Session : Algebra and Computer Security

Decoding LDPC Codes by Information Geometry and Alternating Projections

A. ADDADI[1], B.BAKKAS[2] H.BEN-AZZA[3], I.CHANA[4]

[1] azddine.addadi@yahoo.com, ENSAM, Moulay Ismail University, Meknes
[2] brahim.bakkas@gmail.com, ENSAM, Moulay Ismail University, Meknes
[3] hbenazza@yahoo.com, ENSAM, Moulay Ismail University, Meknes
[4]idrisschana@gmail.com, EST, Moulay Ismail University, Meknes

Abstract

We present an algorithm for decoding LDPC codes based on information geometry as introduced by Ikeda et al. For the purpose of the implementation of this algorithm, we explicitly compute the m-projection to an e-flat submanifold, in the case of a binary symmetric channel and the Gaussian channel. The same paradigm is applicable to Turbo decoding, which is a manifestation of the belief propagationn algorithm. We also give a theorem based on alternating projections in the realm of information geometry, which is compared to alternating projections in the realm of convex programming.

Références

[1] Amari, H. Nagaoka, *Methods of Information Geometry. AMS and Oxford University press*, 2000.

[2] Shiro Ikeda, Toshiyuki Tanaka, and Shun-ichi Amari, *Information geometry of turbo and low-density parity-check codes*. IEEE transaction on Information Theory, vol.50, No.6, pp.1097-1114, June 2004.

Half-integral weight modular forms and real quadratic p-rational fields

J. Assim[1],and Z. Bouazzaoui[2]

[1]Mathematics department, Moulay Ismail University, Meknes
[2]Mathematics department, Moulay Ismail University, Meknes

Résumé/Abstract

Using half-integral weight modular forms we give a criterion for the existence of real quadratic p-rational fields [2, 3]. Modular forms are particular holomorphic functions whose Fourier coefficients are most of time interesting arithmetic functions. Here we use Cohen-Eisenstein series which gives special values of L-functions of quadratic fields as Fourier coefficients [1]. We give our results after studying the p-adic valuation of these coefficients. For $p = 5$ we prove the existence of infinitely many real quadratic p-rational fields.

Références

[1] H. Cohen, *Sums involving the values at negative integers of L-functions of quadratic characters*, Math. Ann. 217 (1975), 271-285.

[2] R. Greenberg, *Galois representations with open image*, Annales mathématiques du Québec, 40 (2016), 83-119.

[3] A. Movahhedi, *Sur les p-extensions des corps p-rationnels*, Thèse Paris VII (1988).

[4] J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, L'Ensein. Math. 22 (1976), 227- 260.

Les Codes Quantiques (Survol)

M.E. Charkani[1] and B. Boudine[2]

[1] [2]Laboratoire LAGA, Université Sidi Mohamed Ben Abdellah, FEZ

Résumé
En 23 Octobre 2019, Google a annoncé avoir atteint la suprématie Quantique grâce au premier ordinateur Quantique Sycamore ayant 53 qubits. Cette réalisation est une fruit de plusieurs travaux pour transformer le langage informatique classique basé sur les bits au langage quantique basé sur les "Qubits". Ces efforts n'étaient jamais juste un jeu de loisir, mais plutôt une forte conviction que la machine classique atteint ses limites et que celles quantiques seront l'alternative pour répondre aux besoins de l'intelligence artificielle et aux ambitions des scientifiques en général.
En 1995, Calderbank et Shor [6], et puis Steane [9] en 1996 ont démontré la possibilité théorique de construire des bons codes quantiques. Mais la quantité des travaux sur ce sujet restait limitée car la machine quantique n'était qu'un rêve dont on était trop loin à réaliser.
Depuis 2014, les recherches en codes quantiques ont commencé à s'accélérer grâce surtout aux travaux de Ashraf et Mohammad [1] [2] [3], Gao et Wang [8], puis c'est Bag [4] [5] et Dinh [7] qui ont exploité le développement déjà réalisé en codage classique afin de le transformer en codage quantique en utilisant les techniques décrites par Calderbank [6]. Ce genre des Codes Quantiques est tout simplement les codes auto-duaux parmi les codes qui existent déjà.

Références

[1] M. Ashraf and G. Mohammad, *Quantum Codes From Cyclic Codes Over* $\mathbb{F}_3 + v\mathbb{F}_3$, Int. J. Quantum Inf. , 12-6(2014).

