{\overbrace{2^{r-s_1}k}^{par}-\overbrace{(d-1)\gamma_1}^{impar}}{\underbrace{\gamma_1}_{impar}}$. *Entonces, β es impar, con $\beta \in \mathbb{Z}$. Por lo tanto f no es estabilizable.*

Ahora, si la condición (ii) ó (iv) se cumplen entonces note que β debe ser impar, para que f sea estabilizable. Note que, $\beta = \dfrac{2^{r-s_1}k-(d-1)\gamma_1}{\gamma_1}$.

Además, dado que d es impar en las condiciones (ii) y (iv), por tanto $\beta = \dfrac{\overbrace{2^{r-s_1}k}^{par}-\overbrace{(d-1)\gamma_1}^{par}}{\underbrace{\gamma_1}_{impar}}$. *Entonces, β es par, con $\beta \in \mathbb{Z}$. Por lo tanto f no es estabilizable.*

Supongamos que $a \neq 1$, a es impar y $b \neq 0$ es par. Además, supongamos que $a-1 = 2^{s_1}\gamma_1$, $b = 2^{s_2}\gamma_2$ tales que γ_1, γ_2 son impares con $\gamma_1, \gamma_2 \in \mathbb{Z}$ y además $0 < s_1 < r$, $0 < s_2 < r$ con $s_1, s_2 \in \mathbb{Z}$.

Supongamos que $s_1 \geq s_2$. Entonces veamos que f es estabilizable para cada una de las cuatro condiciones. Para $l_2 \in \mathbb{Z}$,

$$\alpha = l_2\frac{(a-1)}{b} - c = 2^{s_1-s_2}l_2\frac{\gamma_1}{\gamma_2} - c$$

$$\beta = \frac{2^r k}{a-1} + l_2 - (d-1) = 2^{r-s_1}\frac{k}{\gamma_1} + l_2 - (d-1)$$

Escogemos $l_2 \in \mathbb{Z}$ impar tal que $\alpha \in \mathbb{Z}^+$. También escogemos $k \in \mathbb{Z}$ tal que $\beta \in \mathbb{Z}^+$.

Note que no importa la paridad de α, ya que puede ser de cualquier paridad en cada una de las cuatro condiciones.

Supongamos que se cumple la condición (i) ó la condición (iii). Si se cumple la condicion (i), entonces β es par ya que d es par y l_2 es impar. Por lo tanto f es

estabilizable.

Análogamente, si se cumple la condición (iii), dado que la condición (iii) y la condición (i) difieren únicamente de la paridad de c, entonces β es par ya que d es par y l_2 es impar. Así f es estabilizable.

Supongamos que se cumple la condición (ii) ó la condición (iv). Si se cumple la condición (ii) entonces β es impar ya que d es impar y l_2 es impar.

Análogamente, si se cumple la condición (iv), dado que la condición (iv) y la condición (ii) difieren únicamente de la paridad de c, entonces β es impar ya que d es impar y l_2 es impar. Por lo tanto f es estabilizable.

($\Leftarrow$) *Ahora, supongamos que $s_2 > s_1$. Entonces veamos que f no es estabilizable en cada una de las cuatro condiciones. En efecto, recordamos que $a-1 = 2^{s_1}\gamma_1$, $b = 2^{s_2}\gamma_2$.*

Entonces,

$$\begin{aligned}\beta &= \frac{2^r k}{a-1} - (c+\alpha)\frac{b}{a-1} - (d-1)\\ &= 2^{r-s_1}\frac{k}{\gamma_1} + 2^{s_2-s_1}(c+\alpha)\frac{\gamma_2}{\gamma_1} - (d-1)\\ &= \frac{2^{r-s_1}k + 2^{s_2-s_1}(c+\alpha)\gamma_2 - (d-1)\gamma_1}{\gamma_1}\end{aligned}$$

No importa la paridad de α ya que su paridad es arbitraria en cada una de las cuatro condiciones. Si la condición (i) ó (iii) se cumplen entonces note que β debe ser par, para que f sea estabilizable. Además, note que d es par en las condiciones (i) y (iii). Por lo tanto,

$$\beta = \frac{\overbrace{2^{r-s_1}k}^{par} + \overbrace{2^{s_2-s_1}(c+\alpha)\gamma_2}^{par} - \overbrace{(d-1)\gamma_1}^{impar}}{\underbrace{\gamma_1}_{impar}}$$

Entonces, β es impar, con $\beta \in \mathbb{Z}$. Así, f no es estabilizable.

Si la condición (ii) ó (iv) se cumplen entonces note que β debe ser impar para que

f sea estabilizable. Además, note que d es impar en las condiciones (ii) y (iv). Por lo tanto,

$$\beta = \frac{\overbrace{2^{r-s_1}k}^{par} + \overbrace{2^{s_2-s_1}(c+\alpha)\gamma_2}^{par} - \overbrace{(d-1)\gamma_1}^{par}}{\underbrace{\gamma_1}_{impar}}$$

Entonces β es par, con $\beta \in \mathbb{Z}$. Así, f no es estabilizable.

Prueba Caso (3)

$(\Rightarrow)$ *Para esta implicación haremos la prueba por contrapositivo. Supongamos que* $\epsilon_1 = 1$ *y* $\epsilon_2 = 1$.

