Sesión Especial 20

Matemáticas de la Teoría de la Información

Organizadoras

- Sara Díaz Cardell (Universidade Estadual de Campinas, Brasil)
- Irene Márquez Corbella (Universidad de La Laguna)
- Adriana Suárez Corona (Universidad de León)

Descripción

La teoría de la información, también llamada teoría matemática de la comunicación, fue introducida por Claude Shannon y Warren Weaver a finales de los años 1940. Corresponde a una rama de las matemáticas y de la computación que estudia la transmisión y el procesamiento de datos. También se ocupa de medir y representar la información y de estudiar la capacidad de los sistemas de comunicación para procesar y trasmitir esa información. Constituye una de las áreas más activas de la matemática aplicada y sus aplicaciones abarcan desde las ciencias de la computación (criptografía, compresión de datos), la ingeniería eléctrica (teoría de la comunicación y teoría de la codificación), la estadística o la biología (secuencias de ADN, código genético). Además, sus distintas aplicaciones en protocolos criptográficos, protocolos de comunicación, pagos y transacciones electrónicas, autenticación, compartición de secretos, esteganografía, etc, son una pequeña muestra de la aplicabilidad de la teoría de la información en gran cantidad de sectores de la tecnología actual.

Programa

Martes, 5 de febrero (tarde)

17:00 – 17:30	Verónica Requena (Universitat d'Alacant) *Códigos Convolucionales sobre canales de borrado en ráfaga con bajo retardo*
17:30 – 18:00	José Ignacio Iglesias Curto (Universidad de Salamanca) *Una caracterización de códigos convolucionales MDS*
18:00 – 18:30	Francisco J. Plaza-Martín (Universidad de Salamanca) *Rosenthal's decoding algorithm for certain 1-dimensional convolutional codes*
18:30 – 19:00	Gabriel Navarro (Department of Computer Sciences and AI, University of Granada) *Decoding constacyclic codes by means of non commutative polynomials*

Jueves, 7 de febrero (mañana)

11:30 – 12:00	Juan Antonio López Ramos (Universidad de Almería) *Control de claves en grupos: ¿tienen sentido los protocolos distribuidos?*
12:00 – 12:30	Josep M. Miret (Universitat de Lleida) *Protocolos Diffie-Hellman de intercambio de claves con isogenias*
12:30 – 13:00	Oriol Farràs (Universitat Rovira i Virgili) *Improving the Linear Programming Technique in the Search for Lower Bounds in Secret Sharing*
13:00 – 13:30	María Isabel González Vasco (Universidad Rey Juan Carlos) *GPAKE for a priori unknown partners*

Jueves, 7 de febrero (tarde)

15:30 – 16:00	Jorge Jiménez Urroz (Universidad Politécnica de Catalunya) *Visitando la factorización de números que son producto de dos primos*
16:00 – 16:30	Adriana Suárez Corona (Universidad de León) *Integrating classical preprocessing into an optical encryption scheme*
16:30 – 17:00	Markel Epelde (UPV/EHU, TECNALIA Research & Innovation) *Aplicaciones de códigos no lineales en criptografía*
17:30 – 18:00	Amparo Fúster-Sabater (Instituto de Tecnologías Físicas y de la Información, CSIC) *Propiedades estructurales de los generadores t-modificados*
18:00 – 18:30	Sara D. Cardell (Universidade Estadual de Campinas, Brazil) *Binomial representation of sequences*

VIERNES, 8 de febrero (mañana)

