Sesión Especial 18

Sesión especial de la red MATSI: Teoría de Códigos

Organizadores:

- Sara Díaz Cardell (Universidade Estadual Paulista)
- Helena Martín Cruz (Universitat Jaume I)
- Verónica Requena (Universidad de Alicante)
- Carlos Vela Cabello (Universidade de Aveiro)

Descripción:
La teoría de códigos se ha convertido en los últimos 60 años, motivada por el auge de las comunicaciones, en un área activa de investigación que trata las leyes de la codificación de la información y el problema de detectar y corregir los posibles errores producidos en su transmisión. Para ello se codifica, es decir, se transforma en una señal convenida para su transmisión, agregándole cierta información extra que nos ayudará a detectarlos y corregirlos. Decodificar es el proceso inverso, mediante el cual la señal transmitida se transforma en la información original. La teoría de códigos hace uso de técnicas algebraicas clásicas y modernas que involucran cuerpos finitos, teoría de grupos y álgebra polinomial. En la actualidad, los avances que se están produciendo están encaminados hacia la utilización de las bases de Gröbner como herramienta para la codificación y decodificación en los códigos correctores de errores. El objetivo de esta sesión es reunir a especialistas en esta área para poner en común los progresos e investigaciones relacionados con los problemas abiertos de códigos.

Programa

Jueves, 25 de enero:

11:30 – 12:00	Xaro Soler Escrivà (Universidad de Alicante) *Linear and semilinear equivalency of flag codes*
12:00 – 12:30	Diego Ruano (Universidad de Valladolid) *Relative hulls and quantum codes*
12:30 – 13:00	José Iglesias Curto (Universidad de Salamanca) *Construcción de códigos complete MDP*
13:00 – 13:30	Diego Napp (Universidad de Alicante) *Weighted Reed-Solomon Convolutional Codes*
16:00 – 16:30	Mercè Villanueva (Universitat Autònoma de Barcelona) *Construction of Families of $\mathbb{Z}_p\mathbb{Z}_{p^2}\ldots\mathbb{Z}_{p^s}$-Linear Hadamard Codes, Classification and Permutation Decoding*
16:30 – 17:00	Rodrigo San José Rubio (Universidad de Valladolid) *A recursive construction for projective Reed-Muller codes*
17:00 – 17:30	Juan Jacobo Simón Pinero (Universidad de Murcia) *El algoritmo de Berlekamp-Massey-Sakata*

Viernes, 26 de enero:

11:30 – 12:00	Ángel Luis Muñoz Castañeda (Universidad de León) *Moduli problems, enumerative geometry and coding theory*
12:00 – 12:30	Noemí de Castro García (Universidad de León) *Códigos convolucionales observables con propiedades óptimas de decodificación y distancias utilizando representaciones de I/S/O*
12:30 – 13:00	Fernando Hernando (Universitat Jaume I) *Quantum codes from Generalized Monomial-Cartesian Codes*
13:30 – 14:00	Carlos Cabello Vela (Universidad de Aveiro) *Decoding 2D convolutional codes over erasure channels*

Linear and semilinear equivalency of flag codes

Xaro Soler-Escrivà, Miguel Ángel Navarro-Pérez

Departament de Matemàtiques, Universitat d'Alacant

xaro.soler@ua.es

Abstract: In the context of Network Coding, *flag codes* can be seen as an extension of *constant dimension codes*. In this case, the codewords are sequences of nested subspaces (flags) of a finite dimensional vector space over a finite field. Flag codes were introduced by Liebhold *et al.* in [3] and, since then, several works have deepened the study of these codes and provided different constructions of them (see [1, 2, 4] for instance).
The *projected codes* of a flag code are the constant dimension codes containing all the subspaces of prescribed dimensions that form the flags in the flag code.
In this talk we address the notion of (semi)linear equivalence for flag codes and explore in which situations such an equivalence can be reduced to the (semi)linear equivalence of the corresponding projected codes. In addition, this study leads to new results concerning the automorphism group of certain families of flag codes.

References

[1] C. Alonso-González, M. A. Navarro-Pérez, X. Soler-Escrivà (2021). An Orbital Construction of Optimum Distance Flag Codes. Finite Fields and Their Applications, Vol. 73, 101861.

[2] S. Kurz (2021). Bounds for Flag Codes. Designs, Codes and Cryptography, Vol. 89, 2759-2785.

[3] D. Liebhold, G. Nebe, A. Vazquez-Castro (2018). Network Coding with Flags. Designs, Codes and Cryptography, Vol. 86 (2), 269-284.

