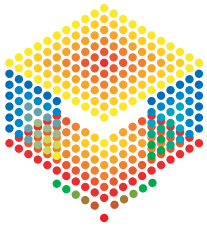
Sixth EACA International School on Computer Algebra and its Applications

July 18–21, 2023

CITMAga, Santiago de Compostela, Spain



CENTRO DE INVESTIGACIÓN Y TECNOLOGÍA MATEMÁTICA DE GALICIA

https://www.usc.es/regaca/eacaschool23/index.html

The school will take place at the Faculty of Mathematics of the University of Santiago de Compostela with the support of:

- Galician Centre for Mathematical Research and Technology - CITMAga
  https://citmaga.gal/es/
- Ministerio de Ciencia e Innovación (AEI) https://www.aei.gob.es/
  "Redes de Investigación" RED2022-134220-T
- Red **EACA**: Red Temática de Cálculo Simbólico, Álgebra Computacional y Aplicaciones
  http://www.unirioja.es/dptos/dmc/RedEACA/
- Facultade de Matemáticas (USC)
  https://www.usc.gal/es/centro/facultad-matematicas
- Consellería de Cultura, Educación, Formación Profesional y Universidades
  https://culturaeducacion.xunta.gal/portada
- Research Group in Mathematics (GiMAT) https://www.usc.es/regaca/gimat/
- Universidade de Santiago de Compostela https://www.usc.gal/es

Sixth EACA International School on Computer Algebra and its Applications

July 18–21, 2023

CITMAga, Santiago de Compostela, Spain

Scientific Committee

- **María Emilia Alonso** (Universidad Complutense de Madrid)
- **Marta Casanellas** (Universitat Politècnica de Catalunya)
- **Francisco Jesús Castro-Jiménez** (Universidad de Sevilla)
- **Carlos D'Andrea** (Universitat de Barcelona)
- **Ignacio García Marco** (Universidad de La Laguna)
- **Philippe Gimenez** (Universidad de Valladolid)
- **José Gómez Torrecillas** (Universidad de Granada)
- **Laureano González Vega** (Universidad CUNEF)
- **Manuel Ladra** (Universidade de Santiago de Compostela)
- **Jorge Martín Morales** (Universidad de Zaragoza)
- **Francisco José Monserrat Delpalillo** (Universidad Politécnica de Valencia)
- **Luis Miguel Pardo Vasallo** (Universidad de Cantabria)
- **Sonia Pérez Díaz** (Universidad de Alcalá de Henares)
- **Ana Romero** (Universidad de La Rioja); Chair

Organizing Committee

- **Manuel Ladra** (Universidade de Santiago de Compostela)
- **Alejandro Fernández Fariña** (Universidade de Santiago de Compostela)
- **Xabier García Martínez** (Universidade de Vigo)
- **Pilar Páez Guillán** (Universidade de Santiago de Compostela)
- **Álex Pazos Moure** (Universidade de Santiago de Compostela)
- **Andrés Pérez Rodríguez** (Universidade de Santiago de Compostela)

Sixth EACA International School

Programme

	TUESDAY 18 JULY	WEDNESDAY 19 JULY	THURSDAY 20 JULY	FRIDAY 21 JULY
09:30–11:00	Rocío González-Díaz	Rocío González-Díaz	Rocío González-Díaz	Rocío González-Díaz
	COFFEE BREAK			
11:30–13:00	Gabriela Jeronimo	Gabriela Jeronimo	Gabriela Jeronimo	María Inés de Frutos-Fernández
	FREE TIME FOR LUNCH			
15:00–16:30	María Inés de Frutos-Fernández	María Inés de Frutos-Fernández	María Inés de Frutos-Fernández	Javier Villar Ortega Javier Perera Lago Brais Ramos Pérez
16:30–17:00	Daniel Miguel Treviño	Rustam Turdibaev	Andrés Pérez Rodríguez	Closing
	COFFEE BREAK			
17:30–18:00	Bernardo Leite da Cunha	Gabriela Jeronimo (until 19:00)	Javier Rández Ibáñez	
18:00–18:30	José Manuel Muñoz		Álex Pazos Moure	

Speakers

María Inés de Frutos-Fernández

Universidad Autónoma de Madrid

Formalizing Mathematics in Lean

- What is formalized mathematics?
- Logic
- Functions
- Abstract Algebra
- Number Theory
- Practice: An online version of Lean will be used
  https://lean.math.hhu.de/
  https://github.com/mariainesdff/EACA_School

https://mariainesdff.github.io/

Rocío González-Díaz

Universidad de Sevilla

Topology Tools for Explainable and Green Artificial Intelligence (topology inside REXASI-PRO)

- Context: Green and Explainable artificial intelligence (REXASI-PRO)
  https://rexasi-pro.spindoxlabs.com/
- Computational topology tools: Persistent homology, barcodes, distance bottleneck, simplicial maps, Persistence modules, morphisms between persistence modules
- Partial matchings between barcodes
- Simplicial maps neural networks
- Practice: Google Colab will be used
  https://colab.research.google.com/?hl=es

https://personal.us.es/rogodi/personal.html

Gabriela Jeronimo

Universidad de Buenos Aires–CONICET, Argentina

Sparse polynomial systems

- The BKK (Bernstein-Khovanskii-Kushnirenko) bound
- Deformation algorithms to compute isolated zeros
- Affine varieties defined by sparse polynomial systems
- Algorithmic solving of sparse systems in affine space
- Sparse effective Nullstellensatz

http://mate.dm.uba.ar/~jeronimo/

Contributed talks

Nilpotent compatible Lie algebras and their classification

Bernardo Leite da Cunha

Bernardo Leite da Cunha (bernardo.mariz@rai.usc.es)
Universidade de Santiago de Compostela
Universidade do Porto

Abstract.

In this talk we will briefly recall the notion of Lie algebra, before moving on to the concept of a compatible Lie algebra, which is a generalisation consisting of an algebra with two Lie products satisfying a certain compatibility condition. We introduce the notion of nilpotency for these structures, and we discuss a method to classify the finite-dimensional ones, for low dimensions. We will comment on the feasibility of an attempt at implementing this program using computational tools such as GAP.

References

[1] I. Z. Golubchik, V. V. Sokolov. Compatible Lie brackets and integrable equations of the principal chiral field model type. *Funct. Anal. Appl.* **36**(3) (2002), 172–181.

[2] J. Liu, Y. Sheng, Ch. Bai. Maurer-Cartan characterization and cohomologies of compatible Lie algebras. *Sci. China Math.* **66**(6) (2023), 1177–1198.

[3] T. Skjelbred, T. Sund. Sur la classification des algebres de Lie nilpotentes. *C. R. Acad. Sci. Paris Ser.* A-B, 286 (1978), A241–A242.

