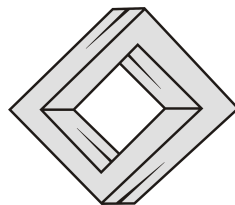


XLV Congreso Nacional Sociedad Matemática Mexicana

Quéretaro, Quéretaro

28 de octubre al 2 de noviembre de 2012

Sede: Universidad Autónoma de Querétaro



Índice general

Presentación	1
Comités y Coordinadores	2
1. Comité Organizador Central	2
2. Coordinadores	3
1. Tabla de horarios	7
2. Resúmenes	9
5. Ciencias de la Computación	9

Presentación

Comités y Coordinadores

1. Comité Organizador Central

Coordinadores Generales	Dr. Alejandro Díaz Barriga Casales Dra. Gabriela Araujo Pardo
Coordinador Ejecutivo	M. en C. Víctor Ibarra Mercado
Presidente de la SMM	Dr. Luis Montejano Peimbert
Coordinador de Áreas de Matemáticas	Dr. Daniel Juan Pineda
Coordinador de Áreas de Docencia	Dra. Rosa Ma. Farfán Marquez
Coordinadores Sesiones Especiales y Mesas Redondas	Dra. Amanda Montejano Cantoral Dra. Natalia García Colín
Coordinadores Conferencias Plenarias	Dr. Hector Juárez Valencia Dr. Mario Pineda Ruelas
Coordinador General del Comité Local	Dr. Carlos Arredondo Velázquez
Coordinadores Ejecutivos del Comité Local	Dra. Carmen Sosa Garza Dra. Déborah Oliveros Braniff Dr. Gerardo Souza Aubert
Comité de Reciprocidad con otras Sociedades Matemáticas	Dr. Emilio Lluís Puebla
Tesorero de la SMM	Dr. José Carlos Gómez Larrañaga

2. Coordinadores

Áreas	
Álgebra	Gerardo Raggi Cárdenas
Análisis	Ricardo Alberto Sáenz Casas
Análisis Numérico y Optimización	Raúl Castillo Pérez
Biomatemáticas	Marcos Aurelio Capistrán Ocampo
Ciencias de la Computación	Johan Van Horebeek
Cursos en Docencia	Erika Marlene Canché Góngora
Ecuaciones Diferenciales y Aplicaciones	Vladislav Kravchenko
Estadística	José Eliud Silva Urrutia
Experiencias de Aprendizaje en Docencia	Erika Marlene Canché Góngora
Física Matemática y Geometría Diferencial	Benjamín Alfonso Itzá Ortiz
Geometría Algebraica	Pedro Luis del Ángel Rodríguez
Historia y Filosofía	Antonio Rivera Figueroa
Lógica y Fundamentos	David Meza Alcántara
Matemática Discreta	Déborah Oliveros Braniff
Matemática Educativa	Juan José Montellano Ballesteros
Matemáticas e Ingeniería	Flor Montserrat Rodríguez Vázquez
Matemáticas Financieras y Economía Matemática	Salvador Botello Rionda
	Francisco Sánchez Sánchez
	Daniel Hernández Hernández
Probabilidad	Gerónimo Uribe Bravo
Sistemas Dinámicos	Ernesto Rosales González
Talleres en Docencia	Erika Marlene Canché Góngora
Teoría de Números y aplicaciones	Wilson Zúñiga Galindo
Topología Algebraica	Enrique Torres Gieseo
Topología General	Patricia Pellicer Covarrubias
	Roberto Pichardo Mendoza

Sesiones Especiales	
Difusión de Posgrados	José Eliud Silva Urrutia
Dinámica Hamiltoniana: teoría y aplicaciones	Arturo Olvera Chávez
	Panayotis Panayotaros
XVII Encuentro de Escuelas Matemáticas	Esperanza Guzmán Ovando
Innovación en Tecnología Educativa	José Luis Abreu León
La SMM en el Bachillerato	Carlos Arredondo
	Natalia García Colín
Las Matemáticas en las Licenciaturas	Ricardo Cruz Castillo
	Rubén Octavio Velez Salazar
Matemáticas en la Industria	Roberto Salas Zuñiga
Miscelánea Matemática	Ana Meda Guardiola
Presentación de Libros	Mario Pineda Ruelas
Problemas Inversos	Fernando Brambila Paz
SMM-SoBolMat	Emilio Lluís Puebla
Software Libre en Matemáticas	Rafael Villarroel Flores
The 16th workshop on Elliptic Curve Cryptography, ECC 2012	Francisco Rodríguez Henríquez

