1ER ENCUENTRO DE LÓGICA Y COMPUTACIÓN
Coalcomán, Michoacán

http://www.filosoficas.unam.mx/~Modus/AML.htm

25 y 26 de mayo de 2010

INSTITUTO TECNOLOGICO SUPERIOR DE COALCOMÁN

ACADEMIA MEXICANA DE LÓGICA

Academia Mexicana de Lógica

Instituto Tecnológico Superior de Coalcomán

COECYT MICHOACAN

Consejo Estatal de Ciencia y Tecnología

UNID
UNIVERSIDAD INTERAMERICANA PARA EL DESARROLLO

Universidad Interamericana Para el Desarrollo

Directiva de la AML

Mtra. Virginia Sánchez - Presidente
Mtra. Gabriela Guevara - Vicepresidenta
Lic. César López- Secretario
Mtra. Maricarmen Cadena Roa - Tesorera

Directorio del ITSC

Director: Mtro. Lauro Guillermo Pallares
Subdirección de Planeación y Vinculación: Biol. Martha Mireya Ortega
Subdirección Académica: Ing. Eduardo Iván Ávila
Jefe de Departamento Administrativo: C. P. Pedro Preciado Sánchez

Directorio del COECYT

Director: Mtro. Pedro Mata Vázquez
Subdirección de Difusión: DG. Lilia Vázquez
Subdirección de Planeación y Fomento: Lic. Romeo Amaurí López Calderón
Subdirección de Vinculación y Desarrollo Tecnológico: M.C. Rubén Salazar

Directorio de la UNID.

Director: Mtra. Paulina Adalid Fernández
Subdirector: Lic. Cesar González
Coordinador Académico: Dr. Carlos Guizar
Coordinador de la Maestría en Educación: Mtra. Guadalupe Fuentes
Coordinación de Tecnología de Información: Mtro. Claudio Florián Arenas
Coordinación de Comunicaciones: Lic. Marco Antonio Muñoz

Comité Organizador

Mtro. Jesús Castañeda R.
Mtro. Lauro G. Pallares.
Ing. Emanuel Gómez H.
Ing. Eduardo Iván Ávila R.
Ing. David A. Rangel S.
Ing. Víctor M. Preciado
Ing. Oscar G. Madrigal
Lic. Naara Bautista S.

Bienvenidos al 1er Encuentro de Lógica y Computación.

Coalcomán de Vázquez Pallares, Michoacán.

Con la finalidad de promover y difundir la investigación y formación matemática en sistemas computacionales y lógica, la Academia Mexicana de Lógica, el Instituto Tecnológico Superior de Coalcomán, la Universidad Interamericana para el Desarrollo y el Consejo Estatal de Ciencia y Tecnología organizan el Primer Encuentro de Lógica y Ciencias de la Computación orientada a profesores y alumnos de la región de Tierra caliente y la Costa Michoacana. Este encuentro promueve los estudios en ciencias e ingeniería, además de fortalecer la capacitación del profesorado de las instituciones de educación media superior y superior de la región.

Las temáticas del Encuentro corresponden a matemáticas aplicadas a la computación y al desarrollo de sistemas informáticos y computacionales. Se tratará sobre lógica computacional, criptografía y teoría de códigos, innovaciones tecnológicas, modelación matemática de sistemas complejos y computo científico.

Mtro. Jesús Castañeda Rivera

Comité Organizador

PRIMER ENCUENTRO DE LÓGICA Y CIENCIAS DE LA COMPUTACIÓN

El encuentro consta de cursos y conferencias magistrales

Conferencias:

Lógica y Computación. Raymundo Morado (IIF-UNAM)

Pensamiento Crítico en el Aula de Matemáticas. Virginia Sánchez (UNAM)

Teorema de Clasificación de los Espacios Duales Afines. Jesús Castañeda (UNID-Preu-UniNova)

Criptografía y Funciones Regulares. Luis Oregel (FCFM-UMSNH)

Cotas sobre Códigos y Códigos Perfectos. Juan J. Reynoso (FCFM- UMSNH)

Implementación de la Retroalimentación de las Estrellas Recién Nacidas Sobre la Nube Madre. Raúl Naranjo Romero (CRYA, UNAM)

"Herramientas de Tecnologías de Información en el Ámbito Educativo". Claudio Florián (UNID-ITSM)

Cursos:

C1. Hot Potatoes ejercicios educativos en apoyo a la práctica docente. Mtra. Joanna Koral Chávez. (UNID-UMSNH)

C2. Lógica Digital: principios y Aplicaciones. Edgardo Sotomayor (Colegio Reforma)

C3. **Códigos cíclicos y el lattice de Leech**. Jesús Castañeda Rivera (UNID-Preu-UniNova)

Desarrollo de Sesiones

8:30 Inauguración.

Hora	**25 de Agosto**	**26 de Agosto**
9-10	Inauguración	Oregel
10-11	Sánchez	Naranjo
11-11:30	Café	Café
11:30-13	Florián (postgrado UniNova)	Cursos: C1 (Laboratorio), C3 (salón)
13-14	Castañeda	Cursos: C2 (Laboratorio), C3 (salón)
16:00-17:00	Cursos: C1 (Laboratorio), C2 (salón)	Morado
17:00-18:00	Reynoso	Brindis

CONFERENCIAS

1. Lógica y Computación.

Raymundo Morado Estrada

Instituto de Investigaciones Filosóficas UNAM

www.filosoficas.unam.mx

Pasaremos revista a algunas contribuciones que la lógica ha hecho a la computación. Si bien el uso de mecanismos auxiliares es antiguo (el *Ars Magna* de Ramón Lull, o la lógica experimental de Annibale Pastore, por ejemplo), el poner la lógica al servicio de la computación cobró fuerza a partir de la tercera década del siglo XX. En esos años apareció la teoría de las funciones recursivas, y se sentaron las bases lógicas para estudiar el fenómeno de la complejidad computacional, los circuitos lógicos (para los que se aplica el cálculo proposicional

o álgebra booleana), la programación funcional (vista naturalmente como una instanciación del cálculo lambda), e incluso la programación lógica (con conceptos como la negación como falla, la resolución y la unificación).

Hoy la lógica ayuda a manejar la programación por objetos (inheritance), las semánticas para programas (lógicas lambda, temporales, dinámicas y lineales), el control de sistemas (temporales, dinámicas), la robótica (frame problem) y el manejo de bancos de datos "deductivas" (CWA, lógicas no monotónicas, circunscripción).

Esto ha requerido un cambio conceptual que todavía está en proceso. En el "Modelo Antiguo" empezábamos con axiomas intuitivos y procedíamos mediante deducción. Esto hacía innecesario investigar a fondo el manejo del error o la revisión. Después de todo, los sistemas deductivos clásicos tenían automáticamente monotonicidad por ser compactos.

Pero el mundo cambia y los agentes crean. Nuestras lógicas tienen que ser capaces de modelar estos fenómenos que en sí mismos no constituyen errores lógicos ni epistémicos. Tales modelos lógicos deben dar cabida al hecho de que la información requiere tanto recolección (que puede ser equivocada, contradictoria, incompleta) como procesamiento (que puede saltar a conclusiones para no ser demasiado lento).

Hay de permitir la modelación de la no-monotonicidad. Sin esto no hay un manejo adecuado de los bancos de datos deductivos que frecuentemente asumen el supuesto de mundo cerrado y utilizan varios tipos de circunscripción (especialmente de dominio y de predicado). En robótica, la no-monotonicidad auxilia con el problema del marco de coordenadas (frame) que indican qué propiedades o dimensiones cambian mientras otras permanecen. En el diseño de sistemas, proporciona mayor tolerancia a fallas; algo muy importante pues la complejidad de los sistemas interesantes lleva a la fragilidad. También se aplica al reconocimiento de patrones ya que es común que hagamos conjeturas visuales o fonológicas retractables.

El tratamiento lógico de la no-monotonicidad también nos ayuda a manejar la programación lógica con su noción de negación como falla, la teoría de los sistemas expertos y sus grados de confiabilidad, la representación del conocimiento mediante prototipos y herencia, y la búsqueda en inteligencia artificial del elusivo sentido común.

En resumen, además de todas sus contribuciones clásicas, las nuevas lógicas y los nuevos desarrollos de otras prometen ayudarnos a incorporar y modelar computacionalmente una amplia gama de razonamientos no deductivos,

incluyendo a los inductivos en que se generaliza a partir de algunos casos, los abductivos en que se concluye una explicación, los “prima facie” a los que se llega a falta de información en contra, los probabilísticos y los estadísticos.

La larga lista de contribuciones de la lógica al desarrollo, sistematización y entendimiento de la computación, promete ser incrementada exponencialmente en el siglo XXI. Sería una lástima que nos perdiéramos de estos beneficios por un incompleto conocimiento de ellos.

2. Pensamiento Crítico y sus posibles aplicaciones en el salón de clase.

Mtra. Virginia Sánchez Rivera

Universidad Nacional Autónoma de México

En este texto caracterizaré lo que entiendo como “Pensamiento Crítico” y señalaré tres tipos de asuntos de los que trata y pueden ser aplicables al salón de clases.

El Pensamiento Crítico implica desarrollar las habilidades, los conocimientos y las actitudes del razonamiento público, el diálogo y el debate, promoviendo modelos de educación que hacen énfasis en la pregunta crítica. Se trata de educar a las personas para que fundamenten y defiendan sus conocimientos y creencias presentando razones tanto por escrito como oralmente. Asimismo, el Pensamiento Crítico busca desarrollar en los estudiantes la capacidad de resolver problemas y la toma de decisiones razonables.

Proveniente de la tradición filosófica el Pensamiento Crítico ha sido definido como el pensamiento razonado, reflexivo que no es automático sino que requiere autodeterminación, esfuerzo, autocontrol y metacognición; ya que en su ejecución se evalúa no solamente el resultado sino el proceso mismo de pensamiento.

Se enfatiza el Pensamiento Crítico como una actitud intelectual que se propone evaluar los razonamientos: su forma y consistencia. Los analiza y evalúa en sus contextos naturales, supone la lógica formal en este análisis y evaluación, sin simbolizar los razonamientos sino en el lenguaje natural. Uno de los procedimientos es el de diagramación de los argumentos.

Me interesa señalar tres tipos de estudios posibles:

1) El análisis y evaluación de las creencias que las personas aceptan como verdaderas en la vida cotidiana.

2) La aplicación del método de resolución de problemas.

3) La lectura crítica.

3. CRIPTOGRAFIA Y FUNCIONES REGULARES

Jesús Castañeda Rivera, Luis Alberto Oregel Morales*

Universidad Interamericana Para el Desarrollo, Preuniversitaria, Universidad Nova Spania, Universidad Michoacana de San Nicolás de Hidalgo UMSNH*

Las S-cajas son unos de los componentes principales de los sistemas de cifrado simétrico tipo DES. En estos sistemas la seguridad depende de un conjunto de claves *K* y de la estructura de estas S-cajas (funciones regulares). El problema de seguridad de los sistemas criptográficos simétricos consiste en encontrar las funciones regulares que den al sistema la mayor seguridad informática. Este problema ha sido estudiado con anterioridad por muchos matemáticos y especialistas de la computación desde 1977, principalmente los trabajos ([3], [5], [6], [8]) han contribuido en la búsqueda de funciones que proporcionan sistemas criptográficos con la mayor seguridad posible. En este trabajo continuamos esta búsqueda y damos una solución parcial al problema para espacios de funciones regulares de dimensión pequeña.

1.1 NOTACIÓN Y DEFINICIONES BÁSICAS.

Sea V_n el espacio vectorial de dimensión *n* sobre el campo de dos elementos $\mathbb{F}_2$. Denotaremos a los elementos de V_n con los enteros v , $0 \le v \le 2^{n-1}$, el entero v representará al vector $(x_1, x_2, ..., x_{n-1})$ donde $v = x_0 + 2x_1 + ... + 2^{n-1}x_{n-1} = \sum_{i=1}^{n} 2^{i-1}x_{i-1}$ (aquí los x_i se interpretan como elementos del campo $\mathbb{F}_2$). Por ejemplo, el vector $(1,0,1,0) \in V_4$ es el número $(1,0,1,0) = 1 + 0 \bullet 2 + 1 \bullet 2^2 + 0 \bullet 2^3 = 5$.

Definición 1. *Si S es una función de V_n en V_m, su matriz de distribución es la matriz* $D^{(S)} = \left(d_{ij}(S)\right)$ *de* $2^n \times 2^m$ *en donde* $d_{ij}(S) := \left|\{x \in V_n / S(x) + S(x+i) = j\}\right|$.

Una función $S : V_n \to V_m$ *se llama regular sí* $\left|S^{-1}(y)\right| = 2^{n-m}$ $\forall y \in V_n$. *Es decir, en la sucesión de valores de la función cada elemento j de* V_m *aparece* 2^{n-m} *veces.*

Definición 2. *Sea* $S : V_n \to V_s$, *L el mayor valor de la tabla de distribución diferencial de S (omitiendo el primer renglón); sea R el número de entradas*

distintas de 0 en la primera columna de la tabla (omitiendo el primer renglón). Decimos que S tiene robustez

$$rob(S) = \left(1 - \frac{R}{2^n}\right)\left(1 - \frac{L}{2^n}\right). \qquad 0 \le rob(S) < 1.$$

1.2 GRUPOS OPERANDO EN FUNCIONES REGULARES

Para definir las S-cajas en el Data Encryption Standard no se consideran todas las funciones posibles (ver [1], [2], [3], [4], [5], [8]), se toman en cuenta solamente las llamadas funciones regulares.