9:00 – 9:30	Fernando Hernando (Institut Universitari de Matemàtiques y Aplicacions de Castelló, Universidad Jaume I) *On the computation of the duals of certain Algebraic Geometric codes with an application to quantum codes*
9:30 – 10:00	Diego Ruano (Mathematics Research Institute, Universidad de Valladolid) *Classical and quantum evaluation codes at the trace roots*
10:00 – 10:30	Edgar Martínez-Moro (Universidad de Valladolid) *On polycyclic codes over finite chain rings*
10:30 – 11:00	Joaquim Borges (Universitat Autònoma de Barcelona) *$\mathbb{Z}_{2^k}$-linear Hadamard codes, Hadamard full propelinear codes, and completely regular codes*
11:30 – 12:00	Juan Jacobo Simón Pinero (Universidad de Murcia) *Conjuntos de información a partir de conjuntos de definición para códigos de Reed-Muller de primer y segundo orden*
12:00 – 12:30	María Bras-Amorós (Departament d'Enginyeria Infomàtica i Matemàtiques, Universitat Rovira i Virgili) *On the Inheritance of the Isometry-Dual Property under Puncturing AG Codes*
12:30 – 13:00	Consuelo Martínez (Universidad de Oviedo) *Sobre códigos grupo no abelianos*

Códigos Convolucionales sobre canales de borrado en ráfaga con bajo retardo

Verónica Requena

Universidad de Alicante

vrequena@ua.es

Resumen.

En los últimos años está creciendo la investigación sobre códigos para aplicaciones de transmisión de secuencias de bits, donde se transmite secuencialmente un flujo de datos en tiempo real bajo estrictas restricciones de latencia [1, 2]. Esto se debe al hecho de que en muchas aplicaciones multimedia, como las videoconferencias en tiempo real, la información debe reproducirse de forma secuencial y con un retraso perceptible mínimo en el destino.
En este trabajo, nos centraremos en los códigos convolucionales en canales de borrado de ráfagas (es decir, donde se producen pérdidas de grupos de paquetes). Investigamos y caracterizamos completamente el tipo de codificadores que son óptimos con respecto a la velocidad, el retraso de decodificación y la longitud de ráfaga. Además, presentamos una nueva clase de codificadores definidos sobre el campo binario donde la decodificación es muy sencilla y rápida.

Referencias

[1] R. Mahmood, A. Badr, and A. Khisti, "Streaming-codes for multicast over burst erasure channels", IEEE Trans. Inform. Theory, vol. 61, no. 8, pp. 4181–4208, 2015.

[2] E. Martinian and C. E. W. Sundberg, "Burst erasure correction codes with low decoding delay," IEEE Transactions on Information Theory, vol. 50, no. 10, pp. 2494–2502, 2004.

Trabajo en colaboración con Diego Napp. Financiado por el proyecto otorgado por la Generalitat Valenciana, AICO/2017/128.

Una caracterización de códigos convolucionales MDS.

José Ignacio Iglesias Curto

Universidad de Salamanca

joseig@usal.es

Resumen. El estudio de la distancia libre de los códigos convolucionales es una de las tareas más complejas en el estudio de este tipo de códigos. Esto es particularmente aplicable al estudio de los códigos MDS. Se sabe que aunque cuando el cuerpo base es pequeño dichos códigos pueden ni existir, si el cuerpo es suficientemente grande el conjunto de códigos MDS forma un abierto.
El objetivo de esta charla es presentar una caracterización explícita mediante un conjunto de ecuaciones de códigos convolucionales MDS con parámetros prefijados.

Rosenthal's decoding algorithm for certain 1-dimensional convolutional codes

Francisco J. Plaza-Martín

Universidad de Salamanca

fplaza@usal.es

Abstract.
Convolutional codes were introduced by P. Elias having as objective to have codes with error probability function with better behavior as that of for block codes. The theory of convolutional codes can be established in terms of linear systems and, equivalently, can be also be developed by using purely algebro-geometric techniques.
Among the parameters that determine the properties of a convolutional code, say length, dimension etc, one of the most important is its free distance, since it is closely related to the error-correcting capability of the code. The larger the free distance is, the larger the error-correcting capability of the code. A very important fact in this direction is the existence of an upper bound (Singleton bound) for the free distance for fixed dimension and length. Therefore, those convolutional codes that achieves the Singleton bound (MDS convolutional codes) are of much interest.
An important issue in coding theory is the construction of decoding schemes. If the the transmission channel is noisy, there are two essentially different kind of decoding schemas: probabilistic decoders and algebraic decoders. Despite the former are efficient, they are computationally expensive, while the last ones make use of less physical resources.
In this talk, we look at the performance of Rosenthal's decoding algorithm [1] (that was stated in terms of linear systems) a family of MDS convolutional codes constructed with algebro-geometric techniques.