Mesas Redondas

Los Matemáticos en el Sector Público	Enrique Covarrubias Jaramillo
El Futuro de las Matemáticas en México	Gabriela Araujo
Mujeres en las Matemáticas	Lucero de Teresa y Oteiza
Nuestro Sistema Educativo: Naturaleza y Desafíos	Judith Zubieta

Eventos Especiales

Festival de Matemáticas	Joaquin Delgado Fernandez
De Joven a joven	Ernesto Pérez-Chavela
Homenaje a Ernesto Lacomba Zamora	María José Arroyo Paniagua
Homenaje a Francisco Raggi Cárdenas	Rogelio Fernández Alonso
	José Ríos Montes
	Carlos Signoret Poillon

Modalidad

CAR	Cartel
CDV	Conferencia de Divulgación y de Vinculación
CPI	Conferencia Panorámica de Investigación
CI	Conferencia de Investigación
RI	Reporte de Investigación
RT	Reporte de Tesis

Niveles de Audiencia

Prim	Profesores de Primaria
Sec	Profesores de Secundaria
Bach	Profesores de Bachillerato
1Lic	Primera mitad de la Licenciatura
2Lic	Segunda mitad de la Licenciatura
Pos	Posgrado
Inv	Investigación

Nota: Los números en **negritas** son *INVITADOS*

Tabla de horarios

Ciencias de la Computación pág. 9					
Hora	Lunes	Martes	Miércoles	Jueves	Viernes
9:00-9:20	Inauguración	5.1			
9:20-9:40					5.8
9:40-10:00					5.9
10:00-10:20		5.2		5.10	
10:20-10:40		5.3		5.11	
10:40-11:00	PLENARIA 1	5.4			5.12
11:00-11:30		Café			
11:40-12:00	Traslado	5.5			5.13
12:00-12:50		5.6			5.14
12:50-13:00	Traslado				
13:00-13:30		PLENARIA 2	PLENARIA 3	PLENARIA 4	PLENARIA 5
13:30-13:50					
14:00-16:30	COMIDA		Tarde Libre	COMIDA	
16:40-17:00		5.7			
17:00-17:20					
17:20-17:40					
17:40-18:10	Café			Café	
18:10-18:30				PLENARIA 8	PLENARIA 9
18:30-18:50					
18:50-19:00	Traslado			Traslado	
19:00-19:50	PLENARIA 6	PLENARIA 7		Asamblea General	Clausura
19:50-21:50	HOMENAJE ERNESTO LACOMBA	HOMENAJE FRANCISCO RAGGI			
Salón					

- 5.1 Análisis cuantitativo de malformaciones craneales en infantes

Salvador Ruíz-Correa (Invitado) (CPI, Pos)
- 5.2 “Predictibilidad en el registro de patrones mediante aproximaciones separables de la función kernel”

Patricia Batres Valerio (CI, Inv)
- 5.3 Optimización Inteligente de Cartera de Proyectos Sociales para Minorías en Chihuahua

Carlos Alberto Ochoa Ortiz Zezzatti (RI, 2Lic)
- 5.4 Factorización de Matrices para Sistemas de Recomendación

Aristeo Gutiérrez Hernández (RT, 2Lic)
- 5.5 Reconstrucción densa de escenas 3-D utilizando visión monocular

Sergio Alejandro Mota Gutiérrez (CPI, Pos)
- 5.6 Métodos de optimización en problemas de machine learning

José Luis Morales Pérez (Invitado) (CPI, 2Lic)

