

PROPUESTA DE TRABAJO FIN DE GRADO

Curso: 2015-2016

Profesor/es: Ignacio Luengo Velasco

Título del Trabajo: Criptografía de clave pública con códigos correctores de errores

La criptografía de clave pública basada en códigos correctores de errores fue introducida por Mc Eliece en 1978 y en la actualidad proporciona uno de los mejores candidatos para cifradores de clave pública resistentes a un ordenador cuántico. En estos trabajos se estudiarán las variantes actuales del cifrador de McEliece, su complejidad, seguridad y resistencia al criptoanálisis.

Este trabajo está pensado para dos alumnos y podrían incorporarse más. Uno de los alumnos estudiará la complejidad algorítmica de los sistemas y otro la seguridad y resistencia al criptoanálisis.

Referencias:

R. Overbeck . and . Sendrier "Code-based cryptography" en Post-Quantum_Cryptography-Springer(2008\)
pp 95-144.

Requisitos:

Plazas: 2 (podría incorporarse alguna más)

Alumno a quien se ofrece: Álvaro Peña Menéndez (Grado Ingeniería Matemática) y José Alberto Martínez Ordóñez (Grado de Matemáticas)

Propuesta de Trabajo Fin de Grado

- **Titulación para la que se ofrece el TFG:** Grado en Matemáticas (2 estudiantes)

- **Nombre del trabajo que se propone:** El Problema de la Medida

- **Metodología y programa de trabajo:** El problema en cuestión es el siguiente:
¿Puede asignarse a cada subconjunto A del espacio euclídeo n -dimensional un número $m(A) \geq 0$ (su medida) de modo que:

1.- Si A y B son disjuntos, $m(A \cup B) = m(A) + m(B)$.

2.- Si T es una isometría, $m(T(A)) = m(A)$.

3.- La medida del intervalo unidad n -dimensional es 1 (normalización)?

Se trata de discutir los orígenes del problema y los intentos de solución hasta llegar a la respuesta final dada por Banach (afirmativa para $n=1,2$ y negativa para $n>2$). La respuesta tiene que ver con la estructura del grupo de isometrías del espacio, así como la axiomática conjuntista asumida, en particular el Axioma de Elección.

Bibliografía básica:

R. P. Agnew and A. P. Morse, *Extensions of linear functionals with applications to limits, integrals, measures and densities*.

G. Bachman and L. Narici.- *Functional Analysis*. Dover, 2000

S. Wagon, *The Banach-Tarski paradox*. Cambridge University Press, 1985.

Bibliografía de consulta:

F. Bombal, *Paradojas y rigor: la historia interminable*. R.A.C., Madrid, 2006

- **Profesor:** Fernando Bombal

- **Requisitos:** Es conveniente (no imprescindible) haber cursado Teoría de la Medida y Análisis Funcional.

Propuesta de Trabajo Fin de Grado

- **Titulación para la que se ofrece el TFG:** Grado en Matemáticas
- **Nombre del trabajo que se propone:** El teorema de Hartogs de Holomorfía Separada.
- **Metodología y programa de trabajo:** El alumno presentará una memoria que incluya la demostración completa de ese clásico teorema sobre funciones holomorfas de varias variables complejas.

Bibliografía básica: Narashiman. Several Complex Variables. The University of Chicago Press, cop. 1971.

- **Profesor:** JOSÉ MARÍA MARTÍNEZ ANSEMIL
- **Requisitos:** Haber cursado o comprometerse a hacer este curso la asignatura de ANÁLISIS COMPLEJO del Grado de Matemáticas.
- **Alumno solicitante:**

Propuesta de Trabajo Fin de Grado

- **Titulación para la que se ofrece el TFG:** Grado en Matemáticas.
- **Nombre del trabajo que se propone:** Introducción al Análisis Convexo.
- **Metodología y programa de trabajo:** El alumno debe realizar un estudio detallado de algunos capítulos del libro que se da en la bibliografía y redactar una memoria con sus conclusiones. Contará con la ayuda del profesor tutor para hacer esto y para ello se entrevistará con él semanalmente. De esta manera analizará los avances que vaya realizando y podrá resolver dudas.

Bibliografía básica: Magaryl-Il'yaev, G.G. y Tikhomirov, V.M., "Convex Analysis: Theory and Applications", Translations of Mathematical Monographs 222, American Mathematical Society 2003.