Entonces tenemos las siguientes condiciones:

(i) a, b *son pares y* c, d *son impares.*

(ii) a, d *son pares y* b, c *son impares.*

(iii) a, d *son impares y* b, c *son pares.*

(iv) a, b *son impares y* c, d *es pares.*

No es difícil ver que bajo cualquier otra condición la función f es estabilizable. (ver apéndice A).

$$u = x_1^{\alpha} x_2^{\beta},$$

$$L(f \circ g) = \begin{pmatrix} a+\alpha & b+\beta \\ c+\alpha & d+\beta \end{pmatrix},$$

$$L(f \circ g) - I = \begin{pmatrix} a-1+\alpha & b+\beta \\ c+\alpha & d-1+\beta \end{pmatrix},$$

$$FNS(L(f \circ g) - I) = \begin{pmatrix} gcd(a-1+\alpha, b+\beta, c+\alpha, d-1+\beta) & 0 \\ 0 & \frac{(a-1+\alpha)(d-1+\beta)-(c+\alpha)(b+\beta)}{gcd(a-1+\alpha, b+\beta, c+\alpha, d-1+\beta)} \end{pmatrix}.$$

Observe que:

$$\begin{aligned} gcd(a-1+\alpha, b+\beta, c+\alpha, d-1+\beta) &= gcd(gcd(a-1+\alpha, c+\alpha), gcd(b+\beta, d-1+\beta)) \\ &= gcd(gcd(a-c-1, c+\alpha), gcd(d-b-1, b+\beta)) \\ &\leq gcd(a-c-1, c+\alpha), gcd(d-b-1, b+\beta) \end{aligned}$$

Además, $gcd(a-c-1, c+\alpha) \leq a-c-1$ *y* $gcd(d-b-1, b+\beta) \leq d-b-1$. *Es decir,*

$gcd(a-1+\alpha, b+\beta, c+\alpha, d-1+\beta) \leq a-c-1, d-b-1.$

De una forma similar, $gcd(a-1+\alpha, b+\beta, c+\alpha, d-1+\beta) \leq a-c-1, d-b-1$.

Entonces,

$gcd(a-1+\alpha, b+\beta, c+\alpha, d-1+\beta) \leq |a-c-1|, |d-b-1| \leq 2^r$.

Note que:

Si $d > b$ *entonces* $d-b-1 < 2^r$

Si $a > c$ *entonces* $a-c-1 < 2^r$

Si $b \geq d$ *entonces* $b-d+1 \leq 2^r$

Si $c \geq a$ *entonces* $c-a+1 \leq 2^r$

Supongamos que $|a-c-1| = 2^r$ *ó* $|d-b-1| = 2^r$. *Entonces veamos que* f *es estabilizable en cada una de las cuatro condiciones.*

En efecto, si $|a-c-1| = 2^r$, *entonces* $a-c-1 = \pm 2^r$, *pero* $a-c-1 = 2^r$ *no puede ser ya que* $a = 2^r + c + 1$, *y* $0 \leq a, c \leq 2^r$. *Por lo tanto,* $c-a+1 = 2^r$ *entonces* $c-a = 2^r - 1$ *y las soluciones son* $c = 2^r + k$ *y* $a = 1+k$ *con* $k \in \mathbb{Z}$. *Pero dado que* $0 \leq a, c \leq 2^r$ *entonces* $k = 0, -1$. *Por lo tanto* $a = 1$ *y* $c = 2^r$ *ó* $a = 0$ *y* $c = 2^r - 1$. *Ahora veamos que* f *es estabilizable para cada una de las cuatro condiciones.*

Ahora supongamos que $a = 1$ *y* $c = 2^r$. *Entonces veamos que* f *es estabilizable en las condiciones* (iii) *y* (iv).

En efecto, si la condición (iii) se cumple entonces b es par y d es impar. Escogemos $u = x_2$.

$$L(f \circ g) = \begin{pmatrix} 1 & b+1 \\ 2^r & d+1 \end{pmatrix},$$

$$L(f \circ g) - I = \begin{pmatrix} 0 & b+1 \\ 2^r & d \end{pmatrix},$$

Note que $gcd(b+1, 2^r, d) = 1$. *Entonces,*

$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 2^r(b+1) \end{pmatrix}$, *que satisface la PFNS y además,*

$Bool(L(f \circ g)) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ *que es un spf por lema 3.5.1. Así, f es estabilizable.*

Si la condición (iv) se cumple entonces b es impar y d es par. Escogemos $g \equiv 1$.

$$L(f) = \begin{pmatrix} 1 & b \\ 2^r & d \end{pmatrix},$$

$$L(f) - I = \begin{pmatrix} 0 & b \\ 2^r & d-1 \end{pmatrix},$$

Note que $gcd(b, 2^r, d-1) = 1$. *Entonces,*

$FNS(L(f) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 2^r b \end{pmatrix}$, *que satisface la PFNS y además,*

$Bool(L(f)) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ *que es un spf por lema 3.5.1. Así, f es estabilizable.*

Supongamos que $a = 0$ *y* $c = 2^r - 1$. *Entonces veamos que f es estabilizable en las condiciones (i) y (ii).*

En efecto, si la condición (i) se cumple entonces b es par y d es impar. Escogemos $u = x_1 x_2$. *Entonces,*

$$L(f \circ g) = \begin{pmatrix} 1 & b+1 \\ 2^r & d+1 \end{pmatrix},$$

$$L(f \circ g) - I = \begin{pmatrix} 0 & b+1 \\ 2^r & d \end{pmatrix},$$

Note que $gcd(b+1, 2^r, d) = 1$. *Entonces,*

$$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 2^r(b+1) \end{pmatrix}, \text{ que satisface la PFNS y además,}$$

$$Bool(L(f \circ g)) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \text{ que es un spf por lema 3.5.1. Así, } f \text{ es estabilizable.}$$