[2] M. Ashraf and G. Mohammad, *Construction of Quantum Codes From Cyclic Codes Over* $\mathbb{F}_p + v\mathbb{F}_p$, Int. J. Inf. Coding Theory 2 (2015) : 137–144.

[3] M. Ashraf and G. Mohammad, *Quantum Codes From Cyclic Codes Over* $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, Quantum Inf. process, 15-10(2016) : 4089–4098.

[4] T. Bag and A.K. Upadhyay, *Styde on Negacyclic Codes Over the ring* $\mathbb{Z}_p[u]/(u^{k+1} - u)$, J. Appl. Math. Comput., 59-1-2(2018) : 693–700.

[5] T. Bag, A.K. Upadhyay, M. Ashraf and G. Mohammad, *Quantum Codes From Cyclic Codes Over* $\mathbb{F}_p[u]/(u^3 - u)$, Asian-Europ. J. Math., 13-1(2020).

[6] A.R. Calderbank and P.W. Shor, *Good Quantum Error-Correcting Codes exist*, Physical Review A , 54-2(1996) : 1098–1105.

[7] H.Q. Dinh, T. Bag, A.K. Upadhyay, M. Ashraf, G. Mohammad and W. Chinnakum, *New Quantum Codes From a class of Constacyclic Codes Over Finite Commutative Rings*, J. of Algebra and its Applications, (2019).

[8] J. Gao and Y. Wang, *u-Constacyclic Codes Over* $\mathbb{F}_p + u\mathbb{F}_p$ *and their applications of constructing new non-binary Quantum Codes*, Quantum Inf. process, 17-6(2018) : 1–19.

[9] A.M. Steane, *Simple Quantum Error-Correcting Codes*, Physical Review A , 54-6(1996) : 4741–4751.

The phase topology and bifurcation tori of the Generalized Yang-Mills potantial

W. Chatar[1], J. Kharbach[1], M. Benkhali[1], I. El Fakkousy[1], A. Rezzouk[1] and M. Ouazzani Jamil[2]

[1]Laboratoire de Physique du Solide : Dynamique des Systèmes, Faculté des Sciences Dhar el Mahraz , Université Sidi Mohammed ben Abdellah, Fès
[2]Laboratoire Systèmes et Environnements Durables, Université Privée de Fès, Fès

Abstract

In this paper, we study the Generalized Yang-Mills potential $V = \frac{1}{2}(ax^2 + by^2) + \frac{1}{4}(cx^4 + dy^4) + \frac{1}{2}ex^2y^2$. The structuring and evolution of the real phase space are explored. The bifurcation diagram is found and the bifurcations of solutions are discussed. The periodic solutions and their associated periods for singular common-level sets of the first integrals of motion are explicitly described. Numerical investigations are performed for the integrable case by means of Poincaré surfaces of section and comparing them with nearby living nonintegrable solutions, all generic bifurcations that change the structure of the phase space are illustrated, the problem can exhibit regularity-chaos transition over a range of control parameters of system.

Références

[1] S. Kasperczuk, *Integrability of the Yang-Mills hamiltonian system*, Celestial Mechanics and Dynamical Astronomy , Vol 58, no 4 (1994) : 387–391.

[2] L. Jiménez-Lara and J. Llibre, *Periodic orbits and nonintegrability of generalized classical Yang-Mills Hamiltonian systems*, Journal of Mathematical Physics , Vol 52, no 3 (2011) : 032901.

[3] W. Chatar, M. Benkhali, I. El Fakkousy, J. Kharbach, A. Rezzouk and M. Ouazzani-Jamil, *The phase topology and bifurcation tori of the Hydrogen atom subjected to external fields*, Journal of Physics : Conference Series , Vol 1292, no 1 (2019) : 012007.

[4] W. Chatar, M. Benkhali, I. El Fakkousy, J. Kharbach, A. Rezzouk and M. Ouazzani-Jamil, *Classical mechanics of the Hydrogen atom perturbed by Van der Waals potential interacting with combined electric and magnetic fields*, Journal of Physics : Conference Series , Vol 1292, no, 1 (2019) : 012008.

ECC Fully homomorphic encryption scheme

A. CHILLALI

Sidi Mohamed Ben Abdellah University
FP, LSI, Taza, Morocco
abdelhakim.chillali@usmba.ac.ma

Abstract :

In this paper we introduce a fully homomorphic encryption scheme on a ring R, in particular we are interested in cryptography based on conjugal classical problem in this ring.
We study the problem of conjugal over this non commutative ring.
The problem as stated is generally impossible to solve. Next, we describe a new encryption scheme over this ring based on this problem.
This method of encryption is based on two difficult problems; Discrete logarithm problem and conjugal classical problem.