[4] M. A. Navarro-Pérez, X. Soler-Escrivà (2022). Flag codes of maximum distance and constructions using Singer groups. Finite Fields and Their Applications, Vol. 80, 102011.

Acknowledgments: The authors received financial support of Ministerio de Ciencia e Innovación (PID2022-142159OB-I00) and Conselleria de Innovación, Universidades, Ciencia y Sociedad Digital (CIAICO/2022/167).

Relative hulls and quantum codes

Diego Ruano, Sarah E. Anderson, Eduardo Camps-Moreno, Hiram H. López, Gretchen L. Matthews, Ivan Soprunov

IMUVa-Instituto de Investigación en Matemáticas, Universidad de Valladolid

diego.ruano@uva.es

Abstract: Given two q-ary codes C_1 and C_2, the relative hull of C_1 with respect to C_2 is the intersection $C_1 \cap C_2^{\perp}$. We prove that when $q > 2$, the relative hull dimension can be repeatedly reduced by one, down to a certain bound, by replacing either of the two codes with an equivalent one. The reduction of the relative hull dimension applies to hulls taken with respect to the e-Galois inner product, which has as special cases both the Euclidean and Hermitian inner products. We give conditions under which the relative hull dimension can be increased by one via equivalent codes when $q > 2$. We study some consequences of the relative hull properties on entanglement-assisted quantum error-correcting codes (EAQECCs) [2, 3]. The relative hull dimension is linked to c, the required number of pairs of maximally entangled quantum states for an EAQECC. Our results demonstrate how monomially equivalent codes may be used to tailor the parameter c. Thus, we can reduce the required number of pairs of maximally entangled quantum states while maintaining the net rate and prove the existence of new entanglement-assisted quantum error-correcting maximum distance separable codes, meaning those whose parameters satisfy the quantum Singleton bound [1].

References

[1] S.E. Anderson, E. Camps-Moreno, H.H. López, G.L. Matthews, D. Ruano, I. Soprunov (2022) Relative hulls and quantum codes. arXiv:2212.14521

[2] T. Brun, I. Devetak, M.-H. Hsieh (2006) Correcting Quantum Errors with Entanglement. Science 314, 5798, 436-439

[3] C. Galindo, F. Hernando, R. Matsumoto, D Ruano (2019). Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. Quantum Information Processing 4, 116.

Acknowledgments: The first author was partially supported by Grant TED2021-130358B-I00 funded by MCIN/AEI/10.13039/501100011033 and by the "European Union NextGenerationEU/PRTR", and by QCAYLE project funded by MCIN, the European Union NextGenerationEU (PRTR C17.I1) and Junta de Castilla y León.

Construcción de códigos complete MDP

José Ignacio Iglesias Curto

Departamento de Matemáticas e IUFFyM, Universidad de Salamanca

joseig@usal.es

Resumen: Los códigos MDP se definen por la propiedad de que su secuencia (perfil) de distancias columna es óptima, lo que les permite corregir el máximo número de errores en una ventana temporal de longitud determinada. Esto es particularmente aplicable sobre el canal de borrado. Un código MDP permite una recuperación óptima de coordenadas borradas, condicionada a la existencia de un espacio de resguardo previo a la ventana a decodificar.
Los códigos complete MDP son una subclase de códigos MDP que verifican además algunas propiedades más restrictivas. A cambio, permiten recuperar borrados en ciertas condiciones cuando no existe el espacio de resguardo previo a la ventana. Son, por tanto, los códigos con mejores capacidades para la recuperación de borrados. Las propiedades adicionales que los definen hacen que sea extremadamente complicado obtener códigos de este tipo. Aunque se sabe que puede construirse un código de parámetros dados sobre un cuerpo suficientemente grande, tampoco se conoce en general con exactitud el mínimo tamaño del cuerpo sobre el que puede obtenerse. Tanto el estudio del tamaño del cuerpo como la construcción explícita de códigos complete MDP son materias de indudable interés.
El objetivo de este trabajo es utilizar propiedades conocidas de este tipo de códigos para materializar construcciones y analizar el tamaño del cuerpo sobre el que se pueden realizar.

