SPECIAL SESIONS

Applications of Computer Algebra - ACA2018

June 18–22, 2018

Santiago de Compostela, Spain

S9

Computer Algebra in Coding Theory and Cryptography

Tuesday

Tue 19th, 10:30 - 11:00, Aula 7 – Ruud Pellikaan:
On varieties and codes defined by quadratic equations

Tue 19th, 11:30 - 12:00, Aula 7 – F. Javier Lobillo:
Cyclic structures in convolutional codes and free distance

Tue 19th, 12:00 - 12:30, Aula 7 – Edgar Martínez-Moro:
On additive cyclic codes over chain rings

Tue 19th, 12:30 - 13:00, Aula 7 – Narcís Sayols:
Computer algebra tales on Goppa codes and McEliece cryptography

Tue 19th, 13:00 - 13:30, Aula 7 – Putranto Utomo:
Satisfiability modulo theory in finding the distance distribution of binary constrained arrays

Tue 19th, 15:30 - 16:00, Aula 7 – Stefka Bouyuklieva:
Binary Isodual Codes Having an Automorphism of Odd Prime Order

Tue 19th, 16:00 - 16:30, Aula 7 – Abdullah Dertli:
Quantum codes from constacyclic codes over the finite ring $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p$

Tue 19th, 16:30 - 17:00, Aula 7 – G. Gözde Güzel:
Constacyclic and cyclic codes over the class of finite rings $\mathbb{F}_{2^k} + u\mathbb{F}_{2^k} + u^2\mathbb{F}_{2^k} + v\mathbb{F}_{2^k}$

Tue 19th, 17:30 - 18:00, Aula 7 – Yasemin Çengellenmiş:
On the skew cyclic codes and the reversibility problem for DNA 4-bases

Tue 19th, 18:00 - 18:30, Aula 7 – Arunwan Boripan:
The enumeration of Hermitian self-dual cyclic codes over finite chain rings

Wednesday

Wed 20th, 10:00 - 10:30, Aula 7 – Diana H. Bueno-Carreño:
Multiplying Dimension in Abelian Codes

Wed 20th, 10:30 - 11:00, Aula 7 – Simon Eisenbarth:
Self-dual codes over chain rings

Wed 20th, 11:30 - 12:00, Aula 7 – Emilio Suárez-Canedo:
On the rank and kernel of new HFP-codes

Wed 20th, 12:00 - 1230, Aula 7 – Irene Márquez-Corbella:
Generalized HammingWeights of Binary Linear Codes

Organizers

Irene Márquez Corbella:
Universidad de La Laguna
Spain

Emilio Suárez Canedo:
Universitat Autònoma de Barcelona
Spain

Aim and cope

This session aims to bring together from all areas related to computer algebra (both theoretical and algorithmic) applied to Coding Theory and Cryptography.

Since much of the work related to these topic is recent or is still ongoing, this session will provide a stimulating forum where experts will be able to not only report their recent results, but also to propose new lines of research and discuss open questions.

It will also give us the opportunity to present the interest and the potential applications of these topics to the rest of the scientific community

Expected topics of presentations include (but are not limited to):

- Computer Algebra and Coding Theory
  Codes and applications. Combinatorial structures. Algebraic-geormetric codes. Network coding. Quantum codes. Group codes. . .
- Computer Algebra in Cryptography
  Algebraic Cryptanalysis. Post-quantum cryptography. (Code, Lattice and Hash)–based PKC. Multivariate PKC. . .
- simulation of quantum computation
- Synergies between Computer Algebra, Coding Theory and Cryptography.

