A NEW MODEL OF AFFINE FLAT SPACE-TIME

ALBERTO MEDINA, ANDRÉS VILLABÓN
Institut Alexandre Grothendieck, Université de Montpellier, Montpellier, France
Universidad Nacional Abierta y a Distancia, Medellín, Colombia
alberto.medina@umontpellier.fr
edgar.villabon@unad.edu.co

The goal of this talk is to present elements of the very rich Semi- Riemannian metric Geometry of certain quadratic Lie Groups in the Medina- Revoy sense.

Keywords and keyphrases— Semi-Riemannian metric, quadratic Lie groups.

Palabras y frases clave— Métrica semi-Riemaniana, grupos de Lie cuadráticos.

CÓDIGOS CÍCLICOS LRC-LCD

YISETH KARINA RODRÍGUEZ CÁCERES
Universidad Industrial de Santander, Bucaramanga, Colombia
yiseth2180630@correo.uis.edu.co

En esta charla se establece una conexión entre los códigos localmente recuperables (LRC) y los códigos lineales duales complementarios (LCD), especialmente enfocándose en su variante códigos cíclicos LRC-LCD. Estas herramientas son fundamentales en sistemas de almacenamiento distribuido, desempeñando un papel esencial en la confiabilidad y privacidad de los datos en la era de la información. Los códigos LRC-LCD ofrecen soluciones rentables tanto para la detección y corrección de errores en la transmisión de información digital como para el almacenamiento distribuido, siendo utilizados por gigantes tecnológicos como Facebook y Google. Esta combinación

única de códigos LRC y LCD proporciona una solución versátil y eficaz para abordar ambos desafíos simultáneamente, garantizando la disponibilidad y seguridad de los datos.

Keywords and keyphrases— Linear codes, cyclic codes, LRC codes, LCD codes.

Palabras y frases clave— Códigos lineales, códigos cíclicos, códigos LRC, códigos LCD.

UNA GENERALIZACIÓN DE LOS ÁRBOLES BINARIOS

JUAN JOSÉ ALEGRÍA, DIEGO RUÍZ

Universidad del Cauca, Popayán, Colombia

jjalegriae@unicauca.edu.co

dfruiz@unicauca.edu.co

Las estructuras de datos son uno de los pilares fundamentales de las ciencias de la computación, como también lo es el concepto de autómatas, es así que este trabajo pretende evidenciar una conexión directa entre estos dos conceptos.

Keywords and keyphrases— Data structure, binary trees, automatons.

Palabras y frases clave— Estructuras de datos, árboles binarios, autómatas.

SOBRE PRODUCTO SCHUR DE CÓDIGOS AG

JAZMÍN LISETH MANTILLA ROZO

Universidad del Valle, Cali, Colombia

jazmin.mantilla@correounivalle.edu.co

Los códigos AG son códigos lineales que admiten propiedades heredadas de los códigos Reed-Solomon y sus variantes. Estos códigos se pueden construir explícitamente, decodificar de manera eficiente, admiten buenas cotas en sus parámetros, se mantienen cerca de la cota de Singleton y se comportan bien bajo el producto Schur. Estas propiedades generan ventajas y

limitaciones para la utilización de estos códigos en aplicaciones modernas como el diseño de esquemas para la compartición de secretos y criptografía basada en códigos como el protocolo de McEliece el cual se cree puede resistir a ataques con un computador cuántico.

Keywords and keyphrases— Algebraic geometry codes, post quantum criptography, McEliece cryptosystem, Schur product.

Palabras y frases clave— Códigos algebraico geométricos, criptografía post-cuántica, criptosistema de McEliece, producto Schur.