On a simplicial construction for the Eilenberg–Moore generalized spectral sequence

D. Miguel, A. Guidolin, A. Romero, J. Rubio

Daniel Miguel (damigutr@unirioja.es)
University of La Rioja

Abstract

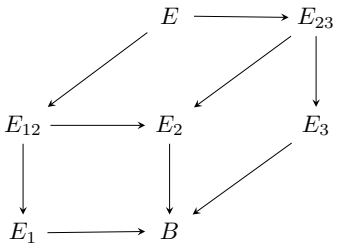
Generalized spectral sequences, also named spectral systems, were introduced by Matschke in his work [1]. The author gave there several examples concerning classic spectral sequences and, in particular, presented a generalization of the Eilenberg–Moore geometric cohomology spectral sequence [2] for cubes of fibrations. From a computational perspective, the Eilenberg–Moore homology spectral sequence is implemented in the computer algebra system Kenzo [3], and it is possible to make computations on spaces of infinite type thanks to the effective homology technique [4]. This technique is based on reductions of chain complexes $C_* \Rightarrow D_*$, which are essentially chain homotopy equivalences.

The current implementation of the Eilenberg–More spectral system in Kenzo follows the original approach [5], in which the Cobar construction plays a primary role. Therefore, in order to find within this framework a construction analogous to Matschke's, we have studied the possibility of a generalized Cobar construction. In this work, we will present some preliminary results, in the form of a new generalized filtered chain complex. Moreover, we will exhibit different issues regarding its effective homology and the convergence of its associated spectral system.

For the main problem, we are given n fibrations $f_i : E_i \to B$, $1 \leq i \leq n$. The goal is to compute the homology of the space E, defined as the pullback of all of them. To do so, we consider intermediate spaces E_I for each subset $I \subseteq \{1, ..., n\}$. E_I is defined as the pullback of the maps $\{f_i | i \in I\}$. Assuming $\pi_1(B) = 0$, it is possible to define a spectral system indexed by 4-tuples of downsets of $\mathbb{Z}^n$, which are defined as downward closed subsets of that space. This spectral system converges to the cohomology of E, $H^*(E)$, and its second page terms are given by

$$S^{pz^*}_{b^*q}((p_1, ..., p_n); n) = \mathrm{Tor}^{p_n}_{HB}(...(Tor^{p_2}_{HB}(Tor^{p_1}_{HB}(HB, HE_1), HE_2), ..., HE_n)).$$

For example, for the case $n = 3$, we have the following diagram.



For our computational purposes, we will assume that all spaces are simplicial sets, and that all fibrations are principal twisted cartesian products. This means that each E_i can be seen as $F_i \times_{\tau_i} B$ for some twisting operator $\tau_i : B_* \to (F_i)_{*-1}$. In our work, we consider the following ideas:

- The geometric spectral system is defined by means of smash products on the category $\mathbf{(Top/B)}_*$ of pointed spaces over B. The algebraic analogue of the smash product is cotensor product. We study the different factors that make hard to give a canonical definition for multiple factors.
- We can define a generalized filtered chain complex

  $$\mathrm{Cobar}^{C_*(B)}(...\mathrm{Cobar}^{C_*(B)}(\mathrm{Cobar}^{C_*(B)}(C_*(E_1), C_*(E_2)), C_*(E_3))..., C_*(E_n)).$$

  It generalizes Eilenberg and Moore's cobar chain complex, and it has effective homology. However, it is defined using trivial coproducts, so we cannot deduce anything about its homology.
- We explore several alternatives in order to modify its differential.
  - There is a coproduct for Adam's cobar construction defined by Baues ([6]). We generalize it to our framework and are able to use it to modify the previous chain complex.
  - In the case of twisted cartesian products, it is possible to use the simplicial homotopy fiber of the total spaces E_i to obtain another simplicial set equivalent to the pullback E. This construction involves the simplicial loop group GB, so it can be related to the Cobar.
  - Since we have reductions $\mathrm{Cobar}^{C_*(B)}(E_i, E_j) \twoheadrightarrow E_{ij}$, it is possible to define coproducts up to homotopy. We explore its definition and study its behaviour.

References

[1] B. Matschke. Successive spectral sequences. *Transactions of the American Mathematical Society*, 375:6205–6254, 2022.

[2] L. Smith. On the construction of the Eilenberg–Moore spectral sequence. *Bulletin of the American Mathematical Society*, 75:873–878, 1969.

[3] X. Dousson, J. Rubio, F. Sergeraert and Y. Siret. The Kenzo Program. `http://www-fourier.ujf-grenoble.fr/~sergerar/Kenzo`, 1999.

[4] J. Rubio and F. Sergeraert. Constructive algebraic topology. *Bulletin des Sciences Mathématiques*, 126(5):389–412, 2002.

[5] S. Eilenberg and J. C. Moore. Homology and fibrations I: Coalgebras, cotensor product and its derived functors *Commentarii Mathematici Helvetici*, 40(1):199–236, 1965.

[6] H.J. Baues. The double bar and cobar constructions. *Compositio Mathematica*, 43(3):331–341, 1981.

Rank error correction up to the Hartmann-Tzeng bound*

J. M. Muñoz

J. M. Muñoz (munoz@ugr.es)
Universidad de Granada

F. J. Lobillo (jlobillo@ugr.es)
Universidad de Granada

Abstract.

The well-known BCH bound establishes that, if $\delta - 1$ consecutive powers of a nonzero element β are roots of the generator polynomial g of a cyclic block code $\mathcal{C}$, then the minimum Hamming distance of $\mathcal{C}$ is at least δ. The set of exponents i such that $g(\beta^i) = 0$ is the β-defining set of the code $\mathcal{C}$, and the hypothesis of the BCH bound can be stated as the existence of a subset of $\delta - 1$ consecutive integers $\{b, b+1, b+2, \ldots, b+\delta-2\} = b + \{0, 1, \ldots, \delta - 2\}$ in the β-defining set. If β is in the coefficient field of g (as opposed to an extension thereof), g generates a Reed-Solomon code, which reaches the Singleton bound.

The BCH bound was generalized into the Hartmann-Tzeng bound in [4], allowing a subset of the β-defining set of the form $b + t_1\{0, 1, \ldots, \delta + 2\} + t_2\{0, 1, \ldots, r\}$, where $(n, t_1) = (n, t_2) = 1$ for n the length of the code and (a, b) being the greatest common divisor of a and b, which is shown to guarantee a minimum distance of at least $\delta + r$ for the cyclic code $\mathcal{C}$. There are known algorithms for nearest-neighbor decoding up to this bound (that is, for finding the closest codeword in the Hamming metric to one given word if the distance to the code is at most $\lfloor(\delta + r - 1)/2\rfloor$), see e.g. [1].

*Supported by grants PRE2020-09325 from MCIN/AEI / 10.13039/501100011033 and FSE "El FSE invierte en tu futuro" and PID2019-110525GB-I00 from Agencia Estatal de Investigación (AEI / 10.13039/501100011033)

Both the BCH bound and the Hartmann-Tzeng bound have been shown to work analogously for skew cyclic (block) codes. In the context of a field F, a field automorphism $\sigma\colon F \to F$ of order n, a skew polynomial ring $F[x;\sigma]$ and some $\beta \in F$, i is in the β-defining set of a generator (skew) polynomial $g \in F[x;\sigma]$ when $x-\sigma^i(\beta)$ right divides g. As shown in [2], if $b+t_1\{0,1,\ldots,\delta+2\} + t_2\{0,1,\ldots,r\}$, where $(n,t_1) = 1$ and $(n,t_2) < \delta$, is a subset of the β-defining set of g, then the Hamming distance of the skew cyclic code $\mathcal{C}$ generated by g is at least $\delta + r$. Nearest-neighbor error correction algorithms are known for these codes in the skew Reed-Solomon case, see e.g. [3], which can readily be extended to the BCH case, that is, when $r = 0$. Further work has shown that, for K the fixed field of σ, this bound also applies to the F/K-rank metric, which is defined so that the rank weight of $v \in F^n$ is the dimension of the K-vector space spanned by the entries of v.

