

Ignacio Fernández Rúa

Departamento de Matemáticas
Facultad de Ciencias, Universidad de Oviedo
C/ Calvo Sotelo s/n
33007 Oviedo
Spain

email: rua@uniovi.es
web: <http://www.uniovi.es/rua>
tfno: +34-985-103344

Current Research Interests

Non-associative finite rings. Applications to Coding Theory and Cryptography.

Computer Algebra. Quantum Computing. Applications to curves and surfaces.

Education

Ph.D. in Mathematics	February 2004
Facultad de Ciencias, Universidad de Oviedo (Spain)	
Dissertation: Anillos no asociativos en Codificación y Criptología.	
Advisor: Dr. Consuelo Martínez López	
Graduate in Mathematics	July 1999
Universidad de Oviedo (Spain)	

Languages

Spanish (native speaker).

English (advanced).

French, Russian (basic).

Professional Experience

Full Professor (Catedrático de Universidad)	August 2022-present
Facultad de Ciencias, Universidad de Oviedo, Oviedo (Spain)	
Associate Professor (Profesor Titular de Universidad)	August 2011-April 2022
Facultad de Ciencias, Universidad de Oviedo, Oviedo (Spain)	
Teaching Assistant (Profesor Ayudante Doctor)	February 2007-July 2011
Facultad de Ciencias, Universidad de Oviedo, Oviedo (Spain)	
Research fellow on a <i>Juan de la Cierva</i> contract	December 2004-February 2007
Facultad de Ciencias, Universidad de Cantabria, Santander (Spain)	
Research fellow	June-September 2004
Facultad de Ciencias, Universidad de Oviedo, Oviedo (Spain)	
Teaching Assistant (Profesor Ayudante)	October-December 2003
E.U. de Informática, Universidad de Oviedo, Gijón (Spain)	
Research fellow	June 2000 - June 2004
Facultad de Ciencias, Universidad de Oviedo, Oviedo (Spain)	

Publications

- An approach to the Classification of Finite Semifields by Quantum Computing; J.M. Hernández Cáceres, I.F. Rúa; Springer series PROMS (Proceedings in Mathematics and Statistics), (to appear).
- Quantum Measurement Detection Algorithms; G. Lugilde Fernández, E.F. Combarro, I.F. Ra; Quantum Information Processing 21,274 (2022).
- Combinatorial and rotational quantum abstract detecting systems; J.M. Hernández Cáceres, E.F. Combarro, I.F. Ra; Quantum Information Processing 21,66 (2022).
- Cardinal Rank Metric Codes over Galois Rings; M. Epelde, I.F. Ra; Finite Fields and their Applications 77, 101946 (2022).
- Quantum Approximate Optimization of the Coset Leader Problem for Binary Linear Codes, M. Epelde, E. Fernández-Combarro, I.F. Rúa, Computational and Mathematical Methods 3(6) (2021).
- On a Poset of Quantum Exact Promise Problems, E. Fernández-Combarro, S. Vallecorsa, A. Di Meglio, A. Piñera-Nicolás, I.F. Rúa, Quantum Information Processing 20, 214 (2021).
- A study of the performance of classical minimizers in the Quantum Approximate Optimization Algorithm, M. Fernández-Pendás, E. Fernández-Combarro, S. Vallecorsa, J. Ranilla, I.F. Rúa, Journal of Computational and Applied Mathematics 404, 113388 (2022).
- On protocols for increasing the uniformity of random bits generated with noisy quantum computers, E. Fernández-Combarro, F. Carminati, S. Vallecorsa, J. Ranilla, I.F. Rúa, Journal of Supercomputing 77, 8063-8081 (2021)
- An explanation of the Bernstein-Vazirani and Deustch-Josza algorithms with the quantum stabilizer formalism, E. Fernández-Combarro, A. Piñera-Nicolás, J. Ranilla and I.F. Rúa, Computational and Mathematical Methods 3 (6), 1-12 (2021)
- Quantum Abstract Detecting Systems, E. Fernández-Combarro, J. Ranilla and I.F. Rúa, Quantum Information Processing 19-258, 1-25 (2020).
- On quaternary Goppa codes, M. Epelde, X. Larrucea and I.F. Rúa, Discrete Mathematics 343(9), (2020).
- Nonbinary Delsarte-Goethals codes and finite semifields, I.F. Rúa, Glasgow Mathematical Journal 62, 186-205 (2020).
- On finite division rings with a designed automorphism group, E. Fernández-Combarro, A. Piñera-Nicolás, J. Ranilla and I.F. Rúa, Mathematical Methods in the Applied Sciences 43(7), 3982-3994 (2020).
- A quantum algorithm for the commutativity of finite dimensional algebras, E. Fernández-Combarro, J. Ranilla and I.F. Rúa, IEEE Access 7 45554-45562 (2019).
- Quantum Walks for the Determination of Commutativity of Finite Dimensional Algebras, E. Fernández-Combarro, J. Ranilla and I.F. Rúa; Journal of Computational and Applied Mathematics 354, 496-506 (2019).
- Experiments Testing the Commutativity of Finite-Dimensional Algebras with a Quantum Adiabatic Algorithm, E. Fernández-Combarro, J. Ranilla and I.F. Rúa; Proceedings of the 2018 International Conference on Computational and Mathematical Methods in Science and Engineering 1, 1-11 (2019).
- Codes over affine algebras with a finite commutative chain coefficient ring, E. Martínez-Moro, A. Piñera-Nicolás and I.F. Rúa; Finite Fields and their Applications 49, 94-107 (2018).
- Cryptographic uncertainty: some experiments on finite semifield based substitution boxes, I.F. Rúa and E. Fernández-Combarro, en The Mathematics of the Uncertain, Studies in Systems, Decision and Control; Studies in Systems, Decision and Control 142, 2198-4182, 978-3-319-73848-2, Springer.