5.7 Análisis espacial basado en gráficas de adyacencia y su uso en contextos arqueológicos

Diego Jiménez Badillo (Invitado) (CI, 2Lic)

5.8 Turing en la Criptografía:

José de Jesús Ángel Ángel (CDV, 2Lic)

5.9 Algoritmos evolutivos y meméticos para optimización multi-objetivo

Adriana Lara López (CDV, 2Lic)

5.10 Implementación en software-hardware de aritmética sobre campos finitos binarios \mathbb{F}_{2^m} en curvas elípticas para aplicaciones criptográficas de llave pública

Arturo Álvarez Gaona (CDV, 2Lic)

5.11 Tipos anidados para estructuras cíclicas puramente funcionales

Alejandro Ehécatl Morales Huitrón (RT, 2Lic)

5.12 Tipos de datos anidados: un enfoque lógico-categorico

Miguel Álvarez Buendía (RT, 2Lic)

5.13 El lenguaje de programación WHILE, un formalismo equivalente a la Máquina de Turing

Favio Ezequiel Miranda Perea (CDV, 2Lic)

5.14 Una nueva estructura de datos para el problema de la subsecuencia común más larga

Francisco Javier Zaragoza Martínez (CI, Inv)

Resúmenes

5. Ciencias de la Computación

5.1. Análisis cuantitativo de malformaciones craneales en infantes (CPI, Pos)

Salvador Ruíz-Correa, src@cimat.mx (*Centro de Investigación en Matemáticas (CIMAT)*)

En esta plática se presentará un panorama de las investigaciones relacionadas con la cuantificación de malformaciones craneofaciales no sindrómicas en infantes.

5.2. Predictibilidad en el registro de patrones mediante aproximaciones separables de la función kernel (CI, Inv)

Patricia Batres Valerio, patyba3v@hotmail.com (*Universidad Autónoma de San Luis Potosí (UASLP)*)

Coautores: Edgar Román Arce Santana, Javier Flavio Viguera Gómez

¿Cómo se determina si un objeto observado en dos vistas es el mismo si se sabe que existe una transformación de tonalidades entre ambas imágenes (por ejemplo, debido a cambios de iluminación o de modalidad de adquisición)? Se han propuesto diversas soluciones en la literatura a este problema usando diferentes medidas de semejanza: información mutua [Viola'97][Maes'97][Dame'10], kernel-predictibilidad [Gómez et al.'08], combinación de campos de distribución [Sevilla'12], etc. Todas las propuestas anteriores ofrecen resultados satisfactorios, pero presentan como principal desventaja que el tiempo de cálculo de las medidas de semejanza depende (i) de forma cuadrática en términos del número de píxeles utilizados en la muestra de la distribución de tonalidades (por lo que se utilizan heurísticas para estimar las distancias en tiempos razonables) o (ii) de forma cuadrática en términos del número de niveles de cuantización, a causa de una doble integral presente en todas estas medidas. Basados en una versión aditiva de la kernel-predictibilidad [Carlos'11], proponemos aproximar la función de kernel mediante sumas de polinomios y senos/cosenos, con lo cual se consigue que la doble integral sea separable y el cálculo de las distancias sea lineal con respecto al número de píxeles de la muestra. El tiempo de cálculo de las medidas de semejanza depende sólo de forma cuadrática del número de términos utilizados en la aproximación pero no se requiere discretizar el espacio de tonalidades, lo cual es un factor crítico en otras metodologías.

5.3. Optimización Inteligente de Cartera de Proyectos Sociales para Minorías en Chihuahua (RI, 2Lic)

Carlos Alberto Ochoa Ortíz Zezzatti, alberto.ochoa@uacj.mx (*Centro de Investigaciones Sociales, Universidad Autónoma de Ciudad Juárez (UACJ)*)