Our current work results in a syndrome-based error-correcting decoding algorithm for codes in a family containing the skew cyclic codes, as well as the Gabidulin codes as defined in [5], up to a Hartmann-Tzeng bound for the rank metric (and therefore for the Hamming metric) derived from a defining set related to the structure of the parity-check matrix of the code, which is reduced to the stated above for skew cyclic codes. The decoding algorithm, which generalizes the one in [6] for Gabidulin codes and can be seen as a generalization of the one in [3] for skew Reed-Solomon codes, decomposes the decoding problem into efficiently solvable linear algebra ones, notably including the skew-feedback shift-register synthesis problem.

References

[1] G.-L. Feng, K. K. Tzeng. A generalization of the Berlekamp-Massey algorithm for multisequence shift-register synthesis with applications to decoding cyclic codes. *IEEE Transactions on Information Theory* **37**(5) (1991), 1274–1287.

[2] J. Gómez-Torrecillas, F. J. Lobillo, G. Navarro. A Sugiyama-Like Decoding Algorithm for Convolutional Codes. *IEEE Transactions on Information Theory* **63**(10) (2017), 6216–6226.

[3] J. Gómez-Torrecillas, F. J. Lobillo, G. Navarro, A. Neri. Hartmann-Tzeng bound and skew cyclic codes of designed Hamming distance. *Finite Fields and Their Applications* **50** (2018), 84–112.

[4] C. R. P. Hartmann, K. K. Tzeng. Generalizations of the BCH bound. *Information and Control* **20**(5) (1972), 489–498.

[5] A. Kshevetskiy, E. Gabidulin. The new construction of rank codes. *Proceedings. International Symposium on Information Theory* (2005), 2105–2108.

[6] V. Sidorenko, L. Jiang, M. Bossert. Skew-Feedback Shift-Register Synthesis and Decoding Interleaved Gabidulin Codes. *IEEE Transactions on Information Theory* **57**(2) (2011), 621–632.

PBW Pairs in Operads and Compatible Algebras

Álex Pazos Moure

Álex Pazos Moure (alex.pazos@rai.usc.es)
Universidade de Santiago de Compostela

Abstract.

Poincaré-Birkhoff-Witt's Theorem contains a fundamental relation between a Lie algebra and its associative universal enveloping algebra. There exist numerous positive and negative results studying the identical situation in other pairs of varieties of algebras. In the present talk, we will exhibit the theoretical framework with which we approach this kind of problems in modern mathematics, generalizing it to the realm of algebraic operads and applying to those an analogue of Gröbner bases. To conclude, we will present results which show the way to go in order to identify the PBW property in any pair of varieties of algebras for which it makes sense.

References

[1] M. R. Bremner, V. Dotsenko. Algebraic Operads: An Algorithmic Companion, Chapman and Hall, New York, 2016.

[2] V. Dotsenko. Freeness Theorems for Operads via Gröbner Bases. *Sémin. Congr.* 26, Societé Mathématique de France, Paris (2013), 61–76.

[3] V. Dotsenko, P. Tamaroff. Endofunctors and Poincaré–Birkhoff–Witt Theorems. *Int. Math. Res. Not. IMRN* **2021** (16) (2021), 12670–12690.

[4] A. A. Mikhalev, I. P. Shestakov. PBW-Pairs of Varieties of Linear Algebras. *Comm. Algebra* **42** (2014), 667–687.

[5] T. Van der Linden. Non-Associative Algebras. *New perspectives in algebra, topology and categories*, Coimbra Math. Texts 1, pp. 225–258, Springer, Cham, 2021.

A study on persistent homology with integer coefficients

Javier Perera-Lago

Javier Perera-Lago (jperera@us.es)
Universidad de Sevilla

Abstract.

Homology is a tool that assigns to a topological space an abelian group for each dimension. Persistent homology is a more modern technique used to analyze the evolution of homology in a topological space that is built step by step. Both homology groups and persistent homology may be different according to the set of coefficients used in the calculations. Persistent homology with coefficients over a field such as $\mathbb{R}$ or $\mathbb{Z}_2$ has been widely studied and applied thanks to it easy computation, its stability and the existence of easy and complete invariants for its classification. Unfortunately, persistent homology over coefficients in $\mathbb{Z}$ is harder to calculate and classify, and because of that it has been barely studied. In [1], we start from the approach and concepts defined in [2] and we give some new results, we generalize the definitions and we give a partial stability result.

Let us introduce the details of [1]. The first step is to consider a topological space built on m steps, that is, an increasing sequence of m spaces. For a given dimension n, each space has its own homology groups, so we can see persistent homology as a diagram

$$0 = H_0 \xrightarrow{\rho_{0,1}} H_1 \xrightarrow{\rho_{1,2}} H_2 \xrightarrow{\rho_{2,3}} \cdots \xrightarrow{\rho_{m-1,m}} H_m \tag{1}$$

where H_i is the homology group in step i and $\rho_{i,j} = \rho_{j-1,j} \circ \cdots \circ \rho_{i,i+1}$ are group homomorphisms. From this diagram, the authors of [2] define the groups $H_{i,j} = \operatorname{Im} \rho_{i,j} = \rho_{i,j}(H_i) \subset H_j$ for $i \leq j$, then they define $H_{i,k,j} = H_{i,k} \cap (\rho_{k,j})^{-1}(H_{i-1,j}) \subset H_k$ for $i \leq k \leq j$, and finally they define the BD groups as

$$BD_{i,j} = \frac{H_{i,i,j}}{H_{i,i,j-1}} = \frac{H_{i,i+1,j}}{H_{i,i+1,j-1}} = \cdots = \frac{H_{i,j-2,j}}{H_{i,j-2,j-1}} = \frac{H_{i,j-1,j}}{H_{i-1,j-1}} \tag{2}$$

According to [2], a non trivial $BD_{i,j}$ group is meant to show that there is a topological feature (a homology class) that is born in step i and dies in step j, but it does not give a formal proof for this affirmation. All these groups can be computed by a module of Kenzo program, using the spectral sequences defined in [3].

In order to connect the $BD_{i,j}$ groups with the theory developed in [5], which always talks in terms of intervals $I = [i, j)$, we proposed in [1] the alternate notation $BD_{I,k} = \frac{H_{i,k,j}}{H_{i,k,j-1}}$ and we proved that the structure of $BD_{I,k}$ is the same for every $k \in I$. After that, we introduced the V groups defined in [5] as $V_{I,k} = V^+_{I,k}/V^-_{I,k}$, where $V^+_{I,k} = \operatorname{Im} \rho_{i,k} \cap \ker \rho_{k,j}$ and $V^-_{I,k} = (\operatorname{Im} \rho_{i,k} \cap \ker \rho_{k,j-1}) + (\operatorname{Im} \rho_{i-1,k} \cap \ker \rho_{k,j})$. To provide intuition to the spaces $V_{I,k}$, notice that when working with field coefficients, it is proved in [4] that the dimension of $V_{I,k}$ shows how many homology classes are born in step i and die at step j.