Bibliografía de consulta: Rockafellar, R.T., Convex Analysis, Princeton University 1997.

- **Profesor:** José Mendoza Casas
- **Requisitos:** -
- **Alumno solicitante:** -

Propuesta de Trabajo Fin de Grado

- **Titulación para la que se ofrece el TFG:** Grado en Matemáticas
- **Nombre del trabajo que se propone:** El teorema de Cartan-Thullen
- **Metodología y programa de trabajo:** El alumno presentará una memoria que incluya la demostración completa de ese clásico teorema sobre funciones holomorfas de varias variables complejas y alguna de sus consecuencias.

Bibliografía básica: NACHBIN. Holomorphic Functions, Domains of holomorphy and Local Properties. North-Holland, 1972.

- **Profesor:** SOCORRO PONTE MIRAMONTES
- **Requisitos:** HABER CURSADO O COMPROMETERSE A HACER ESTE CURSO LA ASIGNATURA DE ANÁLISIS COMPLEJO del Grado de Matemáticas.
- **Alumno solicitante:**

PROPUESTA DE TRABAJO DE FIN DE GRADO

Curso 2015-16

1.- Titulación para la que se ofrece el TFG: Grado en Matemáticas y Estadística; Grado en Ingeniería Matemática

2.- Título del TFG propuesto: Cadenas de Markov en Tiempo-Discreto Aplicadas a Modelos de Epidemias

3.- Descripción del TFG:

El objetivo fundamental del TFG es la revisión de los modelos estocásticos de epidemias formulados como cadenas de Markov en tiempo-discreto.

Los objetivos específicos están vinculados al trabajo de Allen y Burgin (2000), al considerar este trabajo como la principal contribución al análisis en tiempo discreto de epidemias SIS (*susceptible-infected-susceptible*) con población constante, SIS con tamaño poblacional variable y SIR (*susceptible-infected-removed*) con población constante, entre otros.

El TFG centra su atención en realizar un estudio comparativo con los modelos homólogos deterministas, derivar su comportamiento límite hacia las versiones en tiempo-continuo y analizar la probabilidad de ocurrencia de una epidemia, la distribución cuasi-estacionaria y el tiempo de duración de una epidemia, tratando de caracterizar su comportamiento en términos del factor básico de transmisión R_0 .

Para la elaboración del TFG, es obligatorio seguir un calendario de tareas a desarrollar durante el período lectivo, desde el momento de asignación del TFG hasta su lectura.

Referencias de interés:

LJS Allen, AM Burgin (2000) Comparison of deterministic and stochastic SIS and SIR models in discrete time. *Mathematical Biosciences* 163: 1-33.

E Çinlar (1975) *Introduction to Stochastic Processes*. Prentice-Hall, Inc., Englewood Cliffs, NJ.

4.- Profesor/profesores tutores: Antonio Gómez Corral

5.- Requisitos (si procede):

Conocimiento previo de los fundamentos sobre cadenas de Markov en tiempo-discreto; por ejemplo, cursando las asignaturas Procesos Estocásticos (Grado en Matemáticas y Estadística) o Cálculo Estocástico (Grado en Ingeniería Matemática).

Conocimiento de lenguajes de programación (por ejemplo, Fortran, MathLab, C).

Lectura de libros/artículos en inglés.

6.- Número de plazas: 2

7.- Nombre del alumno (en su caso):

PROPUESTA DE TRABAJO DE FIN DE GRADO

Curso 2015-16

1.- Titulación para la que se ofrece el TFG:

Ingeniería Matemática o Matemáticas y estadística.

2.- Título del TFG propuesto:

El problema de Programación lineal; aplicación informática con Matlab.

3.- Descripción del TFG:

Se trata con este trabajo de desarrollar una aplicación informática con Matlab que resuelva el problema de programación lineal y admita variantes que ayuden a introducirse en el problema de programación lineal, sus fundamentos teóricos y su resolución por el algoritmo del simplex. La aplicación debe ser lo suficientemente flexible y amigable que pueda ser utilizada posteriormente como una ayuda a los estudiantes de grado para sus experiencias computacionales y para el estudio inicial del problema.

4.- Profesor/profesores tutores:

Javier Yáñez

5.- Requisitos (si procede):

Conocimiento avanzado de Matlab

6.- Número de plazas

Una

7.- Nombre del alumno (en su caso):

DISPONIBLE

PROPUESTA DE TRABAJO DE FIN DE GRADO

Curso 2015-16

1.- Titulación para la que se ofrece el TFG: Ingeniería Matemática. Matemáticas y Estadística

2.- Título del TFG propuesto: Curvas ROC: Fundamentos teóricos y análisis de las librerías del paquete estadístico R.