RESILIENCIA EN GRAFOS HETEROGÉNEOS CON CRECIMIENTO PREFERENCIAL

CRISTIÁN ÁNGULO, CRISTHIAN URBANO, DIEGO RUÍZ

Universidad del Cauca, Popayán, Colombia

cristiancla@unicauca.edu.co

cristhianleon@unicauca.edu.co

dfruiz@unicauca.edu.co

Dado que los grafos pueden representar sistemas esenciales, como por ejemplo un sistema de transporte urbano en una ciudad o un sistema aeroportuario, una falla en el grafo puede traer consecuencias de alto costo y generar daños, no solo en la parte afectada, sino en gran parte del grafo. Estos ataques incluso pueden terminar causando un daño completo del grafo. De allí surge la importancia de analizar la resiliencia de los grafos, e identificar cómo estos se pueden recuperar después de un ataque. En esta propuesta buscamos evaluar la resiliencia de grafos heterogéneos con conexión preferencial, presentando un breve estudio de simulación con el cual se pretende estimar el tiempo de recuperación a partir de la modularidad, basados en una distribución exponencial para modelar el fenómeno.

Keywords and keyphrases— Heterogeneous graphs, resiliency of graphs.

Palabras y frases clave— Grafos homogéneos, resiliencia de grafos.

UNA RELACIÓN ENTRE REGLAS GOLOMB Y LA ELIMINACIÓN DE DIAFONÍA FWM EN FIBRA ÓPTICA

DIEGO MOLINA, CARLOS MARTOS

Universidad del Cauca, Popayán, Colombia

diegoms@unicauca.edu.co

cmartos@unicauca.edu.co

La necesidad de transmitir grandes cantidades de datos a altas velocidades se resuelve mediante la implementación de fibra óptica. Esta tecnología, que utiliza un material dieléctrico transparente para transmitir señales de luz, resulta ideal para esta tarea. Para hacer frente a esta creciente demanda, los sistemas de multiplexación por división de longitud de onda (WDM) se han convertido en una solución crucial. Sin embargo, debido a la cantidad de señales que se asignan a una misma fibra, estos sistemas pueden verse afectados por un fenómeno conocido como mezcla de la cuarta onda (FWM), lo cual degrada la calidad de la señal. Para abordar este fenómeno, se propone una solución que implica asignar las señales con diferentes distancias de separación, evitando que coincidan. Una regla Golomb es un conjunto ordenado de enteros mayores o iguales a cero donde los resultados de las diferencias positivas de los elementos son todos distintos. En esta ponencia vamos a presentar una relación entre la asignación de canales en la fibra óptica y las reglas Golomb.

Keywords and keyphrases— The structure of complex networks, directed modularity.

Palabras y frases clave— Estructura de redes, modularidad directa.

CÓDIGOS LINEALES Y CONJUNTOS DE SIDON

VIVIANA GUERRERO, JOHN H. CASTILLO

Universidad del Cauca, Popayán, Colombia
Universidad de Nariño, Pasto, Colombia

vivianagp@unicauca.edu.co
jhcastillo@udenar.edu.co

En esta ponencia se presentará una conexión entre la teoría algebraica de códigos y a la teoría de números aditiva, más precisamente, la relación entre códigos lineales binarios y conjuntos de Sidon.

Keywords and keyphrases— Linear codes, Sidon sets.
Palabras y frases clave— Códigos lineales, conjuntos de Sidon.

CONSTRUCTION OF A CRYPTOGRAPHIC FUNCTION BASED ON BOSE-TYPE SIDON SETS

RIGO JULIÁN OSORIO, CARLOS TRUJILLO, DIEGO RUÍZ

Universidad del Cauca, Popayán, Colombia

rosorio@unicauca.edu.co
trujillo@unicauca.edu.co
dfruiz@unicauca.edu.co

Sidon sets have several applications in mathematics and in real world problems, including the generation of secret keys in cryptography, error correcting codes, and the physical problem of compression of signals in telecommunications. In particular, in cryptography, the design of cryptographic functions with optimal properties like nonlinearity, differential uniformity, balance, autocorrelation, absolute indicator, and the avalanche effect play a fundamental role in the development of secure cryptographic systems. Based on the construction of Bose-type Sidon sets, in this work we present the construction of a new cryptographic function with good properties of linearity and differential uniformity.

Keywords and keyphrases— Bose-Sidon sets, criptography.
Palabras y frases clave— Conjuntos de Bose-Sidon, criptografía.