In [1], we also introduced a new definition of BD groups for infinite intervals $I = [i, \infty)$, given by $BD_I = \frac{H_{i,m}}{H_{i-1,m}}$, and we proved that this formula is equivalent to $BD_{[i,m+1),k} = \frac{H_{i,k,m+1}}{H_{i,k,m}}$ if we include a last term $H_{m+1} = 0$ and a null homomorphism $\rho_{m,m+1}$ in the equation 1.

Recall that BD groups were defined in [2] for persistent homology with integer coefficients, while V groups were defined in [5] for field coefficients. In [1], we provided a proof that, when working with field coefficients, $BD_{I,k}$ and $V_{I,k}$ are isomorphic. We also proved that, independently on the choice of coefficients, $V^+_{I,k} \subset H_{i,k,j}$ and $V^-_{I,k} \subset H_{i,k,j-1}$. Finally, a proof or a counterexample for the isomorphism between $BD_{I,k}$ and $V_{I,k}$ when working with integer coefficients was left as future work.

After that, we wanted to prove some stability results for BD and V groups, so we needed to extend their definitions for a more general framework. Observe that Equation 1 can be generalized by having a homology group H_i for each $i \in \mathbb{R}$ and linear maps $\rho_{i,j} : H_i \to H_j$ for $i \leq j$, satisfying that $\rho_{i,j} = \rho_{k,j} \circ \rho_{i,k}$ when $i \leq k \leq j$. In this general framework, the author of [5] gave an extended definition for V groups. The extended definition for BD groups was stated by us in [1]. In both cases, we proved in [1] that these last definitions are indeed a good generalization to those used in the more simple framework with only m steps. After that, we proved that, in this general framework, $BD_{I,k}$ and $V_{I,k}$ are also isomorphic when working with field coefficients. We left as future work the proof in case of working with integer coefficients.

Finally, inspired in the theory developed in [6], we gave first steps to stability considering the 1_ε functor, which induces an ε perturbation into persistent homology. We proved how this perturbation affects our BD definition and V groups: by transforming $BD_{(i,j+\varepsilon),k+\varepsilon}$ into $BD_{(i,j),t}$ and $V_{(i,j+\varepsilon),k+\varepsilon}$ into $V_{(i,j),t}$. We do not explore more stability results, but we consider this a good starting point to completely prove that persistent homology is also stable when working with integer coefficients.

In summary, although persistent homology is more difficult to study and apply when using integer coefficients, we show that it is possible to make some connections with the more developed theory for field coefficients, and we think that it is possible to go beyond.

References

[1] Perera-Lago, Javier Un estudio sobre la homología persistente con coeficientes enteros, *2021*, Advisor: Prof. Rocio Gonzalez-Diaz `https://idus.us.es/handle/11441/130282`.

[2] Romero, Ana and Heras, Jónathan and Rubio, Julio and Sergeraert, Francis Defining and computing persistent Z-homology in the general case, *2014* `https://arxiv.org/abs/1403.7086`

[3] Romero, Ana and Rubio, Julio and Sergeraert, Francis Computing spectral sequences, *2006* `https://www.sciencedirect.com/science/article/pii/S0747717106000460`

[4] Carlsson, Gunnar and De Silva, Vin Zigzag persistence, *2010* `https://link.springer.com/article/10.1007/s10208-010-9066-0`

[5] Crawley-Boevey, William Decomposition of pointwise finite-dimensional persistence modules, *2015* `https://www.worldscientific.com/doi/abs/10.1142/S0219498815500668?casa_token=ztFcpRY50T4AAAAA:rd96PvT-f6KrBofvPGAfHhK-VLs7FmoJ0nzD1YRTe_JxplOr46FPcoaN8Q2UvhVIhOKDPtgNlg`

[6] Chazal, Frédéric and De Silva, Vin and Glisse, Marc and Oudot, Steve The structure and stability of persistence modules, *2016* `https://link.springer.com/content/pdf/10.1007/978-3-319-42545-0.pdf`

On the subalgebra lattice of evolution algebras

Andrés Pérez Rodríguez

Andrés Pérez Rodríguez (andresperez.rodriguez@usc.es)
Universidade de Santiago de Compostela

Abstract.

The relationship between a group and the structure of its lattice of subgroups is highly developed and has aroused enormous interest among many leading algebraists ([4]). In addition, since lattices appear frequently in mathematics, in the literature we can find how this study has been transferred to the right ideals of a ring ([1]) or to the submodules of a module ([2]), among others. Above all, the study of the subalgebra lattice in some non-associative structures stands out, such as in Lie algebras ([3]) or in Leibniz algebras ([5]). However, this relationship is not well known in genetic algebras and in evolution algebras has not been studied yet.

An evolution algebra is an algebra provided with a basis $B = \{e_i : i \in I\}$, called natural basis, such that $e_i e_j = 0$ when $i \neq j$. Indeed, evolution algebras are a new type of commutative but nonassociative algebras introduced by J. P. Tian in 2008 in [6] that arise with the purpose of modeling non-Mendelian genetics, which is the basic language of molecular biology. In addition, these non-associative algebras with dynamic nature also have numerous connections with other fields of mathematics such as graph theory, stochastic processes, group theory or dynamic systems.

The main objective of this talk is to develop the relationship between an evolution algebra and its subalgebra lattice, emphasizing two of its main properties: distributivity and modularity. At the beginning, some problems encountered throughout our investigation will be presented, such as the fact that evolution algebras are not closed under subalgebras or the difficulty to prove the existence of subalgebras in general. Subsequently, the distributivity in the nilpotent evolution algebras will be characterized and it will end by commenting on some results for modularity in the solvable case.

References

[1] H. Brungs. Rings with a distributive lattice of right ideals. *Journal of Algebra* **40** (1976), 392–400.

[2] V. Camillo. Distributive modules. *Journal of Algebra* **36** (1975), 16–25.

[3] B. Kolman. Semi-modular Lie algebras, *J. Sci. Hiroshima Univ. Ser. A-I Math.* **29** (1965), 149–163.

[4] R. Schmidt. Subgroup Lattices of Groups. De Gruyter Exp. Math., 14 Walter de Gruyter & Co., Berlin, 1994.

[5] S. Siciliano, D. A. Towers. On the subalgebra lattice of a Leibniz algebra. *Comm. Algebra* **50** (2021), 255–267.

[6] J. P. Tian. Evolution Algebras and their Applications. Lecture Notes in Math., 1921, Springer, Berlin, 2008.

A categorical isomorphism for Hopf braces

Brais Ramos Pérez

Brais Ramos Pérez (braisramos.perez@usc.es)
Universidade de Santiago de Compostela

Abstract.

Hopf braces are recent algebraic objects introduced by I. Angiono, C. Galindo and L. Vendramin in [1] throughout 2017. This particular kind of objects consist on a pair of Hopf algebras over the same object and with the same underlying coalgebra structure that satisfy a complex relation between the products. What makes these objects particularly interesting is not only their algebraic properties, but also that they induce solutions of the Quantum Yang-Baxter equation.