El número de funciones regulares de V_n en V_m es

$$\frac{2^n!}{\left(2^{n-m}\right)!^{2^m}}$$

Esto es consecuencia de que el grupo simétrico S_{2^n} opera transitivamente en las funciones regulares y el subgrupo que deja fija una función regular es $S_{2^{n-m}} \times ... \times S_{2^{n-m}}$ de 2^m factores.

Consideremos el conjunto $S_{n,m}$ de todas las funciones regulares de V_n en V_m. Los grupos simétricos S_{2^n}, S_{2^m} operan en $S_{n,m}$ de la siguiente manera:

$$S_{2^m} \times S_{n,m} \times S_{2^n} \to S_{n,m}$$
$$(\sigma, S, \tau) \mapsto (\tau \circ S \circ \sigma)(x)$$

$\forall x \in V_n$.

Note que si S es regular, entonces $\tau \circ S \circ \sigma$ es también regular.

1.2.1 EL GRUPO AFÍN $Aff(n,2)$.

El grupo afín $Aff(n,2)$ se define como el producto semidirecto $Aff(n,2) = GL(n,2) \succ V_n$ con respecto a la operación natural de $GL(n,2)$ en V_n. El

grupo $Aff(n,2)$ es subgrupo del grupo simétrico S_{2^n}. En [5] se prueban los siguientes resultados:

(1) *Sean* $T:V_n \to V_n$, $T:V_m \to V_m$ *traslaciones y* $d_{i,((T\circ S)(j))}(T\circ S)$, $d_{ij}(S)$, $d_{i,((S\circ T)(j))}(S\circ T)$ *elementos de la tabla de distribución diferencial* $D^{(T\circ S)}, D^{(S)}, D^{(S\circ T)}$ *respectivamente. Entonces,*

$$d_{i,((T\circ S)(j))}(T\circ S) = d_{ij}(S) = d_{i,((S\circ T)(j))}(S\circ T)$$

Además, por consiguiente

$$rob(T\circ S) = rob(S) = rob(S\circ T)$$

(2) *Sean* $l:V_n \to V_n$, $l':V_m \to V_m$ *dos transformaciones lineales invertibles,* $S:V_n \to V_m$ *función regular. Entonces,*

$$rob(l'\circ S\circ l) = rob(S) = rob(l\circ S\circ l').$$

1.3 CLASES LATERALES DOBLES Y FUNCIONES REGULARES

Denotemos por $S_{3,2}$ el conjunto de todas las funciones regulares de V_3 a V_2**.** El grupo simétrico S_8 opera en $S_{3,2}$ de la siguiente manera

$$S_{3,2}\times S_8 \to S_{3,2}$$
$$(s,\sigma) \mapsto s\circ\sigma$$

Donde $\sigma \in S_8$. Es claro que si S es regular entonces $s\circ\sigma$ también es regular, pues si $y \in V_3$ como s es regular, se cumple que $\left|s^{-1}(y)\right| = 2$, y como $\sigma \in S_8$ es biyectiva $\left|\sigma^{-1}(s^{-1}(y))\right| = 2$. *Diremos que una función booleana* $f:V_n \to GF(2)$ *es balanceada si su imagen tiene el mismo número de Ceros y unos.*

Sea f una función booleana sobre V_n *y sea* $R \subseteq V_n$, *f se llama marginalmente balanceada sobre R si la imagen de R bajo f tiene igual número de ceros y unos.*

Sí $R \subseteq V_n$ y $f_1, f_2, ..., f_n, s > 0$ son funciones booleanas sobre V_n entonces hay una combinación lineal distinta de cero de términos marginalmente balanceados sobre

R. Esto es, hay una no cero combinación lineal de $f_2, f_3,..., f_s$ que es marginalmente balanceada sobre $R \cap f_1^{-1}(0)$ o sobre $R \cap f_1^{-1}(1)$ (R. Lidl y H. Niederreiter, 1983). Sí $R \subseteq V_n$ y $f_1, f_2,..., f_s$ son funciones balanceadas, dados $(y_1, y_2,..., y_s) \in V_s$, entonces f_s es marginalmente balanceada sobre $W = R \cap f_1^{-1}(y_1) \cap f_2^{-1}(y_2) \cap ... \cap f_{s-1}^{-1}(y_{s-1})$ y además $\left|W \cap f_s^{-1}(y_s)\right| = R/2^s$. (H. Tapia, G. Vega y Daltabuit, 1998)

Consideremos las siguientes afirmaciones.

Proposición 1. *Sea* s_0 *una función regular fija*

01	23	45	67
0	1	2	3

Entonces el conjunto $\{s_0 \circ \sigma | \sigma \in S_8\}$ *es igual al conjunto* $S_{3,2}$.

Note que la función $\varphi : S_8 \to S_{3,2}$ definida $s = s_0 \circ \sigma$, $\sigma \in S_8$. ϕ es suprayectiva puesto que dada $s_0 \in S_{3,2}$ y $\sigma \in S_8$, se pueden construir todas las funciones regulares de BR. Sin embargo, ϕ no es inyectiva, pues para s_0 y cada $\sigma \in S_8$ hay 16 permutaciones que dan la misma función.

Los ciclos (0,1), (2,3), (4,5), (6,7) dejan fija a s_0 . Esto es,

$$(0,1)s_0 = s_0, (2,3)s_0 = s_0, (4,5)s_0 = s_0, (6,7)s_0 = s_0$$

Y el subgrupo $H = < (0,1),(2,3),(4,5),(6,7) >$ de S_8 deja fija a s_0 . De lo anterior, tenemos que el número de funciones regulares de $S_{3,2}$ es

$$\left|S_{3,2}\right| = \frac{\left|S_8\right|}{\left|H\right|} = \frac{8!}{16} = 2,520$$

Consideramos el subgrupo $K = < (1,3)(2,4),(3,5)(4,6),(5,7)(6,8) >$ de S_8 , veamos qué $s_0 \circ \sigma k = s_0(\sigma k) = s_0$, $\forall \sigma \in S_8$ y $\forall k \in K$.

La función $\pi : S_8 \to S_{3,2}$ dada por $s_0 \circ \sigma k = s_0(\sigma k) = s_0$ es suprayectiva pero no inyectiva pues para cada clase lateral fija 24 permutaciones de s_0 . Como K es de

orden 4!, con la reducción anterior el número de funciones regulares es $\frac{2{,}520}{4!}=105$. Esto es,

$$\left|S_{3,2}\right|=\frac{\left|S_8\right|}{\left|H\right|\left|K\right|}=\frac{40{,}320}{384}=105.$$

Sea el grupo S_8 con subgrupos H y K, el conjunto de elementos KσH, donde σ es un elemento fijo de S_8 se llama clase lateral doble. Para el elemento $s_0\circ\sigma$, $s_0K\sigma H$ es una clase lateral doble.

Sea G un grupo de permutaciones con elementos $x_1,x_2,x_3,....x_n$ y sea S un subconjunto cualquiera de esos elementos, entonces las permutaciones de S forman un subgrupo H. Las permutaciones que permutan los elementos de S entre ellos forman un subgrupo K que contiene al subgrupo H como normal (M. Hall, 1979).

Para $G=S_8$, $K=<(1,3)(2,4),(3,5)(4,6),(5,7)(6,8)>$ y $H=<(0,1),(2,3),(4,5),(6,7)>$, entonces $H\lhd S_8$ donde $H=\left\{\rho h\rho^{-1}:\forall n\in H,\forall\rho,\rho^{-1}\in K\right\}$. Note que si $s_0\rho H\sigma$ es una clase lateral doble de KS_8H entonces $s_0\rho h\sigma=s_0h\rho\sigma\ \forall\rho\in K,\forall h\in H,\sigma\in S_8$. De lo anterior, se tienen las siguientes proposiciones:

Proposición 2. Sean las funciones regulares $s_0\rho\sigma:V_3\to V_2$ y $\rho's_0\sigma:V_3\to V_2$, $\rho\in K,\rho'\in S_8$. Dado $\rho\in K$ en $s_0\rho\sigma$ existe $\rho'\in S_8$ en $\rho's_0\sigma$ tal que $s_0\rho\sigma$ y $\rho's_0\sigma$ tiene la misma primer columna en la tabla de distribución diferencial D(S).

Sean $s_0\rho\sigma$ y $\rho's_0\sigma$ como en el diagrama

$$\begin{array}{ccc} V_3 & & \\ \downarrow\sigma & & \\ V_3 & \xrightarrow{\ \rho\ } & V_3 \\ \downarrow s_0 & & \downarrow s_0 \\ V_2 & \xrightarrow{\ \rho'\ } & V_2 \end{array}$$

Esto es, dada $\rho\in K$ en $s_0\rho\sigma$ existe $\rho'\in S_8$ en $\rho's_0\sigma$ tal que el diagrama conmuta.

Este resultado, lo podemos extender para cualquier para cualquier elemento del grupo afín *Aff(2,2).*

Corolario 3. Sea $S \in S_{3,2}$, $S_0 \in S_{3,2}$ la función regular fija, $\rho \in H \lhd S_8, \sigma, \rho' \in S_8$ y $a \in Aff(3,2)$. Entonces, en el espacio de funciones regulares $S_{3,2}$ el siguiente diagrama conmuta.

$$\begin{array}{ccc} V_3 & & \\ \sigma \downarrow & & \\ V_3 & \xrightarrow{\rho} & V_3 \\ s_0 \downarrow & & \downarrow s_0 \\ V_2 & \xrightarrow{\rho'} & V_2 \\ & & \downarrow a \\ & & V_2 \end{array}$$

Además, como $as_0\rho\sigma = a\rho' s_0\sigma$, entonces $rob(as_0\rho\sigma) = rob(a\rho' s_0\sigma)$.

1.4 CALCULO DE LA ROBUSTEZ DE FUNCIONES REGULARES EN $S_{3,2}$.

El grupo S_4 opera en el espacio de funciones regulares $S_{n,2}$ por composición:

$$\begin{aligned} S_4 \times S_{n,2} &\to S_{n,2} \\ (\sigma, S) &\mapsto \sigma \circ S \end{aligned}$$

Note que todas las orbitas de $S_{n,2}$ respecto del grupo S_4 tienen 24 elementos, esto es debido a que si $\sigma \circ S = S$ entonces $\sigma = i_d$. Por otra parte, S_4 es isomorfo al grupo Aff(2,2) y por las observaciones (1,2) en 1.2.1 (Ver [5]) los elementos de Aff(2,2) no cambian la robustez de una función regular. Por tanto, para el espacio de funciones regulares $S_{3,2}$ solo es necesario considerar $\frac{2{,}520}{4!} = 105$ funciones regulares.

En este espacio, las funciones solo tienen dos posibles robustez 0 y ¼. Hay 1,344 funciones con robustez ¼ y 1,176 funciones con robustez cero. La máxima robustez obtenida al considerar todas las funciones regulares fue ¼ y la cota teórica correspondiente es 0.416. (Ver [3], [6]) Podemos observar que la cota es significativamente mayor que el resultado experimental.

REFERENCIAS

[1] J**. Castañeda and H. Cárdenas**, “The Data Encryption Standard and Regular Mapping”, *Memories of 4to International Congress and 2do National Congress of Numerical Methods and Applied Mathematics*. Vol. **1**, pp., (2006).

[2] **J. Castañeda and H. Cárdenas**, “The Robust of Regular Mapping”, *Memories of 4to International Congress and 2do National Congress of Numerical Methods and Applied Mathematics*. Vol. **1**, pp., (2006).

[3] **J. Castañeda,** “The Data Encryption Standard And The Robust of Regular Mappings”, *tesis de licenciatura, Facultad de Ciencias Físico-Matemáticas Universidad Michoacana de San Nicolás de Hidalgo,* (2006).

[4] **J. Castañeda and E. Olmedo**, “Grupos que Actúan en Funciones Regulares”, *Contribuciones del VIII Coloquio Nacional de Criptografía, Teoría de Códigos y Aéreas Afines UAM.* Vol. **1**, pp. 3, 28., (2009).

[5] **J. Castañeda**, “Criptografía Numérica y la Robustez de Funciones Regulares”, *Memories of 5to International Congress of Numerical Methods and Applied Mathematics.* Vol. **1**. (2010).

[6] H. Tapia, G. Vega and E. Daltabuit, “Some Results on Regular Mappings”, *Applied algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Computer Science. 12th International Symposium, AAECC-12 Toulouse, France,* (1997).

[7] M. Hall, “The Theory of groups”, *Macmillan Company,* (1973).

[8] J. Seberry, X. Zhang and Y. Zheng, “Systematic generation of cryptographically robust S-boxes”, *In Proceedings of the First ACM Conference on Computer Communications Security, The Association for Computing Machnery New York*., Vol. **1**, pp. 172-182, (1993).

4. EL TEOREMA DE CLASIFICACIÓN DE LOS ESPACIOS DUALES AFINES.

Jesús Castañeda Rivera

Universidad Interamericana Para el Desarrollo, Universidad Nova Spania y Preuniversitaria.

Los espacios duales afines son geometrías con puntos y rectas, las rectas tienen tres puntos y por dos puntos pasa, cuando más, una recta. Además, se tiene que sus planos son los duales del plano afín sobre el campo de dos elementos. Si el espacio es conexo, se le asocian invariantes numéricos. Sea P un espacio dual afín conexo, dos puntos son colíneales si son dos puntos distintos en una recta. Sea p un punto en P y llamaremos D_P al conjunto de puntos de P no colineales

con p. Consideremos los siguientes números: n el número de elementos de P, k el número de elementos de D_P , si $q \notin D_P$ definimos $\mu = \left| D_p \cap D_q \right|$ y si $q \in D_P$ definimos $\lambda = \left| D_p \cap D_q \right|$. Ya que el espacio es conexo, estos números son independientes de la pareja de puntos p y q.