DINÁMICAS Y CONVERGENCIA DE MEDIDAS DE HOMOFILIA EN GRAFOS ALEATORIOS HETEROGÉNEOS

ALEJANDRA MURCIA, NINO PÉREZ, DIEGO RUÍZ

Universidad del Cauca, Popayán, Colombia

mariamur@unicauca.edu.co
ninoyofrani@unicauca
dfruiz@unicauca@unicauca

En la actualidad, la creciente generación de datos nos permite representar fenómenos del mundo real. En contraste con los modelos tradicionales de generación de grafos que asumen nodos idénticos, este trabajo propone un modelo de redes aleatorias heterogéneas donde los nodos se dividen en dos categorias y se analizan las dinámicas y convergencia asintóticas de las medidas de homofilia. Esto nos ayuda a comprender cómo los nodos con características similares establecen conexiones en las redes sociales y su influencia en la formación de enlaces y crecimiento de la red.

Keywords and keyphrases— Random graphs, social networks, hemophilia.

Palabras y frases clave— Grafos aleatorios, redes sociales, homofilia.

CÓDIGOS CASTILLO TORCIDOS PARA CRIPTOGRAFÍA POSTCUÁNTICA

WILSON OLAYA LEÓN

Universidad Industrial de Santander, Bucaramanga, Colombia

wolaya@uis.edu.co

En esta charla presentamos la familia de códigos Castillo torcidos, de manera similar a la construcción de códigos hermitianos torcidos. La importancia de esta nueva construcción es que el cuadrado Schur de estos códigos torcidos es más grande que el de los códigos no torcidos. Esta característica es necesaria para resistir el ataque de distinguir por cuadrado Schur cuando se utilizan códigos AG en el criptosistema McEliece (criptografía basada en códigos). Este criptosistema se cree que es resistente a ataques desde un computador cuántico, pues es uno de los candidatos para la estandarización de criptografía postcuántica.

Keywords and keyphrases— AG Codes, Castillo codes, Schur square, McEliece cryptosystem, post-quantum cryptography.

Palabras y frases clave— Códigos AG, códigos Castillo, cuadrado Schur, criptosistema McEliece, criptografía postcuántica.

USING SIDELINKOV SEQUENCES TO CONSTRUCT MULTIDIMENSIONAL ARRAYS FOR WATERMARKING

CESAR BOLAÑOS, ALCIBIADES BUSTILLO
University of Puerto Rico, Mayaguez, Puerto Rico
cesar.bolanos@upr.edu
alcibiades.bustillo@upr.edu

In this presentation we will describe a new family of multidimensional periodic arrays that have application in digital video or image watermarking. Each array of the family is constructed by composing a base array with a cyclic sequence of shifts. The base array is constructed by using the Chinese remainder Theorem to map a Sidelinkov sequences of period $p^l - 1$, where p is an odd prime and l is a positive integer, into two or more dimensions. The cyclic shift sequences are defined by applying logarithmic quadratic functions to a direct product of additive groups. The cross-correlation properties of this family is a peak value of order p^{2l} and non-peak auto- and cross-correlation of order p^l that is comparable or superior another known construction based on composition.

Keywords and keyphrases— Sidelnikov sequence, digital watermark, periodic arrays, cross-correlation.

Palabras y frases clave— Secuencia de Sidelinkov, marcas de agua digitales, arreglos periódicos.

UN GRAFO ASOCIADO A OPERACIONES DE CÓDIGOS LINEALES BINARIOS

LISBETH DELGADO, JOHN H. CASTILLO
Universidad del Cauca, Popayán, Colombia
Universidad de Nariño, Pasto, Colombia
lddelgado@unicauca.edu.co
jhcastillo@udenar.edu.co