The aim of this talk will be introduce the concept of Brace triple. These obejcts give rise to a new category that is isomorphic to the category of Hopf braces under cocommutativity assumptions.

References

[1] I. Angiono, C. Galindo, L. Vendramin. Hopf braces and Yang-Baxter operators. *Proceedings of the American Mathematical Society* **145**(5) (2017), 1981–1995.

[2] R. González Rodríguez. The fundamental theorem of Hopf modules for Hopf braces. *Linear and Multilinear Algebra* **70**(20) (2022), 5146–5156.

[3] J. A. Guccione, J. J. Guccione, L. Vendramin. Yang-Baxter operators in symmetric categories. *Comm. Algebra* **46**(7) (2018), 2811–2845.

[4] Y. Li, Y. Sheng, R. Tang. Post-Hopf algebras, relative Rota-Baxter operators and solutions of the Yang-Baxter equation. (2022). arXiv:2203.12174.

Skew-derivations on Oscillator real Lie algebras

Javier Rández

Javier Rández (javier.randez@unirioja.es)
Universidad de La Rioja

Pilar Benito (pilar.benito@unirioja.es)
Universidad de La Rioja

Abstract.
In 1985, Hilgert and Hofmann [1] introduced oscillator algebras as split extensions of Heisenberg algebras (see [2] for a formal definition). These algebras are solvable, non-nilpotent, and quadratic, and can be constructed as a double extension of Hilbert spaces. Furthermore, they can be doubly extended into mixed quadratic algebras. To achieve the last assertion, it is necessary to understand the algebra of derivations of the oscillator variety. In particular, the subalgebra of skew-derivations. The general structure of these derivation algebras is described in [3, Proposition 4.3], albeit without proof. In the talk, we will provide a proof with an explicit matrix description of these derivations. This result extends the one given in [4, Theorem 2].

References

[1] J. Hilgert, K. H. Hofmann. Lorentzian cones in real Lie algebras. *Monatshefte für Mathematik*, **100**(3) (1985), 183–210.

[2] K. H. Neeb. Invariant subsemigroups of Lie groups. *American Mathematical Soc.*, 1993.

[3] A. Medina, P. Revoy. Algèbres de Lie et produit scalaire invariant. *Annales scientifiques de l'École normale supérieure* **18**(3) (1985), 553–561.

[4] P. Benito, J. Roldán-López. Metrics related to Oscillator algebras. arXiv:2212.12600, 2022.

The ring of invariant polynomials on two matrices of degree 4

Rustam Turdibaev

Rustam Turdibaev (rustam.turdibaev@usc.es)
Universidade de Santiago de Compostela

Abstract.

The invariant theory of $n \times n$ matrices studies the algebra of invariant of the general linear group GL_n acting on the direct product of square matrices of size n by simultaneous conjugation. The problem consists of two parts: determining a minimum set of generators of the algebra of such polynomials and finding the polynomial relations between them. It is well-known that this algebra is generated by the traces of monomials in generic matrices and all relations are deduced from the Cayley-Hamilton theorem. However, a minimal generating set of this algebra and exact relations among them remain largely open problems. In this talk we present a solution for the case $n = 4$.

References

[1] V. Drensky, R. La Scala. Defining relations of low degree of invariants of two 4×4 matrices. *Internat. J. Algebra Comput.* **19**(1) (2009), 107–127.

[2] Z. Normatov, R. Turdibaev. Calogero-Moser spaces and the invariants of two matrices of degree 3. To appear in *Transform. Groups*, 2022.

[3] C. Procesi. The invariant theory of $n \times n$ matrices. *Advances in Math.* **19** (3) (1976), 306–381.

[4] Ju. P. Razmyslov. Identities with trace in full matrix algebras over a field of characteristic zero. *Izv. Akad. Nauk SSSR Ser. Mat.* **38** (1974), 723–756.

The Univalent Program and its semantics

Javier Villar Ortega

Javier Villar Ortega (javillo@unirioja.es)
Universidad de La Rioja

Abstract.

The Univalent Program, the research program that constitutes the main body of work on the field of Homotopy Type Theory, refers to a series of conjectures, proposals and tools regarding the properties of certain Martin-Löf type theories.

These provide a bridge between fields like Categorical Logic, Homotopy Theory, and Theoretical Computing; with the aim of providing a new proposal for the foundation of Mathematics, with an underlying constructivist-oriented type theory that takes into consideration its computational content, in a way useful for the design of proof assistants.

In this talk, we give an overview of the theory, with some historical hints on its development, the general current state of affairs on several of its main questions, and a brief explanation of its connections with the theory of locally Cartesian-closed categories (LCC).

References

[1] The Univalent Foundations Program. Homotopy Type Theory: Univalent Foundations of Mathematics. (2013) arXiv:1308.0729. [1308.0729].

[2] E. Riehl. On the ∞-topos semantics of Homotopy Type Theory. (2022). arXiv:2212.06937. [2212.06937].

[3] S. Awodey, N. Gambino, K. Sojakova. Homotopy-initial algebras in type theory. *Journal of the ACM* **63**(6) (2017), Article 51, pp. 1–45.

[4] D. Annenkov, P. Capriotti, N. Kraus, C. Sattler. Homotopy-initial algebras in type theory. *Mathematical Structures in Computer Science*, Special Issue: Homotopy Type Theory, 2023, pp. 1–56.

[5] P. L. Lumsdaine, M. Shulman. Semantics of higher inductive types. *Mathematical Proceedings of the Cambridge Philosophical Society* **169** (2020), 159–208.

[6] C. Cohen, T. Coquand, S. Huber, A. Mörtberg. Cubical Type Theory: a constructive interpretation of the univalence axiom. (2016). arXiv:1611.02108. [1611.02108].

Posters

Splitting edge ideals as an example of the connection between Commutative Algebra and Combinatorics

Sara Asensio Ferrero

Sara Asensio Ferrero (saraasensioferrero@gmail.com)
Universidad de Valladolid

The study of the minimal graded free resolutions of monomial ideals is classical in Commutative Algebra and allows working with combinatorial tools. In fact, thanks to polarization, we can restrict ourselves to the study of square-free monomial ideals. Square-free quadratic monomial ideals, also called edge ideals, were first introduced by Rafael H. Villarreal in 1990 ([5]).

The main goal of my poster will consist of studying these ideals identifying them with simple graphs and using a tool called "splitting" which was first introduced by Shalom Eliahou and Michel Kervaire in 1990 ([1]) to turn the problem of computing the dimensions of different homology groups into an easier problem in terms of the associated graphs. We will give different examples and show how this new combinatorial method allows us to recover some classical results using more elementary tools. To do this, we will follow a paper that Huy Tài Hà and Adam Van Tuyl published in 2007 ([3]).

Moreover, these authors show in [4] how these results can be generalized to arbitrary square-free monomial ideals. In order to do this, they introduced the notion of "hypergraph", which generalizes in a natural way the graphs that we are used to working with. We will also try to present this work in an understandable way, by giving different examples.

Finally, we will introduce in an elementary way the `EdgeIdeals` package of Macaulay2 ([2]) that allows working with edge ideals associated to graphs and hypergraphs.

References

[1] S. Eliahou and M. Kervaire. Minimal resolutions of some monomial ideals. *Journal of Algebra*, 129:1–25, 1990.