Si la condición (ii) *se cumple entonces* b *es impar y* d *es par. Escogemos* $u = x_1$. *Entonces,*

$$L(f \circ g) = \begin{pmatrix} 1 & b \\ 2^r & d \end{pmatrix},$$

$$L(f \circ g) - I = \begin{pmatrix} 0 & b \\ 2^r & d-1 \end{pmatrix},$$

Note que $gcd(b, 2^r, d-1) = 1$. *Entonces,*

$$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 2^r b \end{pmatrix}, \text{ que satisface la PFNS y además,}$$

$$Bool(L(f \circ g)) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \text{ que es un spf por lema 3.5.1. Así, } f \text{ es estabilizable.}$$

Similarmente a la parte anterior, si $|d - b - 1| = 2^r$ *entonces* $b = 2^r$ *y* $d = 1$ *ó* $b = 2^r - 1$ *y* $d = 0$. *Entonces veamos que* f *es estabilizable para cada una de las cuatro condiciones.*

Supongamos que $b = 2^r$ *y* $d = 1$. *Entonces veamos que* f *es estabilizable en las condiciones* (i) *y* (iii). *En efecto, si la condición* (i) *se cumple entonces* a *es par y* c *es impar. Escogemos* $\alpha = 0$ *y* $\beta = 0$, *es decir,* $g \equiv 1$. *Entonces,*

$$L(f) = \begin{pmatrix} a & 2^r \\ c & 1 \end{pmatrix},$$

$$L(f) - I = \begin{pmatrix} a-1 & 2^r \\ c & 0 \end{pmatrix},$$

Note que $gcd(a-1, 2^r, c) = 1$. *Entonces,*

$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 2^r c \end{pmatrix}$, *que satisface la PFNS y además,*

$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$, *que es un spf por lema 3.5.1. Así,* f *es estabilizable.*

Si la condición (iii) *se cumple entonces* a *es impar y* c *es par. Escogemos* $\alpha = 1$ *y* $\beta = 0$, *es decir,* $u = x_1$. *Entonces,*

$$L(f \circ g) = \begin{pmatrix} a+1 & 2^r \\ c+1 & 1 \end{pmatrix},$$

$$L(f \circ g) - I = \begin{pmatrix} a & 2^r \\ c+1 & 0 \end{pmatrix},$$

Note que $gcd(a, 2^r, c+1) = 1$. *Entonces,*

$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 2^r(c+1) \end{pmatrix}$, *que satisface la PFNS y además,*

$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$, *que es un spf por lema 3.5.1. Así,* f *es estabilizable.*

Supongamos que $b = 2^r - 1$ *y* $d = 0$. *Entonces veamos que* f *es estabilizable en las condiciones* (ii) *y* (iv). *En efecto, si la condición* (ii) *se cumple entonces* a *es par y* c *es impar. Escogemos* $u_{s_0} = x_2$.

$$L(f \circ g) = \begin{pmatrix} a & 2^r \\ c & 1 \end{pmatrix},$$

$$L(f \circ g) - I = \begin{pmatrix} a-1 & 2^r \\ c & 0 \end{pmatrix},$$

Note que $gcd(a-1, 2^r, c) = 1$. *Entonces,*

$$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 2^r c \end{pmatrix}, \text{ que satisface la PFNS y además,}$$

$$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \text{ que es un spf por lema 3.5.1. Así, } f \text{ es estabilizable.}$$

Si la condición (iv) *se cumple entonces* a *es impar y* c *es par. Escogemos* $u = x_1 x_2$. *Entonces,*

$$L(f \circ g) = \begin{pmatrix} a+1 & 2^r \\ c+1 & 1 \end{pmatrix},$$

$$L(f \circ g) - I = \begin{pmatrix} a & 2^r \\ c+1 & 0 \end{pmatrix},$$

Note que $gcd(a, 2^r, c+1) = 1$. *Entonces,*

$$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 2^r(c+1) \end{pmatrix}, \text{ que satisface la PFNS y además,}$$

$$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \text{ que es un spf por lema 3.5.1. Así, } f \text{ es estabilizable.}$$

Supongamos que, $|a - c - 1| < 2^r$ *y* $|d - b - 1| < 2^r$. *Entonces, dado que* $gcd(a-1+\alpha, b+\beta, c+\alpha, d-1+\beta) \leq |a-c-1|, |d-b-1| < 2^r$. *Entonces,* $gcd(a-1+\alpha, b+\beta, c+\alpha, d-1+\beta) < 2^r$.