References :

[1] Diffie, W., Hellman, M.: New directions in cryptography. IEEE Transactions on Information Theory (1976).
[2] Boulbot, A., Chillali, A., Mouhib, A.: Cryptographic Protocols on the non-commutative Ring R. International Journal of Mathematical and Computational Methods. 2 p. 138-141 (2017).
[3] Sahmoudi, M., Chillali, A.: Key exchange over particular algebraic closure ring. TATRA MOUNTAINS Mathematical Publications. 70 (2017).
[4] Boulbot, A., Chillali, A., Mouhib, A.: Elliptic curves over the ring R. Gulf J. Math. pp.123-129 (2016).
[5] Tadmori, A., Chillali, A., Ziane, M.: Elliptic Curve over Ring A. Applied Mathematical Sciences (2015).
[6] Chillali, A.: Cryptography over elliptic curve of the ring. World Academy of Science, Engineering and Technology. 78 pp. 848-850 (2011).

Solving the closest vector problem with the reduced centered law method

M. EL HASSANI, A. CHILLALI, Ali MOUHIB

Sidi Mohamed Ben Abdellah University
FP, LSI, Taza, Morocco
abouaminem@gmail.com

Abstract :

In this work we expose a new method for the resolution of the closest vector problem in a Lattice. Given a vector U in $\mathbb{R}^n$, find a vector W of the Lattice ; $\mathcal{L}$ which minimizes the distance between U and $\mathcal{L}$. This problem is NP hard.
Our contribution uses data analysis, making the vector W that we have to look for at a reduced centered vector V, the latter written in linear combination, whose integer coefficients are to be sought to give a rounded vector equal to the vector $(1,1,\ldots,1)$.

References :

[1] M. Ajtai,"GereratingHardinstancesoflatticeproblems,"Inproceedings of the 28th ACM symposium on theory of computing, New York, USA, (1996).
[2] O. Goldreich, S. Goldwasser, and S. Halevi, "Public-key cryptosystems from lattice reduction problems," In B.Kaliski editor, Advences in cryptology-CRYPTO'97, volume 1294 of lecture notes in computer science, pages 112-131 Springer Berlin/ Heidelberg, (1997).
[3] D. Micciancio, "Lattice -based cryptography," University of California, San diego, (2003).
[4] D. Miccinco, O.Regev, "Lattice- based cryptography," In Proceedings of cryptography 2009, page 577-594, Springer, (2008).
[5] T. Plantard, M. Rose and S. Willy, "Impprovement of Lattice - based cryptography using CRT," School of comuter and software Engineering. University of Wollongong NSW Australia, (2009).

Pólya fields of some real biquadratic number fields K

P. Nom[1], Said EL MADRARI[2] and Mohammed TAOUS[1,2]

[1]Faculty of Sciences and Technology, Moulay Ismail University of Meknes, Errachidia, Morocco
[2]Faculty of Sciences and Technology, Moulay Ismail University of Meknes, Errachidia, Morocco

Résumé/Abstract

Let K be a number field and $\mathcal{O}_K$ its ring of integers, denote by $\prod_q(K)$ the product of all the prime ideals of $\mathcal{O}_K$,with norm $q \geq 2$. K is a Pólya field if $\prod_q(K)$ are principal ideals of $\mathcal{O}_K$. In this work, we will determine the first cohomology group of units of $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, $(d_1, d_2) = 1$ where $N\epsilon_1 = N\epsilon_2 = -N\epsilon_3 = -1$, $N\epsilon_i$ the norm of fundamental unit of $k_i = \mathbb{Q}(\sqrt{d_i})$, and we will conclude all Pólya fields of K.

Références

[1] A. Azizi, Unités de certains corps de nombres imaginiares et abéliens sur $\mathbb{Q}$, Ann.Sci. Math.Québec 23 (1999), 87-93

[2] A. Ostrowski, *Über ganzwertige Polynome in algebraischen Zahlkörpren*, J. reine angew. Math. **149** (1919), 117-124.

[3] B. Heidaryan and A. Rajaei, biquadratic Pólya fields with only one quadratic Pólya subfield, J. Number Theory. 143(2014), 279-285.

[4] Blair K. Spearman and Kenneth S. Williams, Unramified Quadratic Extensions of a Quadratic Field,J of Mathematics Volume 26, Number 2, Spring 1996

[5] H. Zantema, Integer valued polynomials over a number field, Manuscr. Math.40 (1982), 155-203.