Estos espacios son en particular graficas, las aristas son pares de puntos colineales. En 1964, D. Higman encontró para una clase de graficas, que incluía las de los espacios duales afines, las siguientes relaciones:

Definimos los números $l = n - k - 1, \mu = \frac{3(k+1) - n}{2}, \lambda = k - 1 - \frac{l\mu}{k}$ y $h = \frac{l - (k - \lambda - 1)}{4}$.

1. *μ, λ, h, l son enteros positivos y n>k>μ, λ.*
2. $(\lambda - \mu)^2 + 4(k - \mu) = \delta^2$ *, donde* δ *es un número entero.*
3. δ *divide a* $D = 2k + (\lambda - \mu)(l + k)$ *.*
4. *Si n es un entero par, entonces* 2δ *no divide a D, si n es impar tenemos que* 2δ *divide a D.*

Una pregunta natural que surge: ¿Para qué parejas de números naturales (*n, k)* existen espacios duales afines P con $\left|P\right| = n$ y $\left|D_P\right| = k$?. Estos espacios han sido clasificados (Cárdenas; 1997, 1999, 2001, 2002, 2003); de esta clasificación se da respuesta a la pregunta.

El tema de este trabajo es resolver el mismo problema, sin recurrir a la clasificación geométrica, utilizando las propiedades algebraicas de las parejas (n, k) que cumplen las condiciones (1-4); y algunas propiedades que adicionare que distinguen los espacios duales afines de otras graficas consideradas por D. Higman.

A las parejas (n, k) que satisfacen las condiciones que se mencionan antes y propiedades adicionales se las llamaremos espacios duales afines numéricos. El resultado principal de la tesis es:

Teorema de Clasificación. *Sea (n, k) un espacio dual afín numérico, este puede ser:*

a) *Si h=1 , existe un entero* $t \geq 6$ tal que $n = \binom{t}{2}, k = \binom{t-2}{2}$

b) *Si h>1 , existe un entero* $t \geq 3$

I) $n = \binom{2^t}{2}, k = 2^t - 1$ *(Ortogonales+)*

II) $n = \binom{2^t + 1}{2}, k = 2^t - 1$ *(Ortogonales -)*

III) $n = 2^{2t} - 1, k = 2(2^{2(t-1)} - 1)$ *(Simplécticos)*

A los espacios del tipo a) se les llama espacios de Desargues y los espacios del tipo b) espacios de Reye.

ESPACIOS DUALES AFINES NUMÉRICOS

1.1 DEFINICIONES.

Sea *(n, k)* un par de enteros positivos con *n>k*. Definimos los números $l = n - k - 1, \mu = \frac{3(k+1) - n}{2}, \lambda = k - 1 - \frac{l\mu}{k}$, $h = \frac{l - (k - \lambda - 1)}{4}$.

Consideremos las parejas de números (n, k) que satisfacen las siguientes condiciones:

1. *μ, λ, h, l son enteros positivos y n>k>μ, λ.*
2. $(\lambda - \mu)^2 + 4(k - \mu) = \delta^2$ *, donde* δ *es un número entero.*
3. δ *divide a* $D = 2k + (\lambda - \mu)(l + k)$ *.*
4. *Si n es un entero par, entonces* 2δ *no divide a D, si n es impar tenemos que* 2δ *divide a D.*

5. Si $n \leq 36$ la pareja de números (n, k) es alguna de la lista: $\{(15,6),(21,10)(28,15),(36,15)\}$. A estas parejas se les llama primitivas.

   A cada pareja de números (n, k) que satisface las condiciones (1-4) podemos asociar una pareja de números (n', k') mediante la función $D:\{(n,k)\} \to \{(n',k')\}$ definida como $D(n,k) = \left(\frac{3(k+1)-n}{2}, \frac{3(\lambda+1)-k}{2} \right)$.

6. Si en la pareja (n, k) el número n>36 existe un entero positivo q tal que $D^q(n,k)$ es una pareja primitiva.

Definición 1. Un espacio dual afín numérico es *una pareja de números (n, k) que satisface las condiciones (1-6).*

Por brevedad, en adelante llamaré a los espacios duales afines numéricos, espacios afines.

Si (x, y) es un espacio afín y D(x, y)= (n, k) diremos que (x, y) es el sucesor de (n, k). En estos espacios, el sucesor no siempre es único.

Para la clasificación es útil notar, que la clase de los espacios duales afines numéricos con la operación de sucesor y el conjunto de parejas primitivas como elementos que no son sucesor de ningún otro es semejante a la descrita por Gussepe Peano para caracterizar los números naturales. Seguiremos el procedimiento natural de buscar subclases más simples.

Como es natural una subclase de la clase de los espacios duales afines numéricos es un subconjunto cerrado respecto a la operación de sucesor. En este caso, estudiaremos tres subclases especiales.

1.1 ESPACIOS DE DESARGUES.

Lema 1*. Si (n, k) es una pareja de números que satisface (1), entonces*

1. $lu = k(k - \lambda - 1)$

2. $l = 2(k - \mu + 1)$.

3. $l(l-2)=8hk$.

Prueba. *Se sigue directamente de las definiciones de μ, λ, h, l.*

De lo anterior obtenemos,

Proposición 1. *Sea (n, k) una pareja de números que satisface (1) con h=1, entonces existe un entero* $t \geq 6$ *tal que*

$$n=\binom{t}{2},\quad k=\binom{t-2}{2},\ \mu=\binom{t-3}{2}\ y\ \ \lambda=\binom{t-4}{2}$$

Prueba. Se sigue directamente de las relaciones del lema (1).

Definición 2*. Las parejas (n, k) con h=1 se llaman espacios de Desargues.*

Proposición 2. *Si (n, k) es un espacio de Desargues, entonces (n, k) es un espacio dual afín numérico. Además, es una subclase.*

Prueba. De la proposición anterior, $n=\binom{t}{2},\quad k=\binom{t-2}{2},\ \mu=\binom{t-3}{2},\quad \lambda=\binom{t-4}{2}$ *y se cumple (1). La condición (2) se sigue de que* $\delta=(t-2)$ *es un entero positivo para* $t\geq 3$ *. Para* $t\geq 5$, $D=(t-2)(t-3)-(t-4)(n-2)=2k-(t-4)(n-2)$ *y* $\frac{D}{\delta}=(t-3)-\frac{(t-4)(t+1)}{2}$ *es entero positivo y se cumple (3). Además, se cumple la condición (4),* $2\delta=2(t-2)$ *no divide a D. (5)* Las parejas primitivas (15,6), (21,10) y (28,15) son espacios de Desargues y el sucesor de un *espacio de Desargues con n>36 es otro espacio de Desargues*. De la condición (6), Para un espacio (x, y) de Desargues existe un entero positivo q tal que $D^q(x,y)=(28,15)$ o $D^q(x,y)=(21,10)$ o $D^q(x,y)=(15,6)$. Observe que, estos espacios son de la forma: $\left(\binom{t+3s}{2},\binom{t+3s-2}{2}\right)$ con s un entero positivo, t=8,7,6 y se cumple que $D^s(n,k)=\left(\binom{t}{2},\binom{t-2}{2}\right)$.

1.2 ESPACIOS DE REYE.

***Definición 3**. Un espacio dual afín numérico (n, k) se llama de Reye si h>1.*

Lema 2. *Sea (x, y) un una pareja de números positivos que satisface la condición (1) en la definición de espacio afín y (n, k) un espacio afín, entonces las condiciones*

a) y es raíz de la ecuación $y^2-(3n+k)y+3n(n-1)=0$.

b) D(x, y)=(n, k)

Son equivalentes.

Prueba. Directamente de la definición (1).

I) ESPACIOS SIMPLÉCTICOS S_P

Consideraremos los espacios afines con h>1 tal que para un entero m positivo $D^m(x,y)=(15,6)$. Cabe mencionar que, D (63,30) = (15,6). Note que el par (15,6) es de la forma $n=2k+3$.

Definición 4. Si para un espacio afín (n, k) existe un entero positivo m tal que $D^m(n,k)=(15,6)$ este espacio se llama simpléctico.

Proposición 3. Sea *(n, k)* un espacio afín tal que $k\equiv 6(\mathrm{mod}\,8)$ y $n=2k+3$, si $x=8k+15$ y $y=4k+6$ entonces *(x, y)* es un espacio dual afín numérico con *D(x, y)=(n, k). Además, si n>15 este par es el único sucesor de (n, k).*

Note que, si k=6, tenemos dos soluciones de $y^2-(3n+k)y+3n(n-1)=0$ que nos dan dos espacios numéricos (15,6), uno de Desargues y otro simpléctico.

Proposición 4. Si (n, k) es un espacio simpléctico, entonces $n=2^{2t}-1, k=2(2^{2(t-1)}-1)$

II) ESPACIOS ORTOGONALES

Consideremos los espacios afines *(n, k)* con $D^m(n,k)=(10,6)$ y $D^m(n,k)=(36,15)$, donde m es un entero positivo.

Definición 5. Si para un espacio afín (n, k) existe un entero positivo m tal que $D^m(n,k)=(10,6)$ o $D^m(n,k)=(36,15)$. El espacio (n, k) se llama ortogonal.

Observe que (10,6) y (36,15) son espacios de la forma *n =t(2t+1),* $k=t^2-1$ para *t=2,4* respectivamente. Tomemos los espacios *(n, k)* con *n =t(2t+1)* y $k=t^2-1$ donde t es un entero positivo mayor o igual a 2.

Proposición 5. Sea (n, k) un espacio afín tal que *n =t(2t+1) y* $k=t^2-1$ para t un entero par, $t\geq 2$. Si $x=(2t)(2(2t)-1), y=(2t)^2-1$ *entonces (x, y) es un espacio afín y D(x, y)=(n, k). Además, este par es el único sucesor de (n, k).*

Proposición 6. *Si (n, k) es un espacio ortogonal, entonces para* $t\geq 3$

I) $n=\binom{2^t}{2}, k=2^t-1$ *(Ortogonales+)*

II) $n=\binom{2^t+1}{2}, k=2^t-1$ *(Ortogonales -)*

Note que el sucesor de un espacio ortogonal (+,-) es un espacio ortogonal (-,+).

TEOREMA DE CLASIFICACIÓN

Teorema 1. *Sea (n, k) un espacio dual afín numérico, este puede ser:*

1. *Si h=1 , existe un entero* $t\geq 6$ tal que $n=\binom{t}{2}, k=\binom{t-2}{2}$
2. *Si h>1, existe un entero* $t\geq 3$

III) $n=\binom{2^t}{2}, k=2^t-1$ *(Ortogonales+)*

IV) $n = \binom{2^t + 1}{2}, k = 2^t - 1$ *(Ortogonales -)*

V) $n = 2^{2t} - 1, k = 2(2^{2(t-1)} - 1)$ *(Simplécticos)*

A los espacios del tipo 1) se les llama espacios de Desargues y los espacios del tipo 2) espacios de Reye.

REFERENCIAS.

[1]. Aschbacher, M. (1986). Finite Groups Theory. Cambridge Tracts in Mathematics 10.

[2]. Aschbacher, M. (1994). Sporadic Groups. Cambridge Tracts in Mathematics 104.

[3]. Batten L.M. (1997). Combinatorics of Finite Geometries. Second edition. Cambridge University Press.

[4]. Brown, R. and Humphiries, S. P. (1986). Orbits under Symplectic Transvections i and ii. Proc. London Math. Soc. 52, pp. 517-531, 532-556.

[5]. Castañeda, Jesús. (2011). Tesis de Maestría “Espacios Duales Afines Numéricos”. Universidad Interamericana Para el Desarrollo Campus Morelia.

[6]. Cárdenas, H. and Eat. (2001). Diagrams In categories of Partial Linear Spaces of Order Two. Communications in Algebra, pp. 1-6.

[7]. Cárdenas, H. Lluis, E. Raggi-Cárdenas, A. G. and Agustin, R. San. (1999). Diagrams for Symplectic Type configurations. Comm. In Algebra 27:7, pp. 3201-3210.

[8]. Cárdenas, H. and Eat. (2003). Diagrams In the Category of Fisher Spaces. Publicaciones preliminares. Instituto de Matemáticas, UNAM, pp. 3-5.

[9]. Cárdenas, H. and Eat. (2002). Partial Linear Spaces With Dual Affine Planes. Communications in Algebra, pp. 1-14.

[10]. Cárdenas, H. Lluis, E. Raggi-Cárdenas, A. G. and Agustin, R. San. (1997).Diagramas par alas Configuraciones Simplecticas y Ortogonales. Revista Iberoamericana de Matemáticas. I, Fasc. V. pp. 3-19.

[11]. Cárdenas, H. Lluis, E. Raggi-Cárdenas, A. G. and Agustin, R. Aan. (1997). A Diagram for the Partial Linear Space. Publ. Prel. Inst. Mat. 552. Pp- 1-6.

[12]. Cuypers, H. and hall, J. I. (1992). The Classifications of 3-Transposition Groups with Trivial Center. Proc. London Math.soc. 165. pp 121-138.

[13]. Fisher, B. (1971). Finite groups Generated by 3-Transpositions, Invetiones math. 13. Pp. 3-19.

[14]. Hall J. I. (1989). Graphs, Geometry, 3-Transpositions ans Symplectic-Transvection Groups. Proc. London. math. Soc. 58. Pp. 89-111.

[15]. Hall J. I. (1989). Some 3-Transpositions Groups with Normal 2-Subgroups. Proc. London. math. Soc. 58. Pp.112-136.

[16]. Hall J. I. (1983). Linear Representations of Cotriangular Spaces. Lin. Alg. And Appl. 49. Pp. 257-273.

[17]. Hall M. (1976). The Theory of Groups. Second edition. Chelsea Publishing Company.