3.- Descripción del TFG:

El análisis de curvas ROC (del inglés Receiver Operating Characteristic) es una técnica estadística de decisión que juega un papel fundamental en muchos ámbitos y que en las últimas décadas, se ha utilizado mucho en medicina para evaluar y analizar procedimientos de diagnóstico de enfermedades. Las curvas de ROC se han convertido en herramientas muy útiles y de un uso muy extendido y ha tenido un auge importante por su capacidad para resumir en una única medida la precisión o eficacia diagnóstica de una prueba.

El propósito de este trabajo es realizar una revisión de los conceptos y fundamentos básicos de esta teoría, analizar las librerías que el paquete estadístico R tiene a disposición de profesionales e investigadores para representar, analizar, suavizar y comparar curvas de ROC y finalmente ilustrar su uso a través de su aplicación a un conjunto de datos biomédicos.

4.- Profesor/profesores tutores: Rosa Alonso Sanz

5.- Requisitos (si procede):

6.- Número de plazas 2

7.- Nombre del alumno (en su caso):

PROPUESTA DE TRABAJO DE FIN DE GRADO

Curso 2015-16

1.- Titulación para la que se ofrece el TFG: Grado de Matemáticas y Estadística

2.- Título del TFG propuesto: Descomposición de la varianza en experimentos para control de calidad

3.- Descripción del TFG:

En el campo del control de calidad, la variabilidad de un proceso de producción constituye un elemento esencial para valorar la calidad de los productos realizados mediante ese proceso. En la práctica, sin embargo, tal variabilidad suele ser resultado de la conjunción de una serie de componentes asociadas con diversos factores, que han de ser aislados para entender las posibilidades de mejora que permite el proceso.

En este trabajo se ampliará el temario de las asignaturas de Control de Calidad y Diseño de Experimentos, atendiendo a las técnicas de descomposición de la varianza que surgen en los modelos de análisis de experimentos factoriales con factores aleatorios. En particular, se hará énfasis en los métodos de estimación puntual y por intervalos de las componentes de la varianza basadas en técnicas de máxima verosimilitud.

4.- Profesor/profesores tutores: Tinguaro Rodríguez

5.- Requisitos (si procede):

6.- Número de plazas: 1

7.- Nombre del alumno (en su caso):

PROPUESTA DE TRABAJO FIN DE GRADO

Curso: 2015-2016

Título del trabajo: Algebras de Lie resolubles y nilpotentes.

Las álgebras de Lie aparecen de forma natural en multitud de contextos, desde consideraciones del Álgebra Lineal y la teoría de matrices, pasando por la Geometría Diferencial y la derivada de Lie de campos de vectores hasta el corchete de Poisson empleado en el formalismo hamiltoniano de la Mecánica.

El objetivo fundamental del trabajo es estudiar las propiedades estructurales y cohomológicas fundamentales de las álgebras de Lie resolubles y nilpotentes complejas y reales, con especial énfasis en las clasificaciones en baja dimensión. Específicamente, se analizarán las filtraciones características de estas clases de álgebras, las propiedades del tensor de estructura, la estructura de los grupos de cohomología de Chevalley con coeficientes en los módulos trivial y adjunto, así como las nociones de completitud y resolubilidad completa.

Referencias:

1. Y. Chow. General Theory of Lie Algebras, Gordon and Breach, N. Y., 1978.
2. J. Dixmier. Algèbres de Lie, Centre de Documentation Universitaire, Paris, 1958.
3. A. A. Kirillov. An Introduction to Lie Groups and Lie Algebras, CUP, Cambridge, 2008.
4. G. M. Mubarakzyanov. On solvable Lie algebras, Izv. Vuzov Mat. 32 (1963), 114-123.
5. W. H. Steeb. Continuous Symmetries, Lie Algebras, Differential Equations and Computer Algebra, World Scientific, Singapore, 2007.

Profesor/es: J. M. Ancochea Bermúdez

Requisitos: Es requisito haber cursado con aprovechamiento las asignaturas de Álgebra Lineal, así como tener nociones básicas de Geometría Diferencial. Es conveniente, pero no indispensable, haber cursado las asignaturas optativas de Geometría de Variedades.