[6] G. Pólya, *Über ganzwertige Polynome in algebraischen Zahlkörpern*, J. Reine Angew. Math. **149** (1919), 97-116.

[7] M. Taous and A. Zekhnini, Pólya groups of the imaginary bicyclic biquadratic number fields, J. Number Theory. 177(2017), 307-327.

Properties of twisted on the Ring $\mathbb{F}_q[e], e^2 = e$

Moha ben taleb Elhamam[1], Abdelhakim Chillali[2] and Lhoussain El Fadil[1]

[1] Sidi Mohamed Ben Abdellah University, FSDM,LSMA, Fez, Morocco
[2] Sidi Mohamed Ben Abdellah University, FP, LSI, Taza, Morocco

Abstract

Let $\mathbb{F}_q[e]$ be a finite field of q elements, where q is a power of a prime number p. In this paper, we study the Twisted Hessian curves denoted $H_{a,d}(\mathbb{F}_q[e])$ over the ring $\mathbb{F}_q[e]$, where $e^2 = e$ and $(a, d) \in (\mathbb{F}_q[e])^2$. Using the Twisted Hessian equation, we define the Twisted Hessian curves $H_{a,d}(\mathbb{F}_q[e])$ and we will show that $H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q)$ and $H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ are two Twisted Hessian curves over the field $\mathbb{F}_q$, where π_0 and π_1 are respectively the canonical projection and the sum projection of coordinates of $X \in \mathbb{F}_q[e]$. Precisely, we give a bijection between the sets $H_{a,d}(\mathbb{F}_q[e])$ and $H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$.

Keywords
Twisted Hessian curves, Elliptic Curves, Finite Ring, Finite field, Local ring, Cryptography.

References

[1] A. Boulbot, A. Chillali, A. Mouhib, *Elliptic Curves Over the Ring R*, Bol. Soc. Paran. Mat, v. 38 3 (2020): 193-201.

[2] Daniel J. Bernstein, Chitchanok Chuengsatiansup, David Kohel, and Tanja Lange, *Twisted Hessian Curves*, In LATINCRYPT 2015, pages 269-294, 2015. http://cr.yp.to/papers.html#hessian.

[3] M. Joye and J. Quisquater, *Hessian elliptic curves and sidechannel attacks*, Cryptographic Hardware and Embedded Systems - CHES 2001, Lecture Notes in Computer Science Vol. 2162, Springer, pp. 402-410, 2001.

A note on isodual constacyclic codes of length p^s over the chain ring $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$

Jamal LAAOUINE

Department of Mathematics
Faculty of Sciences Dhar El Mahraz
P.O. Box 1796 Atlas Fez, Morocco
laaouine.jamal@gmail.com

Abstract

Let $\mathcal{R} = \mathbb{F}_{p^m}[u]/\langle u^3\rangle$ be the finite commutative chain ring with unity, where p is a prime, m is a positive integer and $\mathbb{F}_{p^m}$ is a finite field with p^m elements. In this paper, we determine all constacyclic codes of length p^s over $\mathcal{R}$, their sizes and their dual codes. As an application, we list some isodual constacyclic codes over $\mathcal{R}$.

Références

[1] M. F. Atiyah et I. G. MacDonald, Introduction to Commutative Algebra, Addison Wesley Publishing Company, (1969).

[2] H.Q. Dinh, Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, J. Algebra 324 (2010) 940-950.

[3] H. Q. Dinh, A. Sharma, S. Rani, and S. Sriboonchitta, Cyclic and negacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, J. Algebra Appl. 17 (2018) 185073.

[4] H.Q. Dinh and S.R. López-Permouth, Cyclic and Negacyclic Codes over Finite Chain Rings, IEEE Trans. Inform. Theory 50 (2004) 1728-1744.

[5] S.T. Dougherty, Y.H. Park, On modular cyclic codes, Finite Fields Appl. 13 (2007) 31 ?57.

[6] W.C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.

[7] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, 10th Impression, North-Holland, Amsterdam, 1998.

[8] A. Sharma and T. Sidana, Repeated-root constacyclic codes over the chain ring $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$, arXiv :1706.08869v2 [maths.NT].

[9] R. Sobhani, Z. Sun, L. Wang, S. Zhu, A not on complete classification of $(\delta+\alpha u^2)$-constacyclic codes of length p^k over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$, arXiv :1702.04694 [cs.IT].