[18]. Higman, D. (1964). Finite Permutation Groups of Rank 3. Math. Zeistchr. 86.

5. Cotas sobre Códigos y Códigos Perfectos.

Juan José Reynoso Cerano*, Jesús Castañeda Rivera
UNID, Preuniversitaria, UniNova, UMSNH*

Consideremos una fuente de mensajes X y un espacio vectorial F^n, denominamos código-bloque de longitud n, al conjunto $\phi(X) \subset F^n$ donde $\phi: X \to F^n$ es una función inyectiva. Para cualquier x en X, el elemento $\phi(x)$ se llama palabra código. Si el cardinal de X es M, nos referimos al código $\phi(X)$ como el código con parámetros C(M, n). Dados dos elementos x, y de F^n, la distancia de Hamming entre ellos es $d(x,y) = \left|\left\{i \middle| 1 \le i \le n, x_i \ne y_i\right\}\right|$. Para un código C(M, n) su distancia mínima es $\delta = \min\left\{d(x,y) \middle| x \ne y, x, y \in C\right\}$ y su radio de recubrimiento es $\rho = \max_{x \in F^n}\left\{\min_{v \in C}\left\{d(x,v) \middle| v \in C, x \in F^n\right\}\right\}$. Diremos que un código C(n, k) es lineal si es un subespacio vectorial de F^n con dimensión k. Consideremos las siguientes observaciones:

1. *La distancia de Hamming cumple las propiedades de distancia y define una métrica en* Q^n

Prueba: $\forall x, y, z \in Q^n$ se cumple

(i) $d(x,y) \geq 0$ y $d(x,y) = 0 \Leftrightarrow x = y$

(ii) $d(x,y) = d(y,x)$

(iii) $d(x,y) \leq d(x,z) + d(z,y)$

2. Si a la entrada de un canal hay una palabra código (x) y a la salida obtenemos un vector y, si $t = d(x,y)$ diremos que en la transmisión han ocurrido t-errores.

3. Note que a menor δ más facilidad tendremos de interpretar el elemento y si aumentamos δ aumenta la longitud del código n con lo que hay pérdida de velocidad de transmisión.

4. Si $|F| = q$ y es un código $C(M,n)$ construido sobre F^n, llamaremos tasa de transmisión de la información del código C al número

$$R = \frac{\log M}{\log q^n} = \frac{\log_q M}{n}$$

5. Si consideremos que F es $GF(q)$. Entonces dar un código-bloque $C(M,n)$ consiste en dar un subconjunto de F^n de cardinalidad M. En el campo $GF^n(q)$, podemos considerar las bolas $B_r(x)$ centradas en x, con x cada código palabra y r máximo posible. *El radio de estas bolas se puede calcular* $c = \left[\frac{\delta - 1}{2}\right]$ *donde* δ *es la distancia mínima. Llamamos capacidad correctora del código* $C(M,n)$ *al valor* $c = \left[\frac{\delta - 1}{2}\right]$ *también decimos que* C *es un código c-corrector.*

6. Sea C *un código* $C(M,n)$ *de* $GF^n(q)$*. Las bolas* $B_c(x)$ *son disjuntas.*

Prueba. En efecto si hay dos bolas con intersección no vacía existen $x, y \in C$ y $v \in GF^n(q)$, tal que $v \in B_c(x) \cap B_c(y)$. Entonces $d(x,v) \leq c$ y $d(v,y) \leq c$, por lo tanto

$$d(x,y) \leq d(x,v) + d(v,y) = c + c = 2c \leq \delta - 1 < \delta \quad \square$$

Probaremos los siguientes resultados:

1. Cota de Hamming. Para cualquier código C(M,n) en F^n, donde el cardinal de F es q, de capacidad correctora c y radio de recubrimiento ρ se cumple que $\frac{q^n}{\sum_{i=0}^{c} \binom{n}{i} (q-1)^i} \geq M \geq \frac{q^n}{\sum_{i=0}^{\rho} \binom{n}{i} (q-1)^i}$.

2. Cota de Gilbert-Varshamov. Para cualquier código C(M, n) en F^n,tenemos que $A(n,\delta) \geq \frac{q^n}{|B_{\delta-1}|}$, donde $|B_{\delta-1}|$ es la cantidad de elementos que hay en la bola de radio (δ-1), centrada en un vector de F^n y $A(n,\delta)$ es la cantidad de palabras código que tiene el mejor código de todos los que tienen longitud n y distancia mínima δ.
3. Cota de Plotkin. Sea C(n, k) un código lineal en F^n, donde *F=GF(q).* si $\delta > \theta n$ y $\theta = 1 - \frac{1}{q}$, entonces $q^k \leq \frac{\delta}{(\delta - \theta n)}$.
4. Cota de Singleton. En todo código lineal C(n, k) se cumple que $\delta \leq n - k + 1$.

REFERENCIAS.

[1]. J.H. Van. Lint. "*Introduction to Coding Theory"*. Springer-Verlag. (1982).

[2]. J. Castañeda, M. C. Suarez, E. Olmedo. "Numerical Self-Dual Codes", *Memories of 5to International Congress of Numerical Methods and Applied Mathematics.* Vol. **1**. (2010).

[3]. J. H. Conway and N. J. A. Sloane, "Sphere Packing's, Lattices and Groups", *Springer,* Vol. **190,** (1998).

6. TECNOLOGÍAS DE INFORMACION APLICADAS A LA EDUCACIÓN

Claudio Ernesto Florián Arenas, Universidad Interamericana para el Desarrollo.

En las últimas tres décadas el uso de Herramientas de Tecnologías de Información ha causado cambios en las actividades del ser humano, provocando con ello una constante innovación en las actividades cotidianas.

La información se ha convertido en el activo más valioso de las organizaciones. Donald Sanders lo predijo a principios de los años noventas: *"Es predecible con alto grado de probabilidad que la actividad del ser humano consistirá, independientemente de la carrera que escoja, en que se encuentre una estación de trabajo en su futuro; recibirá información de alguna fuente, hará algo con esa información y la remitirá a otra persona o estación. En pocas palabras, pasará el resto de su vida en una sociedad en la que la mayoría de las personas se ocupan de manipular y transmitir información"*[1]. En esos momentos era impensable el creer dicha predicción, pero al día de hoy eso se ha extendido, no solo para las personas que pertenecen a una organización, sino para cada individuo.

La comunicación es uno de los elementos esenciales en los que se apoya cualquier tipo de relación humana y es benéfica en prácticamente todos los sectores de la sociedad [2]. En este contexto es importante identificar que han surgido Tecnologías de Información que han causado diversos cambios en la forma de comunicarnos.

Con el surgimiento de Internet en el año de 1969 y la Web veinte años después [3], estos cambios se agudizaron y en un esfuerzo por mencionar los más utilizados y que representan un cambio radical, iniciamos mencionando el cambio en el correo postal sustituido por el correo electrónico, con la importante aportación de un símbolo que en un principio no tenía mucho significado: la @ arroba. La lectura de noticias tradicional en los periódicos a temprana hora, por la consulta de sitios de noticias por Internet, incluso las noticias en tu dispositivo móvil a través de un mensaje de texto (SMS). El cambio de formato de los libros impresos, a libros electrónicos. Acortando distancias, recursos y costos podemos mencionar la mensajería instantánea, video llamadas y foros; posteriormente con el surgimiento de la tan mencionada Web 2.0, podemos mencionar los sitios Web personales, blogs y redes sociales.

La forma de adquirir bienes y servicios también se ha visto inmiscuidos en este sector, incluso teniendo derrama económica hasta por $1,768 MUSD generados en el sector del comercio electrónico en 2008 en México [4].

Estas formas de comunicarse normalmente se han posicionado privilegiadamente en su momento encontrando en el entretenimiento la puerta de entrada al éxito. Sin embargo las personas involucradas en las Tecnologías de Información, se han encargado de encontrar otro tipo de utilidades a estas herramientas de tal forma que lejos de quedarse como entretenimiento se ajustan a herramientas productivas en cualquier ámbito.

Tal es el caso del ámbito educativo que nos ha involucrado a la gran mayoría en algún momento de nuestra formación. Partiendo de la idea que la relación de la Tecnología con la Educación desde dos vertientes: la administración educativa que se enfoca a los procesos administrativos y escolares como por ejemplo: los procesos que se llevan a cabo en las direcciones de servicios y control escolar, los de vinculación, orientación educativa, administrativos entre otros; y la segunda, en el proceso enseñanza – aprendizaje, en un inicio dentro del aula, y precisamente a través del uso de tecnología, fortaleciendo la formación en modalidad abierta, a distancia, en línea, móvil o alguna combinación entre ellas.

Y es que la tecnología se ha convertido en un factor de innovación constante en el quehacer cotidiano educativo y con ella, un sin número de soluciones con la firme

intención de obtener notables mejoras en las actividades que conduzcan al éxito educativo.

Sin embargo la tecnología de información por más robusta y eficiente que ésta sea, no es la solución a los problemas de formación a los que nos enfrentamos día a día, es un medio que proporciona algunos elementos que permiten influir en factores tales como ganar la atención del alumno, la diversidad de información, el poder cubrir en nuestras sesiones a un mayor número de tipo de alumnos a los que nos dirigimos, a la variedad de elementos y materiales de apoyo que se pueden exponer y producir, es decir, motivando hacia la innovación y creatividad de los educandos sin perder de vista que la guía y orientación sigue siendo responsabilidad del docente.

A lo anterior tendríamos que sumar situaciones que impiden que esto suceda con un mayor impacto dentro de nuestra sociedad: las condiciones socioeconómicas de algunos sectores que el país padece, en el sentido de poder llevar la tecnología apropiada a toda la población. En nuestro país, haciendo referencia a un estudio de infraestructura en el año 2010 realizado por la Asociación Mexicana de Internet (AMIPCI) [5], se menciona que solo 35.6 millones de personas tienen acceso a una computadora; de un total de 27.5 millones de hogares, solo 7.1 millones tienen acceso a Internet, esto refleja la carencia que se tiene al respecto. La resistencia al cambio por parte de las personas involucradas, el conformismo por no actualizarse en el ámbito de tecnologías de información dado que se considera aún, por increíble que parezca, que la computadora sustituye el capital humano.

Por otro lado, haciendo especial énfasis en el proceso enseñanza - aprendizaje, la falta de interés de algunos académicos por generar un ambiente de aprendizaje innovador y creativo, la falta de responsabilidad y compromiso por parte de los alumnos, al generar documentos, tareas e investigaciones plagiadas de Internet y/o de sus compañeros. Y entonces ¿Qué hacer ante la necesidad de involucrarse con el uso de las Tecnologías de Información en la Educación ante esta serie de problemáticas?

Y es aquí donde se inicia la lucha contra las barreras mencionadas en líneas anteriores, donde la labor de la gente dedicada al área del tratamiento de la información está orientada a brindar una amplia gama de soluciones diversas que se ajusten a las necesidades específicas de cada sector y nivel educativo, modalidad y de los actores involucrados.

Es objetivo de esta participación mostrar las diversas herramientas de Tecnologías de Información que pueden ser empleadas en el ámbito educativo abarcando sus dos vertientes: administración educativa y especialmente proceso enseñanza

aprendizaje, con la convicción de responder a la pregunta planteada dos párrafos arriba:

Promover el uso racional de Tecnologías de información como un medio de apoyo en el proceso enseñanza – aprendizaje que brinde a los involucrados, docentes y alumnos, los medios necesarios para cumplir los objetivos planteados para cada asignatura y así, coadyuvar a la formación de profesionistas competentes que con su labor, realicen aportaciones relevantes al desarrollo de nuestro país.

REFERENCIAS

[1] Sanders, D. (1993). *Informática presente y futuro.* USA. Mc Graw Hill.

[2] La importancia de la comunicación (s.f.) *En Pulevasalud de Pulevasalud.com* Recuperado de http://www.pulevasalud.com/ps/subcategoria.jsp?ID_CATEGORIA= 2073&RUTA=1-3-2071-2073

[3] Laudon, K. (2009). *E-commerce negocios, tecnología, sociedad.* México. Pearson Educación.

[4] Asociación Mexicana de Internet. *Estudio AMIPCI Ecommerce 2009.* México, D.F. Recuperado de http://www.amipci.org.mx/temp/AMIPCI_ECOMMERCE_2009-03444520012573566 17OB.pdf

[5] Asociación Mexicana de Internet. *Estudio AMIPCI Ecommerce 2009.* México, D.F. Recuperado de http://www.amipci.org.mx/temp/EstudioInfraestructuraAMIPCIresumenejecutivofinal-022331600126947999 6OB.pdf

7. Implementación de la Retroalimentación de las Estrellas Recién Nacidas Sobre la Nube Madre

Raúl Naranjo Romero, Centro de Radioastronomía y Astrofísica, UNAM, Campus Morelia

En el presente trabajo se describe la implementación en el código numérico Gadget2 del algoritmo para modelado de fotoionización por radiación propuesto por Dale, Ercolano & Clarke (2007), para su posterior uso en el estudio numérico de la evolución del Medio Interestelar (MI) bajo el efecto de dicho proceso. Primeramente se presenta un resúmen de la teoría relevante al medio interestelar, en particular a las nubes moleculares y las regiones dentro de ellas ionizadas por las estrellas recién formadas. Posteriormente, se describe el código Gadget2 y la implementación del algoritmo, que consiste en la selección de las partículas SPH que serán _ionizadas_ por la estrella a través de un criterio de radio de Strömgren de la estrella a la partícula. A continuación se describe la prueba del algoritmo,

consistente en verificar la evolución temporal del frente de ionización producido. Finalmente, se discuten las limitaciones y aplicaciones futuras del código.