[2] C. A. Francisco, A. Hoefel and A. Van Tuyl. EdgeIdeals: A package for (hyper)graphs. *The Journal of Software for Algebra and Geometry*, 1:1–4, 2009.

[3] H. T. Hà and A. Van Tuyl. Splittable ideals and the resolutions of monomial ideals. *Journal of Algebra*, 309:405–425, 2007.

[4] H. T. Hà and A. Van Tuyl. Monomial ideals, edge ideals of hypergraphs, and their graded Betti numbers. *Journal of Algebraic Combinatorics*, 27:215–245, 2008.

[5] R. H. Villarreal. Cohen-Macaulay graphs. *Manuscripta Mathematica*, 66(3):277–293, 1990.

Algebraic fault injection attack on the Snow family of stream ciphers

Itciar Fernández Elízaga

Itciar Fernández Elízaga (alu0101323848@ull.edu.es)
Universidad de La Laguna

Abstract. Nowadays, cryptography is key to ensuring the security of information transmission between computer devices, especially on mobile phones. Currently, the most widely used communication system is known as 5G technology, which emerges to improve the security issues of its predecessor, 4G, whose cryptographic system is based on the Snow 3G generator. Snow 3G is based on Snow 2.0 but has been designed to be more resistant to algebraic attacks.

This work will study the components of stream ciphers, specifically symmetric key ciphers (same key for encryption and decryption) where plaintext digits (unencrypted text) are combined with a stream of pseudorandom digits (keystream) to obtain the encrypted text. In particular, we will study linear feedback shift registers (LFSR), examining their properties, representations, and uses. The Fibonacci representation can be seen in the Figure 1. The fact that they can be defined through linear recurrence relations over a finite field and through polynomials with coefficients in a finite field implies the acquisition of very interesting properties. The representation using dual bases and matrices is also demonstrated.

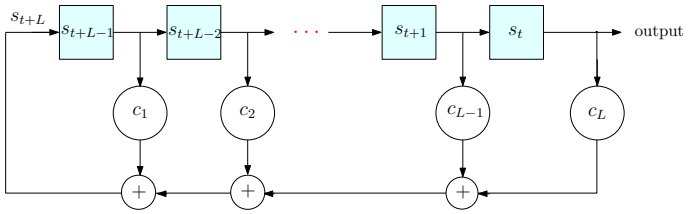


Figure 1: Fibonacci representation of an LFSR.

Furthermore, the structure of Snow 3G will be analyzed, which consists of two main parts: a Linear Feedback Shift Register (LFSR) and a Finite State Machine (FSM) (see Figure 2).

In addition, the study will focus on representing the modular addition operation as a system of algebraic equations of at most degree two, which will be crucial when conducting the attack. Initially, the method of Armknecht and Meier will be studied, which demonstrates a fault induction attack for the generic case of a combined generator with memory. This will help understand the attack on Snow 3G. As an example, the attack that can be performed on Snow 2.0, the predecessor of Snow 3G, using this technique will be explained.

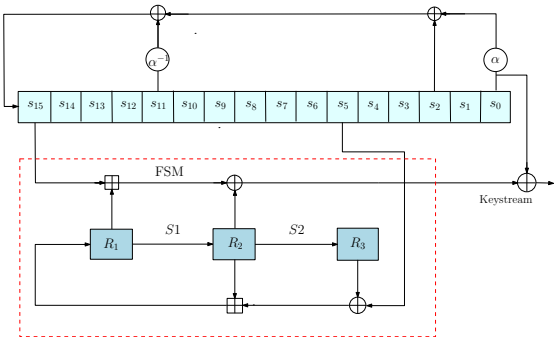


Figure 2: Representation of Snow 3G.

Later, the attack on Snow 3G is presented, with the objective of recovering a complete state of the LFSR. This attack is based on inducing a fault in certain locations of the LFSR (s_2, s_3, s_4) since it is proven that this is where the most equations can be obtained. Furthermore, by inducing a fault in one of these locations, the difference between the fault-free value and the fault in that location $(s_i \oplus s_i')$ can be recovered. This allows us to determine the difference in all stages $(s_0, s_1, \ldots, s_{15})$ due to the linearity of the recurrence relation. Then, taking into account how modular addition is written and using the XOR operation and the equations governing Snow 3G, we can represent the equation $s_{15}^t \boxplus R_1^t = \underbrace{R_2^t \oplus s_0^t \oplus z^t}_{w^t}$ as a system of 32 equations and 32×3 variables, which are the unknown bits of s_{15}^t, R_1^t, and w^t. By knowing the output differences and the stage differences, and considering that the fault did not reach the FSM (which constitutes the nonlinear part of the algorithm), we can obtain new systems of equations in the same variables but with different coefficients.

With all the studied techniques using Gröbner bases with lexicographic monomial ordering, linear systems of equations are obtained that depend only on the bits of s_{15}^t. However, it is studied that inducing a fault in the same location and at the same moment does not provide the minimum number of linear equations needed to recover a complete state of the LFSR (512, one for each bit). Therefore, the attacker will have to induce faults at different moments and locations in order to obtain the necessary equations for successful recovery.

References

[1] Canteaut, A. Linear Feedback Shift Register. *Encyclopedia of Cryptography and Security*, 2011.

[2] Debraize, B., & Corbella, I. M. Fault Analysis of the Stream Cipher Snow 3G. *Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC).*, pp. 103-110, 2009.

Distributed matrix multiplication via algebraic-geometric codes

Adrián Fidalgo-Díaz

Adrián Fidalgo Díaz (adrian.fidalgo22@uva.es)
University of Valladolid

Abstract. Matrix multiplication is a crucial part of machine learning and signal processing algorithms. Motivated by this, different approaches have been proposed for using parallel computing to perform this operation faster [1]. They are based on splitting the original multiplication into smaller ones that can be executed simultaneously by a distributed system of computing nodes. Afterwards, a master node gathers and merges the results to return the output of the original multiplication.

When implementing this in real life, the worker nodes can suffer from straggling or become non-responsive. To mitigate this, a variety of algorithms using techniques from error-correcting codes have been created [2]. We consider using algebraic-geometric codes to perform distributed matrix multiplication with straggling resistance, generalizing the previous approaches. We use one-point codes and study the Weierstrass semigroup associated with the curve to obtain codes with good parameters.

References

[1] V. Cadambe and P. Grover Codes for Distributed Computing: A Tutorial *IEEE Information Theory Society Newsletter*, 67(4):3–15, 2017.

[2] S. Dutta, M. Fahim, F. Haddadpour, H. Jeong, V. Cadambe and P. Grover On the Optimal Recovery Threshold of Coded Matrix Multiplication *IEEE Trans. Info. Theory*, 66(1):278–301, 2019.

Algebraic Machine Leaning and some applications

Daniel Jaén

María del Socorro García Román (mgarciro@ull.edu.es)
University of La Laguna

Daniel Jaén Guedes (alu0101360676@ull.edu.es)
Graduate from University of La Laguna

Abstract.