Supongamos que $d = b+1$, *entonces veamos que* f *es estabilizable para cada una de las cuatro condiciones.*

En efecto, si se cumplen las condiciones (i) *ó* (ii) *entonces* a *es par y* c *es impar con* b *de distinta paridad que* d. *Escogemos* $u = x_2^{2^r - b}$. *Entonces,*

$$L(f \circ g) = \begin{pmatrix} a & 2^r \\ c & 2^r + 1 \end{pmatrix},$$

$$L(f \circ g) - I = \begin{pmatrix} a - 1 & 2^r \\ c & 2^r \end{pmatrix},$$

Note que $gcd(a - 1, 2^r, c) = 1$. *Entonces,*

$$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 2^r(a - c - 1) \end{pmatrix},$$ *que satisface la PFNS y además,*

$$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix},$$ *que es un spf por lema 3.5.1. Así,* f *es estabilizable.*

Si se cumplen las condiciones (iii) *ó* (iv), *entonces* a *es impar y* c *es par con* b *de distinta paridad que* d. *Escogemos* $u = x_1 x_2^{2^r - b}$. *Entonces,*

$$L(f \circ g) = \begin{pmatrix} a + 1 & 2^r \\ c + 1 & 2^r + 1 \end{pmatrix},$$

$$L(f \circ g) - I = \begin{pmatrix} a & 2^r \\ c + 1 & 2^r \end{pmatrix},$$

Note que $gcd(a, 2^r, c + 1) = 1$. *Entonces,*

$$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 2^r(a - c - 1) \end{pmatrix},$$ *que satisface la PFNS y además,*

$$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix},$$ *que es un spf por lema 3.5.1. Así,* f *es estabilizable.*

Supongamos que $a = c + 1$, *entonces veamos que* f *es estabilizable para cada una de las cuatro condiciones. En efecto, si se cumplen las condiciones* (i) *ó* (iii) *entonces* b *es par y* d *es impar con* a *de distinta paridad que* c. *Escogemos* $u = x_1^{2^r - c} x_2$. *Entonces,*

$$L(f \circ g) = \begin{pmatrix} 2^r + 1 & b+1 \\ 2^r & d+1 \end{pmatrix},$$

$$L(f \circ g) - I = \begin{pmatrix} 2^r & b+1 \\ 2^r & d \end{pmatrix},$$

Note que $gcd(2^r, b+1, d) = 1$. *Entonces,*

$$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 2^r(d-b-1) \end{pmatrix}, \text{ que satisface la PFNS y además,}$$

$$Bool(L(f \circ g)) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \text{ que es un spf por lema 3.5.1. Así, } f \text{ es estabilizable.}$$

Si se cumplen las condiciones (ii) *ó* (iv) *entonces* b *es impar y* d *es par con* a *de distinta paridad que* c. *Escogemos* $u = x_1^{2^r - c}$. *Entonces,*

$$L(f \circ g) = \begin{pmatrix} 2^r + 1 & b \\ 2^r & d \end{pmatrix},$$

$$L(f \circ g) - I = \begin{pmatrix} 2^r & b \\ 2^r & d-1 \end{pmatrix},$$

Note que $gcd(2^r, b, d-1) = 1$. *Entonces,*

$$FNS(L(f \circ g) - I) = \begin{pmatrix} 1 & 0 \\ 0 & 2^r(d-b-1) \end{pmatrix}, \text{ que satisface la PFNS y además,}$$

$$Bool(L(f \circ g)) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \text{ que es un spf por lema 3.5.1. Así, } f \text{ es estabilizable.}$$

Recordamos que asumimos $u = x_1^{\alpha} x_2^{\beta}$. *Además,*

$$FNS(L(f \circ g) - I) = \begin{pmatrix} gcd(a-1+\alpha, b+\beta, c+\alpha, d-1+\beta) & 0 \\ 0 & \frac{(a-1+\alpha)(d-1+\beta)-(c+\alpha)(b+\beta)}{gcd(a-1+\alpha, b+\beta, c+\alpha, d-1+\beta)} \end{pmatrix}.$$

Si la condición (i) *se cumple entonces dado que,*

$gcd(a-1+\alpha, b+\beta, c+\alpha, d-1+\beta) < 2^r$, *entonces para que la PFNS se cumpla,*

$gcd(a-1+\alpha, b+\beta, c+\alpha, d-1+\beta)$ debe ser impar. Para ello debemos escoger α par o β impar, pero si α es par y β es impar entonces,

$Bool(L(f \circ g)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, que no es un spf por lema 3.5.1. Por lo tanto, esos α y β deben ser: α par y β par ó α impar y β impar, para que la función f pueda ser estabilizable.

De un análisis similar, para que la función f sea estabilizable debemos escoger a α y β de la siguiente manera:

Si la condición (ii) se cumple entonces α es par y β es impar ó α es impar y β es par.

Si la condición (iii) se cumple entonces α es impar y β es par ó α es par y β es impar y si la condición (iv) se cumple entonces α es impar y β es impar ó α es par y β es par.

Al escoger los α y β que correspondan a cada una de las cuatro condiciones, note que $(a-1+\alpha)(d-1+\beta)-(c+\alpha)(b+\beta)$ es par, por lo tanto queremos hallar α y β enteros positivos tales que $(a-1+\alpha)(d-1+\beta)-(c+\alpha)(b+\beta) = 2^r k$, $k \in \mathbb{Z}$. Entonces, para $k \in \mathbb{Z}$

$$\alpha = \frac{2^r}{d-b-1}k - (d-1+\beta)\frac{a-c-1}{d-b-1} - c$$

ó

$$\beta = \frac{2^r}{a-c-1}k - (a-1+\alpha)\frac{(d-b-1)}{a-c-1} - b$$

Note que para cualquier condición, $a-c-1$ es par. Similarmente, $d-b-1$ es par, para cualquier condición. Asumamos que $a-c-1 = 2^{s_1}\gamma_1$ con $\gamma_1 \in \mathbb{Z}$ impar y $0 < s_1 < r$, $s_1 \in \mathbb{Z}$. Análogamente, $d-b-1 = 2^{s_2}\gamma_2$, con $\gamma_2 \in \mathbb{Z}$ impar y $0 < s_2 < r$, $s_2 \in \mathbb{Z}$.