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

The enumeration of Hermitian self-dual cyclic codes over finite chain rings

Arunwan Boripan[1], **Somphong Jitman**[2], **and Patanee Udomkavanich**[3]

Let $\mathbb{F}_{q^2}$ be a finite field of order q^2 and let $R := \mathbb{F}_{q^2}[u]/\langle u^t \rangle$ be a finite chain ring, where $t \geq 2$ is an integer. Cyclic codes over R have been of interest due to their rich algebraic structures and wide applications. Here, the characterization and enumeration of Hermitian self-dual cyclic codes of length n over R have been given based on self-conjugate-reciprocal irreducible monic(SCRIM) factors of $x^n - 1$ over $\mathbb{F}_{q^2}$. Subsequently, the number of SCRIM factors of $x^n - 1$ over $\mathbb{F}_{q^2}$ has been investigated. Finally, some computational results obtained from computer algebra MAGMA have been discussed.

Keywords: Cyclic codes, Hermitian self-dual cyclic code, Finite chain ring

References

[1] A. BORIPAN; S. JITMAN; P. UDOMKAVANICH, Self-Conjugate-Reciprocal Irreducible Monic Polynomials over Finite Fields. In *Proccedings of the 20th Annual Meeting in Mathematics 2015*, Department of Mathematics, Faculty of Sceince, Silapakorn University, 34–43. Nakorn Pathom, 2015.

[2] B. CHEN; S. LING; G. ZHANG, Enumeration formulas for self-dual cyclic codes. *Finite Fields and Their Applications* **42**, 1–22 (2016).

[1]Department of Mathematics and Computer Science, Faculty of Science
Chulalongkorn University
Bangkok 10330, Thailand
boripan-arunwan@hotmail.com

[2]Department of Mathematics, Faculty of Science
Silapakorn University
Nakhon Pathom 73000, Thailand
sjitman@gmail.com

[3]Department of Mathematics and Computer Science, Faculty of Science
Chulalongkorn University
Bangkok 10330, Thailand
pattanee.u@chula.ac.th

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Binary Isodual Codes Having an Automorphism of Odd Prime Order*

Stefka Bouyuklieva[1], **Radka Russeva**[2], **Emine Karatash**[2]

The purpose of this talk is to describe the structure and properties of the binary isodual codes having automorphisms of odd prime order and to present a method for their construction. If a code C is equivalent to its orthogonal complement $C^{\perp}$, then it is termed *isodual*, and if $C = C^{\perp}$, C is a *self-dual* code. Recently, there has been growing interest in the isodual codes, and the authors use different methods for their construction (see for example [5]).

A linear code C is formally self-dual if C and its dual $C^{\perp}$ have the same weight enumerator. While self-dual codes contain only even weight vectors, formally self-dual codes may contain odd weight codewords as well. Many authors consider only even formally self-dual codes because their weight enumerators are combinations of Gleason polynomials. The class of isodual codes is between the self-dual and formally self-dual (fsd) codes. Since all isodual codes are also formally self-dual, they possess all the properties of the fsd codes.

The minimum weight d of a formally self-dual even code of length n is bounded by $d \leq 2[n/8] + 2$. An fsd even code meeting this upper bound is called extremal. Self-dual codes meeting this bound exist only for lengths $n = 2$, 4, 6, 8, 12, 14, 22 and 24 [3]. Extremal formally self-dual even codes which are not self-dual exist only for lengths 6, 10, 12, 14, 18, 20, 22, 28 and 30, and all these codes are classified [2]. For some lengths, there are odd fsd codes with higher minimum weight than the even ones. For example, the unique linear $[16, 8, 5]$ code has dual distance 5 and therefore it is formally self-dual, but the highest possible minimum weight of an even code of the same length is 4 (see [6]). The smallest length for which a fsd code is not isodual is 14, and there are 28 such codes amongst 6 weight enumerators. The even fsd $[30, 15, 8]$ codes are classified (see [2]) but it is still not known whether odd fsd codes with these parameters exist.