Plazas: 1

PROPUESTA DE TRABAJO FIN DE GRADO

Curso: 2015-2016, segundo cuatrimestre.

Título del trabajo: Subgrupos de transformaciones de Möbius.

El objetivo de este trabajo es:

- El estudio detallado de las transformaciones de Möbius y su acción en el plano complejo.
- El estudio de algunos subgrupos de estas transformaciones, como los grupos de Schottky o los grupos quasifuchsianos. Una herramienta principal será dibujar en ordenador sus conjuntos límite.

Referencias:

1. D. Mumford, C. Series, D. Wright, *Indra's Pearls*. Cambridge University Press, 2002
2. J. Anderson, *Hyperbolic geometry*. Springer, 2005.

Profesor/es: Raquel Díaz Sánchez

Requisitos: recomendable conocer un lenguaje de programación.

Plazas: 1

Nombre de los alumnos: (en caso de estar ya adjudicado o solicitado)

PROPUESTA DE TRABAJO FIN DE GRADO

Curso: 2015-2016

Título del trabajo: Normalidad en grupos topológicos

La estructura algebraica en los grupos topológicos refuerza muchas de sus propiedades topológicas. Prueba de ello podría ser la afirmación de que un grupo topológico de Hausdorff (ó incluso T_0) es automáticamente completamente regular y por tanto espacio de Tychonoff. No ocurre así con la **Normalidad**. Por ejemplo, un producto de una cantidad no numerable de copias del grupo de los enteros es un grupo de Hausdorff que no es normal. Markov (1945) se preguntó si todo grupo abstracto no numerable admite una topología de grupo no-normal. Una respuesta negativa fue obtenida por Trigos en 1994.

Por otra parte, los grupos localmente compactos y Hausdorff son normales (una afirmación así no puede hacerse para espacios topológicos en general).

Estos hechos señalan que la propiedad de normalidad debe estudiarse explícitamente en la categoría de los grupos topológicos. En el presente trabajo estudiaremos la normalidad para grupos abelianos precompactos, y propiedades relacionadas. Esto exigirá un conocimiento de la topología de Bohr de un grupo, así cómo entender los ejemplos arriba mencionados. También investigaremos en qué casos (es decir, para qué tipo de grupos) se puede dar la afirmación: “precompacto + normal implica compacto”.

Referencias:

“*General Topology*”, R. Engelking, Helderman 1989.

“*Normal topological spaces*”, R. Aló and H. Shapiro, Cambridge University Press 1974.

“*Pontryagin duality and the structure of locally compact abelian groups*”, S. Morris, Cambridge University Press 1977.

“*Normality in topological groups*”, E. Martín Peinador (Contribuciones Matemáticas en homenaje a Juan Tarrés, Editorial Complutense, 2012)

“ *The maximal totally bounded group topology on G and the biggest minimal G -space, for abelian groups G* ”, E. K. van Douwen, Topology and Appl. **34** (1990) 69--91.

“*Every uncountable Abelian group admits a nonnormal group topology*” F. J. Trigos-Arrieta, Proc. Amer. Math. Soc., 122, n° 3 (1994), 907--909.

Profesor/es: Elena Martín Peinador

Requisitos: Haber cursado con buen rendimiento las asignaturas de Topología Elemental y Estructuras Algebraicas que se ofrecen en el Grado.

Plazas: 3

Nombre de los alumnos: (David Leon y Stiven Alberto Gutiérrez Sierra)

PROPUESTA DE TRABAJO FIN DE GRADO

Curso: 2015-2016

Título del trabajo: En torno a una topología que da a los reales \mathbb{R} estructura de grupo topológico compacto y Hausdorff.

Una topología de grupo T , compacta y Hausdorff, en el grupo aditivo de los reales fue definida por Halmos en 1944. Estudiaremos en este trabajo la definición de T , así como sus propiedades más notables. Se trata de una topología que hace de \mathbb{R} un espacio conexo, no conexo por caminos ni localmente conexo. Por tanto (\mathbb{R}, T) no es grupo de Lie, ni una curva en el sentido de Hahn-Mazurkiewicz.

