Timetable

S7: "Computer Algebra in Coding Theory and Cryptography"

Applications of Computer Algebra – ACA 2021

Virtual. Online | July 23-27, 2021

All times are Central European Summer Time

Friday, July 23, 2021

15:00	**Welcome remarks session 7**		
15:00–15:30	S7	**Carlos Agrinsoni** University of Puerto Rico	Resolution of the Conjecture on Exceptional APN Function When the First and the Second Terms Have Odd Degrees
15:30–16:00	S7	**Eddie A. Arrieta** University of Puerto Rico	Two and Three Weight Codes via Our GU Codes
16:00–16:30	S7	**Ramakrishna Bandi** Institute of Technology Naya Raipur	Construction of Entangled Assisted Quantum Error Correcting Codes from Monomial-Cartesian codes
16:30–17:00	S7	**Dipak K. Bhunia** Universitat Autònoma de Barcelona	Construction and Linearity of Some $\mathbb{Z}_{p^s}$-Linear Generalized Hadamard Codes

17:00–17:30	S7	**Reza Dastbasteh** Simon Fraser University	Recent conjectures on the equivalence of linear cyclic codes
17:30–18:00	S7	**Md Ajaharul Hossain** Institute of Technology Naya Raipur	Hulls of additive conju-cyclic codes over F4 with respect to a trace dual
18:00–18:30	S7	**Fernando Piñero** University of Puerto Rico	Quantum Error-Correcting Codes over small fields from AG curves
18:30	**End of the first part of the session**		

Tuesday, July 27, 2021

15:00	**Welcome to the second part of session 7**		
15:00–15:30	S7	**Stefka Bouyuklieva** St. Cyril and St. Methodius University of Veliko Tarnovo	A software program for equivalence of linear codes over finite fields
15:30–16:00	S7	**Mehmet E. Köroğlu** Yildiz Technical University	Skew constacyclic codes over a non-chain ring
16:00–16:30	S7	**Shikha Patel** Indian Institute of Technology Patna	$\mathbb{F}_q\mathcal{R}$-Skew Cyclic Codes

16:30–17:00	S7	**Roberto Reyes Carranza** University of Puerto Rico	A New Algorithm on Finite Fields for the Construction of Differentially 4-Uniform Permutations with Optimal Algebraic Degree
17:00–17:30	S7	**RJose W. Velazquez** University of Puerto Rico	Enumeration and Construction of New Boolean Bent/Near-bent Functions of the Gold and Kasami-Welch Type
17:30–18:00	S7	**Shikha Yadav** Indian Institute of Technology Patna	Some Constructions of l-Galois LCD codes
18:00	**End of the session**		

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Computer Algebra in Coding Theory and Cryptography”*

Resolution of the Conjecture on Exceptional APN Function When the First and the Second Terms Have Odd Degrees

Carlos Agrinsoni[1]***, Heeralal Janwa***[1]***, Moises Delgado***[2]
[{carlos.agrinsoni,heeralal.janwa,moises.delgado}@upr.edu]

[1] Department of Mathematics
University of Puerto Rico at Rio Piedras
17 University Ave. Ste 1701 San Juan PR, 00925-2537
[2] Mathematics Physics
University of Puerto Rico Cayey
205 Calle Antonio R. Barcelo, Cayey, 00736

An almost perfect non-linear (APN) function on $\mathbb{F}_{2^n}$ is one whose directional derivative on nonzero elements is at most two to one. The APN functions have applications in coding theory, cryptography, and sequence designs. A function that is APN over $\mathbb{F}_{2^n}$ and also on infinitely many extensions is called an exceptional APN function. Janwa and Wilson, Janwa, McGuire and Wilson, Jedlicka, and finally McGuire and Hernando in 2011 [1] proved that the exceptional APN monomials up to CCZ equivalence are the Gold $f(x) = x^{2^k+1}$ and Kasami-Welch $f(x) = x^{2^{2k}-2^k+1}$ monomials. Aubrey, McGuire, and Rodier [5] conjectured that up to CCZ equivalence, the only exceptional APN functions are the ones from these two families of monomials. They also established that the odd degrees are necessarily the Gold or Kasami-Welch exponents. For the converse, substantial progress has been made by Delgado and Janwa [3, 4], and Ferard [2] when the degree of the second term is odd. Only a few exceptions remain in the literature for these cases. Here we present proofs for the remaining cases and thus establish a resolution of this conjecture. We deduce our results as a consequence of our recent theorems and algorithms for absolute irreducibility testing of multivariate polynomials over finite fields. These absolute irreducibility results are of considerable importance in applications of computer algebra in coding theory and cryptography.

References

[1] Hernando, Fernando; McGuire, Gary, *Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions*, Journal of Algebra, 2011

[2] Férard, Eric, *A infinite class of Kasami functions that are not APN infinitely often*, Contemp. Math., Vol. 686, pag. 45–63, 2017

[3] Delgado, Moises; Janwa, Heeralal, *Some new results on the conjecture on exceptional APN functions and absolutely irreducible polynomials: the Gold case*, Advances in Mathematics of Communications, 2017

[4] Delgado, Moises; Janwa, Heeralal, *On the absolute irreducibility of hyperplane sections of generalized Fermat varieties in $\mathbb{P}^3$ and the conjecture on exceptional APN functions: the Kasami-Welch degree case*, 2016

[5] Aubry, Yves; McGuire, Gary; Rodier, François, *A few more functions that are not APN infinitely often*, Finite fields: theory and applications, Amer. Math. Soc., Providence, RI, 2010

Two and Three Weight Codes via Our GU Codes

***Eddie A. Arrieta*, Heeralal Janwa** [{eddie.arrieta,heeralal.janwa}@upr.edu]

Department of Mathematics
University of Puerto Rico at Rio Piedras
17 University Ave. Ste 1701 San Juan PR, 00925-2537

Linear codes with few weights have applications in cryptography, association schemes, designs, strongly regular graphs, finite group theory, finite geometries, among other disciplines. For two weight codes, see [4] , for three and few weights codes [5], [6], and [7]. We use our GU code construction to obtain two-weight, three-weight and few-weights linear codes. Consequently, we also give elementary constructions of two-weight codes in Calderbank and Kantor [4], of three-weight codes and few weights codes given by Ding [6], and Tonchev and Jungnickel [7]. We determine the optimal parameters of additive quaternary codes of short length.