Supongamos que $s_1 > s_2$. Entonces veamos que f es estabilizable en cada una de las

cuatro condiciones. En efecto,

Para $l_1 \in \mathbb{Z}$,

$$\alpha = l_1\frac{(a-c-1)}{d-b-1} - (a-1) = 2^{s_1-s_2}l_1\frac{\gamma_1}{\gamma_2} - (a-1)$$

$$\beta = \frac{2^r}{a-c-1}k - l_1 - b$$

Escogemos $l_1 \in \mathbb{Z}$, *impar tal que* $\alpha \in \mathbb{Z}^+$ *y escogemos* $k \in \mathbb{Z}$, *tal que* $\beta \in \mathbb{Z}^+$.
Si se cumple la condición (i), *entonces* α *es impar ya que* a *es par y* β *es impar ya que* b *es par y* l_1 *es impar. Así,* f *es estabilizable.*
Si se cumple la condición (ii) *entonces* α *es impar ya que* a *es par y* β *es par ya que* b *es impar y* l_1 *es impar. Así,* f *es estabilizable.*
Si se cumple la condición (iii) *entonces* α *es par ya que* a *es impar y* β *es impar ya que* b *es par y* l_1 *es impar. Así,* f *es estabilizable.*
Si se cumple la condición (iv) *entonces* α *es par ya que* a *es impar y* β *es par ya que* b *es impar y* l_1 *es impar. Así,* f *es estabilizable.*

Similarmente, supongamos que $s_2 > s_1$. *Entonces veamos que* f *es estabilizable en cada una de las cuatro condiciones. En efecto,*

Para $l_2 \in \mathbb{Z}$,

$$\alpha = \frac{2^r}{d-b-1}k - l_2 - c$$

$$\beta = l_2\frac{d-b-1}{a-c-1} - (d-1) = 2^{s_2-s_1}l_2\frac{\gamma_2}{\gamma_1} - (d-1)$$

Escogemos $l_2 \in \mathbb{Z}$, *impar tal que* $\beta \in \mathbb{Z}^+$ *y escogemos* $k \in \mathbb{Z}$, *tal que* $\alpha \in \mathbb{Z}^+$.
Si se cumple la condición (i), *entonces* α *es par ya que* c *es impar y* l_2 *es impar. Además,* β *es par ya que* d *es impar. Así,* f *es estabilizable.*

Si se cumple la condición (ii) entonces α es par ya que c es impar y l_2 es impar. Además, β es impar ya que d es par. Así, f es estabilizable.
Si la condición (iii) se cumple entonces α es impar ya que c es par y l_2 es impar. Además, β es par ya que d es impar.. Así, f es estabilizable.
Si la condición (iv) se cumple entonces α es impar ya que c es par y l_2 es impar. Además, β es impar ya que d es par. Así, f es estabilizable.

($\Leftarrow$) *Supongamos que $s_1 = s_2$. Entonces veamos que f no es estabilizable en cada una de las cuatro condiciones.*
En efecto, recordamos que $a - c - 1 = 2^{s_1}\gamma_1$, con $0 < s_1 < r$ y $d - b - 1 = 2^{s_2}\gamma_2$ con $0 < s_2 < r$. Entonces,

$$\begin{aligned}\alpha &= \frac{2^r k}{d-b-1} - (d-1+\beta)\frac{(a-c-1)}{d-b-1} - c \\ &= 2^{r-s_2}\frac{k}{\gamma_2} - (d-1+\beta)\frac{\gamma_1}{\gamma_2} - c \\ &= \frac{2^{r-s_2}k - (d-1+\beta)\gamma_1 - c\gamma_2}{\gamma_2}\end{aligned}$$

$$\begin{aligned}\beta &= \frac{2^r k}{a-c-1} - (a-1+\alpha)\frac{(d-b-1)}{a-c-1} - b \\ &= 2^{r-s_1}\frac{k}{\gamma_1} - (a-1+\alpha)\frac{\gamma_2}{\gamma_1} - b \\ &= \frac{2^{r-s_1}k - (a-1+\alpha)\gamma_2 - b\gamma_1}{\gamma_1}\end{aligned}$$

Supongamos que se cumple la condición (i), entonces a, b son pares y c, d son impares.

Si α es par, entonces

$$\beta = \frac{\overbrace{2^{r-s_1}}^{par}k - \overbrace{(a-1+\alpha)\gamma_2}^{impar} - \overbrace{b\gamma_1}^{par}}{\underbrace{\gamma_1}_{impar}},$$

Por tanto β *es impar con* $\beta \in \mathbb{Z}^+$.

Si α *es impar, entonces*

$$\beta = \frac{\overbrace{2^{r-s_1}k}^{par} - \overbrace{(a-1+\alpha)\gamma_2}^{par} - \overbrace{b\gamma_1}^{par}}{\underbrace{\gamma_1}_{impar}},$$

Por tanto β *es par con* $\beta \in \mathbb{Z}^+$.

Análogamente,

Si β *es par, entonces*

$$\alpha = \frac{\overbrace{2^{r-s_2}k}^{par} - \overbrace{(d-1+\beta)\gamma_1}^{par} - \overbrace{c\gamma_2}^{impar}}{\underbrace{\gamma_2}_{impar}},$$

Por tanto α *es impar con* $\alpha \in \mathbb{Z}^+$.