Referencias

[1] J. Rosenthal, An Algebraic Decoding Algorithm for Convolutional Codes. In: Picci G., Gilliam D.S. (eds) Dynamical Systems, Control, Coding, Computer Vision. Progress in Systems and Control Theory, vol. 25. Birkhäuser Basel (1999) pp 343-360.

Trabajo en colaboración con Ángel L. Munõz y José M. Munõz.
Financiado por MTM2015-66760-P.

Decoding constacyclic codes by means of non commutative polynomials

Gabriel Navarro

Department of Computer Sciences and AI, University of Granada

gnavarro@ugr.es

Abstract. Skew constacyclic (block) codes of length n over a finite field $\mathbb{F}$ are defined as those vector subspaces of $\mathbb{F}^n$ with a structure of left ideal of $\mathbb{F}[x;\sigma]/\langle x^n - \lambda\rangle$, via the standard coordinate map, where $\mathbb{F}[x;\sigma]$ denotes the ring of skew polynomials and $\lambda \in \mathbb{F}$ is invariant under σ. In this talk we show several decoding methods similar to those developed in [1, 2] for skew cyclic codes. As an application, we obtain decoding algorithms for some (commutative) constacyclic codes by using a suitable embedding of the ring of (commutative) polynomials into a ring of skew polynomials.

Referencias

[1] J. Gómez-Torrecillas, F.J. Lobillo, and G. Navarro, A Sugiyama-like decoding algorithm for convolutional codes, IEEE Trans. Inform. Theory 63 (2017) 6216–6226.

[2] J. Gómez-Torrecillas, F.J. Lobillo, and G. Navarro, Peterson-Gorenstein-Zierler algorithm for skew RS codes, Linear and Multilinear Algebra 66 (2018), 469–487.

Joint work with José Gómez-Torrecillas, Péter Kutas and F. J. Lobillo.
Supported by grant MTM2016-78364-P from AEI and FEDER.

Control de claves en grupos: ¿tienen sentido los protocolos distribuídos?

Juan Antonio López Ramos

Universidad de Almería

jlopez@ual.es

Resumen. Los protocolos de control de claves en grupos se dividen, tradicionalmente, en tres grupos [1]: centralizados, donde una única entidad se encarga de la creación y distribución de la clave de grupo, así, como de los procesos de renovación; descentralizados, en los que los comunicantes se distribuyen en subgrupos controlados, cada uno de ellos por un usuario destacado; y distribuídos, en los que todos los usuarios intervienen de forma colaborativa en todos los procesos. El propósito de esta charla es mostrar cómo algunos de los principales protocolos de tipo distribuído, tales como los presentados en [2] o [3] sucumben a ataques basados una variación del ataque Man-in-the-Middle y que permiten al atacante tomar el control del grupo. Mostraremos algunas variantes de los mismos, como [4], que no son afectados por los mismos, pero que modifican ligeramente el concepto de protocolo distribuído, aproximándose al de centralizado.

Referencias

[1] Rafaeli, S. and Hutchison, D. , A survey of key management for secure group communication, ACM Comput. Surv. 35(3) (2003), 309–329.

[2] Steiner, M., Tsudik, G. and Waidner, M., Key agreement in dynamic peer groups, IEEE Trans. Parall. Distr. 11(8) (2000), 769–780.

[3] Burmester, M, Desmedt, I., A secure and scalable group key exchange system, Inf. Process. Lett. 94 (2005), 137–143.

[4] Lopez-Ramos, J.A., Rosenthal, J., Schipani, D., Schnyder, R. An application of group theory in confidential network communications, por aparecer en Math. Meth. Appl. Sci.

Trabajo en colaboración con Joachim Rosenthal, Davide Schipani y Reto Schnyder, de la Universidad de Zurich.