References

[1] Arrieta, Eddie A., and Janwa, Heeralal.: A Go-Up Code Construction from Linear Codes Yielding Additive Codes for Quantum Stabilizer Codes. Proceedings of the $52nd$ Southeastern International Conference on Combinatorics, Graph Theory, and Computing, PROMS.

[2] Bonisoli, Arrigo.: Every Equidistant Linear Code is a Sequence of dual Hamming Codes. Ars Combinatoria. 18: $181 - 186$, 1983.

[3] Borges, Joaquim and Rifa, Josep and Zinoviev, Victor A.: On q-ary Linear Completely Regular Codes with $\rho = 2$ and Antipodal dual.

[4] Calderbank, Robert and Kantor, William M.: The Geometry of Two-Weight Codes. Bulletin of the London Mathematical Society. $18(2)$: $97 - 122$, 1986.

[5] Ding, Cunsheng and Luo, Jinquan and Niederreiter, Harald.: Two-weight Codes Punctured from Irreducible Cyclic Codes. Coding And Cryptology, World Scientific. pp $119 - 124$, 2008.

[6] Ding, Kelan and Ding, Cunsheng.: A Class of Two-Weight and Three-Weight Codes and Their Applications in Secret Sharing. IEEE Transactions on Information Theory. $61(11)$: $5835 - 5842$, 2015.

[7] Crnkovic, Dean and Svob, Andrea and Tonchev, Vladimir D.: Cyclotomic Trace Codes. Algorithms. $12(8)$, 2019.

[8] Assmus Jr, E.F and Mattson, Harold F.: Error-correcting codes: An axiomatic approach. Information and Control. $6(4)$: $315 - 330$, 1963.

[9] W. Wesley Peterson and E. J. Weldon, Jr.: ERROR-CORRECTING CODES. The Massachusetts Institute of Technology. 1972.

[10] Jungnickel, Dieter and Tonchev, Vladimir D.: On Bonisolis theorem and the block codes of Steiner triple systems. Designs, Codes and Cryptography. $86(3)$: $449 - 462$, 2018.

[11] Huffman, W Cary and Pless, Vera.: Fundamentals of Error-Correcting Codes. Cambridge university press. 2010.

[12] Ward, Harold N.: An Introduction to Divisible Codes. Designs, Codes and Cryptography. $17(1)$: $73 - 79$, 1999.

Construction of Entangled Assisted Quantum Error Correcting Codes from Monomial-Cartesian codes

Ramakrishna Bandi[1]***, Sanjit Bhowmick***[2]***, Satya Bagchi***[2]
[ramakrishna@iiitnr.edu.in, sanjitbhowmick392@gmail.com,
satya.bagchi@maths.nitdgp.ac.in]

[1] Department of Mathematics
International Institute of Technology Naya Raipur
Nava Raipur - 493661, India
[2] Department of Mathematics
National Institute of Technology Durgapur
Durgapur, India

A monomial-Cartesian code is evaluated through monomials on Cartesian sets. It is a generalization of toric codes, affine Cartesian codes and J-affine variety codes, etc. In this talk, we discuss monomial-Cartesian codes. First compute the minimum distance of a monomial-Cartesian code and then determine the dual of monomial-Cartesian code using the tools of linear algebra. later, using duality, we give a necessary and sufficient condition on an LCD, self-orthogonal and self-dual codes. As an application, we consider a class of Quantum codes called Entanglement Assisted Quantum Qrror Correcting Code (EAQECC)s. Here we first prove that an EAQECC is maximum distance seperable (MDS) if and only if the corresponding linear code is MDS. This leads to the construction of MDS EAQECCs to MDS codes with l dimensional Hulls. We later show that there exists an MDS code of dimension k with l dimensional Hull, $0 \leq l \leq k$. Finally, we present some MDS EAQECCs with the minimum distance better than the EAQECCs available in the literature for a given entangled state c.

Construction and Linearity of Some $\mathbb{Z}_{p^s}$-Linear Generalized Hadamard Codes[*]

Dipak K. Bhunia* , *Cristina Fernández-Córdoba, Mercè Villanueva
[{Dipak.Bhunia,Cristina.Fernandez,Merce.Villanueva}@uab.cat]

Department of Information and Communications Engineering
Universitat Autònoma de Barcelona
08193 Cerdanyola del Vallès, Spain

Let $\mathbb{Z}_{p^s}$ be the ring of integers modulo p^s with $s \geq 1$ and p prime. The set of n-tuples over $\mathbb{Z}_{p^s}$ is denoted by $\mathbb{Z}_{p^s}^n$. A code over $\mathbb{Z}_p$ of length n is a nonempty subset of $\mathbb{Z}_p^n$, and it is linear if it is a subspace of $\mathbb{Z}_p^n$. Similarly, a nonempty subset of $\mathbb{Z}_{p^s}^n$ is a $\mathbb{Z}_{p^s}$-additive if it is a subgroup of $\mathbb{Z}_{p^s}^n$. Note that, when $p = 2$ and $s = 1$, a $\mathbb{Z}_{p^s}$-additive code is a binary linear code and, when $p = 2$ and $s = 2$, it is a quaternary linear code or a linear code over $\mathbb{Z}_4$.