In the eighties of the last century, Huffman and Yorgov proposed a method for constructing and classifying binary self-dual codes with an automorphism of odd prime order (see [4, 7]). This method can be modified and applied to other linear codes. The closest class is the class of binary isodual codes, and therefore we study the structure of those isodual codes that have an automorphism of odd prime order. Let C be a binary linear code of length n and σ be an automorphism of C of odd prime order p with c independent p-cycles. Without loss of generality we can assume

*This research is supported by Bulgarian Science Fund under Contract DN-02-2/13.12.2016 and by Shumen University, Project RD-08-111/ 05.02.2018

that $\sigma = \Omega_1 \dots \Omega_c \Omega_{c+1} \dots \Omega_{c+f}$, where $\Omega_i = ((i-1)p+1, \dots, ip), i = 1, \dots, c$, are the cycles of length p, and $\Omega_{c+i} = (cp+i), i = 1, \dots, f$, are the fixed points. Obviously, $cp + f = n$.

Let $F_\sigma(C) = \{v \in C : v\sigma = v\}$ and $E_\sigma(C)$=$\{v \in C : wt(v|\Omega_i) \equiv 0 \pmod 2, i = 1, \dots, c+f\}$, where $v|\Omega_i$ is the restriction of v on Ω_i. Then the code C is a direct sum of the subcodes $F_\sigma(C)$ (fixed subcode) and $E_\sigma(C)$ (even subcode).

Consider first the fixed subcode. Clearly, $v \in F_\sigma(C)$ if and only if $v \in C$ and v is constant on each cycle. Let $\pi : F_\sigma(C) \to F_2^{c+f}$ be the projection map, so if $v \in F_\sigma(C)$, $(v\pi)_i = v_j$ for some $j \in \Omega_i, i = 1, 2, \dots, c+f$. Denote by C_π the code $\pi(F_\sigma(C))$.

For $v \in E_\sigma(C)$ and $1 \le i \le c$, we identify $v|\Omega_i = (v_0, v_1, \cdots, v_{p-1})$ with the polynomial $v_0 + v_1 x + \cdots + v_{p-1}x^{p-1}$ from $\mathcal{P}$, where $\mathcal{P}$ is the set of even-weight polynomials in $\mathbb{F}_2[x]/(x^p - 1)$. Thus we obtain the map $\phi : E_\sigma(C) \to P^c$. Denote $\phi(E_\sigma(C))$ by C_ϕ. Obviously, C_ϕ is a $\mathcal{P}$-module, and if $\mathcal{P}$ is a field then C_ϕ is a linear code. On $\mathcal{P}^c$, we use the Hermitian inner product:

$$\langle u, v \rangle = \sum_{j=1}^{c} u_j \overline{v_j}, \tag{1}$$

where $\overline{v_j} = v_j(x^{-1}) = v_j(x^{p-1})$, $u = (u_1, \dots, u_c)$, $v = (v_1, v_2, \dots, v_c)$.

For the equivalence we use the following theorem

Theorem 1: *The following transformations preserve the decomposition and send the code C to an equivalent one:*

a) the substitution $x \to x^t$ in C_φ, where t is an integer, $1 \le t \le p-1$;

b) multiplication of the jth coordinate of C_φ by x^{t_j} where t_j is an integer, $0 \le t_j \le p-1$, $j = 1, 2, \dots, c$;

c) permutation of the first c cycles of C;

d) permutation of the last f coordinates of C.

If $\sigma \in Aut(C)$, $\sigma \in Aut(C')$, and p^2 does not divide the orders of both groups, then the codes C and C' are equivalent if and only if C' can be obtained from C by applying a sequence of the given transformations.

The proof is similar to the proof of Theorem 3 in [7].

Now let C be a binary isodual code, so $C \cong C^\perp$. Since $Aut(C) = Aut(C^\perp)$, the permutation σ is an automorphism of $C^\perp$, too. Hence $C^\perp = F_\sigma(C^\perp) \oplus E_\sigma(C^\perp)$. Let $C'_\pi = \pi(F_\sigma(C^\perp))$, and $C'_\phi = \phi(E_\sigma(C^\perp)^*)$.

If 2 is a multiplicative root modulo p then $\mathcal{P}$ is a field with 2^{p-1} elements and C_ϕ is a linear code over this field. Therefore here we consider only such primes p. We say that two codes over $\mathcal{P}$ are equivalent if one of them can be obtain from the other one after a sequence of transformations of types a), b) and c) from Theorem 1. Using this theorem, we obtain the following results.