Protocolos Diffie-Hellman de intercambio de claves con isogenias

Josep M. Miret

Universitat de Lleida

miret@matematica.udl.cat

Resumen. En 1976, W. Diffie y M.E. Hellman [1] propusieron un intercambio de claves seguro entre dos usuarios, que marcó el origen de la criptografía de clave pública. En 2004, A. Joux [2] diseñó usando emparejamientos un protocolo de intercambio a tres bandas en el que solo es necesario una ronda para establecer la clave compartida. Más recientemente, De Feo, Jao y Plût [3] han planteado un intercambio basado en isogenias de curvas elípticas supersingulares que se cree que es resistente a ataques cuánticos. En esta charla, haremos una revisión de estos protocolos criptográficos, describiendo algunos de los requisitos que deben satisfacer sus parámetros para que sean seguros y eficientes.

Referencias

[1] W. Diffie y M. E. Hellman: "New Directions in Cryptography", *IEEE Trans. Inf. Theor.*, vol. 22, n. 6, pp. 644–654, 1976.

[2] A. Joux: "A one round protocol for tripartite Diffie-Hellman", *Journal of Cryptology*, vol. 17, n. 4, pp. 263–276, 2004.

[3] L. De Feo, D. Jao y J. Plût: "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies", *Journal of Mathematical Cryptology*, vol. 8, n. 3, pp. 209–247, 2014.

Trabajo en colaboración con D. Sadornil, J. Tena y J. Valera.
Financiado por el Ministerio de Economía, Industria y Competitividad mediante los proyectos MTM2014-55421-P y MTM2017-83271-R y por la Generalitat de Catalunya mediante el grupo 2017SGR 1158.

Improving the Linear Programming Technique in the Search for Lower Bounds in Secret Sharing

Oriol Farràs

Universitat Rovira i Virgili

oriol.farras@urv.cat

Abstract. A secret sharing scheme is a method by which a dealer distributes shares to parties such that only authorized subsets of parties can reconstruct the secret. The access structure of a scheme is the family of authorized subsets. Every monotone increasing family of subsets is the access structure of a secret sharing scheme.
The information ratio of a secret sharing scheme is the size in bits of the largest share of the scheme divided by the size of the secret. The optimal information ratio of an access structure is the infimum of the information ratio among all schemes realizing the access structure. In general, it does not exist an efficient method to compute the optimal information ratio of an access structures.
We present a new improvement in the linear programming technique to derive lower bounds on the optimal information ratio. We use the Ahlswede–Körner lemma and the common information of random variables, avoiding the use of explicit non-Shannon information inequalities. In this way, we obtained better lower bounds and we could determine the optimal information ratio of linear secret sharing schemes for several families of access structures [1].

Referencias

[1] Farràs, O., Kaced, T., Martín, S., Padró, C.: Improving the Linear Programming Technique in the Search for Lower Bounds in Secret Sharing. *Advances in Cryptology — Eurocrypt 2018, Lecture Notes in Comput. Sci.* **10820** (2018) 597–621.

Joint work with Tarik Kaced, Sebastià Martín and Carles Padró.

GPAKE for a priori unknown partners

María Isabel González Vasco

Universidad Rey Juan Carlos

mariaisabel.vasco@urjc.es

Abstract. Secure key establishment is often the first step towards secure communication through cryptographic techniques. Key establishment is typically preformed using either digital signatures or passwords to authenticate legitimate group members. Most often, when passwords are used for authentication, messages constructed with non-matching passwords are identified as adversarial and result in a protocol abort. In [2], we recently put forward the notion of *partitioned* GPAKE, which will tolerate users that run the protocol on different passwords. We will briefly introduce this new theoretical framework, and give a construction using simple techniques from privacy-preserving set-theoretical operations. We prove its security under the *Computational Diffie - Hellman assumption* on the underlying cyclic group.

Referencias

[1] Bellare, M., Pointcheval, D., and Rogaway, P. (2000) Authenticated Key Exchange Secure Against Dictionary Attacks. *Advances in Cryptology – EUROCRYPT 2000*, pp. 139–155.