Machine Learning (ML) is an important branch of Artificial Intelligence, developed in recent times, that allows us to learn characteristics and predict the value of variables for which we only have examples. However, several of the classical ML methods are usually based on function minimization to fit a large number of parameters in a randomly created model. This method presents several problems, such as the difficulty in finding minima of complicated functions with many variables, or the appearance of the so-called "overfitting", i.e. the model fits too closely to the training data and does not generalize well.

In this work we present the alternative proposed in [1] for this type of algorithms, based on algebraic structures, mainly graphs and semilattices, to find a predictive model. This new approach, called Algebraic Machine Learning (AML), is completely parameter-free, and furthermore, when applied in experiments, no evidence of overfitting has been found.

Although it can be applied to a lot of different problems, the main focus of this work is its use as a classification algorithm, that is, oriented to obtain a model that allows us to predict whether an element possesses a certain property, starting from a set of elements of which we know a priori if they fulfill this property.

The authors of [1] state that the AML algorithm is applicable to a wide variety of examples of both supervised and unsupervised learning (the learning process is basically the same, only the encoding of the problem changes), including the "vertical bar problem", the "handwritten digits problem", the "queens completion problem", "finding Hamiltoninan paths", etc.

Using our own programming in Python, we solve a classic ML problem, such as the recognition of handwritten digits problem using the AML algorithm, in order to be able to compare it with its resolution by means of already known ML/Deep Learning algorithms, so we can obtain comparative empirical results on the efficiency of both. Furthermore, in studying this recent line of research, we have found that some slight optimizations of the AML algorithm can be applied.

References

[1] F. Martin-Maroto, G. García de Polavieja. Algebraic Machine Learning. DOL: arXiv:1803.05252v2, 2018.

[2] D. Jaén Guedes. Introducción al Algebraic Machine Learning [unpublished undergraduate thesis], University of La Laguna, Bachelor's Degree in Mathematics, 2023.

Verifiable Computation on encrypted data

Miguel Morona Mínguez

Miguel Morona Mínguez (miguel.morona@imdea.org, mimorona@ucm.es)
IMDEA Software Institute & Complutense University of Madrid.

Abstract.

The rise of new tools such as Cloud Computing can become a double-edged sword if we take into account the many dangers that can arise. Verifiable Computation (VC) is a state-of-the-art cryptographic technique that aims to overcome the risks of remote computing and to guarantee properties such as correctness or privacy.

In this master thesis, a Verifiable Computation scheme combining homomorphic encryption and homomorphic authentication techniques is proposed. After a security analysis, a variation of these techniques is proposed that allows for greater efficiency, in terms of communication cost between the parties. This work also includes a precise estimation of this cost, along with an estimation of the computational time in executing the required algorithms.

Keywords: Homomorphic encryption, Verifiable Computation, MAC, Semantic security, Unforgeability.

1 Motivation

In recent years, there has been a significant increase in the adoption of cloud computing and outsourcing of computational tasks to remote servers. This trend has provided numerous benefits, such as cost-effectiveness and scalability. However, it has also raised concerns regarding the security and privacy of sensitive data. Users often hesitate to outsource their computations due to the fear of exposing their confidential information to untrusted third parties.

Verifiable computation on encrypted data has emerged as a promising solution to address these security concerns. The idea behind this approach is to enable clients to delegate computationally intensive tasks to remote servers while ensuring the correctness and integrity of the results. By leveraging encryption techniques, the client can encrypt their data before outsourcing it, thus preserving the confidentiality of the information.

The need for verifiable computation arises from the inherent lack of trust in the remote servers. Clients must be able to verify that the server performs the computations correctly and that the results obtained are valid. This verification becomes even more critical when dealing with sensitive data, such as personal or financial information, where the consequences of malicious or erroneous computations can be severe.

2 Our contribution

Verifiable Computation it is a well known topic [GGP10, Gol+13] that enables a computationally weak client to "outsource" the computation of a function F on various inputs $x_1, \ldots, x_k$ to one or more workers. To our knowledge, these were the first relevant works that consider privacy in the context of $\mathcal{VC}$. Both of these solutions are, however not very satisfactory in terms of efficiency. Another approach was the one done in [FGP14] where they proposed to use homomorphic MACs in order to prove that the evaluation of FHE ciphertexts has been done correctly. Their solution is inherently bound to computations of quadratic functions. One more recent work in this area is [FNP20] where the authors proposed a new protocol for verifiable computation on encrypted data that supports homomorphic computations of multiplicative depth larger than 1.

This work is along the same lines as the ones mentioned above. We propose a generic $\mathcal{VC}$ scheme where we suppose an homomorphic encryption to preserve data privacy and an homomorphic MAC to authenticate the ciphertexts. As an homomorphic encryption consider the BV encryption and the CF13 as the homomorphic MAC. This authenticator procedure is very efficient but the only problem it has for our scheme is the input space that restricts us to authenticate messages $m \in \mathbb{Z}_p$. Since the BV encryption outputs ciphertexts that belong to rings, we will modify (not in essence, but structurally) this homomorphic MAC procedure in order to be able to authenticate ring values (we will call it $\widetilde{\text{CF13}}$).

It is well known that for many homomorphic encryption schemes, the size of the ciphertext is directly related to the degree of the homomorphic function f. So, due to efficiency and despite [FNP20], this work is meant to only contemplate low-degree functions.

References

[FGP14] D. Fiore, R. Gennaro, V. Pastro. Efficiently verifiable computation on encrypted data. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* 2014, pp. 844–855.

[FNP20] D. Fiore, A. Nitulescu, D. Pointcheval. Boosting verifiable computation on encrypted data. In: *Public-Key Cryptography–PKC 2020*: 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4-7, 2020, Proceedings, Part II 23. Springer. 2020, pp. 124–154.

[GGP10] R. Gennaro, C. Gentry, B. Parno. Non-interactive verifiable computing: Outsourcing computation to untrusted workers. In: *Advances in Cryptology–CRYPTO 2010*: 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings 30. Springer. 2010, pp. 465–482.

[Gol+13] S. Goldwasser et al. How to run turing machines on encrypted data. In: *Advances in Cryptology–CRYPTO 2013*: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II. Springer. 2013, pp. 536–553.

Which family of codes is suitable for code-based cryptography?

Oswaldo José Pérez Luis

Oswaldo José Pérez Luis (operezlu@ull.edu.es)
University of La Laguna

Abstract.

In 2017, the NIST initiated a post-quantum cryptography competition aimed at identifying robust public key alternatives capable of withstanding attacks from quantum computers. A total of 69 proposals were submitted and by 2022 four finalists had emerged, albeit none of the finalists belonged to the field of Code-based Cryptography. It is important to note that the absence of code-based solutions among the finalists does not imply their insecurity. Currently, a new competition is underway to select digital signature schemes based on public key cryptography that exhibit resistance against quantum computer attacks reflecting the ongoing search for secure proposals that meet the desired criteria, as NIST remains cautious in the selection process.

In the field of code-based cryptography, numerous encoding and decoding schemes exist that meet the necessary criteria. However, determining the optimal code selection in terms of maximizing the number of correctable errors for a given information rate and length remains unclear. There has been a significant amount of study on quantum computers—machines that use quantum mechanical processes to solve mathematical problems that are difficult for traditional computers—in recent years. If large-scale quantum computers are ever created, they will be capable of breaking many of the current public-key cryptosystems, jeopardizing the privacy and security of digital communications. The goal of post-quantum cryptography—also known as quantum-resistant cryptography—is to create cryptographic systems that are secure against both quantum and classical computers while also being able to communicate with existing communication protocols and networks.