Un tema central y polémico con mucha frecuencia en el análisis de políticas públicas es la asignación de fondos para proyectos de grupos minoritarios. Los recursos públicos para el financiamiento de proyectos sociales de este tipo son particularmente muy escasos. Muy a menudo la relación entre el presupuesto solicitado y el que puede ser recibido es abrumadora, ya que es muy poco probable que lo más necesario sea lo que puede ser concedido. Además, los criterios estratégicos, políticos e ideológicos impregnan la toma de decisiones sobre dichas asignaciones. Para satisfacer estos criterios normativos, que subyacen en cualquiera de las políticas públicas predominantes o la ideología del gobierno, es evidente que debe ser conveniente que tanto para dar prioridad a los proyectos y al desarrollo de carteras de proyectos, estas deben de ser acordes con principios racionales (por ejemplo, la maximización de los beneficios sociales). Por lo que utilizando Cómputo Bioinspirado se pueden caracterizar como sigue: -Pueden ser, sin duda, rentables, pero sus beneficios son indirectos, tal vez sólo a largo plazo puede ser visible y difícil de cuantificar. -Aparte de su potencial contribución económica para el bienestar social, no son beneficios intangibles, los que deben ser considerados para lograr una visión integral de su impacto social. -Equidad, en relación con la magnitud del impacto de los proyectos, así como las condiciones sociales de las personas beneficiadas, también debe ser considerado. En la presente investigación se desarrolló una aproximación al problema utilizando optimización inteligente para las cuatro minorías de Chihuahua: Rarámuris, Mennonitas, Mormones e Inmigrantes de la Federación.

5.4. Factorización de Matrices para Sistemas de Recomendación (RT, 2Lic)

Aristeo Gutiérrez Hernández, aristeo@cimat.mx (*Centro de Investigación en Matemáticas, A.C. (CIMAT)*)

Hoy en día, la gran cantidad de opciones de productos y de servicios hace difícil la tarea de elegir al consumidor. Es por ello que cada vez más tiendas electrónicas y proveedores de contenido, hacen uso de sistemas de recomendación para brindarle al usuario recomendaciones acertadas con base en sus gustos personales. En el presente trabajo proponemos una extensión del modelo básico de factorización de matrices, uno de los modelos más exitosos para sistemas de recomendación, mediante la introducción de términos de agrupamiento sobre los usuarios y sobre los productos. Resolvemos el problema de optimización subyacente y mostramos cómo con esta información adicional se puede mejorar la calidad de las recomendaciones. Realizamos pruebas sobre la base de datos de películas de MovieLens y exploramos su potencial para datos de una biblioteca pública en México.

5.5. Reconstrucción densa de escenas 3-D utilizando visión monocular (CPI, Pos)

Sergio Alejandro Mota Gutiérrez, samota@cimat.mx (*Centro de Investigación en Matemáticas (CIMAT)*)

Presentamos un enfoque para reconstrucción de escenas 3-D en el que se utiliza una cámara monocular como único sensor. Aproximamos la estructura de la escena por medio de un conjunto de superficies planares. Los parámetros de estas superficies son determinados a partir tanto de características visuales de las imágenes adquiridas como de características geométricas de la escena. Aprendemos de forma supervisada las relaciones entre estas variables.

5.6. Métodos de optimización en problemas de machine learning (CPI, 2Lic)

José Luis Morales Pérez, jlm.p.morales@gmail.com (*Instituto Tecnológico Autónomo de México (ITAM) Departamento de Matemáticas*)

En esta plática presentaremos una panorámica de los problemas y métodos de optimización que se presentan en el área de machine learning.

5.7. Análisis espacial basado en gráficas de adyacencia y su uso en contextos arqueológicos (CI, 2Lic)

Diego Jiménez Badillo, diego_jimenez@inah.gob.mx (*Instituto Nacional de Antropología e Historia*)