In [5], a Gray map from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ is defined as $\phi(0) = (0, 0)$, $\phi(1) = (0, 1)$, $\phi(2) = (1, 1)$ and $\phi(3) = (1, 0)$. There exist different generalizations of this Gray map, which go from $\mathbb{Z}_{p^s}$ to

$\mathbb{Z}_p^{p^{s-1}}$ [2, 3, 6, 7]. The one given in [2] is the map $\phi : \mathbb{Z}_{p^s} \to \mathbb{Z}_p^{p^{s-1}}$ defined as follows:

$$\phi(u) = (u_{s-1}, \dots, u_{s-1}) + (u_0, \dots, u_{s-2})Y, \tag{1}$$

where $u \in \mathbb{Z}_{p^s}$, $[u_0, u_1, \dots, u_{s-1}]_p$ is the p-ary expansion of u, that is, $u = \sum_{i=0}^{s-1} p^i u_i$, and Y is a matrix of size $(s-1) \times p^{s-1}$ which columns are the elements of $\mathbb{Z}_p^{s-1}$.

Then, we define $\Phi : \mathbb{Z}_{p^s}^n \to \mathbb{Z}_p^{np^{s-1}}$ as the component-wise Gray map ϕ.

Let $\mathcal{C}$ be a $\mathbb{Z}_{p^s}$-additive code of length n. We say that its image $C = \Phi(\mathcal{C})$ is a $\mathbb{Z}_{p^s}$-linear code of length $p^{s-1}n$. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_{p^s}^n$, it is isomorphic to an abelian structure $\mathbb{Z}_{p^s}^{t_1} \times \mathbb{Z}_{p^{s-1}}^{t_2} \times \cdots \times \mathbb{Z}_{p^2}^{t_{s-1}} \times \mathbb{Z}_p^{t_s}$, and we say that $\mathcal{C}$, or equivalently $C = \Phi(\mathcal{C})$, is of type $(n; t_1, \dots, t_s)$. Note that $|\mathcal{C}| = p^{st_1} p^{(s-1)t_2} \cdots p^{t_s}$.

A generalized Hadamard (GH) matrix $H(p, \lambda) = (h_{ij})$ of order $n = p\lambda$ over $\mathbb{Z}_p$ is a $p\lambda \times p\lambda$ matrix with entries from $\mathbb{Z}_p$ with the property that for every i, j, $1 \leq i < j \leq p\lambda$, each of the multisets $\{h_{is} - h_{js} : 1 \leq s \leq p\lambda\}$ contains every element of $\mathbb{Z}_p$ exactly λ times [11].

An ordinary Hadamard matrix of order 4μ corresponds to a GH matrix $H(2, \lambda)$ over $\mathbb{Z}_2$, where $\lambda = 2\mu$ [1]. Two GH matrices of order n are said to be equivalent if one can be obtained from the other by a permutation of the rows and columns and adding the same element of $\mathbb{Z}_p$ to all the coordinates in a row or in a column. We can always change the first row and column of a GH matrix into zeros and we obtain an equivalent GH matrix which is called normalized. From a normalized Hadamard matrix H, we denote by F_H the code over $\mathbb{Z}_p$ consisting of the rows of H, and C_H the one defined as $C_H = \bigcup_{\alpha \in \mathbb{F}_q}(F_H + \alpha\mathbf{1})$, where $F_H + \alpha\mathbf{1} = \{\mathbf{h} + \alpha\mathbf{1} : \mathbf{h} \in F_H\}$ and $\mathbf{1}$ denotes the all-one vector. The code C_H over $\mathbb{Z}_p$ is

[*] This work has been partially supported by the Spanish MINECO under Grant PID2019-104664GB-I00 / AEI / 10.13039/501100011033.

called generalized Hadamard (GH) code [10]. Note that C_H is generally nonlinear over $\mathbb{Z}_p$. The $\mathbb{Z}_{p^s}$-additive codes that, under the Gray map Φ, give a GH code are called $\mathbb{Z}_{p^s}$-additive GH codes and the corresponding Gray map images are called $\mathbb{Z}_{p^s}$-linear GH codes.

The linearity of $\mathbb{Z}_4$-linear Hadamard codes of length 2^t was proved in [8, 9]. Later, in [4], an iterative construction for $\mathbb{Z}_{2^s}$-linear Hadamard codes was described, and the linearity of these codes was established. In this paper, we generalize these results for $\mathbb{Z}_{p^s}$-linear GH codes. Specifically, first, we show some results related to the Carlet's generalized Gray map. Then, we describe an iterative construction to obtain $\mathbb{Z}_{p^s}$-additive GH codes of type $(n; t_1, \dots, t_s)$. Finally, we show for which types the corresponding $\mathbb{Z}_{p^s}$-linear codes are nonlinear codes over $\mathbb{Z}_p$ when $p \neq 2$.

References

[1] E. F. Assmus; J. D. Key, Designs and Their Codes, Cambridge University Press, Great Britain, 1992.

[2] C. Carlet, *$\mathbb{Z}_{2^k}$-linear codes*, IEEE Trans. Inform. Theory, 44, no. 4, pp. 1543–1547, 1998.