Cuando observamos la Vía Láctea, vemos únicamente una parte de nuestra pequeña isla dentro del Universo, una galaxia espiral formada hace aproximadamente 1.5×10^{10} años y que contiene más de 10^{11} estrellas acompañadas de cerca de $10^9 M_\odot$[1] de gas y polvo.

Nuestra Galaxia comprende un disco con radio $\sim 25-32\,\mathrm{kpc}$ [2] y un espesor efectivo de $\sim 400-600\,\mathrm{pc}$ acompañado de un sistema esférico compuesto de un bulbo de radio $\sim 2-3\,\mathrm{kpc}$ y un halo extendiéndose a más de $30\,\mathrm{kpc}$ a partir del centro (Binney & Merrifield, 1998). El Sol reside en el disco galáctico aproximadamente $15\,\mathrm{pc}$ arriba del plano medio (Cohen, 1995; Magnani *et al.*, 1996) y a $\lesssim 8\,\mathrm{kpc}$ del centro galáctico (Groenewegen *et al.*, 2008).

Las estrellas que pertenecen al disco rotan en órbitas casi circulares y su tasa de rotación angular es una función decreciente de su distancia radial, de manera que la velocidad tangencial es casi constante a lo largo de la dirección radial. A la distancia galactocéntrica del Sol, la velocidad de rotación es de $\simeq 220\,\mathrm{km\,s^{-1}}$ (Kerr & Lynden-Bell, 1986), correspondiendo a un periodo orbital de cerca de 240 millones de años. La dispersión de velocidades de las estrellas en el disco es de $\sim 10-40\,\mathrm{km\,s^{-1}}$ (Mihalas & Binney, 1981), lo cual causa que una estrella tenga pequeñas oscilaciones alrededor de una órbita circular, tanto en el plano galáctico (epiciclos) como en el plano vertical. En contraste, las estrellas presentes en el bulbo y en el halo rotan lentamente y a menudo tienen órbitas muy excéntricas.

El Medio Interestelar (MI) es material formado en su mayoría por gas en estados ionizado, atómico y molecular, en rangos muy amplios de temperaturas, densidades y presiones característicos, además de partículas de polvo, rayos X y rayos cósmicos, inmersos dentro de un campo magnético.

Construir un modelo, incluso aproximado, de la Galaxia implica una gran dificultad. Sin embargo, podemos observar galaxias parecidas a la nuestra (p. ej. M31, la galaxia Andrómeda). Haciendo comparaciones entre observaciones, resultados analíticos y simulaciones numéricas es posible mejorar nuestros modelos con el fin de averiguar el por qué de la estructura y dinámica de la Galaxia o de sus componentes como las estrellas o el gas.

Referencias

[1] Binney, J. & Merrifield M. 1998. Galactic astronomy. Princeton University Press. 1998gaas.book.....B.

[2] Carroll B. W. & Ostlie D. A. 1996. An introduction to modern astrophysics, AddisonWesley. 1996ima..book.....C

[3] Dale J. E., Ercolano B. & Clarke C. J., 2007. A new algorithm for modeling photoionizing radiation in smoothed particle hydrodynamics. 2007MNRAS.382.1759D.

[4] Dyson J. E. & Williams, D. A. 1980. The physics of the interstellar medium. ISBN: 0-201-54730-9.

CURSOS:

C1. Hot Potatoes Ejercicios Educativos en Apoyo a la Práctica Docente.

I.S.C. Joanna Koral Chávez López
Facultad de Psicología. Universidad Michoacana de San Nicolás de Hidalgo

Los procesos de enseñanza deben irse actualizando debido a que la educación debe tener una visión renovada, es decir, debe existir una congruencia entre las necesidades de la sociedad y el campo productivo, lo cual obliga a las Instituciones de Educación a la continua revisión curricular.

Dado que el campo de estudio del maestro es heterogéneo y está determinado por las políticas hacia la educación, por la interacción maestro – alumno y por la institución y su curricula, etc. es necesario estar actualizándose en otras áreas que no necesariamente sean del campo de estudio en el cual se está especializado con la finalidad de que el docente desarrolle habilidades que le permitan transmitir el conocimiento para facilitar el aprendizaje a los alumnos.

Ya que el maestro se enfrenta a situaciones en las cuales es necesario recurrir a conocimientos de diferentes áreas en las que no se concentró su formación profesional, sino que son adquiridos por experiencia personal, por necesidad o por un deseo de superación personal.

Es por ello que necesario introducir a los docentes a impartir sus materias integrando las Tecnologías de la Información y Comunicación en cualquier nivel educativo a través de la realización de ejercicios interactivos que servirán de apoyo en las diferentes unidades de aprendizaje de cualquier materia, con la intensión de empezar a cambiar el proceso de enseñanza-aprendizaje tradicional, y poder desarrollar otras habilidades y competencias en alumnos y maestros para así mismo tratar de mejorar el proceso de enseñanza hacia los alumnos.

Apoyando con ello la visualización de otros campos de estudio que pueden ser implementados en su desarrollo profesional.

La necesidad no surge solo en introducir el uso eficiente de las nuevas tecnologías sino también en como poder conjuntar la didáctica, el diseño y la comunicación en los productos finales que coadyuven en mejorar del proceso de enseñanza – aprendizaje, generando en el alumno aprendizajes que ayuden a prepararse en la solución de problemas cercanos a su realidad y poder estimular su crecimiento como ser humano.

El rol de las tecnologías en el aprendizaje no es el de tratar de enseñar a los estudiantes, sino más bien el de servir de herramientas de construcción del conocimiento, para que los estudiantes aprendan con ellas.

Justificación

El desarrollo de las Tecnologías de Información y Comunicación ha permitido un área de trabajo para desarrollar contenidos, en un inicio la integración del concepto multimedia seguido de la interactividad que se puede agregar a dichos contenidos.

Con el desarrollo de contenidos interactivos a través de Internet, se ha permitido la creación de una serie de aplicaciones para crear ejercicios haciendo uso de las nuevas tecnologías. Ejercicios mediante los cuales brindan ventajas a alumnos, en el sentido de mostrarles la información de una manera más atractiva y a profesores que mediante estos recursos pueden motivar y familiarizar al alumno con las nuevas Tecnologías,

HotPotatoes es un programa que muchas comunidades educativas nacionales e internacional han estado aplicando, por lo cual es necesario el conocimiento para cualquier profesional en el ámbito educativo.

Destinatario

Maestros y aspirantes a la función docente en cualquier nivel educativo, estudiantes que proyectan su acción profesional en el campo de la educación.

Objetivo General

- Conocer la utilidad de HotPotatoes.
- Aprender a realizar los diferentes tipos de ejercicios que se pueden crear con HotPotatoes.
- Ser capaz de crear configuraciones personalizadas y poder usarlas de forma conveniente.
- Ser capaz de crear ejercicios que integren vídeo, imágenes y sonidos.
- Obtener la habilidad necesaria para crear ejercicios atractivos visualmente para el alumnado.

Contenido

- **Unidad 1: Instalando y Configurando Hotpotatoes**
    1. Introducción
        - Características de HotPotatoes
    2. Descarga e Instalación
    3. Primer Uso de HotPotatoes
    4. Menús y Configuración de HotPotatoes
        - Menú Archivo
        - Menú Potatoes
        - Menú Opciones
        - Menú Ayuda

    5. Opciones de Configuración Comunes
        - Configurar el formato del archivo originado
            - ✓ Títulos / Instrucciones
            - ✓ Avisos / Indicaciones
            - ✓ Botones
            - ✓ Aspecto
            - ✓ Contador
            - ✓ Otros
            - ✓ Personalizar

        - Fuentes
        - Derecha a Izquierda
        - Opciones de la Barra de Herramientas

        - Cambiar y restaurar la ubicación de los archivos fuente
        - Guardar la configuración

    6. Opciones para la Edición de Contenidos
    7. Conclusión
- **Unidad 2: Las Bases de HotPotatoes**
    1. Un ejercicio de muestra con JQuiz
        - Configuración
        - Crear el ejercicio
        - Cambiar el aspecto del ejercicio
            - ✓ Imagen de fondo
            - ✓ Colores
            - ✓ Tipo de letra
            - ✓ Guardar la configuración
            - ✓ Resultados
    2. Opciones para los Archivos
        - Tratamiento básico del archivo
        - Añadir contenidos al archivo
        - Exportar: Elegir el formato de salida del archivo del ejercicio
    3. Nociones Básicas de HTML
    4. Realizar un Ejercicio con JMix
        - Configuración
        - Creando un ejercicio
    5. Conclusión
- **Unidad 3: Ejercicios avanzados con HotPotatoes**
    1. Introducción
    2. Entender y Organizar los Archivos

        - Un caso práctico

    3. Conclusión
- **Unidad 4: The Masher**
    1. The Masher
        - La Interfaz del Programa
            - ✓ Menú Archivo
            - ✓ Menú Acciones
            - ✓ Menú Opciones
            - ✓ Menú HotPotatoes.net
            - ✓ Menú Ayuda
        - Agrupando ejercicios en una unidad didáctica con The Masher

- Modificando el Archivo Índice
- Construyendo el Archivo Índice de forma independiente

2. Conclusiones

Evaluación

Cada uno de los participantes expondrá sus ejercicios elaborados de un tema de alguna de sus materias y los compañeros retroalimentarán lo expuesto.

Metodología

Se utilizará una página http://www.congresopsicologia.com/producto_multimedia/HOTPOTATOES2.htm de apoyo durante el curso en la cual podrán ver información de cada uno de los temas del contenido del taller, así como ejemplos para cada unidad para cada unidad se presentaran objetivos particulares, actividades de aprendizaje, estrategias de enseñanza, para que los asistentes puedan ver que se están cumpliendo con los objetivos planteados con todo esto se podrá observar las ventajas que este tipo de ejercicios ofrece tanto a alumnos y profesores en el proceso de enseñanza-aprendizaje.

Referencias

Hot Potatoes .Versión 6.Recuperado de http://blogtics-oaxaca.blogspot.com/
http://hotpot.uvic.ca/
http://platea.pntic.mec.es/~iali/CN/Hot_Potatoes/intro.htm

Chávez, Joanna. (2011). Proyecto aplicativos "Las tecnologías de información y comunicación (TIC'S) como apoyo en la actividad docente universitaria: una propuesta de elaboración de ejercicios interactivos". Universidad Interamericana para el Desarrollo. Campus Morelia.

C2. LÓGICA DIGITAL: PRINCIPIOS Y APLICACIONES. Lic. Edgardo Sotomayor (AML)

C3. CÓDIGOS CICLICOS Y EL LATTICE DE LEECH. Mtro. Jesús Castañeda Rivera (UNID).

Este es un curso introductorio a la teoría de códigos cíclicos detectores de errores (Hamming y Golay) y algunas estructuras algebraicas que enriquecen su análisis matemático. La teoría de códigos algebraicos se encuentra ligada a problemas de transmisión de la información y señales, codificación de información digital como:

Internet, telefonía celular, CD´s, y otros dispositivos electrónicos. El problema de encontrar códigos uniformemente perfectos (aquellos que transmiten sin error alguno la información) ha sido estudiado desde muchos años, introduciendo a esta área nuevas técnicas matemáticas como la teoría de grupos finitos, teoría de módulos, algebras de Lie, algebras de Griess, algebras de vértices, formas modulares y teoría de números.

0. PRELIMINARES.

Consideremos un conjunto F con las operaciones de suma y producto usuales, diremos que F es un campo si cumple las siguientes condiciones:

1. Clausura: a = c y b = d implica (a + b) = (c + d) y a · b = c · d
2. Asociatividad: (a + b) + c = a + (b + c) (a · b) · c = a · (b · c)
3. Elementos neutros: a + 0 = a y a · 1 = a, además 0 es distinto de 1.
4. Inversos aditivos: existe (−a) tal que a + (−a) = 0
5. Conmutativa: a + b = b + a a · b = b · a
6. Distributiva: a · (b + c) = a · b + a · c
7. inversos para el producto: si a es distinto de 0 existe a^* talque a · a^* = a^* · a = 1

Un ejemplo de campo son los números reales, números racionales y los números complejos con sus operaciones usuales.

El campo más pequeño puede tener al menos dos elementos {0,1} que llamamos F_2. En este caso, al conjunto de los números enteros lo dividimos en dos clases, los números pares a quienes asignamos el valor 0 y los números impares a quienes asignamos el 1. Por ello, es común la notación $F_2 = Z/2Z$. A continuamos escribimos el campo que corresponde a F_2.

F_2:

```
+ | 0 1        · | 0 1
--+----        --+----
0 | 0 1        0 | 0 0
1 | 1 0        1 | 0 1
```

Otro ejemplo interesante, es el campo de tres elementos.

F_3:

```
+ | 0 1 2      · | 0 1 2
  --+------      --+------
  0 | 0 1 2      0 | 0 0 0
  1 | 1 2 0      1 | 0 1 2
  2 | 2 0 1      2 | 0 2 1
```

Dado un numero primo p y Z el conjunto de los números enteros, podemos construir campos finitos dividiendo a los enteros en p clases. Esto es, formando el conjunto $F_p = Z / pZ$.

Grupos

Un conjunto G con una operación $\circ$ se llama grupo si cumple las condiciones:

$a)(\forall a,b \in G)(a \circ b \in G)$
$b)(\forall a,b,c \in G)(a \circ (b \circ c) = (a \circ b) \circ c)$
$c)(\exists 1 \in G)(\forall a \in G)(a \circ 1 = a = 1 \circ a)$
$d)(\forall a, a^* \in G)(\exists 1 \in G)(a \circ a^* = 1 = a^* \circ a)$

Donde a*es el inverso de a. Si además, G cumple la condición $(\forall a,b \in G)(a \circ b = b \circ a)$ se llama grupo abeliano o conmutativo.