Si β *es impar, entonces*

$$\alpha = \frac{\overbrace{2^{r-s_2}k}^{par} - \overbrace{(d-1+\beta)\gamma_1}^{impar} - \overbrace{c\gamma_2}^{impar}}{\underbrace{\gamma_2}_{impar}},$$

Por tanto α *es par con* $\alpha \in \mathbb{Z}^+$.

Esos α *y* β *no estabilizan a* f *y por lo tanto* f *no es estabilizable en la condición* (i).

Si la condición (ii) *se cumple entonces* a, d *son pares y* b, c *son impares.*

Si α *es par, entonces*

$$\beta = \frac{\overbrace{2^{r-s_1}k}^{par} - \overbrace{(a-1+\alpha)\gamma_2}^{impar} - \overbrace{b\gamma_1}^{impar}}{\underbrace{\gamma_1}_{impar}},$$

Por tanto β *es par con* $\beta \in \mathbb{Z}^+$.

Si α es impar, entonces

$$\beta = \frac{\overbrace{2^{r-s_1}}^{par}k - \overbrace{(a-1+\alpha)\gamma_2}^{par} - \overbrace{b\gamma_1}^{impar}}{\underbrace{\gamma_1}_{impar}},$$

Por tanto β es impar con $\beta \in \mathbb{Z}^+$.

Análogamente,

Si β es par, entonces

$$\alpha = \frac{\overbrace{2^{r-s_2}}^{par}k - \overbrace{(d-1+\beta)\gamma_1}^{impar} - \overbrace{c\gamma_2}^{impar}}{\underbrace{\gamma_2}_{impar}},$$

Por tanto α es par con $\alpha \in \mathbb{Z}^+$.

Si β es impar, entonces

$$\alpha = \frac{\overbrace{2^{r-s_2}}^{par}k - \overbrace{(d-1+\beta)\gamma_1}^{par} - \overbrace{c\gamma_2}^{impar}}{\underbrace{\gamma_2}_{impar}},$$

Por tanto α es impar con $\alpha \in \mathbb{Z}^+$.

Esos α y β no estabilizan a f y por lo tanto f no es estabilizable en la condición (ii).

Si la condición (iii) se cumple entonces a, d son impares y b, c son pares.

Si α es par, entonces

$$\beta = \frac{\overbrace{2^{r-s_1}}^{par}k - \overbrace{(a-1+\alpha)\gamma_2}^{par} - \overbrace{b\gamma_1}^{par}}{\underbrace{\gamma_1}_{impar}},$$

Por tanto β es par con $\beta \in \mathbb{Z}^+$.

Si α es impar, entonces

$$\beta = \frac{\overbrace{2^{r-s_1}}^{par}k - \overbrace{(a-1+\alpha)\gamma_2}^{impar} - \overbrace{b\gamma_1}^{par}}{\underbrace{\gamma_1}_{impar}},$$

Por tanto β es impar con $\beta \in \mathbb{Z}^+$.

Análogamente,

Si β es par, entonces

$$\alpha = \frac{\overbrace{2^{r-s_2}k}^{par} - \overbrace{(d-1+\beta)\gamma_1}^{par} - \overbrace{c\gamma_2}^{par}}{\underbrace{\gamma_2}_{impar}},$$

Por tanto α es par con $\alpha \in \mathbb{Z}^+$.

Si β es impar, entonces

$$\alpha = \frac{\overbrace{2^{r-s_2}k}^{par} - \overbrace{(d-1+\beta)\gamma_1}^{impar} - \overbrace{c\gamma_2}^{par}}{\underbrace{\gamma_2}_{impar}},$$

Por tanto α es impar con $\alpha \in \mathbb{Z}^+$.

Esos α y β no estabilizan a f y por lo tanto f no es estabilizable en la condición (iii).

Si la condición (iv) se cumple entonces a, b son impares y c, d son pares.

Si α es par, entonces

$$\beta = \frac{\overbrace{2^{r-s_1}k}^{par} - \overbrace{(a-1+\alpha)\gamma_2}^{par} - \overbrace{b\gamma_1}^{impar}}{\underbrace{\gamma_1}_{impar}},$$

Por tanto β es impar con $\beta \in \mathbb{Z}^+$.

Si α es impar, entonces

$$\beta = \frac{\overbrace{2^{r-s_1}k}^{par} - \overbrace{(a-1+\alpha)\gamma_2}^{impar} - \overbrace{b\gamma_1}^{impar}}{\underbrace{\gamma_1}_{impar}},$$

Por tanto β es par con $\beta \in \mathbb{Z}^+$.

Análogamente,

Si β es par, entonces

$$\alpha = \frac{\overbrace{2^{r-s_2}k}^{par} - \overbrace{(d-1+\beta)\gamma_1}^{impar} - \overbrace{c\gamma_2}^{par}}{\underbrace{\gamma_2}_{impar}},$$

Por tanto α *es impar con* $\alpha \in \mathbb{Z}^+$.

Si β *es impar, entonces*

$$\alpha = \frac{\overbrace{2^{r-s_2}k}^{par} - \overbrace{(d-1+\beta)\gamma_1}^{par} - \overbrace{c\gamma_2}^{par}}{\underbrace{\gamma_2}_{impar}},$$

Por tanto α *es par con* $\alpha \in \mathbb{Z}^+$.

Esos α *y* β *no estabilizan a* f *y por lo tanto* f *no es estabilizable en la condición* (iv).

Así, en cada una de las cuatro condiciones f *no es estabilizable.*□

Veamos los siguientes ejemplos del Teorema 3.20.