Theorem 2: *The binary codes C_π and C'_π are equivalent. The same is true for the codes C_ϕ and C'_ϕ over the field $\mathcal{P}$.*

Theorem 3: *Let C be a binary linear $[2k, k, d]$ code having an automorphism σ of odd prime order p. If 2 is a multiplicative root modulo p and p^2 does not divide the order of Aut(C) then C is an isodual code if and only if the codes C_π and C_ϕ are isodual.*

As an application of the presented structure we focus on the isodual $[30, 15, \geq 7]$ codes with an automorphism of order 5 with 6 independent 5-cycles. If C is such a code, then C is a direct sum of a $[30, 3, \geq 10]$ fixed subcode projected in a binary $[6, 3, \geq 2]$ isodual code C_π, and a $[30, 12, \geq 8]$ even code $E_\sigma(C)$. There exist exactly six binary isodual codes of length 6, one of them has minimum distance 3, and the other five codes have minimum distance 2, including the only self-dual $[6, 3, 2]$ code. The only isodual $[6, 3, 3]$ code has weight enumerator $1 + 4y^3 + 3y^4$ [6].

The image of the even subcode under the map ϕ is a $[6, 3, d_\phi]$ linear code over the field $\mathcal{P} \cong GF(16)$. For the field we have $\mathcal{P}^* = \{\alpha^i \delta^j,\ i = 0, 1, \ldots, 4,\ j = 0, 1, 2\}$, where $e = x + x^2 + x^3 + x^4$ is the identity element, $\alpha = xe$ is an element of order 5, and $\delta = x + x^4$ is of order 3.

First, we constructed all $[6, 3, d_\phi]$ linear codes over $\mathcal{P}$ such that $d(\phi^{-1}(M)) \geq 8$. There are 61 $[6, 3, 3]$ and 326 $[6, 3, 4]$ inequivalent codes with the needed properties. Then we combined these codes with all codes $\pi^{-1}(C')$ where C' is equivalent to any of the isodual $[6, 3, \geq 2]$ binary codes. After that we check all these binary isodual codes of length 30 for minimum weight and also for equivalence, using the program Q-EXTENSION [1]. In this way we obtained exactly 642 binary isodual $[30, 15, \geq 7]$ inequivalent codes having an automorphism of order 5 with 6 independent 5-cycles. Only 13 of these codes have minimum weight 8. All constructed $[30, 15, 8]$ codes have the same weight enumerator $1 + 450y^8 + \cdots + y^{30}$ and so they are even isodual codes.

Keywords: linear codes, isodual codes, automorphisms

Mathematics Subject Classification 2010: 94B05, 94B60

References

[1] I. BOUYUKLIEV, What is Q-EXTENSION? *Serdica J. Computing* **1**, 115–130, (2007).

[2] S. BOUYUKLIEVA; I. BOUYUKLIEV, Classification of the extremal formally self-dual even codes of length 30. *Adv. in Mathematics of Communications* **4**, 433–439, (2010).

[3] J.H. CONWAY; N.J.A. SLOANE, A new upper bound on the minimal distance of self-dual codes. *IEEE Trans. Inform. Theory* **36** 1319–1333, (1991).

[4] W.C. HUFFMAN, Automorphisms of codes with application to extremal doubly-even codes of lenght 48. *IEEE Trans. Inform. Theory* **28**, 511–521 (1982).

[5] H.J. KIM; Y. LEE, Construction of isodual codes over $GF(q)$. *Finite Fields and Their Applications* **45**, 372–385, (2017).

[6] SUNGHYU HAN; HEISOOK LEE; YOONJIN LEE, Binary formally self-dual odd codes. *Designs, Codes and Cryptography* **61**, 141–150 (2011).

[7] V. YORGOV, A method for constructing inequivalent self-dual codes with applications to length 56. *IEEE Trans. Inform. Theory* **33**, 77–82 (1987).