Multivariable codes in principal ideal polynomial quotient rings with applications to additive modular bivariate codes over \mathbb{F}_4 , E. Martínez-Moro, A. Piñera-Nicolás and I.F. Rúa; Journal of Pure and Applied Algebra 222, 359-367 (2017).

On power sums of matrices over a finite commutative ring, P. Fortuny, J.M. Grau, A.M. Oller-Marcén and I.F. Rúa; International Journal of Algebra and Computation 27 (5), 547-560 (2017).

Primitive semifields of order 2^{4e} , I.F. Rúa; Designs, Codes and Cryptography 83 (2), 345-356 (2017).

On the primitivity of four-dimensional finite semifields, I.F. Rúa; Finite Fields and their Applications 33, 212-229 (2015).

On additive modular bivariate codes over F_4 , E. Martínez-Moro, A. Piñera-Nicolás and I.F. Rúa; Finite Fields and their Applications 28, 199-213 (2014).

Computing the Topology of a Real Algebraic Plane Curve whose Equation is not Directly Available, Robert M. Corless, Gema M Díaz-Toca, Mario Fioravanti, Laureano González-Vega, Ignacio F. Rúa and Azar Shakoori Computer Aided Geometric Design 30 (7), 675-706 (2013).

Additive semisimple multivariable codes over \mathbb{F}_4 , E. Martínez-Moro, A. Piñera-Nicolás and I.F. Rúa; Designs, Codes and Cryptography 69, 161-180 (2013).

On Trace Codes and Galois Invariance over Finite Commutative Chain Rings, E. Martínez-Moro, A. Piñera-Nicolás and I.F. Rúa Finite Fields and their Applications 22, 114-121 (2013).

Determination of division algebras with 243 elements, I.F. Rúa, E. Fernández-Combarro and J. Ranilla; Finite Fields and their Applications 18, 1148-1155 (2012).

Finite Semifields with 7^4 elements, E. Fernández-Combarro, I.F. Rúa and J. Ranilla; International Journal of Computer Mathematics 89 (13-14), 1865-1878 (2012).

Commutative semifields of order 3^5 , I.F. Rúa and E. Fernández-Combarro; Communications in Algebra 40 (3), 988-996 (2012).

New advances in the computational exploration of semifields, E. Fernández-Combarro, I.F. Rúa and J. Ranilla; International Journal of Computer Mathematics 88 (9), 1990-2000 (2011).

On Commutative Semifields of Dimension 4, E. Fernández-Combarro, I.F. Rúa and J. Ranilla; Proceedings of the 2010 International Conference on Computational and Mathematical Methods in Science and Engineering, ISBN 978-84-613-5510-5, 393-396 (2010).

Witt index for Galois Ring valued quadratic forms, M.C. López-Díaz and I.F. Rúa; Finite Fields and their Applications 16, 175-186 (2010).