Sea $\mathcal{C}$ un código lineal binario, se define una clase lateral de $\mathbf{x} \in \mathbb{F}_2^n$ sobre $\mathcal{C}$ como el conjunto $\mathbf{x} + \mathcal{C} = \{\mathbf{x} + \mathbf{y} : \mathbf{y} \in \mathcal{C}\}$. Para una clase lateral $\mathcal{C}_1$ de $\mathcal{C}$ se define $\mathrm{wt}(\mathcal{C}_1) = \min\{\mathrm{wt}(\mathbf{y}) : \mathbf{y} \in \mathcal{C}_1\}$ y un líder de $\mathcal{C}_1$ es un vector $\mathbf{x}$ tal

que $\mathrm{wt}(\mathbf{x}) = \mathrm{wt}(\mathcal{C}_1)$. Se puede establecer un orden parcial en el conjunto de clases laterales de un código $\mathcal{C}$ como sigue: si $\mathcal{C}_1$ y $\mathcal{C}_2$ son dos clases laterales de $\mathcal{C}$, entonces $\mathcal{C}_1 \prec \mathcal{C}_2$ siempre que existan líderes $\mathbf{x}_1$ de $\mathcal{C}_1$ y $\mathbf{x}_2$ de $\mathcal{C}_2$, tales que $\mathrm{supp}(\mathbf{x}_1) \subset \mathrm{supp}(\mathbf{x}_2)$. Se define el grafo $\Gamma(\mathcal{C}) = (V_{\mathcal{C}}, E_{\mathcal{C}})$ donde $V_{\mathcal{C}}$ es el conjunto de las clases laterales de $\mathcal{C}$ y $\{\mathcal{C}_1, \mathcal{C}_2\} \in E_{\mathcal{C}}$ si $\mathcal{C}_1 \prec \mathcal{C}_2$ y $\mathrm{wt}(\mathcal{C}_1) = \mathrm{wt}(\mathcal{C}_2) - 1$. En esta ponencia se presentan algunas operaciones de códigos lineales binarios y propiedades de los grafos asociados al código resultante de la operación.

Palabras y frases clave— Binary linear codes, Hamming distance, graphs.

Keywords and keyphrases— Códigos lineales binarios, distancia de Hamming, grafos.

ELLIPTIC CURVES APPLIED TO SIGNAL PROCESSING

ALCIBIADES BUSTILLO, CESAR BOLAÑOS

University of Puerto Rico, Mayaguez, Puerto Rico

alcibiades.bustillo@upr.edu

cesar.bolanos@upr.edu

We construct a new family of 3D watermarks by composing the 2-dimensional Legendre array with shift sequences derived from cyclic groups of points on a elliptic curve over $GF(p) \times GF(p)$. We show that that family have good auto and cross correlation values in the sense that the peak auto correlation value maintain good ratio with off-peak values.

Keywords and keyphrases–Elliptic curves, watermarks, auto-Correlation, Cross-Correlation.

Palabras y frases clave— Curvas elípticas, marcas de agua, auto correlación, Correlación cruzada.

DIFFERENTIAL FORMS IN C^∞-RINGED SPACES

CRISTIÁN DANILO OLARTE
Universidad de Antioquia, Medellín, Colombia
cristian.olarte@udea.edu.co

C^∞-algebraic geometry, the differential analog of Grothendieck's algebraic geometry, was recently developed by Dominic Joyce in his Derived Differential Geometry program. In this framework, rings are replaced by C^∞-rings, which are objects that generalize $\mathbb{R}$-algebras since they have not only the sum and product operations but also one operation for every smooth function $f \in C^\infty(\mathbb{R}^n)$ and every $n \in \mathbb{N}$. Therefore, geometric objects such as ringed spaces have their C^∞ counterparts. In particular, we can define C^∞-schemes and C^∞-stacks, which generalize several notions of differentiable spaces such as smooth manifolds and orbifolds.
In this presentation, we will address some facts about the construction of a complex of differential forms on a locally C^∞-ringed space. This construction, as in the case of manifolds, turns out to be functorial; therefore, forms can be integrated over simplices, and a version of Stoke's theorem holds.

Keywords and keyphrases— C^∞-rings, C^∞-ringed spaces, C^∞ -schemes, differential forms, Kähler differentials, De Rham Complex.

Palabras y frases clave— Anillos - C^∞, esquemas - C^∞, formas diferenciales, diferenciales de Kähler.