[3] S. T. Dougherty; C. Fernández-Córdoba, *Codes over $\mathbb{Z}_{2^k}$, Gray map and self-dual codes*, Advances in Mathematics of Communications, 5, no. 4, pp. 571–588, 2011.

[4] C. Fernández-Córdoba; C. Vela; M. Villanueva, *On $\mathbb{Z}_{2^s}$-linear Hadamard codes: kernel and partial classification*, Designs, Codes and Cryptography, vol. 87, no. 2-3, pp. 417–435, 2019.

[5] A. R. Hammons; P. V. Kumar; A. R. Calderbank; N. J. A. Sloane; P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory, 40, no. 2, pp. 301–319, 1994.

[6] A. A. Nechaev; T. Khonol'd, *Weighted modules and representations of codes*, Probl. Inf. Transm., 35, no. 3, pp. 205–223, 1999.

[7] D. S. Krotov, *On $\mathbb{Z}_{2^k}$-dual binary codes*, IEEE Trans. Inform. Theory, 53, no 4, pp. 1532–1537, 2007.

[8] D. S. Krotov, *$\mathbb{Z}_4$-linear Hadamard and extended perfect codes*, International Workshop on Coding and Cryptography, ser. Electron. Notes Discrete Math. 6, pp. 107–112, 2001.

[9] K. T. Phelps; J. Rifà; M. Villanueva, *On the additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes: rank and kernel*, IEEE Trans. Inform. Theory, 52, no. 1, pp. 316–319, 2006.

[10] S. T. Dougherty; J. Rifà; M. Villanueva, *Ranks and kernels of codes from generalized Hadamard matrices*, IEEE Trans. Inform. Theory, 62, no. 2, pp. 687–694, 2016.

[11] D. Jungnickel, *On difference matrices, resolvable transversal designs and generalized Hadamard matrices*, Math. Zeitschrift, vol. 167, no. 1, pp. 49-60, 1979.

A software program for equivalence of linear codes over finite fields[†]

Iliya Bouyukliev, Stefka Bouyuklieva `[{iliyab,stefka}@math.bas.bg]`

Faculty of Mathematics and Informatics
St. Cyril and St. Methodius University of Veliko Tarnovo
Veliko Tarnovo, Bulgaria

The equivalence test is a main part in any classification problem. In this talk, we present the algorithm for equivalence of linear codes over finite fields implemented in the program LCEQUIVALENCE which is a module of the software package QEXTNEWEDITION [1]. The program is designed to obtain the inequivalent codes in a set of linear codes over a finite field $\mathbb{F}_q$ with $q \leq 64$ elements. Moreover, the program calculates the orders of the automorphism groups and orbits of the coordinates. The use does not require special programming language skills. Although there are many classification results, software for equivalence of linear codes is presented only in the works of J. Leon [6], Thomas Feulner [4] and Iliya Bouyukliev [2] (up to our knowledge). The main advantages of the program LCEQUIVALENCE are: (1) it works for codes over fields with $q \leq 64$ elements; (2) it can be used to find the inequivalent among a huge number of linear codes; (3) there is no restrictions on the length and dimension of the considered codes (this depends only on the used hardware and the computational time).

The main idea in the algorithm is not new - we associate with each code a $\{0, 1\}$ matrix such that two codes are equivalent if and only if the corresponding binary matrices are isomorphic. A similar idea was used in [2] - the code equivalence problem was reduced to an isomorphism test of binary matrices. The problem in [2] is that not every automorphism of the binary matrix used is an automorphism of the code and therefore additional verification is needed. The authors of [3] proposed to use a different binary matrix as an image of a given q-ary code to avoid the disadvantage of [2]. A new improvement is implemented in the program LCEQUIVALENCE.

Let $\mathbb{F}_q^n$ be the n-dimensional vector space over the finite field $\mathbb{F}_q$. The *Hamming distance* between two vectors of $\mathbb{F}_q^n$ is defined as the number of coordinates in which they differ. A *q-ary linear $[n, k, d]_q$ code* is a k-dimensional linear subspace of $\mathbb{F}_q^n$ with minimum distance d. A *generator matrix G* of a linear code $[n, k]$ code C is any matrix of rank k (over $\mathbb{F}_q$) with rows from C. The most important definitions in our work are the following.

Definition 1: We say that two linear $[n, k]_q$ codes C_1 and C_2 are **equivalent**, if the codewords of C_2 can be obtained from the codewords of C_1 via a finite sequence of transformations of the following types: (1) permutation of coordinate positions; (2) multiplication of the elements in a given position by a non-zero element of $\mathbb{F}_q$; (3) application of a field automorphism to the elements in all coordinate positions.

This definition is well motivated as the transformations (1)–(3) preserve the Hamming distance and the linearity (for more details see [5, Chapter 7.3]). An *automorphism* of a linear code C is a finite sequence of transformations of type (1)–(3), which maps each codeword of

[†] This work is supported in part by the Bulgarian National Science Fund under Contracts KP-06- Russia/33/17.12.2020 and KP-06-N32/2-2019.

C onto a codeword of C. The set of automorphisms of C forms a group which is called the *automorphism group* of the code and denoted by $\mathrm{Aut}(C)$. Clearly, $\mathrm{Aut}(C)$ is the semidirect product of a group of monomial matrices by a subgroup of the Galois group of the considered finite field.

Definition 2: Two binary matrices of the same size are **isomorphic** if the rows of the second one can be obtained from the rows of the first one by a permutation of the columns.