Ejemplo 3.21. *Supongamos* $f = (x_1^7x_2^6u, x_1^8x_2^{15})$ *un SDMC sobre* $\mathbb{F}_{17}^2$. *Entonces,* $c = 8 = 2^3 \times 1$, $d - 1 = 14 = 2 \times 7$. *Note que,* $s_3 = 3 > 1 = s_4$. *Por Teorema anterior, parte* (1), f *no es estabilizable.*

Ejemplo 3.22. *Supongamos* $f = (x_1^{15}x_2^8, x_1^5x_2^{10}u)$ *un SDMC sobre* $\mathbb{F}_{17}^2$. *Entonces,* $a - 1 = 14 = 2 \times 7$, $b = 8 = 2^3 \times 1$. *Note que,* $s_2 = 3 > 1 = s_1$. *Por Teorema anterior, parte* (2), f *no es estabilizable.*

Ejemplo 3.23. *Supongamos* $f = (x_1^{13}x_2^5u, x_1^6x_2^{16}u)$ *un SDMC sobre* $\mathbb{F}_{17}^2$. *Entonces,* $a - c - 1 = 6 = 2 \times 3$, $d - b - 1 = 10 = 2 \times 5$. *Note que,* $s_1 = 1 = s_2$. *Por Teorema anterior, parte* (3), f *no es estabilizable.*

3.1. Conclusiones

En este trabajo hemos desarrollado criterios para determinar cuando un Sistema Dinámico Monomial de Control con una única variable sobre $\mathbb{F}_{2^r+1}^2$ es estabilizable.

Hemos utilizado resultados anteriores sobre Sistemas Dinámicos Monomiales, entre otros, para encontrar condiciones suficientes y necesarias para determinar su estabilidad. Utilizamos el Teorema 2.15, la Proposición 2.14, y otros más, para estabilizar un sistema dinámico monomial de control con una única variable. Al agregar más variables de control no se pudo estabilizar, ya que, las ecuaciones que nos generaban al utilizar la Proposición 2.14, envolvían más variables lo cuál dificultaba encontrar los valores pertinentes para estabilizar el sistema.

3.2. Trabajos Futuros

Necesitaremos crear criterios para determinar cuando un Sistema Dinámico Monomial de Control es estabilizable. Los que trabajan en esta área pueden considerar los siguientes:

1. Proveer criterios para determinar la estabilidad de un SDMC utilizando varias variables de control sobre $\mathbb{F}_q^2$, con $q \neq (2^r + 1)$ primo.

2. Proveer criterios para determinar la estabilidad de un SDMC con una única variable de control sobre $\mathbb{F}_q^2$, con $q \neq (2^r + 1)$ primo.

3. Proveer criterios para determinar la estabilidad de un SDMC utilizando varias variables de control sobre $\mathbb{F}_q^n$, con $n \in \mathbb{Z}^+$, $n \neq 2$ y q un primo arbitrario.

4. Proveer criterios para determinar la estabilidad de un SDMC con una única variable de control sobre $\mathbb{F}_q^n$, con $n \in \mathbb{Z}^+$, $n \neq 2$ y q un primo arbitrario.

5. Analizar la complejidad de los algoritmos para que un SDMC sea estabilizable.

6. Crear un algoritmo que provea una función de realimentación, si existe, para un SDMC sobre un cuerpo finito.

Apéndice A
TABLAS DE CONTROL

En las siguientes tablas daremos todas las posibles condiciones para que un sistema dinámico monomial de control sea estabiblizable. Suponemos que $u = x_1^{\alpha} x_2^{\beta}$, donde los α, β serán los exponentes que estabilizarán el sistema dinámico monomial de control. Observe que encontraremos casos en donde $\alpha = 0$, $\beta = 0$, ya que el sistema dinámico monomial desde un principio es un spf. Denotaremos impar con i y par con p.

Cuadro A–1: $f = (x_1^a x_2^b u, x_1^c x_2^d)$ con $0 < a, b, c, d \leq 2^r$

$f = (x_1^a x_2^b u, x_1^c x_2^d)$ con $0 < a, b, c, d \leq 2^r$, $u = x_1^\alpha x_2^\beta$						
	a	b	c	d	$gcd(a-1+\alpha, d-1, b, c, b+\beta)$	$(a-1+\alpha)(d-1) - c(b+\beta)$
(1)	p	p	p	p	i	$\alpha = 0$, $\beta = 0$, i
(2)	p	p	p	i	α par y β paridad arbitraria	PAR
(3)	p	p	i	p	i	$\alpha = 0$, $\beta = 0$, i
(4)	p	p	i	i	i	$\alpha = 1$, $\beta = 1$, i
(5)	p	i	p	p	i	$\alpha = 0$, $\beta = 0$, i
(6)	p	i	p	i	α par y β paridad arbitraria	PAR
(7)	p	i	i	p	i	$\alpha = 0$, $\beta = 1$, i
(8)	p	i	i	i	i	$\alpha = 1$, $\beta = 0$, i
(9)	i	p	p	p	i	$\alpha = 1$, $\beta = 0$, i
(10)	i	p	p	i	α impar y β paridad arbitraria	PAR
(11)	i	p	i	p	i	$\alpha = 1$, $\beta = 0$, i
(12)	i	p	i	i	i	$\alpha = 0$, $\beta = 1$, i
(13)	i	i	p	p	i	$\alpha = 1$, $\beta = 0$, i
(14)	i	i	p	i	α impar y β paridad arbitraria	PAR
(15)	i	i	i	p	i	$\alpha = 1$, $\beta = 1$, i
(16)	i	i	i	i	i	$\alpha = 0$, $\beta = 0$, i