Esta ponencia presenta un nuevo método de análisis espacial orientado al reconocimiento de patrones de conectividad en conjuntos de puntos. El método se basa en la noción de vecindad relativa, así como en la extracción de una interesante clase de gráficas de adyacencia, entre las que destacan la gráfica de vecindad relativa, la gráfica Gabriel, el esqueleto-beta y la gráfica de vecindad limitada. En la ponencia se enfatiza la utilidad del método para explorar la estructura espacial de contextos arqueológicos. Como caso de estudio se ha elegido un conjunto de ofrendas mexicas encontradas durante las excavaciones del Templo Mayor de los aztecas. En dichas ofrendas los objetos fueron cuidadosamente distribuidos de tal forma que la ubicación espacial de cada elemento influye en el simbolismo del conjunto. Con el método propuesto ha sido posible identificar patrones de asociación significativos que han ayudado a interpretar estos contextos arqueológicos. El método es genérico y puede utilizarse para resolver muchos otros problemas que involucren el análisis de conectividad en conjuntos de puntos a partir de gráficas de proximidad o adyacencia. Durante la presentación nos gustaría destacar algunos puntos de convergencia para el desarrollo de nuevas aplicaciones del método, especialmente en otras áreas de las Humanidades y las Matemáticas.

5.8. Turing en la Criptografía: (CDV, 2Lic)

José de Jesús Ángel Ángel, jjaa@math.com.mx (*Facultad de Ingeniería*)

Como recuerdo a 100 años del nacimiento de Alan Turing, repasamos algo de su trabajo hecho en criptografía. Particularmente relatamos el funcionamiento y el criptoanálisis de ENIGMA, hablamos de la máquina Bomba y otros trabajos relacionados que Turing realizó. La máquina ENIGMA realiza de manera general una combinación de permutaciones y atacarla significa encontrar las permutaciones inversas conociendo pocos datos. La máquina bomba efectúa un ataque de texto conocido y fuerza bruta, con lo que los aliados pudieron descifrar mensajes alemanes desde 1942.

5.9. Algoritmos evolutivos y meméticos para optimización multi-objetivo (CDV, 2Lic)

Adriana Lara López, adriana@esfm.ipn.mx (*Escuela Superior de Física y Matemáticas del Instituto Politécnico Nacional (ESFM-IPN)*)

Los algoritmos meméticos se describen como la adaptación de buscadores locales dentro de algoritmos de computación evolutiva. En esta plática se describen los problemas de optimización multi-objetivo y su abordaje con computación evolutiva. Se dan ejemplos y pautas para el acoplamiento de buscadores locales dentro de estas técnicas.

5.10. Implementación en software-hardware de aritmética sobre campos finitos binarios \mathbb{F}_{2^m} en curvas elípticas para aplicaciones criptográficas de llave pública (CDV, 2Lic)

Arturo Álvarez Gaona, aalvarez@buromc.com (*Universidad Autónoma Metropolitana-Azcapotzalco (UAM) Departamento de Ciencias Básicas*)

Coautores: Oscar Alvarado Nava, Pedro Ricardo López Bautista

Interdisciplinariamente, conjugamos electrónica, ciencias de la computación y matemáticas para construir criptosistemas de llave pública basados en curvas elípticas sobre campos finitos binarios \mathbb{F}_{2^m} . Mostramos el desarrollo en software de la generación de llaves públicas así como una implementación utilizando la multiplicación escalar para el intercambio de llaves mediante el protocolo de Diffie-Hellman elíptico. Mención aparte, implementamos la multiplicación y elevar al cuadrado sobre campos finitos binarios $\mathbb{F}_{2^{233}}$ en el lenguaje de descripción de circuitos VHDL mostrando los resultados obtenidos mediante la simulación y el análisis de los resultados.

5.11. Tipos anidados para estructuras cíclicas puramente funcionales (RT, 2Lic)

Alejandro Ehécatl Morales Huitrón, alejandroe@ciencias.unam.mx (*Universidad Nacional Autónoma de México (UNAM), Facultad de Ciencias, Departamento de Matemáticas*)

Los tipos de datos anidados surgen en una línea de investigación referente a la matemática de construcción de programas como constructores inductivos de segundo orden. En una declaración de tipo de dato regular, las ocurrencias de tipo en la derecha de la expresión son copias del lado izquierdo. En cambio un tipo anidado (no regular) es un tipo parametrizado en el que las ocurrencias de tipo declaradas a la derecha aparecen con diferentes instancias del parámetro que lo definen. En la tesis se trabaja con estructuras cíclicas puramente funcionales como listas y árboles con tipos anidados, comparando respecto a las implementaciones con tipos regulares, dando un panorama de los conceptos fundamentales de las estructuras de datos funcionales como son la persistencia y la programación mediante operadores desplegado (fold, unfold). La implementación se realiza en el lenguaje Haskell. (Esta investigación es parte del proyecto UNAM-PAPIIT-IN117711)