Any permutation of the columns of a binary matrix A which maps the rows of A into the rows of the same matrix, is called an automorphism of A. The set of all automorphisms of A is a subgroup of the symmetric group S_n and we denote it by $\mathrm{Aut}(A)$.

Let C be a linear code over the field $\mathbb{F}_q$ with $q = p^m$ elements, where p is a prime, and let α be a primitive element of $\mathbb{F}_q$. To any element of $\mathbb{F}_q$ we juxtapose a circulant binary matrix of order $q-1$ in the following way:

$$0 \mapsto \mathrm{circ}(00\dots0), \quad \alpha^i \mapsto \mathrm{circ}(0\dots0\underbrace{1}_{i}0\dots0) \text{ for } i = 0, 1, \dots, q-2.$$

Instead of a generator matrix, we use a generating set D_C for the code C. This is a set of codewords that is stable under the action of the group $\mathrm{Aut}(C)$ and generates the code as a linear space over $\mathbb{F}_q$. Obviously, if $v \in D_C$ then $\alpha^i v \in D_C$ for $i = 0, \dots, q-2$. Therefore we take a subset $D'_C \subset D_C$ such that any two vectors in D'_C are nonproportional and any vector from D_C is proportional to a vector in D'_C. We substitute any vector $v = (v_1, v_2, \dots, v_n) \in D'_C$ with a binary $(q-1) \times 2n(q-1)$ matrix in the following way: first, we extend v to $v' = (0, v_1, 0, v_2, \dots, 0, v_n) \in \mathbb{F}_q^{2n}$ and then we replace each coordinate of v' by its corresponding circulant matrix. In this way we correspond to the set D'_C a binary $t(q-1) \times 2n(q-1)$ matrix A'_C, where $t = |D'_C|$. We then add a few more rows in order to restrict the automorphisms of the binary matrix to those permutations that correspond to the automorphisms of the linear code.

The basic features of the program LCEQUIVALENCE are presented on the website [1]. A more detailed description will be given in the talk.

References

[1] I. Bouyukliev, *QextNewEdition - LCequivalence module* (2021). Online available at `http://www.moi.math.bas.bg/moiuser/~data/Software/QextNewEditionLCequiv.html`.

[2] I. Bouyukliev, *About the code equivalence*, in *Advances in Coding Theory and Cryptology*, T. Shaska, W. Huffman, D. Joyner, and V. Ustimenko, Eds., pp. 126–151, 2007.

[3] I. Bouyukliev; M. Dzhumalieva-Stoeva, *Representing equivalence problems for combinatorial objects*, Serdica J. Computing **8**(4), 327–354 (2014)

[4] T. Feulner, *The automorphism groups of linear codes and canonical representatives of their semilinear isometry classes*, Advances in Mathematics of Communication **3**(4), 363-383 (2009)

[5] P. Kaski; P. R. J. Östergård, *Classification Algorithms for Codes and Designs*, Springer-Verlag Berlin Heidelberg, 2006.

[6] J. Leon, Computing automorphism groups of error-correcting codes, IEEE Transactions on Information Theory **28**, 496–511 (1982)

Recent conjectures on the equivalence of linear cyclic codes

Reza Dastbasteh, Petr Lisoněk [{rdastbas,plisonek}@sfu.ca]

Department of Mathematics,
Simon Fraser University
Burnaby, Canada

In this work, three recent conjectures on the equivalence of linear cyclic codes over finite fields will be answered. These conjectures were recently proposed by Aydin et al. (2019) based on their computational results on the parameters of linear cyclic codes. In particular, we prove the following statements.

1. If $g_1(x)$ and $g_2(x)$ are the generator polynomials of two monomially equivalent linear cyclic codes of length n over $\mathbb{F}_q$, then $g_1(x)$ and $g_2(x)$ generate two monomially equivalent linear cyclic codes of length nm, provided that $\gcd(mn, q) = 1$.
2. Let A_1 and A_2 be the defining sets of two linear cyclic codes of length n over $\mathbb{F}_q$. If the shift map $\phi(x) = (x + b) \mod n$ is a bijection from A_1 to A_2, then the linear cyclic codes with the defining sets A_1 and A_2 are monomially equivalent and $n \mid |A_1|(q-1)b$.
3. We show that there are monomially equivalent linear cyclic codes that are not equivalent by an affine map.

Most of our results were motivated by computer algebra experiments. As an application, several infinite families of monomially equivalent linear cyclic codes are provided.

References

[1] N. Aydin; J. Lambrinos; O. VandenBerg, *On equivalence of cyclic codes, generalization of a quasi-twisted search algorithm, and new linear codes*, Designs, Codes and Cryptography, 2019 Oct 1;87(10):2199-212.

[2] K. Bogart; D. Goldberg; J. Gordon, *An elementary proof of the MacWilliams theorem on equivalence of codes*, Information and Control, 1978 Apr 1;37(1):19-22.

[3] PP. Palfy, *Isomorphism problem for relational structures with a cyclic automorphism. European Journal of Combinatorics*, 1987 Jan 1;8(1):35-43.

[4] F.J. MacWilliams; N.J.A. Sloane, *The theory of error-correcting codes*, Elsevier.