[2] Dario Fiore, Maria Isabel Gonzalez Vasco, and Claudio Soriente. Partitioned group password-based authenticated key exchange. *Comput. J.*, 60(12):1912–1922, 2017.

Joint work with Dario Fiore and Claudio Soriente.
Founded by MINECO project MTM2016-77213-R and by the NATO Science for Peace and Security Programme under grant G5448.

Visitando la factorización de números que son producto de dos primos

Jorge Jiménez Urroz

Universidad Politécnica de Catalunya

jorge.urroz@upc.edu

Resumen. Factorizar un módulo RSA n es un problema difícil. Motivados en aplicaciones criptográficas, Paillier and Villar se consideraron si podría existir otro número n' independiente de n de forma que la factorización de n' facilitase factorizar n, y conjeturaron que no existiría tal n'. Junto con L. Dieulefait probamos que tal conjetura es erronea y construimos un n' cuya factorización permite factorizar n en tiempo polinómico.

Integrating classical preprocessing into an optical encryption scheme

Adriana Suárez Corona

Universidad de León

asuac@unileon.es

Abstract. The AlphaEta protocol has been designed to exploit properties of coherent states of light to transmit data securely over an optical channel. AlphaEta aims to draw security from the uncertainty of any measurement of the transmitted coherent states due to intrinsic quantum noise.

In this talk, we propose a framework to combine this protocol with classical preprocessing, taking into account error-correction for the optical channel and establishing a strong provable security guarantee. Integrating a state-of-the-art solution for fast authenticated encryption is straightforward, but in this case the security analysis requires heuristic reasoning.

Joint work with Hai Pham and Rainer Steinwandt.
Founded by project MTM 2017-83506-C2-2-P.

Aplicaciones de códigos no lineales en criptografía

Markel Epelde

UPV/EHU, TECNALIA Research & Innovation

markel.epelde@tecnalia.com

Resumen. En 1948, Shannon presenta en [1] y [2] el primer trabajo de la Teoría de la Información, en el cual se centra en el problema de la transmisión de información. En el proceso de codificación de la información, el emisor transforma el mensaje en un elemento del código denominado palabra. Aún produciendose alteraciones en la palabra durante su transmisión, el receptor puede recuperar el mensaje original a partir de la palabra recibida. Si bien las formas habituales de codificación utilizadas hoy en día se basan en códigos lineales y utilizan propiedades de álgebra lineal, también existen códigos no lineales tales como los de Kerdock y Preparata. Estos últimos, cuya preimagen mediante la aplicación de Gray los hace $\mathbb{Z}/4\mathbb{Z}$-lineales [3], poseen propiedades que pueden ser utilizadas en otros ámbitos fuera de la Teoría de Códigos [4]. En esta charla se presentará una posible aplicación criptográfica de códigos no lineales.

Referencias

[1] Shannon, Claude E."A Mathematical Theory of Communication". Bell System Technical Journal, julio de 1948.

[2] Shannon, Claude E."A Mathematical Theory of Communication". Bell System Technical Journal, octubre de 1948.

[3] Roger Hammons, A.; Vijay Kumar, P.; Calderbank, A. R.; Sloane, N. J. A.; Solé, P., "The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals, and Related Codes". IEEE Transactions on Information Theory, 1994.

[4] Rao, T. R. N; Nam, K. H. "Private-Key Algebraic-Coded Cryptosystem", Lecture Notes in Computer Science 263; Advances in Cryptology - Proceedings of CRYPTO'86, 1987.

Trabajo en colaboración con Ignacio Fernández Rúa.
Financiado por TECNALIA Research & Innovation.

Propiedades estructurales de los generadores t-modificados

Amparo Fúster Sabater

Instituto de Tecnologías Físicas y de la Información, CSIC, Serrano 144, 28006, Madrid

amparo@iec.csic.es

Resumen. En este trabajo se define y analiza una familia de generadores de secuencia de uso criptográfico: los generadores t-modificados. Dicha familia incluye entre sus elementos al generador *self-shrinking* (SSG) [1] y al generador *modified self-shrinking* (MSSG) [2]. Asimismo, se demuestra que, bajo determinadas condiciones, las secuencias t-modificadas corresponden a secuencias producidas por el generador *generalized self-shrinking* [3], cuyas propiedades criptográficas están bien delimitadas. A partir de esta correspondencia, se puede mejorar cuantitativamente el rango de parámetros criptográficos (período, complejidad lineal, grado de equilibrio) de las secuencias descritas en [1] y [2], puesto que ya pueden estudiarse en términos de secuencias generalizadas.