Cuadro A–2: $f = (x_1^a x_2^b, x_1^c x_2^d u)$ con $0 < a, b, c, d \leq 2^r$

$f = (x_1^a x_2^b, x_1^c x_2^d u)$ con $0 < a, b, c, d \leq 2^r$, $u = x_1^\alpha x_2^\beta$						
	a	b	c	d	$gcd(a-1, d-1+\beta, b, c+\alpha)$	$(a-1)(d-1+\beta) - b(c+\alpha)$
(1)	p	p	p	p	i	$\alpha = 0$, $\beta = 0$, i
(2)	p	p	p	i	i	$\alpha = 0$, $\beta = 1$, i
(3)	p	p	i	p	i	$\alpha = 0$, $\beta = 0$, i
(4)	p	p	i	i	i	$\alpha = 0$, $\beta = 1$, i
(5)	p	i	p	p	i	$\alpha = 0$, $\beta = 0$, i
(6)	p	i	p	i	i	$\alpha = 0$, $\beta = 1$, i
(7)	p	i	i	p	i	$\alpha = 1$, $\beta = 0$, i
(8)	p	i	i	i	i	$\alpha = 1$, $\beta = 1$, i
(9)	i	p	p	p	α paridad arbitraria y β par	PAR
(10)	i	p	p	i	α paridad arbitraria y β impar	PAR
(11)	i	p	i	p	α paridad arbitraria y β par	PAR
(12)	i	p	i	i	α paridad arbitraria y β impar	PAR
(13)	i	i	p	p	i	$\alpha = 1$, $\beta = 1$, i
(14)	i	i	p	i	i	$\alpha = 1$, $\beta = 0$, i
(15)	i	i	i	p	i	$\alpha = 0$, $\beta = 1$, i
(16)	i	i	i	i	i	$\alpha = 0$, $\beta = 0$, i

Cuadro A–3: $f = (x_1^a x_2^b u, x_1^c x_2^d u)$ con $0 < a, b, c, d \leq 2^r$

$f = (x_1^a x_2^b u, x_1^c x_2^d u)$ con $0 < a, b, c, d \leq 2^r$, $u = x_1^\alpha x_2^\beta$						
	a	b	c	d	$gcd(a-1+\alpha, d-1+\beta, b+\beta, c+\alpha)$	t
(1)	p	p	p	p	i	$\alpha = 0$, $\beta = 0$, i
(2)	p	p	p	i	i	$\alpha = 0$, $\beta = 1$, i
(3)	p	p	i	p	i	$\alpha = 0$, $\beta = 0$, i
(4)	p	p	i	i	α par y β par ó α impar y β impar	PAR
(5)	p	i	p	p	i	$\alpha = 0$, $\beta = 0$, i
(6)	p	i	p	i	i	$\alpha = 0$, $\beta = 1$, i
(7)	p	i	i	p	α par y β impar ó α impar y β par	PAR
(8)	p	i	i	i	i	$\alpha = 0$, $\beta = 1$, i
(9)	i	p	p	p	i	$\alpha = 1$, $\beta = 0$, i
(10)	i	p	p	i	α par y β impar ó α impar y β par	PAR
(11)	i	p	i	p	i	$\alpha = 1$, $\beta = 0$, i
(12)	i	p	i	i	i	$\alpha = 1$, $\beta = 1$, i
(13)	i	i	p	p	α par y β par ó α impar y β impar	PAR
(14)	i	i	p	i	i	$\alpha = 1$, $\beta = 1$, i
(15)	i	i	i	p	i	$\alpha = 1$, $\beta = 0$, i
(16)	i	i	i	i	i	$\alpha = 0$, $\beta = 0$, i

Donde $t = (a-1+\alpha)(d-1+\beta) - (c+\alpha)(b+\beta)$.

Bibliografía

[1] Bollman, D., Colón-Reyes, O., Ocasio, V. A., and Orozco, E. (2010). A control theory for boolean monomial dynamical systems. *Discrete Event Dynamic Systems*, 20(1):19–35.

[2] Bollman, D., Colón-Reyes, O., and Orozco, E. (2007). Fixed points in discrete models for regulatory genetic networks. *EURASIP Journal on Bioinformatics and Systems Biology*, 2007:10–10.

[3] Colón-Reyes, O. (2005). *Monomial Dynamical Systems over Finite Fields*. Phd thesis, Virginia Tech.

[4] Colón-Reyes, O., Laubenbacher, R., and Pareigis, B. (2005). Boolean monomial dynamical systems. *Annals of Combinatorics*, 8(4):425–439.

[5] Colón-Reyes, Omar and Jarrah, A and Laubenbacher, Reinhard and Sturmfels, Bernd (2006). Monomial dynamical systems over finite fields. *arXiv preprint math/0605439*.

[6] Deng, G. (2015). Cycles of linear dynamical systems over finite local rings. *Journal of Algebra*, 433:243–261.

[7] Elspas, B. (1959). The theory of autonomous linear sequential networks. *Circuit Theory, IRE Transactions on*, 6(1):45–60.

[8] Ocasio, V. (2009). *Stability of Boolean Dynamical Systems and Graph Periodicity*. Master thesis, Univerisity of Puerto Rico at Mayagüez.

[9] Xu, G. and Zou, Y. M. (2009). Linear dynamical systems over finite rings. *Journal of Algebra*, 321(8):2149–2155.