Hulls of additive conju-cyclic codes over F4 with respect to a trace dual

Md Ajaharul Hossain[1] ***, Ramakrishna Bandi***[1]***, Sanjit Bhowmick***[2]***,***
`[{mdajaharul,ramakrishna}@iiitnr.edu.in,`
`sanjitbhowmick392@gmail.com]`

[1] Department of Mathematics
International Institute of Technology Naya Raipur
Nava Raipur - 493661, India
[2] Department of Mathematics
National Institute of Technology Durgapur
Durgapur, India

Conjucyclic codes are closed under the conjugate cyclic shift operations. Additive Conjucyclic codes are useful in quantum error-correction, for which this class of codes are new topic of interest in algebraic coding theory. In this talk, we discuss additive conjucyclic codes over $\mathbb{F}_4$ with respect to the trace dual and obtain conditions for an additive conjucyclic code to be self-orthogonal and self-dual. Later we find the trace hull of an additive conjucyclic code and its dimension. A necessary and sufficient condition for a conjucyclic code to have an additive complementary dual (ACD) is obtained. Finally, a condition on additive conjucyclic complementary pair of codes over $\mathbb{F}_4$ is found using trace dual. We end the talk by presenting some good quantum codes constructing using the conjucyclic codes.

Quantum Error-Correcting Codes over small fields from AG curves

Heeralal Janwa, Fernando Piñero `[{heeralal.janwa,fernando.pinero1}@upr.edu]`

Department of Mathematics
University of Puerto Rico at Rio Piedras
17 University Ave. Ste 1701 San Juan PR, 00925-2537

In this article we use hyperbolic codes from algebraic curves over high degree extensions of $\mathbb{F}_2$ to construct self–orthogonal code pairs for Quatum Error Correcting codes. We also present bounds on the parameters of the resulting subfield codes over $\mathbb{F}_2$ or $\mathbb{F}_4$ from Hermitian curves, Norm–Trace curves, quasi–Hermitian curves, and others. Several of these results are novel and provide a pathway to make progress towards making quantum computers feasible and practical during the next decade.

References

[1] Hernando, Fernando; McGuire, Gary, *Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions*, Journal of Algebra, 2011

[2] Férard, Eric, *A infinite class of Kasami functions that are not APN infinitely often*, Contemp. Math., Vol. 686, pag. 45–63, 2017

[3] Delgado, Moises; Janwa, Heeralal, *Some new results on the conjecture on exceptional APN functions and absolutely irreducible polynomials: the Gold case*, Advances in Mathematics of Communications, 2017

[4] Delgado, Moises; Janwa, Heeralal, *On the absolute irreducibility of hyperplane sections of generalized Fermat varieties in $\mathbb{P}^3$ and the conjecture on exceptional APN functions: the Kasami-Welch degree case*, 2016

[5] Aubry, Yves; McGuire, Gary; Rodier, François, *A few more functions that are not APN infinitely often*, Finite fields: theory and applications, Amer. Math. Soc., Providence, RI, 2010

Skew constacyclic codes over a non-chain ring

***Mehmet E. Köroğlu*, Mustafa Sarı**
[{mkoroglu,musari}@yildiz.edu.tr]

Department of Mathematics
Yildiz Technical University
Esenler 34220, Istanbul-Turkey

A subspace of the vector space $\mathbb{F}_q^n$ with dimension k is called a linear code of length n and dimension k over $\mathbb{F}_q$. The elements of a linear code are termed as codewords. The minimum Hamming distance d of a linear code $\mathcal{C}$ is the minimum Hamming weight $w_H(\mathcal{C})$ of $\mathcal{C}$, where $w_H(\mathcal{C}) = \min\{w_H(c) : 0 \neq c \in \mathcal{C}\}$ and $w_H(c) = |\{i : c_i \neq 0, i \in \{0, 1, \ldots, n-1\}\}|$. A linear code $\mathcal{C}$ over $\mathbb{F}_q$ of length n, dimension k and minimum distance d is denoted by the triple $[n, k, d]_q$ and this code corrects up to $\lfloor \frac{d-1}{2} \rfloor$ errors. An $[n, k, d]_q$ linear code is called maximum distance separable (MDS) if $k = n - d + 1$. A linear code $\mathcal{C}$ over $\mathbb{F}_q$ is called a linear complementary dual (LCD) code if $Hull(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^{\perp} = \{\mathbf{0}\}$, where $\mathcal{C}^{\perp} = \left\{ y \in \mathbb{F}_q^n : \sum\limits_{i=0}^{n-1} x_i y_i = 0, \forall x \in \mathcal{C} \right\}$.

For a given automorphism θ of $\mathbb{F}_q$, the set

$$\mathbb{F}_q[x;\theta] = \{a_0 + a_1 x + \ldots + a_1 x^n | a_i \in \mathbb{F}_q \text{ and } n \in \mathbb{N}\}$$

of formal polynomials forms a ring under the usual addition of polynomials and the polynomial multiplication with the restriction $xb = \theta(b)x$. The multiplication is extended to all the elements of $\mathbb{F}_q[x;\theta]$ via distributivity and associativity. This ring is called the *skew polynomial ring* over $\mathbb{F}_q$.

For a given element $\lambda \in \mathbb{F}_q - \{0\}$ and an automorphism θ of $\mathbb{F}_q$ a skew λ-constacyclic code over the finite field $\mathbb{F}_q$ of length n is a linear code $\mathcal{C}$ satisfying that

$$(\lambda\theta\left(c_{n-1}\right), \theta\left(c_0\right), \ldots, \theta\left(c_{n-2}\right)) \in \mathcal{C}$$

for each codeword $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in \mathcal{C}$.