Referencias

[1] Meier, W., Staffelbach, O.: The self-shrinking generator. Proceedings – EUROCRYPT 1994. LNCS **950** Springer-Verlag (1994) 205–214

[2] Kanso, A.: Modified self-shrinking generator. Compt Electr Eng **36**(1) (2010) 993–1001

[3] Y. Hu, G. Xiao.: Generalized Self-Shrinking Generator. IEEE T Inform Theory **50**(4) (2004) 714–719

Trabajo en colaboración con Sara D. Cardell de la Universidad de Campinas en Brasil (financiada por CAPES).
Financiado por el Ministerio de Economía, Industria y Competitividad (MINECO), la Agencia Estatal de Investigación (AEI) y el Fondo Europeo de Desarrollo Regional (FEDER, UE), bajo proyecto COPCIS, TIN2017-84844-C2-1-R.

Binomial representation of sequences

Sara D. Cardell

Universidade Estadual de Campinas (Brazil)

sdcardell@ime.unicamp.br

Abstract. Different binary sequence generators produce sequences whose period is a power of two. Although these sequences exhibit good cryptographic properties, such sequences can be obtained as output sequences from simple linear structures. More precisely, every one of these sequences is a particular solution of a linear difference equation with binary coefficients [1]. Moreover, it can be shown that all these binary sequences can be obtained by XORing a finite number of binomial sequences [1] that correspond to the diagonals of the Pascal's triangle reduced modulo 2. Consequently, such a linearity makes the generators that produce the previous sequences vulnerable against cryptanalysis and makes them not suitable as part of more complex cryptographic structures.

Referencias

[1] Amparo Fúster-Sabater. Generation of cryptographic sequences by means of difference equations. *Applied Mathematics & Information Sciences*, 8(2):475–484, 2014.

Joint work with Amparo Fúster-Sabater (Consejo Superior de Investigaciones Científicas).
The work of the first author was supported by CAPES (Brazil). This research has been partially supported by Ministerio de Economía, Industria y Competitividad (MINECO), Agencia Estatal de Investigación (AEI), and Fondo Europeo de Desarrollo Regional (FEDER, UE) under project COPCIS, reference TIN2017-84844-C2-1-R, and by Comunidad de Madrid (Spain) under project reference S2013/ICE-3095-CIBERDINE-CM.

On the computation of the duals of certain Algebraic Geometric codes with an application to quantum codes

Fernando Hernando

IMAC(Institut Universitari de matemàtiques y Aplicacions de Castelló). Universidad Jaume I

carrillf@uji.es

Abstract. We consider a family of smooth projective and absolutely irreducible plane curves over $\mathbb{F}_q$. We compute the number of rational points and a canonical divisor for it. Thanks to it we can deduce when the associated algebraic geometric code is self-orthogonal and construct stabilizer quantum codes. This work was inspired by reference [6].

Referencias

[1] Galindo, C., Hernando, F. Quantum codes from affine variety codes and their subfield subcodes, *Des. Codes Crytogr.* **76** (2015) 89-100.

[2] Galindo, C., Hernando, F., Ruano, D. New quantum codes from evaluation and matrix-product codes, *Finite Fields Appl.* **36** (2015) 98-120.

[3] Galindo, C., Hernando, F., Ruano, D. Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement, *Quantum Inf. Process.* **14** (2015) 3211-3231.

[4] Galindo, C., Geil, O., Hernando, F., Ruano, D. On the distance of stabilizer quantum codes from J-affine variety codes, *Quantum Inf. Process.* **16** (2017) 111.