Referencias:

1. P. R. Halmos: *Comment on the real line*. *Bull. Amer. Math. Soc.* {50} (1944), 877–878.
2. E. Martín-Peinador and C.T. Stevens: *Completeness properties of group topologies for \mathbb{R}* . *Topology Appl.* 192 (2015) 169–175.
3. E. Cillero: *Caracteres del grupo aditivo de los racionales*. *Rev. Real Academia de Ciencias de Zaragoza.* {58} (2003), 115--128.
4. L. Aussenhofer, M.J. Chasco and X. Domínguez: *Arcs in the Pontryagin dual of a topological abelian group*. *J. Math. Anal. Appl.* {425} (2015) no. 1, 337--348
5. M. J. Dixmier: *Quelques propriétés des groupes abéliens localement compacts*. *Bull. Sci. Math.* (2) {81} (1957), 38--48.
6. E. Hewitt and K. A. Ross: *Abstract Harmonic Analysis. Vol. I* {115} Springer-Verlag, Berlin, (1963).
7. P. Nickolas: *Reflexivity of topological groups*. *Proc. Amer. Math. Soc.* {65} (1977), no. 1, 137-141.

Profesor/es: Elena Martín Peinador

Requisitos: Haber cursado con buen rendimiento las asignaturas de Topología Elemental y Estructuras Algebraicas que se ofrecen en el Grado.

Plazas: 3

Nombre de los alumnos: (Tayomara Anjara Borsich González)

PROPUESTA DE TRABAJO FIN DE GRADO

DINÁMICA DE POBLACIONES.

Breve descripción del trabajo propuesto.

El propósito de este trabajo es el estudio de modelos matemáticos que permiten describir aspectos cruciales del comportamiento colectivo de grandes poblaciones biológicas, partiendo del conocimiento de un número reducido de reglas básicas que regulan su comportamiento individual y sus estrategias de interacción.

Entre los ejemplos clásicos susceptibles de estudio podemos citar :

- 1) Propagación de epidemias .
- 2) Dinámica de especies que compiten en un medio y los correspondientes estados de equilibrio ecológico.
- 3) Modelos de selección natural. Evolución prebiótica.

Requisitos .

Haber superado cursos básicos de ecuaciones diferenciales ordinarias , ecuaciones en derivadas parciales y análisis numérico.

Directores : Dr. Juan Carlos López Alfonso (Universidad Técnica de Dresde, Alemania) y Dr. Miguel Angel Herrero Garcia (Universidad Complutense de Madrid).

Contacto.

Dr. Miguel A. Herrero (herrero@mat.ucm.es)

Departamento de Matemática Aplicada

Universidad Complutense de Madrid

<http://maherrero.wix.com/inicio>

Título: Test de unidad en Maude

Tutor: Adrián Riesco Rodríguez

Alumnos: 2

Descripción: Los test de unidad se utilizan para comprobar que las funciones de un cierto programa funcionan usando predicados de la forma `assert`, que indican que algo se evalúa a `true`, `assertEqual`, que indican que 2 valores son iguales, o `assertNotEqual`, que indican que 2 valores son diferentes. En este trabajo se propone definir test de unidad para el lenguaje declarativo Maude, por lo que los objetivos del curso son: (i) aprender Maude al nivel necesario para poder definir el marco pretendido en el trabajo, (ii) pensar qué tests son los más adecuados para el lenguaje y (iii) implementar los tests definidos en el apartado anterior.

Título: Modelos Formales de la Concurrency

Tutor: David de Frutos Escrig

Alumnos: 2

El desarrollo de sistemas concurrentes que permita sacar partido tanto al paralelismo natural de los procesos a modelizar, como de la multiplicación de los procesadores de los que se dispone para ejecutar los mismos, tiene sus principales dificultades en la propia modelización y posteriormente en la comprobación de que la implementación propuesta es acorde con aquella.

A lo largo de los pasados 30 años han aparecido distintos formalismos que buscan facilitar ambas tareas, destacando entre ellos los que se apoyan en las llamadas Algebras de Procesos y las Redes de Petri.

La temática es tremendamente amplia y en principio casi totalmente desconocida para los alumnos que cursan el Grado en Matemáticas, por lo que aparte de una introducción general considero oportuno dejar mi propuesta totalmente abierta de manera que posteriormente centren una segunda parte más específica de su trabajo en aquellas líneas que más llamen su atención, naturalmente tras haberlo determinado conmigo. En particular ello permitirá centrar la atención en los aspectos más teóricos o por contra dar al trabajo un tinte más aplicado que pasaría por el descubrimiento y uso de algunas de las herramientas bastante sofisticadas que se han desarrollado para el diseño y análisis automático de los sistemas concurrentes.