We explain the differences between Coding Theory and Cryptography, and how they can be merged in Code-based Cryptography (CBC), one of the pro-

posals to resist attacks from a quantum computer—post-quantum cryptography. In addition, we explain which families of codes are suitable for CBC according to their security, that is, based on the fact that the chosen family is indistinguishable from a random code. Then, we introduce and we study the fundamental properties of some families of polynomial codes. In particular, Reed-Solomon codes and their generalizations, as well as Reed-Muller codes. We study subfield-subcodes of the previously named families, such as the Goppa codes, which can be studied as a subfield-subcode of a generalized Reed-Solomon code.

Code-based cryptography is one of the few mathematical techniques that enables the construction of public-key cryptosystems that are secure against a quantum computer adversary. In 1978, early in the history of public-key cryptography, McEliece proposed to use a generator matrix as a public key, and encrypted a codeword by adding a specified number of errors to it. The scheme's security relies on two computational assumptions: generic decoding is hard on average, and the public key—the generator matrix of a Goppa code—is hard to distinguish from a matrix of a random code.

A significant aspect of this study involves examining codes denoted as $(n, k)_{\mathcal{A}}$, where the message consists of k symbols and the coded word has a fixed length of n symbols from the alphabet $\mathcal{A}$. Furthermore, linear codes are specifically introduced for the scenario where the alphabet is a finite field. These codes possess additional structure, making them more tangible and comprehensible compared to arbitrary codes.

Evaluation codes are a family of codes defined from the evaluation of polynomials, such as Reed-Solomon codes and Reed-Muller codes. Following the breakthrough of Reed- Solomon (RS) codes, a new avenue of research emerged, focusing on the development of efficient decoding algorithms, exploring the relationship between Reed-Solomon codes and cyclic codes, demonstrating that specific decoding algorithms designed for cyclic codes and Bose-Chaudhuri-Hocquenghem (BCH) codes, which form a class of cycling error-correcting codes, can be effectively employed for this particular code family.

The Generalized Reed-Solomon (GRS) codes were proposed for code-based cryptography by Niederreiter in 1986 but its strong linear structure allowed Sidelnikov and Shestakov to describe an attack in 1992. Some years later, in 2005, Berger and Loidreau proposed a subcode of a generalized Reed-Solomon code, but this one was attacked by Wieschebrink in 2010.

The Reed-Muller (RM) codes, which date back to the early days of coding theory, represent, in a wide sense, a generalization of Reed-Solomon codes in multiple variables. Initially introduced by E. Muller in 1954, these codes garnered significant attention. It was S. Reed who later proposed the first

efficient decoding algorithm for Reed-Muller codes, further contributing to their prominence in the field. Later on, the binary Reed- Muller codes were proposed by Sidelnikov in 1994 although this family also turned out to not be secure since Minder and Shokrollahi provided an attack in 2007.

A technique arises from representing the finite field $\mathbb{F}_{q^m}$ as a vector space over its subfield $\mathbb{F}_q$. By employing this approach, it becomes possible to construct a code with the same length n as the original code but with an increased minimum distance. Initially utilizing linear codes in $\mathbb{F}_{q^m}$, the technique ultimately transforms them into linear codes in $\mathbb{F}_q$. The alternating codes, which are constructed as a family of GRS codes based on the constraints imposed by the subfield $\mathbb{F}_q$. In particular, every linear code with a minimum distance of $d \geq 2$ is, in fact, an alternating code.

Finally, we can introduce Goppa codes, a family of codes formally defined as linear codes in $\mathbb{F}_q$ and represent a distinct subset of alternating codes. Specifically, binary Goppa codes, initially introduced by McEliece in 1978 for the purpose of cipher block chaining (CBC), have demonstrated enduring security and continue to be utilized in cryptographic applications.

List of participants

Alonso Tarrío, Leovigildo	Universidade de Santiago de Compostela
Álvarez Díaz, Beatriz	Universidade de Santiago de Compostela
Alvite Pazo, Raúl	Universidade de Santiago de Compostela
Alvite Pazo, Samuel	Universidade de Santiago de Compostela
Asensio Ferrero, Sara	Universidad de Valladolid
D'Andrea, Carlos	Universitat de Barcelona
de Frutos-Fernández, María Inés	Universidad Autónoma de Madrid
de los Ríos de Antonio, Miguel	Universidad de Valladolid
Diz Pita, Érika	Universidade de Santiago de Compostela
Fernández Elízaga, Itciar	Universidade de La Laguna
Fernández Fariña, Alejandro	Universidade de Santiago de Compostela
Fernández Vilaboa, José Manuel	Universidade de Santiago de Compostela
Fidalgo Díaz, Adrián	Universidad de Valladolid
Gago, Felipe	Universidade de Santiago de Compostela
García Cortés, Francisco	Universidad de Sevilla
García Martínez, Xabier	Universidade de Vigo
González-Díaz, Rocío	Universidad de Sevilla
Gutiérrez Rodríguez, Ixchel D.	Universidade de Vigo
Jaén, Daniel	Universidad de La Laguna
Jeremías López, Ana	Universidade de Santiago de Compostela
Jeronimo, Gabriela	Universidad de Buenos Aires-CONICET
Khmaladze, Emzar	University of Georgia
Ladra, Manuel	Universidade de Santiago de Compostela
Leite da Cunha, Bernardo	Universidade de Santiago de Compostela
Mesablishvili, Tamar	Universidad de Granada
Miguel Treviño, Daniel	Universidad de La Rioja
Morona Mínguez, Miguel	IMDEA Software Institute & Universidad Complutense de Madrid
Muñoz, José Manuel	Universidad de Granada
Páez Guillán, Pilar	Universität Wien
Pazos Moure, Álex	Universidade de Santiago de Compostela
Perera Lago, Javier	Universidad de Sevilla
Pérez Luis, Oswaldo José	Universidad de La Laguna
Pérez Rodríguez, Andrés	Universidade de Santiago de Compostela
Ramos Pérez, Brais	Universidade de Santiago de Compostela

Rández Ibáñez, Javier	Universidad de la Rioja
Turdibaev, Rustam	Universidade de Santiago de Compostela
Villar Ortega, Javier	Universidad de la Rioja

Sponsors

- Galician Centre for Mathematical Research and Technology - CITMAga
  https://citmaga.gal/es/

- Ministerio de Ciencia e Innovación (AEI) https://www.aei.gob.es/
  "Redes de Investigación" RED2022-134220-T

- Red **EACA**: Red Temática de Cálculo Simbólico, Álgebra Computacional y Aplicaciones
  http://www.unirioja.es/dptos/dmc/RedEACA/

- Facultade de Matemáticas (USC)
  https://www.usc.gal/es/centro/facultad-matematicas

- Consellería de Cultura, Educación, Formación Profesional y Universidades
  https://culturaeducacion.xunta.gal/portada

Rede: ED341D R2016/022

- Research Group in Mathematics (GiMAT) `https://www.usc.es/regaca/gimat/`

- Universidade de Santiago de Compostela `https://www.usc.gal/es`