[5] C. Galindo, F. Hernando, D. Ruano: Classical and quantum evaluation codes at the trace roots. Accepted for publication at *IEEE Transactions on Information Theory*. DOI: 10.1109/TIT.2018.2868442 (2018).

[6] C. Munuera, W. Tenorio, F. Torres: Quantum error-correcting codes from Algebraic Geometry codes of Castle type. *Quantum Information Processing*. **15** (2016), pp 4071–4088.

Joint work with Gary McGuire (University College Dublin) and Francisco Monserrat (Universidad Politécnica de Valencia).
Suported by Spanish MINECO/FEDER (Grant No. MTM2015-65764-C3-2-P, MTM2015-69138-REDT and UJI P1-1B2015-02.

Classical and quantum evaluation codes at the trace roots

Diego Ruano

IMUVA (Mathematics Research Institute). Universidad de Valladolid

diego.ruano@uva.es

Abstract. We introduce a new class of evaluation linear codes by evaluating polynomials at the roots of a suitable trace function. We give conditions for self-orthogonality of these codes and their subfield-subcodes with respect to the Hermitian inner product. They allow us to construct stabilizer quantum codes over several finite fields which substantially improve the codes in the literature. For the binary case, we obtain records at `http://codetables.de/`. Moreover, we obtain several classical linear codes over the field $\mathbb{F}_4$ which are records at `http://codetables.de/`.

Referencias

[1] C. Galindo, F. Hernando, D. Ruano: Classical and quantum evaluation codes at the trace roots. Accepted for publication at IEEE Transactions on Information Theory. DOI: 10.1109/TIT.2018.2868442 (2018).

Joint work with Carlos Galindo and Fernando Hernando (Jaume I University).
Suported by Spanish MINECO/FEDER (Grant No. MTM2015-65764-C3-2-P, MTM2015-69138-REDT and RYC-2016-20208 (AEI/FSE/UE)).

On polycyclic codes over finite chain rings

Edgar Martínez-Moro

Universidad de Valladolid

edgar.martinez@uva.es

Abstract. A structural theorem for polycyclic codes over a finite chain ring S is established using the concept of strong Gröbner bases. We explore the action of the Galois group $\mathtt{Aut}(S) = \langle\sigma\rangle$ on polycyclic codes over S whose period is relatively prime to p. For any divisor r of m the complete $\langle\,\sigma^r\,\rangle$-disjoint polycyclic codes are characterized. Finally an analogue Delsarte's theorem for the annihilator dual is established.

Joint work with A. Fotue Tabue (University of Yaoundé I) and T. Blackford (Western Illinois University).
Partially funded by MINECO MTM2015-65764-C3-1-P.

$\mathbb{Z}_{2^k}$-linear Hadamard codes, Hadamard full propelinear codes, and completely regular codes

Joaquim Borges

Universitat Autònoma de Barcelona

quim@deic.uab.cat

Abstract. In [3], a partial classification of $\mathbb{Z}_{2^s}$-linear Hadamard codes is given. Moreover, it is proven that there exist families of such codes which are equivalent with different values of s.
Hadamard full propelinear (HFP) codes are equivalent to Hadamard groups and cocyclic Hadamard matrices. In [1], the rank and dimension of the kernel are computed for a class of HFP-codes which are isomorphic to extensions of $C_{2t} \times C_2$.
We also present our last constructions of completely regular codes [2].

Referencias

[1] I. Bailera, J. Borges, J. Rifà. "Hadamard full propelinear codes with associated group $C_{2t} \times C_2$; rank and kernel,"submitted to *Designs, Codes and Cryptography*, arXiv: 1808.08747v1, 2018.

[2] J. Borges, J. Rifà, V. Zinoviev. "Completely regular codes by concatenating Hamming codes," *Advances in Mathematics of Communication, 12(2), pp. 337-349, 2018.*

[3] C. Fernández-Cordoba, C. Vela, M. Villanueva. "On $\mathbb{Z}_{2^s}$-linear Hadamard codes: kernel and partial classification,"to appear in Designs, Codes and Cryptography*, 2018. DOI: 10.1007/s10623-018-0546-6.*

Joint work with I. Bailera, C. Fernández-Córdoba, J. Rifà, C. Vela, M. Villanueva, V. Zinoviev.
This work has been partially supported by the Spanish MINECO grant TIN2016-77918-P(AEI/FEDER, UE).