5.12. Tipos de datos anidados: un enfoque lógico-categórico (RT, 2Lic)

Miguel Álvarez Buendía, miguelalvarezb@gmail.com (*Universidad Nacional Autónoma de México (UNAM)*)

Un concepto muy importante en programación funcional es el de tipo inductivo, el cual se obtiene mediante una definición recursiva. Usualmente estos son regulares, es decir, que en su definición recursiva no existe un cambio de parámetro como es el caso de las listas finitas. En contraste los tipos de datos anidados son aquellos cuya definición recursiva requiere un cambio de parámetro. Nuestro trabajo consiste en estudiar los tipos de datos anidados desde un punto de vista teórico, apoyándonos de la lógica matemática y la teoría de las categorías. Se pretende revisar algunos aspectos sintácticos y semánticos de éstos tipos, su definición mediante ciertas lógicas de orden superior, sus operadores de plegado y su semántica operacional. (Esta investigación es parte del Proyecto UNAM-PAPIIT-IN117711)

5.13. El lenguaje de programación WHILE, un formalismo equivalente a la Máquina de Turing (CDV, 2Lic)

Favio Ezequiel Miranda Perea, favioemp@gmail.com (*Departamento de Matemáticas Facultad de Ciencias Universidad Nacional Autónoma de México (UNAM)*)

Coautores: Araceli Liliana Reyes Cabello, Lourdes del Carmen González Huesca

La Máquina de Turing es el modelo de computación por antonomasia. Su definición conceptualmente simple y elegante la ha convertido en la piedra angular de las teorías de la computabilidad y de la complejidad computacional. Sin embargo, en nuestra opinión, este modelo resulta difícil de entenderse y visualizarse como un sistema de programación puesto que es más cercano al lenguaje de máquina. En esta charla presentamos un lenguaje de programación imperativo minimal, llamado WHILE que, como es de esperarse es Turing-completo, pero que le será más familiar al estudiante de ciencias de la computación, ya que se sirve de conceptos de la teoría de lenguajes de programación y de técnicas de programación a las que este ha sido expuesto en la práctica. Se hará énfasis en la equivalencia de la Máquina de Turing con este lenguaje, así como en su expresividad.

5.14. Una nueva estructura de datos para el problema de la subsecuencia común más larga (CI, Inv)

Francisco Javier Zaragoza Martínez, franz@correo.azc.uam.mx (*Universidad Autónoma Metropolitana Azcapotzalco Departamento de Sistemas*)

Coautor: Rodrigo Alexander Castro Campos

Los algoritmos más rápidos para encontrar la subsecuencia común más larga entre dos cadenas con un alfabeto de tamaño fijo utilizan estructuras de datos auxiliares para avanzar más rápido sobre la tabla dinámica. En esta plática presentaremos una estructura de datos nueva que permite diseñar un algoritmo que corre en tiempo $O(SD)$ donde S es el tamaño del alfabeto y D el número de coincidencias dominantes entre las cadenas.

Índice alfabético

Álvarez Buendía Miguel, 11
Álvarez Gaona Arturo, 11
Ángel Ángel José de Jesús, 10

Batres Valerio Patricia, 9

Gutiérrez Hernández Aristeo, 10

Jiménez Badillo Diego, 10

Lara López Adriana, 10

Miranda Perea Favio Ezequiel, 11
Morales Huitrón Alejandro Ehécatl, 11
Morales Pérez José Luis, 10
Mota Gutiérrez Sergio Alejandro, 10

Ochoa Ortiz Zezzatti Carlos Alberto, 9

Ruíz-Correa Salvador, 9

Zaragoza Martínez Francisco Javier, 12

Estos programas se terminaron de imprimir

El tiro fue de ejemplares