Weighted Reed-Solomon Convolutional Codes

Gianira N. Alfarano, Diego Napp, Alessandro Neri, Verónica Requena

Departamento de Matemáticas, Universidad de Alicante

diego.napp@ua.es

Resumen: En esta charla presentamos una construcción algebraica concreta de una nueva clase de códigos convolucionales. Estos códigos se basan en matrices de Vandermonde generalizadas y, por lo tanto, pueden verse como una extensión natural de los códigos bloque Reed-Solomon en el contexto de los códigos convolucionales. Por esta razón los llamamos Weighted Reed-Solomon convolutional codes(WRS). Mostramos que, bajo algunas restricciones en los parámetros que definen estos códigos, son códigos MDP, lo que significa que tienen el máximo crecimiento posible respecto a la distancia columna. Estudiamos el tamaño del cuerpo necesario para obtener códigos convolucionales WRS que son MDP y lo comparamos con las construcciones generales existentes de códigos convolucionales MDP en la literatura, mostrando que en muchos casos los códigos convolucionales aquí presentados requieren cuerpos significativamente más pequeños.

Agradecimientos: Los autores Diego Napp y Verónica Requena recibieron soporte financiero del Ministerio de Ciencia e Innovación (PID2022-142159OB-I00) y de la Conselleria de Innovación, Universidades, Ciencia y Sociedad Digital (CIAICO/2022/167).

Construction of Families of $\mathbb{Z}_p\mathbb{Z}_{p^2}\dots\mathbb{Z}_{p^s}$-Linear Hadamard Codes, Classification and Permutation Decoding

Mercè Villanueva, Dipak K. Bhunia, Cristina Fernández-Córdoba, Josep Rifà, Adrián Torres-Martín

Departamento de Ingeniería de la Información y de las Comunicaciones
Universitat Autònoma de Barcelona

merce.villanueva@uab.cat

Abstract: The $\mathbb{Z}_p\mathbb{Z}_{p^2}\dots\mathbb{Z}_{p^s}$-additive codes are subgroups of $\mathbb{Z}_p^{\alpha_1}\times\mathbb{Z}_{p^2}^{\alpha_2}\times\cdots\times\mathbb{Z}_{p^s}^{\alpha_s}$. A $\mathbb{Z}_p\mathbb{Z}_{p^2}\dots\mathbb{Z}_{p^s}$-linear Hadamard code is a generalized Hadamard code over $\mathbb{Z}_p$ which is the Gray map image of a $\mathbb{Z}_p\mathbb{Z}_{p^2}\dots\mathbb{Z}_{p^s}$-additive code. Recursive constructions for some families of these codes of type $(\alpha_1,\dots,\alpha_s;t_1,\dots,t_s)$ are described. First, it is shown for which types the corresponding generalized Hadamard codes of length 2^t are nonlinear. For these codes, the rank and dimension of the kernel, which allow us to give a partial classification of these codes, are computed. In some cases, a complete classification can be provided, by giving the exact amount of nonequivalent such codes for a given length. The equivalence relations between several infinite families of these codes are studied. For example, $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-linear Hadamard codes of length 2^{11} with nonzero $\alpha_1,\alpha_2,\alpha_3$ are not equivalent to each other, nor are they equivalent to any $\mathbb{Z}_2\mathbb{Z}_4$-linear or $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s\geq 2$, with the same length 2^{11}.

Since $\mathbb{Z}_{p^s}$-linear codes are systematic, the permutation decoding method can be applied to these codes. This technique also requires the existence of r-PD-sets, which are subsets of the permutation automorphism group of the code. The permutation automorphism group for $\mathbb{Z}_{p^s}$-linear generalized Hadamard codes is determined and, in order to be able to perform a partial permutation decoding for these codes, we show how to construct r-PD-sets of minimum size $r+1$, for all r up to an upper bound.

References

[1] D. K. Bhunia, C. Fernández-Córdoba, M. Villanueva (2023). Linearity and classification of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear generalized Hadamard codes, Finite Fields Their Appl., 102140.

[2] A. Torres-Martín, M. Villanueva (2023). Partial permutation decoding and PD-sets for $\mathbb{Z}_{p^s}$-linear generalized Hadamard codes, Finite Fields Their Appl., 102316.

Acknowledgments: This work has been partially supported by the Spanish Ministerio de Ciencia e Innovación under Grants PID2019-104664GB-I00, PID2022-137924NB-I00, and RED2022-134306-T (AEI/10.13039/501100011033) and by the Catalan AGAUR grant 2021SGR 00643.