Conjuntos de información a partir de conjuntos de definición para códigos de Reed-Muller de primer y segundo orden

Juan Jacobo Simón Pinero

Universidad de Murcia

jsimon@um.es

Resumen. Los códigos de Reed-Muller pueden ser vistos como afín-invariantes para obtener conjuntos de información. Desde este punto de vista, estos códigos pueden ser vistos como códigos cíclicos extendidos (a códigos de grupo) y de este modo, los conjuntos de información del código cíclico es claramente un conjunto de información del código de Reed-Muller; aún más, existe una relación directa entre los conjuntos de definición de ambos códigos. Por otro lado, en [1] introdujimos un método para construir conjuntos de información en códigos abelianos en términos del conjunto de definición. Así, en este trabajo obtenemos conjuntos de información para códigos de Reed-Muller de primer y segundo órdenes vistos como códigos abelianos multivariables.

Referencias

[1] J. J. Bernal, J. J. Simón: Information sets from defining sets in abelian codes. IEEE Trans. Inform. Theory, vol. 57, no. 12, 7990-7999 (2011)

Trabajo en colaboración con J. J. Bernal.
Financiado por MINECO, MTM2016-77445-P, and Fundación Séneca of Murcia, 19880/GERM/15.

On the Inheritance of the Isometry-Dual Property under Puncturing AG Codes

María Bras-Amorós

Departament d'Enginyeria Infomàtica i Matemàtiques, Universitat Rovira i Virgili

maria.bras@urv.cat

Abstract. Consider a sequence of AG codes evaluating at a set of evaluation points $P_1, \ldots, P_n$ the functions having only poles at a defining point QQ, with the sequence of codes satisfying the isometry-dual condition (ie containing at the same time primal and their dual codes). We prove a necessary condition under which, after taking out a number of evaluation points (ie puncturing), the resulting AG codes can still satisfy the isometry-dual property. The condition has to do with the so-called maximum sparse ideals of the Weierstrass semigroup of Q.

Sobre códigos grupo no abelianos

Consuelo Martínez

Universidad de Oviedo

cmartinez@uniovi.es

Resumen.
Sea F un cuerpo y G un grupo. Un código grupo sobre G se puede identificar con un ideal del álgebra de grupo FG. Estos códigos grupo se pueden considerar como la generalización natural de los códigos cíclicos y se pueden construir para cualquier grupo (finito) G, no necesariamente abeliano.
En [1] probamos que efectivamente se pueden construir códigos grupo usando grupos no abelianos con parámetros que no pueden ser conseguidos usando grupos abelianos. En [2] nos planteamos determinar la dimensión mínima que puede tener un código grupo no abeliano. Conocemos ejemplos en dimensión 4 y también se sabía que no existen tales códigos en dimensión 1. Por tanto el problema se centraba en las dimensiones 2 y 3. En [2], usando técnicas algebraicas de teoría de grupos y anillos hemos probado que todo código grupo de dimensión ≤ 3 es necesariamente abeliano, es decir, es permutacionalmente equivalente a un código grupo obtenido a través de un grupo abelliano. Se da así una respuesta completa al problema inicialmente planteado.

Referencias

[1] C. García-Pillado, S. González, V. Markov and C. Martínez. Group codes over non-abelian groups. *J. Algebra Appl.*, 12 (2013), 1350037-1–1350037-20.

[2] C. García Pillado, S. González, V. Markov, O. Markova and C. Martínez. Group codes over non-abelian groups. *J. Finite Fields and their Applications*,55 (2019), 167-176.

Trabajo en colaboración con C. García Pillado, Santos González, Victor Markov y Olga Markova. Financiado por MTM 2013-45588-C3-1-P, MTM 2017-83506-C2-2-P y GRUPIN 14-142 (Principado de Asturias).