[1]Faculty of Mathematics and Informatics
"St. Cyril and St. Methodius" University of Veliko Tarnovo
Bulgaria
stefka@ts.uni-vt.bg

[2]Faculty of Mathematics and Informatics
Shumen University
Bulgaria
russeva@fmi.shu-bg.net, e.karatash@abv.bg

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Multiplying Dimension in Abelian Codes

José Joaquín Bernal[1], **Diana H. Bueno-Carreño**[2] , **Juan Jacobo Simón**[1]

In [1], we improve the notion and computation of the apparent distance for abelian codes given in [4] and [7] by means of the q-orbit structure of defining sets of abelian codes. These results allows us to design, based on a suitable election of q-orbits, abelian codes having nice bounds and parameters. In this note, we apply those techniques to construct bivariate BCH codes from cyclic codes, in such a way that we preserve apparent distance but multiplying their dimension; in particular, this drives us to multiply Reed-Solomon codes to abelian codes. As it happens with others families of abelian codes, there are alternative constructions to get this one (see, for example [6]); however, we think that this point of view allows us to determine many structural properties, parameters and even true minimum distance, in a better way.

We denote $I = \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$ and for $i = 1, 2$, we denote by U_{r_i} the set of all r_i-th primitive roots of unity and define $U = U_{r_1} \times U_{r_2}$. It is a known fact that, for a fixed $\hat{\alpha} = (\alpha, \beta) \in U$, any abelian code C is determined by its defining set, with respect to $\hat{\alpha}$, which is defined as

$$\mathcal{D}_{\hat{\alpha}}(C) = \left\{ (a, b) \in I \ : \ c(\alpha^a, \beta^b) = 0, \ \forall c \in C \right\}.$$

In [1], we introduced the notion of strong apparent distance of polynomials and hypermatrices and we applied it to define and study a notion of multivariate BCH bound and BCH abelian codes. As it was pointed out in the mentioned paper, the notion of strong apparent distance was based in the ideas and results in [4] and [7].

We use those results and techniques to prove the following results, among others.

Theorem 1. *Let n and r be positive integers such that $\gcd(q, nr) = 1$. Let C be a nonzero cyclic code in $\mathbb{F}_q(r) = \mathbb{F}_q[y]/(y^r - 1)$ with $sd^*(C) = \delta > 1$ and $\hat{\alpha} = (\alpha_1, \alpha_2) \in U_n \times \mathcal{R}(C)$. Then, the abelian code C_n in $\mathbb{F}_q(n, r) = \mathbb{F}_q[x, y]/(x^n - 1, y^r - 1)$ with defining set $\mathcal{D}_{\hat{\alpha}}(C_n) = \mathbb{Z}_n \times \mathcal{D}_{\alpha_2}(C)$ verifies that $sd^*(C_n) = \delta$ and $\dim_{\mathbb{F}_q}(C_n) = n \dim_{\mathbb{F}_q}(C)$.*

Proposition 2. *Let n and r be positive integers with $\gcd(q, nr) = 1$ and let C be a nonzero cyclic code in $\mathbb{F}_q(r)$ such that $sd^*(C) = d(C)$. Then there exists $\hat{\alpha} = (\alpha_1, \alpha_2) \in U_n \times \mathcal{R}(C)$ such that the abelian code C_n in $\mathbb{F}_q(n, r)$ with defining set $\mathcal{D}_{\hat{\alpha}}(C_n) = \mathbb{Z}_n \times \mathcal{D}_{\alpha_2}(C)$ verifies the equality $d(C_n) = d(C)$.*

BCH multivariate codes have also been defined in [1, Definition 33]. Following this definition we prove the following result.

Proposition 3. *Let $\alpha \in U_r$ and let $R = B_q(\alpha, \delta, b)$ be a Reed-Solomon code. Then, for each positive integer n and any $\alpha' \in U_n$, there exists a multivariate BCH code, $C = B_q((\alpha', \alpha), \{2\}, \{\delta\}, \{b\})$, such that $\dim(C) = (r - \delta + 1)\, n = n \cdot \dim(R)$ and $d(C) = sd^*_{\hat{\alpha}}(C) = \delta$.*

Some examples and applications will be presented.