A recursive construction for projective Reed-Muller codes

Rodrigo San José

Universidad de Valladolid

rodrigo.san-jose@uva.es

Abstract: Binary affine Reed-Muller codes can be constructed recursively via the $(u \mid u+v)$ construction. Generally, q-ary affine Reed-Muller codes can be constructed recursively using a matrix-product code construction. We are interested in a recursive construction for projective Reed-Muller codes, a generalization of affine Reed-Muller codes obtained by evaluating homogeneous polynomials in the projective space $\mathbb{P}^m$. We apply this recursive construction to obtain information about the subfield subcodes and generalized Hamming weights of projective Reed-Muller codes. Given a code $C \subset \mathbb{F}_{q^s}^n$, its subfield subcode with respect to the extension $\mathbb{F}_{q^s} \supset \mathbb{F}_q$ is the linear code $C \cap \mathbb{F}_q^n$. With this technique, it is possible to construct long linear codes with good parameters over a small finite field. The main task is the computation of a basis for the subfield subcode, which, in particular, gives its dimension. We show that, for certain degrees, the recursive construction we obtain for projective Reed-Muller codes can be applied to their subfield subcodes as well. This directly gives the dimension of these subfield subcodes in a recursive manner, for any $m \geq 2$, and allows us to obtain a set of polynomials such that its evaluation is a basis for the subfield subcode. We can obtain a description of the subfield subcode as an evaluation code. For some particular degrees, we obtain codes with good parameters: codes with the best known parameters and many codes surpassing the Gilbert-Varshamov bound. The generalized Hamming weights of a code are a set of parameters that generalize the minimum distance. Although the complete weight hierarchy of affine Reed-Muller codes was determined, the computation of the generalized Hamming weights of projective Reed-Muller codes remains an open problem and only partial results are known. We obtain a recursive lower bound for the generalized Hamming weights of a projective Reed-Muller code of any degree. Moreover, we provide an upper bound that gives us a criterion to ensure that the bound is sharp in many cases. By considering the monotonicity and duality properties of the generalized Hamming weights and our bounds, we obtain the exact values of the generalized Hamming weights of projective Reed-Muller codes in many cases.

El Algoritmo de Berlekamp-Massey-Sakata.

J. J. Simón, J. J. Bernal

Departamento de Matemáticas, Universidad de Murcia

jsimon@um.es

Resumen: El algoritmo de Berlekamp-Massey-Sakata (aBMS) es una generalización a dos variables del algoritmo de Berlekamp-Massey que consiste en, dada una sucesión periódica en un cuerpo finito, encontrar la fórmula de recurrencia que la genere. En el caso de dos variables, consiste en encontrar una base de Groebner para determinar el sistema de recurrencias lineales.
Existen muchos métodos de descodificación basados en este algoritmo; entre otros, la descodificación por localización que se aplica en códigos abelianos y algebraico-geométricos.
En esta charla, vamos a mostrar un panorama sobre su funcionamiento y comentaremos algunas de nuestras aportaciones en un trabajo conjunto con José Joaquín Bernal. Entre otras, cabe mencionar la siguiente: para una tabla de orden $r_1 \times r_2$ (o bien, doblemente periódica), obtenida por una fórmula polinomial (por síndromes) que tiene $t \leq \min\{\lfloor \frac{r_1}{2} \rfloor, \lfloor \frac{r_2}{2} \rfloor\}$ términos, existe un conjunto mínimo de índices sobre el que basta ejecutar el algoritmo para obtener la base de Groebner, garantizando que el proceso terminará en, a lo más, $\frac{t^2+7t}{2} - 1$ pasos.

Agradecimientos: This work was partially supported by MINECO, project PID2020-113206GB- I00/AEI/10.13039 /501100011033, and Fundación Séneca of Murcia, project 22004/PI/22.

Moduli problems, enumerative geometry and coding theory

Ángel Luis Muñoz Castañeda

Departamento de Matemáticas, Universidad de León

amunc@unileon.es

Abstract: Let k, n, g be natural numbers such that $n/2 > k > 2g - 2$. In this talk I will show a close relationship between three problems different in nature. On one hand, the existence of a very strong algebraic-geometric structure for a given convolutional code of rate k/n. On the other hand, the existence of a (twisted) smooth projective curve X in the $(k-1)$-dimensional projective space passing through n different rational points. And finally, the existence of an n-pointed smooth projective curve whose associated moduli space of line bundles with level structures $M(X, D)$ contains a given rational point of the Grassmannian $Gr(k, n)$ through its canonical immersion $M(X, D) \hookrightarrow Gr(k, n)$.

Acknowledgments: This work was partially supported by MINECO, project TED2021-121158A-I00.