Si H es un subconjunto de G y, cumple que $(\forall a,b,c \in H)(a \circ (b \circ c) = (a \circ b) \circ c)$, entonces diremos que H es un subgrupo de G. Un ejemplo de grupo son los enteros Z con la operación suma.

Dos grupos G, G* con las operaciones $(\bullet, *)$ respectivamente, son isomorfos si existe una función biyectiva $f : G \to G^*$ tal que

$$(\forall g, g' \in G)(f(g \bullet g') = f(g) * f(g'))$$

Es compatible con las operaciones.

El isomorfismo f entre un mismo grupo G se llama automorfismo. El conjunto de los automorfismos de un grupo G, Aut(G) forman un grupo con la operación de composición.

Anillos.

Sea A un conjunto con las operaciones usuales de suma y producto, llamaremos A anillo si cumple las siguientes condiciones:

a) A es un grupo abeliano respecto a la suma.

$b)(\forall a,b,c \in A)(a(bc) = (ab)c)$

$c)(\forall a,b,c \in A)(a(b+c) = (ab + ac))$

El elemento identidad de A respecto a la operación de suma es el cero (0). Si un anillo cumple adicionalmente que $(\forall a,b\in A)(ab=ba)$ Llamamos a este anillo conmutativo. Por ejemplo, los números enteros Z forman un anillo conmutativo o el conjunto de polinomios P(x) sobre un campo F, forman otro anillo conmutativo.

Sea A un anillo y S un subconjunto no vacío de A, entonces llamamos ideal si cumple las condiciones:

$a)(\forall a,b\in S)(a-b\in S)$
$b)(\forall a,b\in S)(ab\in S \quad y \quad ba\in S)$

Un módulo izquierdo sobre un anillo Z es un grupo abeliano (G,+) y una operación

$$Z\times G\to G$$
$$(r,x)\mapsto rx\in G$$

Que cumple las siguientes propiedades:

$a)(rs)x=r(sx)$
$b)(r+s)x=rx+sx$
$c)r(x+y)=rx+ry$
$d)1\bullet x=x$

Que también llamamos Z-módulo izquierdo o simplemente, ${}_Z$M. Un Z-modulo derecho M_Z se define con las mismas propiedades, pero con la operación por derecha

$$G\times Z\to G$$
$$(x,r)\mapsto xr\in G$$

Si Z es conmutativo, lo Z-módulos por izquierda son lo mismo que los Z-módulos por derecha y se llama simplemente Z-módulo.

Sea M un Z-modulo. Si H es un subgrupo de G (el grupo de M), entonces H es un submodulo de M. Un modulo es finitamente generado si existe un número finito de elementos $x_1,x_2,...,x_n$ en G tales que cada elemento de G es una combinación lineal de esos coeficientes del anillo escalar Z.

Espacios Vectoriales.

Sea (V,+) un grupo abeliano, F un campo finito. Lamamos V espacio vectorial si la relación

$$F_2 \times V \to V$$
$$(a, v) \to a \circ v$$

Cumple las siguientes condiciones:

$a)(\forall a \in V)(1 \circ a \in V)$
$b)(\forall \alpha, \beta \in F_2)(\forall a \in V)(\alpha \circ (\beta \circ a) = (\alpha \circ \beta) \circ a))$
$c)(\forall \alpha, \beta \in F_2)(\forall a \in V)((\alpha + \beta) \circ a) = (\alpha \circ a + \beta \circ a))$

Si W es subconjunto de V y cumple las condiciones (a, b y c), W se llama subespacio vectorial de V. Un ejemplo de espacio vectorial es el espacio R^n de n dimensiones y el espacio de los polinomios p(x) sobre un campo F, que denotamos F[x].

Una aplicación $F : V \times V \to R$ se llama forma bilineal sobre un espacio vectorial V si cumple las siguientes condiciones:

$a)(\forall u, u^*, v \in V)(F(u + u^*, v) = F(u, v) + F(u^*, v))$
$b)(\forall u, u^*, v \in V)(F(v, u + u^*) = F(v, u) + F(v, u^*))$
$c)(\forall u, v \in V, t \in R)(F(tv, u) = tF(u, v)); \quad (F(v, tu) = tF(u, v))$

Si $(\forall u, v \in V)(F(u, v) = F(v, u))$ decimos que la forma bilineal es simetrica. El núcleo de F es el conjunto $\ker F := \{ y \in V \mid F(x, y) = 0, \forall x \in V \}$. El *ker(F)* contiene al elemento identidad de V y es subespacio vectorial de V. Decimos que la forma bilineal es regular si *ker(F)={identidad de V}.* Si *ker(F)* es distinto de *{identidad de V}*, la forma bilineal se llama singular.

Se denomina forma cuadrática sobre V a toda aplicación $q : V \to R$ que cumple que:

$$(\forall v \in V)(q(v) = F(v, v))$$

Donde F es una forma bilineal sobre V.

I.CÓDIGOS CICLICOS.

Sea F_2 el campo de dos elementos $F_2 = \{0,1\}$. Denotemos a Z como el conjunto de los números enteros y $F_2^n = \{0,1\}^n$ un espacio vectorial. Un código C es un subconjunto de F_2^n; cuando C es un subespacio vectorial de dimensión k en F_2^n

decimos que el código C es lineal. En este caso, decimos que C es un C(n,k) código.

Un código C de longitud n es cíclico si para toda permutación $\pi:\{v_0,v_1,...,v_{n-1}\}\to\{v_0,v_1,...,v_{n-1}\}$ de un elemento de C es también otro elemento de C. Esto es, si $v:=(v_0,v_1,...,v_{n-1})\in C$ entonces $v\circ\pi:=(v_{n-1},v_0,...,v_{n-2})\in C$.

Para estudiar las propiedades algebraicas de estos códigos es posible utilizar una descripción polinomial. A cada elemento v de C podemos asociarle un polinomio v(x). Llamaremos C(x) al conjunto de polinomios asociados a los elementos de C. El grado de cada polinomio v(x) será menor o igual a la dimensión n del espacio. Observemos que cada polinomio $(v\circ\pi)(x)$ será producto de algún polinomio v(x) por x modulo (x^n-1).

Proposición 1. *Un código C(n, k) es cíclico si y solo si C(x) es un ideal de anillo* $F_2[x]/<x^n-1>$.

Prueba. Sean u, v elementos del código C entonces u+v es elementos de C. Por tanto, u(x), v(x) son polinomios de C(x) y u(x)+v(x) es polinomio de C(x). Por definición de las operaciones en $F_2[x]/<x^n-1>$, $(u+v)(x)=u(x)+v(x)\in C(x)$, luego C(x) es un subgrupo de $F_2[x]/<x^n-1>$. Por otro lado, si v(x) es un polinomio de C(x) entonces $x\bullet v(x)$ es un polinomio de C(x) y por inducción sobre i, $0\le i\le n-1$, $x^i\bullet v(x)\in C(x)$. Por linealidad sobre el subespacio C, $a_i(x^i\bullet v(x))\in C(x)$ para cualquier $a_i\in F$. Esto es, $\sum_{i=0}^{n}(a_ix^i)\bullet v(x)\in C(x)$. Que también podemos escribir $v(x)\bullet a(x)C(x)$ donde $a(x)\in F_2[x]/<x^n-1>$.

Proposición 2. *Sea C un código cíclico de longitud n y C(x) un ideal en* $F_2[x]/<x^n-1>$*, g(x) un polinomio mónico en C(x) de grado r. Entonces,*

(1) g(x) es el único polinomio mónico de grado r del ideal C(x).
(2) g(x) genera a C(x) como ideal principal. Esto es,

$$C(x)=<g(x)>=\{r(x)g(x)\,|\,grad(r(x))<n-r\}.$$

(3) g(x) divide a x^n-1.
(4) $\{x^i\bullet g(x)\,|\,0\le i\le n-r-1\}$ *genera a C(x) como subespacio vectorial. En particular,* $\{g(x),xg(x),x^2g(x),...,x^{n-r-1}g(x)\}$ *es una base de C.*

Proposición 3. *A todo divisor mónico g(x) de* x^n-1 *le corresponde un código cíclico de longitud n, donde los polinomios asociados a v de C, son los múltiplos de g(x) y si r es el grado de g(x), entonces la dimensión del código asociado es k=n-r y su matriz generadora es*

$$G=\begin{bmatrix} g_0 & g_1 & g_2 & ... & 1 & 1 & 0 & ... & 0 \\ 0 & g_0 & g_1 & ... & g_{r-1} & 1 & 0 & ... & 0 \\ 0 & 0 & g_0 & ... & g_{r-2} & g_{r-1} & 1 & ... & 0 \\ . & . & . & ... & . & . & . & ... & . \\ . & . & . & ... & . & . & . & ... & . \\ . & . & . & ... & . & . & . & ... & . \\ 0 & 0 & 0 & ... & g_0 & g_1 & g_3 & ... & 1 \end{bmatrix} \begin{matrix} \leftrightarrow & g(x) \\ \leftrightarrow & xg(x) \\ \leftrightarrow & x^2g(x) \\ . & . \\ . & . \\ . & . \\ \leftrightarrow & x^{n-r-1}g(x) \end{matrix}$$

Prueba. En efecto, v(x) está en C(x), y se escribe v(x)=a(x)g(x) con el grado de a(x) menor que n-r. Consideremos que a(x) es un polinomio asociado a $a=(a_0,a_1,...,a_{k-1})$. Si $v(x)=v_0+v_1x+v_2x^2+...+v_{n-1}x^{n-1}$, resulta que

$$\begin{aligned} v_0 &= a_0g_0 \\ v_1 &= a_0g_1+a_1g_0 \\ v_2 &= a_0g_2+a_1g_1+a_2g_0 \\ &.... \end{aligned}$$

Y observamos que los mismos valores de v_i son obtenidos por el producto

$$(a_0,a_1,...,a_{k-1})\bullet G=(a_0g_0,a_0g_1+a_1g_0,a_0g_2+a_1g_1+a_2g_0,...)$$

Siendo G la matriz generadora del código.

Veamos una forma polinomial de construir matrices de control para códigos.

Sea $h(x)=\dfrac{x^n-1}{g(x)}$ donde <g(x)>=C(x) con longitud n y dimensión k=n-r. Llamamos h(x) al polinomio de control de C(x). Consideremos c(x)=v(x)h(x). Los coeficientes c_i del polinomio C(x) son:

$$
\begin{aligned}
c_0 &= v_0h_0 + v_1h_{n-1} + v_2h_{n-2} + ... + v_{n-1}h_1 \\
c_1 &= v_0h_1 + v_1h_0 + v_2h_{n-1} + ... + v_{n-1}h_2 \\
&... \\
c_k &= v_0h_k + v_1h_{k-1} + ... + v_{k-1}h_1 + v_kh_0 \\
c_{k+1} &= v_0h_k + v_2h_{k-1} + ... + v_kh_1 + v_{k+1}h_0 \\
&... \\
c_{n-1} &= v_{n-k-1}h_k + v_{n-k-2}h_{k-1} + ... + v_{n-2}h_1 + v_{n-1}h_0
\end{aligned}
$$

Note que los coeficientes c_i son coordenadas de $H'(v)$ con H' la matriz:

$$
H' = \begin{bmatrix}
h_0 & 0 & 0 & ... & 0 & h_k & h_{k-1} & h_{k-2} & ... & h_1 \\
h_1 & h_0 & 0 & ... & 0 & 0 & h_k & h_{k-1} & ... & h_2 \\
h_2 & h_1 & h_0 & ... & 0 & 0 & 0 & h_k & ... & h_3 \\
. & . & . & ... & . & . & . & . & ... & . \\
. & . & . & ... & . & . & . & . & ... & . \\
. & . & . & ... & . & . & . & . & ... & . \\
h_k & h_{k-1} & h_{k-2} & ... & h_3 & h_2 & h_1 & h_0 & ... & 0 \\
0 & h_k & h_{k-1} & ... & h_4 & h_3 & h_2 & h_1 & ... & 0 \\
. & . & . & ... & . & . & . & . & ... & . \\
. & . & . & ... & . & . & . & . & ... & . \\
. & . & . & ... & . & . & . & . & ... & . \\
. & . & . & ... & . & . & . & . & ... & . \\
. & . & . & ... & . & . & . & . & ... & . \\
0 & 0 & 0 & ... & h_k & h_{k-1} & h_{k-2} & h_{k-3} & ... & h_0
\end{bmatrix}
$$

La matriz H' tiene filas dependientes. Solo habrá (n-k) filas linealmente independientes; con las ultimas(n-k) filas linealmente independientes formaremos una matriz que genera el código dual (ortogonal a C) que llamamos C*. Llamamos H a la matriz:

$$H=\begin{bmatrix} h_k & h_{k-1} & h_{k-2} & .... & h_1 & h_0 & 0 & 0 & ... & 0 \\ 0 & h_k & h_{k-1} & ... & h_2 & h_1 & h_0 & 0 & ... & 0 \\ 0 & 0 & h_k & ... & h_3 & h_2 & h_1 & h_0 & ... & 0 \\ . & . & . & ... & . & . & . & . & ... & . \\ . & . & . & ... & . & . & . & . & ... & . \\ . & . & . & ... & . & . & . & . & ... & . \\ 0 & 0 & 0 & ... & h_k & h_{k-1} & h_{k-2} & h_{k-3} & ... & h_0 \end{bmatrix}$$

Note que H es la matriz generadora del código cíclico del polinomio generado h*(x), cuyos coeficientes son justamente los de h(x) en orden inverso. $h^*(x)=x^k h(x^{-1})$ es llamado polinomio reciproco.