In the last few decades, codes over finite commutative chain rings were studied extensively (see Refs. [1, 2, 3, 4, 5, 6]). In recent years, some special non-chain rings have been used as an alphabet for codes (see Refs. [7, 8, 9, 10]). One important class of linear codes is the class of constacyclic codes since their algebraic structure and their applications to other disciplines including classical and quantum communication systems. Over the conventional polynomial rings, the algebraic structure of λ-constacyclic codes of length n is determined by the factors of the cyclotomic polynomial $x^n - \lambda$. In [11], Boucher, Solé and Ulmer used skew polynomials to describe the structure of constacyclic codes under a skew constacyclic shift. Later, in the [12, 13, 14], Boucher and Ulmer investigated more properties and good examples of these codes.

In this study, we examine the algebraic structure of the semi-local ring $\mathcal{R}_q = \mathbb{F}_q[v]/\langle v^2+1\rangle$, where $q = p^k$ is a prime power and for positive integers a and b, $p = a^2 + b^2$, and determine the automorphisms of this ring to study the algebraic structure of the skew constacyclic codes and their dual over this ring. We provide the necessary and sufficient conditions for the existence of the self-dual and self orthogonal skew constacyclic codes. In addition, we give the conditions for the existence of the linear complementary dual skew cyclic codes and skew negacyclic codes.

References

[1] M.C.V. Amarra; F.R. Nemenzo, *On* $(1-u)$*-cyclic codes over* $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$, Appl. Math. Letters, **21**, 1129-1133 (2008).

[2] A. Bonnecaze; P. Udaya, *Cyclic codes and self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory, **45**(4), 1250-1255 (1999).

[3] H.Q. Dinh; S. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory, **50**(8), 1728-1744 (2004).

[4] S. Jitman; S. Ling; P. Udomkavanich, *Skew constacyclic codes over finite chain rings*, Adv. Math. Commun., **6**(1), 39-63 (2012).

[5] E. Martínez-Moro; I.F. Rúa, *Multivariable codes over finite chain rings: serial codes*, SIAM J. Discrete Math., **20**(4), 947-959 (2006).

[6] G.H. Norton; A. Sâlâgean, *Strong Gröbner bases and cyclic codes over a finite-chain ring*, Electron. Notes Discrete Math., **6**, 240-250 (2001).

[7] J. Gao; F. Ma; F. Fu, *Skew constacyclic codes over the ring* $\mathbb{F}_q + v\mathbb{F}_q$, Appl. Comput. Math, **6**(3), 286-295 (2017).

[8] J. Gao, *Skew cyclic codes over* $\mathbb{F}_q + v\mathbb{F}_q$, J Appl Math Informatics, **31**(3-4), 337-342 (2013).

[9] F. Gursoy; I. Siap; B. Yildiz, *Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$*, Adv. Math. Commun., **8**(3), 313-322 (2014).

[10] M. Shi; T. Yao; P. Solé, *Skew cyclic codes over a non-chain ring*, Chin. J. Electron., **26**(3), 544-547 (2017).

[11] D. Boucher; P. Solé; F. Ulmer, *Skew constacyclic codes over Galois rings*, Adv. Math. Commun., **2**(3), 273-292 (2008).

[12] D. Boucher; F. Ulmer, *Codes as modules over skew polynomial rings*, Lecture Notes Comput. Sci., **5291**, 38-55 (2009).

[13] D. Boucher; F. Ulmer, *Coding with skew polynomial rings*, J. Symbolic Comput., **44**(12), 1644-1656 (2009).

[14] D. Boucher; F. Ulmer, *Self-dual skew codes and factorization of skew polynomials*, J. Symbolic Comput., **60** 47-61 (2014).

$\mathbb{F}_q\mathcal{R}$-Skew Cyclic Codes

Shikha Patel*, *Om Prakash [{shikha_1821ma05,om}@iitp.ac.in]

Department of Mathematics
Indian Institute of Technology Patna
Bihta, Patna - 801 106, India

Let p be a prime and $\mathbb{F}_q$ be a finite field of order $q = p^m$. In this paper, we study skew cyclic codes over $\mathbb{F}_q\mathcal{R}$ where $\mathcal{R} := \mathbb{F}_q + u\mathbb{F}_q$ with $u^2 = u$. To characterize $\mathbb{F}_q\mathcal{R}$-skew cyclic codes, first we establish the algebraic structure and then by considering an inner product the self-orthogonality of these codes are discussed. Further, we construct a Gray map over $\mathbb{F}_q\mathcal{R}$ and discuss the Gray images of $\mathbb{F}_q\mathcal{R}$-skew cyclic codes over $\mathbb{F}_q$. Finally, we provide various examples of skew cyclic codes over $\mathbb{F}_q\mathcal{R}$ and their respective Gray images for different lengths.

Keywords
Cyclic code, Skew cyclic code, Self-orthogonal code, Gray map.

A New Algorithm on Finite Fields for the Construction of Differentially 4-Uniform Permutations with Optimal Algebraic Degree[‡]

Roberto Reyes Carranza[1]**, *Heeralal Janwa***[2]

[{roberto.reyes,heeralal.janwa}@upr.edu]

[1] College of Business
University of Puerto Rico at Mayaguez
Mayaguez PR 00682, USA
[2] Department of Mathematics
University of Puerto Rico at Rio Piedras
17 University Ave. Ste 1701 San Juan PR, 00925-2537

The Advanced Encryption Standard uses the inverse function, which is a differential 4-uniform function. Finding differential 4-uniform permutations with high nonlinearity on even degree field extensions is a current big challenge. In [1], Bracken and Leander listed that as an open problem (only a few results are know). It is known that if *f* is an permutation on F_{2^n}, then $\deg(f) \leq n-1$. If *f* attains the equality Zha [2] calls it optimal algebraic degree function. To know more about a class of sporadic binomials permutations with low differential uniformity ($\delta = 4$, 6), see the work of Charpin and Kyureghyan (2017) in [3]. Yu and Wang built differential 6 and 4-uniform permutations from the inverse function [5]. Then Qu et al. [4] gives us a survey of differentially 4-uniform permutation families, even without the requirement of high nonlinearity (see Carlet [6], and Zha [2]).