Códigos convolucionales observables con propiedades óptimas de decodificación y distancia mediante representaciones I/S/O

N. DeCastro-García, Á.L. Muñoz Castañeda, M. V. Carriegos

Departamento de Matemáticas, Universidad de León

ncasg@unileon.es

Resumen: Los códigos convolucionales son códigos de detección y corrección de errores utilizados para transmitir, detectar y corregir la información enviada a través de un canal. En esta charla, nos centraremos en los códigos convoluciones desde su descripción como submódulos libres $\mathcal{C} \subset R[z]^n$ de rango k, siendo R un cuerpo finito o determinados anillos conmutativos. Un problema fundamental en la teoría de códigos convolucionales es encontrar métodos para construir códigos convolucionales con buenas propiedades, como la no propagación de errores (observabilidad) o un buen desempeño cuando se aplica un algoritmo de decodificación. Por otro lado, otra propiedad deseable de un código convolucional es que tenga una buena distancia. En este caso, el código tendrá una tasa de recuperación óptima.

Esta charla tiene como objetivo presentar diferentes formas de construir códigos convolucionales observables con buenas propiedades de decodificación mediante los sistemas lineales dinámicos que tienen asociados; es decir, mediante lo que se conoce como una representación de *entrada/estado/salida* (I/S/O) del código.Esta aproximación es útil porque nos permite utilizar las propiedades algebraicas estructurales de sistemas lineales para trabajar en teoría de codificación, considerando propiedades específicas en las matrices que componen las representaciones I/S/O.

Agradecimientos: Este trabajo se enmarca dentro del proyecto *Algebraic Methods for the Recovery, Correction and Security of Digital Information (MARCSID)*, concedido en la convocatoria de *Proyectos Estratégicos Orientados a la Transición Ecológica y a la Transición Digital 2021* TED2021-131158A-I00 por el Ministerio de Ciencia e Innovación.

Quantum Codes from Generalized Monomial-Cartesian Codes

Fernando Hernando, Beatriz Barbero-Lucas, Helena Martín-Cruz and Gary McGuire

Departamento de Matemáticas e Instituto de Matemáticas y Aplicaciones de Castellón (IMAC), Universitat Jaume I

carrillf@uji.es

Abstract: We construct new stabilizer quantum error-correcting codes from generalized monomial-Cartesian codes. Our construction uses an explicitly defined twist vector, and we present formulas for the minimum distance and dimension. Generalized monomial-Cartesian codes arise from polynomials in m variables. When $m = 1$ our codes are MDS, and when $m = 2$ and our lower bound for the minimum distance is 3 the codes are at least Hermitian Almost MDS. For an infinite family of parameters when $m = 2$ we prove that our codes beat the Gilbert-Varshamov bound. We also present many examples of our codes that are better than any known code in the literature.

Decoding 2D convolutional codes over erasure channels

Carlos Vela Cabello, Raquel Pinto, Marcos Spreafico

Departamento de Matemática, Universidade de Aveiro

carlos.vela@ua.pt

Abstract: In this talk we address the problem of constructing optimal 2D convolutional codes for decoding algorithm over an erasure channel. It is well-known that when transmitting over an erasure channel the symbols sent either arrive correctly or they are erased. Convolutional codes are proven to be more efficient than classical block codes when communication over these [2]. Even though there exist decoding methods [1], there is a lack of constructions of optimal codes for them. We propose the construction of two families of 2D convolutional codes (one optimal) based on an optimal 1D convolutional code [3, 4] .

References

[1] J. Lieb, R. Pinto (2023). A decoding algorithm for 2D convolutional codes over the erasure channel. Advances in Mathematics of Communications, 17(4): 935-959. doi: 10.3934/amc.2021031.

[2] V. Tomas, J. Rosenthal, R. Smarandache (2012). Decoding of Convolutional Codes Over the Erasure Channel. IEEE Transactions on Information Theory, vol. 58, no. 1, pp. 90-108, doi: 10.1109/TIT.2011.2171530.

[3] J. Lieb (2019). Complete MDP convolutional codes. Journal of Algebra and Its Applications, Vol. 18, No. 06, 1950105 doi: 10.1142/S0219498819501056

[4] J.-J. Climent, D. Napp, R. Pinto, R. Simões (2016). Decoding of 2D convolutional codes over an erasure channel. Advances in Mathematics of Communications, 10(1): 179-193. doi: 10.3934/amc.2016.10.179

Acknowledgments: This work was supported by The Center for Research and Development in Mathematics and Applications (CIDMA) through the Portuguese Foundation for Science and Technology (FCT - Fundação para a Ciência e Tecnologia), references UIDB/04106/2020.