Proposición 4. *Sea C un código cíclico, el código ortogonal (dual) C* es cíclico y tiene polinomio generador g*(x)=h*(x).*

La matriz de control del código cíclico C* tiene por filas los coeficientes de los polinomios

$$h^*(x), xh^*(x), x^2h^*(x), ..., x^{n-k-1}h^*(x)$$

CÓDIGOS CÍCLICOS C(7, 4)

El polinomio x^7-1 puede descomponerse en el siguiente producto de polinomios irreducibles:

$$x^7-1=x(x^3+x+1)(x^3+x^2+1)$$

El polinomio $g(x)=x^3+x+1$ divide a $(x^7-1)\in F_2[x]$. Entonces, g(x) genera un código lineal cíclico y tiene por matriz generadora

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \begin{matrix} \leftrightarrow & x^3+x+1 \\ \leftrightarrow & x(x^3+x+1) \\ \leftrightarrow & x^2(x^3+x+1) \\ \leftrightarrow & x^3(x^3+x+1) \end{matrix}$$

Su polinomio de control es $h(x)=\dfrac{x^7-1}{x^3+x+1}=x^4+x^2+x+1$, y por tanto, el polinomio reciproco es $h^*(x)=x^4(x^{-4}+x^{-2}+x^{-1}+1)=1+x^2+x^3+x^4$ que genera una matriz de control

$$H=\begin{pmatrix}1&0&1&1&1&0&0\\0&1&0&1&1&1&0\\0&0&1&0&1&1&1\end{pmatrix}\begin{matrix}\leftrightarrow\ h^*(x)\\\leftrightarrow\ xh^*(x)\\\leftrightarrow x^2h^*(x)\end{matrix}$$

La matriz H es equivalente a la matriz de control de un código de Hamming, para parámetro t=3. Un código de Hamming es un subespacio vectorial H con $n=2^t-1, k=2^t-1-t$. Para la matriz H con t=3, su código H(7,4) es un código de Hamming (extendido).

El polinomio $(x^7-1)\in F_2[x]$ podemos factorizarlo

$$H(x)=x^7+1=x(x^3+x+1)(x^3+x^2+1)$$

En donde los dos polinomios irreducibles $(x^3+x+1),(x^3+x^2+1)$ generan un código de Hamming (no extendido), uno ortogonal (dual) del otro, al formar los ideales $H=Z_2[x]/(x^3+x+1)$ y $H^*=Z_2[x]/(x^3+x^2+1)$. El ideal

$F_2^3[x]/(x^3+x+1)=\{0,1,\alpha,\alpha^2,\alpha^3=\alpha+1,\alpha^4=\alpha^2+\alpha,\alpha^5=\alpha^2+\alpha+1,\alpha^6=\alpha^2+\alpha\}$ genera el campo finito:

$+$	0	1	α	α^2	α^3	α^4	α^5	α^6
0	0	1	α	α^2	α^3	α^4	α^5	α^6
1	1	0	$\alpha+1$	α^2+1	α	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2
α	α	$1+\alpha$	0	$\alpha^2+\alpha$	1	α^2	α^2+1	$\alpha^2+\alpha+1$
α^2	α^2	α^2+1	$\alpha^2+\alpha$	0	$\alpha^2+\alpha+1$	α	$\alpha+1$	1
α^3	α^3	α	1	$\alpha^2+\alpha+1$	0	α^2+1	α^2	$\alpha^2+\alpha$
α^4	α^4	$\alpha^2+\alpha+1$	α^2	α	α^2+1	0	1	$\alpha+1$
α^5	α^5	$\alpha^2+\alpha$	α^2+1	$\alpha+1$	α^2	1	0	α
α^6	α^6	α^2	$\alpha^2+\alpha+1$	1	$\alpha^2+\alpha$	$\alpha+1$	α	0

Que podemos escribir en potencias de α:

$+$	0	1	$\alpha 3$	α^2	α^3	α^4	α^5	α^6
0	0	1	α	α^2	α^3	α^4	α^5	α^6
1	1	0	α^3	α^6	α	α^5	α^4	α^2
α	α	α^3	0	α^4	1	α^2	α^6	α^5
α^2	α^2	α^6	α^4	0	α^5	α	α^3	1
α^3	α^3	α	1	α^5	0	α^6	α^2	α^4
α^4	α^4	α^5	α^2	α	α^6	0	1	α^3
α^5	α^5	α^4	α^6	α^3	α^2	1	0	α
α^6	α^6	α^2	α^5	1	α^4	α^3	α	0

En este caso, el polinomio (x^3+x+1) es divisor mónico de x^7+1 y el ideal $z_2[x]/(x^3+x+1)$ está contenido en el ideal $z_2[x]/(x^7+1)$ como ideal principal, que describimos en el siguiente diagrama

$$\begin{array}{ccccc} (x^7+1) & \rightarrow & z_2[x] & \rightarrow & z_2[x]/(x^7+1) \\ \downarrow & & \downarrow & & \downarrow \\ (x^3+x+1) & \rightarrow & z_2[x] & \rightarrow & z_2[x]/(x^3+x+1) \end{array}$$

Para el ideal

$F_2^3[x]/(x^3+x^2+1)=\{0,1,\beta,\beta^2,\beta^3=\beta^2+1,\beta^4=\beta^2+\beta+1,\beta^5=\beta+1,\beta^6=\beta^2+\beta\}$ el campo finito que le corresponde es

$+$	0	1	β	β^2	β^3	β^4	β^5	β^6
0	0	1	β	β^2	β^3	β^4	β^5	β^6
1	1	0	β^5	β^3	β^2	β^6	β	β^4
β	β	β^5	0	β^6	β^4	β^3	1	β^2
β^2	β^2	β^3	β^6	0	1	β^5	β^4	β
β^3	β^3	β^2	β^4	1	0	β	β^6	β^5
β^4	β^4	β^6	β^3	β^5	β	0	β^2	1
β^5	β^5	β	1	β^4	β^6	β^2	0	β^3
β^6	β^6	β^4	β^2	β	β^5	1	β^3	0

En este caso, el polinomio (x^3+x^2+1) es divisor mónico de x^7+1 y el ideal $z_2[x]/(x^3+x^2+1)$ esta contenido en el ideal $z_2[x]/(x^7+1)$, como ideal principal, que describimos en el siguiente diagrama

$$\begin{array}{ccccc} (x^7+1) & \rightarrow & z_2[x] & \rightarrow & z_2[x]/(x^7+1) \\ \downarrow & & \downarrow & & \downarrow \\ (x^3+x^2+1) & \rightarrow & z_2[x] & \rightarrow & z_2[x]/(x^3+x^2+1) \end{array}$$

Se puede verificar que $H \cong H^*$. H es un código autodual, pues H es isomorfo a su ortogonal H*.

II. CÓDIGOS AUTODUALES Y EL LLATICE DE LEECH.

Sea Ω un conjunto finito de *n* elementos. El conjunto potencia de Ω es $P(\Omega)=\{S \mid S \subset \Omega\}$ y puede verse como un GF(2)-espacio vectorial bajo la operación + de la diferencia simétrica. Un código lineal binario C es un GF(2)-subespacio vectorial de $P(\Omega)$. La cardinalidad $|c|$ de un elemento c de un código es llamada el peso de c. *Un código C es del tipo I si* $n \in 2Z$ *y para todo* $c \in C$ *se tiene que* $|c| \in 2Z$ *y* $\Omega \in C$. *Un código C es del tipo II si* $n \in 4Z$ *y para todo* $c \in C$ *se tiene que* $|c| \in 4Z$ *y* $\Omega \in C$. Z es el conjunto de los números enteros.

Dado un código C, su código dual C es* $C^* = \{S \subset \Omega \| S \cap C| \in 2Z, \forall c \in C\}$.

Note que C es el aniquilador de C en* $P(\Omega)$ *con respecto a la forma bilineal simétrica no singular* $(S_1, S_2) \mapsto |S_1 \cap S_2| + 2Z$ *sobre* $P(\Omega)$.

Observaciones:

1.1 El producto $\langle \bullet, \bullet \rangle : P(\Omega) \times P(\Omega) \rightarrow F_2$ *definido por* $(S,T) := |S \cap T| \bmod 2$ *es una forma bilineal simétrica.*

Prueba. Veamos qué $\langle S+S', T \rangle = \langle S,T \rangle + \langle S',T \rangle$. Note que $\langle S,T \rangle = |S \cap T| \bmod 2$ y $\langle S',T \rangle = |S' \cap T| \bmod 2$.

$$\langle S+S', T \rangle = |(S+S') \cap T| \bmod 2 = |((S \cup S') \cap T) - ((S \cap S') \cap T)| \bmod 2 =$$

$$= |S \cap T| \bmod 2 + |S' \cap T| \bmod 2 = \langle S,T \rangle + \langle S',T \rangle$$

Por otra parte,

$$\langle S,T\rangle = |S\cap T| \bmod 2 = |T\cap S| \bmod 2 = \langle T,S\rangle .$$

1.2 Un código C es auto-dual si C=C.*

$$C^* := \{T \mid \langle T,T\rangle = 0, (\forall T)(T\in C)\}$$

Si n es par, se cumple que $\dim C_{F_2} + \dim C^*_{F_2} = \dim V$ *, donde V es* $P(\Omega)$ *y tiene dimensión n. Si el código es autodual C=C* y* $\dim C_{F_2} = \dim C^*_{F_2}$ *. Tenemos que*

$$\dim C_{F_2} + \dim C^*_{F_2} = \dim C_{F_2} + \dim C_{F_2} = 2\dim C_{F_2} = \dim V = n .$$

Entonces,

$$\dim C_{F_2} = n/2 .$$

1.3 Consideremos el conjunto $\varepsilon(\Omega) := \{S\subset\Omega \,\|S|\in 2Z\}$ *. La función* $q := \varepsilon(\Omega)\to Z/2Z := F_2$ *definida* $S\mapsto \frac{|S|}{2}+2Z$ *es una forma cuadrática sobre* $\varepsilon(\Omega)$ *con una forma bilineal asociada* $\langle\bullet,\bullet\rangle : P(\Omega)\times P(\Omega)\to F_2$ *dada por* $(S_1,S_2)\mapsto |S_1\cap S_2|+2Z$ *.*

Prueba. En el caso $n\in 2Z$, $F_2\Omega$ es el radical de la forma q definida por $q(S) := \frac{|S|}{2} \bmod 2$.

Veamos que $q(S+S') = q(S)+q(S')+2\langle S,S'\rangle$. Note que $2\langle S,S'\rangle = 0$ y

$$q(S)+q(S') = \frac{|S|}{2}\bmod 2 + \frac{|S'|}{2}\bmod 2 = \frac{1}{2}\left[|S|+|S'|\right]\bmod 2 = \frac{1}{2}|S+S'| \bmod 2 = q(S+S')$$

Llamaremos H(C) a la distribución de peso de un código C: $H(C) = \sum_{c\in C} q^{|C|} \in Z[q]$

2.1 CÓDIGOS NUMÉRICOS AUTODUALES.

Una construcción del Lattice de Leech se presenta en [3], mediante la construcción del código de Golay. Una forma de construir el código de Golay es construyendo el código de Hamming. Estudiaremos esta construcción.

Proposición 5. *Hay un código auto-dual C de tipo II sobre un conjunto Ω de 8-elementos. Este código es el código de Hamming.*

Podemos identificar Ω con la línea proyectiva sobre el campo de siete elementos F_7. Esto es, $\Omega = P^1(F_7) = F_7 \cup \{\infty\}$, en donde podemos considerar los conjuntos $\pi^* = \{x^2 \,|\, x \in F_7\} = \{0,1,2,4\}$ y $\pi = \Omega / \pi^* = \{3,5,6,\infty\}$. Podemos definir los Subespacios $C_1 = \{\pi + i \,|\, i \in F_7\}$ y $C_2 = \{-\pi - i \,|\, i \in F_7\}$ de $\varepsilon(\Omega)$.

Los subespacios C_1, C_2 forman un código de Hamming. La dimensión de cada subespacio es 4 y su forma cuadrática en ambos casos es cero. El espacio suma $C_1+C_2=\varepsilon(\Omega)$ y la intersección de C_1 y C_2 es $F_2\Omega$.

El Código de Hamming H es único (salvo isomorfismo) y tiene distribución de peso $1+14q^4+q^8$.

Proposición 6. *Hay un código auto-dual C de tipo II sobre un conjunto Ω de 24-elementos tales que C no tiene elementos de peso 4. Este código C es el código de Golay.*

Sean C, C códigos de Hamming en ε(Ω). Denotemos por 3Ω al conjunto unión de tres copias de Ω. En el espacio 24-dimensional P(3Ω), definimos C como*

$$C = \langle (S,S,\varnothing),(S,\varnothing,S),(T,T,T) \,|\, S \in C, T \in C^* \rangle$$

El espacio C es una suma directa ortogonal de los tres subespacios 4-dimensionales totalmente singulares de *ε(3Ω). Así, C es código autodual de tipo II y totalmente singular.*

El código de Golay es único (salvo isomorfismo) y tiene distribución de peso $1+759q^8+257q^{12}+759q^{16}+q^{24}$. Los 759 elementos del código de Golay de peso 8 son llamamos octetos. El conjunto unión de todos los octetos es el código de Golay. En este caso, el grupo de automorfismos de C es el grupo de Mathieu M_{24}.

$$M_{24}=Aut(C)$$

El grupo M_{24} es un grupo simple no abeliano. Una representación natural de M_{24} sobre P(Ω) en la lista completa de submódulos es

$$0 \subset \langle \Omega \rangle \subset C \subset \varepsilon(\Omega) \subset P(\Omega)$$

En particular C/<Ω> y ε(Ω)/C son módulos irreducibles para Aut(C).