We construct new families of δ-uniform permutations in even degree field extensions (also for odd degree extensions), where δ can be $4, 6, 8$. It is important to underline that the functions given by almost all authors are defined implicitly, or are given as a piecewise function. While our functions are given via an explicit formula in polynomial representation, which is the more desired representation. In this process, we obtain a new general and practical theorem that can be widely applied in any finite field, e.g., to new S-Boxes.

References

[1] Carl Bracken; Gregor Leander, *A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree*, *Finite Fields Appl.*, 16(4):231–242, 2010.

[2] Zhengbang Zha; Lei Hu; Siwei Sun, *Constructing new differentially 4-uniform permutations from the inverse function*, *Finite Fields Appl.*, 25:64–78, 2014.

[3] Pascale Charpin; Gohar M. Kyureghyan, *On sets determining the differential spectrum of mappings*, *Int. J. Inf. Coding Theory*, 4(2-3):170–184, 2017.

[‡] The research of Roberto Carlos Reyes Carranza was partially supported by the NSF. The research of Heeralal Janwa was supported by NASA. Some of the computations were carried out at the High Performance Computing Center of UPR.

[4] Longjiang Qu; Yin Tan; Chik How Tan; Chao Li, *Constructing differentially 4-uniform permutations over $F_{2^{2k}}$ via the switching method*, *IEEE Trans. Inform. Theory*, 59(7):4675–4686, 2013.

[5] Yuyin Yu; Mingsheng Wang; Yongqiang Li, *Constructing differentially 4 uniform permutations from known ones*, *Chinese Journal of Electronics*, 22(3):495–499, 2013.

[6] Claude Carlet, *On known and new differentially uniform functions*, *Australasian Conference on Information Security and Privacy*, pages 1–15. Springer, 2011.

Enumeration and Construction of New Boolean Bent/Near-bent Functions of the Gold and Kasami-Welch Type[§]

Jose W. Velazquez, Heeralal Janwa [{jose.velazquez16,heeralal.janwa}@upr.edu]

Department of Mathematics
University of Puerto Rico at Rio Piedras
17 University Ave. Ste 1701 San Juan PR, 00925-2537

A vectorial (m,k) Boolean function is defined as $f : F_{2^m} \to F_{2^k}, 1 \leq k \leq m$. Boolean functions ($k = 1$) have their nonlinearity bounded above by $2^{m-1} - 2^{\frac{m}{2}-1}$. Bent Boolean functions have maximum nonlinearity; a measure of their distance to the set of affine functions (i.e., the first-order Reed-Muller codes). Janwa and Wilson gave construction of error-correcting-codes [4] from non-linear function. Janwa, McGuire and Wilson [3] conjectured that such codes are 2-error-correcting if and only if the exponents are the Gold or Kasami-Welch type ($d = 2^l + 1, 2^{2l} - 2^l + 1, (l, m) = 1$) (i.e., the functions are APN). One can can construct Boolean functions as trace functions on F_{2^m}. Well known Boolean functions are the Gold and Kasami-Welch near-bent functions of the form $Tr(x^d)$ [1]. Corresponding to these exponents, Dillon and Dobbertin [2] proposed a construction of bent functions of the type $Tr(\lambda x^d)$ with $\lambda \in F_{2^m}^*$ a non-cube. In this work, we generalize the results of Dillon and Dobbertin. We also give results on the classification and enumeration of the Gold and Kasami-Welch near-bent functions via cyclotomic coset equivalence analysis. Consequently, we prove theorems and obtain bounds on the number of equivalence classes of such near-bent functions. We also prove some such results for the bent functions of Dillon and Dobbertin and of our generalization.

References

[1] C. Carlet and S. Mesnager. Four decades of research on bent functions. *Designs, Codes and Cryptography*, 78(1):5–50, 2016.

[2] J. Dillon and H. Dobbertin. New cyclic difference sets with singer parameters. *Finite Fields and Their Applications*, 10(3):342–389, 2004.

[§] This research is funded by the PR Space Grant Consortium, NASA Cooperative Agreement 80NSSC20M0052

[3] H. Janwa, G. Mcguire, and R. M. Wilson. Double-error-correcting cyclic codes and absolutely irreducible polynomials over gf (2). *Journal of Algebra*, 178(2):665–676, 1995.

[4] H. Janwa and R. M. Wilson. Hyperplane sections of fermat varieties in p3 in char. 2 and some applications to cyclic codes. In G. Cohen, T. Mora, and O. Moreno, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 180–194, Berlin, Heidelberg, 1993. Springer Berlin Heidelberg.

Some Constructions of l-Galois LCD codes

Shikha Yadav*, *Om Prakash [{1821ma10,om}@iitp.ac.in]

Department of Mathematics
Indian Institute of Technology Patna
Bihta, Patna - 801 106, India

Let F_q be the finite field with q elements, where $q = p^m$ for some prime p and $m > 0$. In this article, we provide three constructions of linear codes over F_q in terms of their generator matrices and characterise LCD codes from them. Here, we consider Galois inner product instead of Euclidean or Hermitian inner products. For these constructions, we use the matrices A for which $A[\sigma^{m-l}(A)]^t = I, 0 \leq l \leq m-1$, where σ is the frobenius map.