Analyzing Group Based Matrix Multiplication Algorithms, J. González-Sánchez, Laureano González-Vega, Alejandro Piñera-Nicolás, Irene Polo-Blanco, Jorge Caravantes and I.F. Rúa; Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation (ISSAC 2009), ACM, 159-165 (2009).

Computational Methods for Finite Semifields, I.F. Rúa, E. Fernández-Combarro and J. Ranilla; Proceedings of the 2009 International Conference on Computational and Mathematical Methods in Science and Engineering, ISBN 978-84-612-9727-6, 937-944 (2009).

Solving the implicitation, inversion and reparametrization problems for rational curves through subresultants, L. González-Vega and I.F. Rúa; Computer Aided Geometric Design 26, 941-961 (2009)

Classification of 64-element finite semifields, I.F. Rúa, E. Fernández-Combarro and J. Ranilla; Journal of Algebra 322 (11), 4011-4029 (2009).

Witt's theorems for Galois Ring valued quadratic forms, M.C. López-Díaz and I.F. Rúa; Journal of Pure and Applied Algebra 212, 2493-2502 (2008).

On repeated-root multivariable codes over a finite chain ring, E. Martínez-Moro and I.F. Rúa; *Designs, Codes and Cryptography* 45 (2), 219-227 (2007).

Computing the Topology of a Real Algebraic Plane Curve whose Equation is not Directly Available, D.A. Aruliah, Robert M. Corless, Azar Shakoori, Laureano Gonzalez-Vega and Ignacio F. Rúa; *Proceedings of the 2007 International Workshop on Symbolic-Numeric Computation (SNC 2007)*, ACM, 46-54 (2007).

Primitivity of Finite Semifields with 64 and 81 elements, I.R. Hentzel and I.F. Rúa; *International Journal of Algebra and Computation* 17 (7), 1411-1429 (2007).

An invariant for quadratic forms valued in Galois Rings of characteristic 4, M.C. López-Díaz and I.F. Rúa; *Finite Fields and their Applications* 13 (4), 946-961 (2007).

Symplectic Spread based Generalized Kerdock codes, S. González, C. Martínez and I.F. Rúa; *Designs, Codes and Cryptography* 42 (2), 213-226 (2007).

Multivariable codes over finite chain rings: serial codes, E. Martínez-Moro and I.F. Rúa; *SIAM Journal on Discrete Mathematics* 20 (4), 947-959 (2006).

Cyclicity of Generalized Galois Rings, S. González, V.T. Markov, C. Martínez, A.A. Nechaev and I.F. Rúa; *Communications in Algebra* 33 (12), 1 - 12 (2005).

On cyclic top-associative Generalized Galois Rings, S. González, V.T. Markov, C. Martínez, A.A. Nechaev and I.F. Rúa; *Proceedings on the 7th Symposium on Finite Fields and Applications (FQ7)*, Lecture Notes in Computer Science (2948), 25-37 (2004).

Coordinate Sets of Generalized Galois Rings, S. González, V.T. Markov, C. Martínez, A.A. Nechaev and I.F. Rúa; *Journal of Algebra and Its Applications* 3 (1), 31-48 (2004).

Primitive and non primitive finite semifields, I.F. Rúa; *Communications in Algebra* 32 (2), 793-803 (2004).

Nonassociative Galois Rings, S. González, V.T. Markov, C. Martínez, A.A. Nechaev and I.F. Rúa; *Discrete Mathematics and its Applications* 12-6, 591-606 (2002).

Introducción a los anillos finitos y sus aplicaciones, Ediciones IVIC (Instituto Venezolano de Investigaciones Científicas), G - 20004206-0, ISBN: 978-980-261-151-5.

Anillos no asociativos en Codificación y Criptografía, Tesis Doctoral editada en CD, Servicio de Publicaciones de la Universidad de Oviedo, AS - 1079/2004, ISBN: 84-8317-417-O.

Research submitted and in preparation

Functional quantum abstract detecting systems; G. Lugilde Fernández, E.F. Combarro, I.F. Ra (2022).

A Note on a Standard Model for Galois Rings, E. Martínez-Moro, A. Piñera-Nicolás, I.F. Rúa (2021)

Quantum Algorithms to compute the neighbour list of N-body Simulations, E. Fernández-Combarro, I.F. Rúa, F. Orts, G. Ortega, A.M. Puertas, E.M. Garzón (2020).

New semifield planes of order 81, I.F. Rúa and E. Fernández-Combarro (unpublished, 2008).