2.2 EL CÓDIGO DE GOLAY Y EL LATTICE DE LEECH

Un código C es autodual de tipo II sobre Ω, está dado por un lattice unimodular $h=\coprod_{k\in\Omega}F_{w_k}$, que es un espacio vectorial con base $\{w_k\,|k\in\Omega\}$ con una forma bilineal simétrica asociada $\langle w_k,w_l\rangle=2\delta_{k,l}$ para $k,l\in\Omega$. Para $S\subset\Omega$, el conjunto $w_s=\sum_{k\in S}w_k$ define $h=\coprod_{k\in\Omega}Z_{w_k}$ y para un código C sobre Ω, define el lattice positivo $L_0=\sum_{c\in C}Z\frac{1}{2}w_C+Q$, o equivalentemente, $L_0=\left\{\sum_{k\in\Omega}m_kw_k\,\middle|\,m_k\in\frac{1}{2}Z,\left\{k\,\middle|\,m_k\in Z+\frac{1}{2}\right\}\in C\right\}$. Note que L_0 es par si y solamente si $|c|\in 4Z,\forall c\in C$. Un lattice dual L_0^* de L_0 es el correspondiente lattice sobre un código dual C* (código dual de C). Definimos L_0^*

$$L_0^*=\left\{\sum_{k\in\Omega}m_kw_k\,\middle|\,m_k\in\frac{1}{2}Z,\left\{k\,\middle|\,m_k\in Z+\frac{1}{2}\right\}\in C*\right\}$$

Proposición 7. *Un código C es autodual de tipo II si y solamente si L_0 es autodual o unimodular.*

Prueba. Consideremos la modificación de L_0 respecto a C,

$$L_0=\sum_{c\in C}Z\frac{1}{2}w_C+\sum_{k\in\Omega}Z\left(\frac{1}{4}w_\Omega-w_k\right)=\sum_{c\in C}Z\frac{1}{2}w_C+\sum_{k,l}Z\left(w_C+w_l\right)+Z\left(\frac{1}{4}w_\Omega-w_{k_0}\right)$$

Donde k_0 es un punto fijo de Ω, entonces

$$L_0\cap L_0^*=\sum_{c\in C}Z\frac{1}{2}w_C+\sum_{k,l}Z\left(w_C+w_l\right)$$

Además, L_0^* es unimodular si y solamente L_0 también lo es. La condición necesaria para que L_0^* sea par es que $n=|\Omega|\in 8(2Z+1)$, esto es que $\left\langle\frac{1}{4}w_\Omega-w_k,\frac{1}{4}w_\Omega-w_k\right\rangle=\frac{n}{8}+1$ y k en Ω. Finalmente, podemos dar la siguiente afirmación:

Si $n\in 8(2Z+1)$ y C es un código autodual de tipo II, entonces le corresponde un lattice unimodular $\Lambda=L_0^*$.

Cuando n=24, el lattice Λ se llama lattice de Leech y C es el código de Goley G.

Se puede probar que esta construcción del Lattice de Leech es equivalente a definir al lattice de Leech de la siguiente manera:

Sea *V=P(Ω)* el conjunto potencia del conjunto Ω y sea C un subespacio vectorial de V, consideremos que C es de tipo II, $\Omega \in C$ y $|\Omega| = n$ con $n = 8(2k+1)$. Consideremos el conjunto $\Lambda^* := \{v = (a_i)\}$ de F^n con las siguientes condiciones:

$1) a_i \in Z, i \in \Omega.$

$2) m(v) = \sum a_i / 4 \in Z$

$3) a_i \equiv m(v) \bmod 2, (\forall i)(i \in \Omega)$

Sea $S(v) = \{i \in \Omega | a_i \not\equiv m(v) \bmod 4\}$, entonces

4) $S(c) \in C$.

Se puede probar que el conjunto Λ^* es equivalente a otro conjunto Λ (Λ* es autodual)

Sea F un campo con característica cero, consideremos el mapeo $w: \Omega \to F^n$, definido por $w(S) = w_S = (a_i)$ con $a_i = 1$ cuando $i \in S$ y cero en otro caso.

Asociemos a C un lattice Λ (subgrupo del grupo aditivo F^n), el lattice Λ es generado por $2w_S, S \in C$, y $w_\Omega - 4w_i, i \in \Omega$, la restricción a Λ del producto escalar de F^n es el producto escalar en Λ.

Probaremos que $\Lambda = \Lambda^*$.

Lema 8. *Sean $u, v \in F^{24}$, entonces*

1) $m(u+v) = m(u) + m(v)$

2) $-m(u) = m(-u)$.

3) $S(u+v) = S(u) + S(v)$

Prueba. 1) Note que $m(u+v)=\sum_i \frac{a_i+b_i}{4}=\sum_i \frac{a_i}{4}+\sum_i \frac{b_i}{4}=m(u)+m(v)$.

2) Claramente, $-m(u)=-\sum_i \frac{a_i}{4}=\sum_i \frac{-a_i}{4}=m(-u)$

3)

$$S(u+v)=\{i\in\Omega \,|\, a_i+b_i \not\equiv m(u+v) \bmod 4\}=\{i\in\Omega \,|\, a_i \not\equiv m(u) \bmod 4, b_i \not\equiv m(v) \bmod 4\}=$$

$$=\{i\in\Omega \,|\, a_i \not\equiv m(u) \bmod 4\}+\{i\in\Omega \,|\, b_i \not\equiv m(v) \bmod 4\}=S(u)+S(v)$$

El lema anterior prueba que Λ* es un subgrupo de F^n, es claro que los generadores de Λ están contenidos en Λ*, entonces Λ es subgrupo de Λ*.

Lema 9. Para $i, j\in\Omega$ los vectores $4w_i+4w_j$ y $8w_i$ esta en Λ.

Prueba. Note que $2w_\Omega-(w_\Omega-4w_i+w_\Omega-4w_j)=4w_i+4w_j$. Consideremos $v=(a_i)$ en Λ* con $m(v)\equiv 0(\bmod 4)$, entonces las coordenadas a_i son pares, tenemos que $a_i=8b_i+c_i$ con b_i un entero y $c_i\in\{0,2,4,6\}$. Por el lema (8), el vector $u=8b_i$ esta en Λ y entonces, $v^*=v-u=(c_i)\in\Lambda^*$ con $m(v^*)$ par. Definamos los conjuntos $S:=\{i\in\Omega \,|\, c_i=0,4\}$ y $T:=\{i\in\Omega \,|\, c_i=2,6\}$, de la condición (4) de la definición de Λ* tenemos que $S,T\in C$. Ahora definamos $S^*:=\{i\in\Omega \,|\, c_i=4\}$ y $T^*:=\{i\in\Omega \,|\, c_i=6\}$, donde $|T|=4t$, t entero. Recordemos que C es de tipo II, si $|S^*|=r$ y $|T^*|=s$ (r, s enteros) entonces, $m(v^*)=r+s+2t$ y tenemos que $m(v^*)$ es par, de donde $r+s$ es par. Tomemos una partición P de $S^*\cup T^*$ en subconjuntos U={i,j}, definimos $v_U=4w_i+4w_j$, el vector $v_P=(v_U)\in\Lambda$ y $v^*-v_P=2w_T$ .Finalmente, $v\in\Lambda^*$ y $m(v)\equiv 2(\bmod 4)$, el vector $v^*=v+8w_i$ tiene $m(v)\equiv 0(\bmod 4)$, y si $v\in\Lambda^*$se tiene que $m(v)\equiv 1,3(\bmod 4)$, el vector $v^*=v+w_\Omega-4w_i$ tiene que $m(v)\equiv 2,4(\bmod 4)$.

DISCUSIÓN

Una representación del código de Hamming en Ω es el grupo simple E8, el código de Goley se genera de tres copias de Ω y una forma de definir el lattice de Leech (J**. Leech,** 1966) es $\Lambda=E8\oplus E8\oplus E8$. El descubrimiento de Λ se relaciona con el problema de transmisión de información y el problema de empacamiento de esferas: Dado un código C en un espacio V, es posible construir un código que llene todo el espacio (código perfecto), esto consiste en optimizar los elementos

de C en V con una distancia mínima uniforme. El lattice de Leech es el mejor empacamiento en el espacio de 24 dimensiones (**J. Conway, N. Sloane**, 1998), del estudio de este retículo **J. H. Conway** descubrió tres de los 26 grupos esporádicos (**grupos de Conway,** 1968) del teorema de la clasificación de los grupos finitos. En 1973, **B. Fischer** y **R. Griess** predijeron la existencia del grupo simple finito más grande M, (**J. Thompson**, 1970) demostró su unicidad y (**R. Bocherds**, 1998) probó que el grupo de automorfismos de Λ es el grupo M. Este grupo es llamado el grupo Monster. En los últimos años, sea descubierto la importancia de E8 en la teoría de códigos y el estudio de los grupos finitos, y se han depositado también en el grupo E8 grandes esperanzas de obtener una teoría capaz de la unificación de la teoría de la relatividad de Einstein y la mecánica cuántica. Desde hace relativamente poco tiempo, esto parece posible, en el marco de la teoría física conocida popularmente como "teoría de las supercuerdas" en la cual las partículas elementales se piensan no de la manera tradicional como puntos en el espacio ordinario, en lugar de esto se asumen como cuerdas (por lo que tienen la capacidad de vibrar) formando un espacio de 9 dimensiones, 6 de las cuales se hallan compactadas y no se pueden percibir a una escala macroscópica. Esta teoría considerada como de vanguardia en la física, cuenta con importantes personalidades científicas como (**E. Witten**, 1990), en sus escritos afirma que es posible una versión de la teoría que unifica las cuatro fuerzas presentes en la naturaleza y postula un grupo de simetría que sería $(E8)^2$. Cabe mencionar que, el orden de M coincide con el número de dimensiones propuesto por la teoría de supercuerdas.

Garret Lissi sostiene que inclusive no son necesarias 9 dimensiones para explicar el universo físico y lo intrigante de esto es que también se encuentra E8 involucrado en esta teoría alternativa. Según el articulo de **Garret Lissi** ha encontrado un mecanismo, aun discutido por la comunidad científica, mediante el cual las estructuras matemáticas involucradas en las fuerzas y partículas fundamentales quedan incluidas en el marco del E8, el mayor de los grupos de Lie simples. También propone una posible solución para el problema de la gravedad cuántica y predice el número exacto de partículas fundamentales, sus propiedades y sus masas, la naturaleza del espacio-tiempo y la constante cosmológica. Según Lissi esta nueva teoría es capaz de explicar lo mismo que la teoría de cuerdas pero solo usando las cuatro dimensiones usuales, es decir 3 espaciales y una temporal.

REFERENCIAS

[1]. M. Aschbacher, "Sporadic Groups", *Cambridge Tracs in Mathematics 104*, (1994).

[2]. J. H. Conway and N. J. A. Sloane, "Sphere Packing's, Lattices and Groups",

Springer, Vol. **190,** (1998).

[3]. I. Frankeal and J. Lepowski, “The Moonshine Module: Vertex Algebra and Monster Groups”, *Springer, Vol.1*, (2002).

[4]. R. L. Griess, U. Meierfrankenfeld and Y. Segev, “A Uniqueness Proof for the Monster”, *Annals of Mathematics JSOR, Vol.130*, (1989).

[5]. R. E. Bocherds, “The Leech Lattice”, *Proc. R. Soc. Lond., Vol.389*, (1985).

[6]. J. Castañeda and E. Olmedo, “El Código de Hamming, Código de Golay y el Lattice de Leech”, *Memorias del VIII Coloquio Nacional de Criptografía, Teoría de Códigos y Aéreas Afines, contribución 3.* Vol. **1,** pp. 3-4, (2009).

[7]. J. Castañeda, M. C. Suarez, E. Olmedo. “Codigos Numéricos Autoduales”, *Memories of 5to International Congress of Numerical Methods and Applied Mathematics.* Vol. 1. (2010).

[8]. J. Castañeda. “Numerical Dual Affine Spaces”, *Tesis de Maestría UNID.* (2010)

[9]. A. G. Lissi “An Exceptionally Simple Theory of Everything”, *arXiv.org,* **(**2007).

[10]. A. M. Jaume Aguad`e, “One Hundred Years of E8”, *UAB, Vol.1*, (1991).

[11]. D. Diacunescu, G. Moore and E. Witten, “E8 Gauge Theory, and a Derivation of K-Theory from M-Theory”, *arXiv.org,* **(**2004).

[12]. Roman, S. Coding and Information theory. Ed. Springer-Verlag. 1992.

[13]. Vera Press. Introduction to the theory of error-correcting codes. A Wiley-Intercience publication. 2da edicion. 1989.

El Primer Encuentro de Lógica y Computación es organizado por:

Instituto Tecnológico Superior de Coalcomán

Academia Mexicana de Lógica

Consejo Estatal de Ciencia y Tecnología

Universidad Interamericana Para el Desarrollo.

Institutos y universidades participantes:

Instituto Tecnológico Superior de Coalcomán

Departamento de tecnologías de la Información, Universidad Interamericana Para el Desarrollo.

Departamento de Ciencias y Técnicas de la Comunicación, Universidad Interamericana Para el Desarrollo.

Facultad de Ciencias Físico-Matemáticas, Universidad Michoacana de San Nicolás de Hidalgo.

Facultad de Psicología, Universidad Michoacana de San Nicolás de Hidalgo.

Centro de Radioastronomía y Astrofísica, Universidad Nacional Autónoma de México.

Instituto de Investigaciones Filosóficas, Universidad Nacional Autónoma de México.

Instituto Tecnológico Superior de Morelia.

Colegio de Bachilleres del Estado de Michoacán, Plantel Coalcomán.

Universidad Nova Spania

Preuniversitaria de Morelia

Colegio Reforma

Colegio Novel