Keywords: Abelian codes, Multiplying dimension, Cyclic codes, Reed-Solomon codes

References

[1] J.J. Bernal, D.H. Bueno-Carreño, J.J. Simón, Apparent distance and a notion of BCH multivariate codes. *IEEE Trans. Inform. Theory*, **62**(2), 655-668, 2016.

[2] J.J. Bernal, D.H. Bueno-Carreño, J.J. Simón, Cyclic and BCH Codes whose Minimum Distance Equals their Maximum BCH bound, Adv Math Comm, 10 (2016), 459-474.

[3] J. J. Bernal, M. Guerreiro, J. J. Simón, From ds-bounds for cyclic codes to true minimum distance for abelian codes. Submitted.

[4] P. Camion, *Abelian Codes*, MRC Tech. Sum. Rep. # 1059, University of Wisconsin, 1971.

[5] H. Imai, A theory of two-dimensional cyclic codes. *Information and Control* **34**(1) (1977) 1-21.

[6] J. M. Jensen, The concatenated structure of cyclic and abelian codes, *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 788-793, 1985.

[7] R. Evans Sabin, On Minimum Distance Bounds for Abelian Codes, *Applicable Algebra in Engineering Communication and Computing*, Springer-Verlag, 1992.

[1]Departamento de Matemáticas
Universidad de Murcia, 30100 Murcia, Spain.
{josejoaquin.bernal, jsimon}@um.es

[2]Departamento de Ciencias Naturales y Matemáticas
Pontificia Universidad Javeriana, Cali, Colombia
dhbueno@javerianacali.edu.co

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

On the skew cyclic codes and the reversibility problem for DNA 4-bases

Yasemin CENGELLENMIS[1], **Abdullah DERTLI**[2]

The skew cyclic codes over the finite ring $R = F_4 + uF_4 + vF_4 + uvF_4$, where $u^2 = u, v^2 = v, uv = vu$ are introduced, by defining a non trivial automorphism over R. DNA 4-bases are matched with the elements 256 of the finite ring R. With the method as in [3], the reversible DNA codes are obtained. Moreover, the Gray images of the skew cyclic codes over the finite ring R are determined.

Keywords: Reversible code, DNA cyclic code

References

[1] BAYRAM A.; OZTAS E.; SIAP I., *Codes over $F_4 + vF_4$ and some DNA applications*. Designs, Codes and Cryptography,80,379-393, DOI: 10.1007/s10623-015-0100-8, (2016).

[2] DERTLI A. ; CENGELLENMIS Y, *On cyclic DNA codes over the finite rings $Z_4 + wZ_4$ and $Z_4 + wZ_4 + vZ_4 + wvZ_4$*, *Biomath* , **6**, 1-11 ,(2017).

[3] GURSOY F.; OZTAS S. E.; SIAP I, *Reversible DNA codes over $F_{16} + uF_{16} + vF_{16} + uvF_{16}$*, arXiv:1703.10189v1, (2017).

[1]Department of Mathematics
Trakya University
Balkan Campus, Edirne ,Turkey
ycengellenmis@gmail.com

[2]Department of Mathematics
Ondokuz Mayıs University
Samsun, Turkey
abdullah.dertli@gmail.com

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Quantum codes from constacyclic codes over the finite ring $F_p + uF_p + vF_p$

Abdullah Dertli[1], **Yasemin Cengellenmis**[2]

In this paper, the quantum codes over F_p from constacyclic codes over the finite ring $F_p + uF_p + vF_p$, where $u^2 = u, v^2 = v, uv = vu = 0$, p is an odd prime are studied. A constacyclic codes over the finite ring $F_p + uF_p + vF_p$ is decomposed into three codes over F_p in order to determine the parameters of the corresponding quantum codes. Finally, we have constructed some examples of quantum error-correcting codes.

Keywords: Quantum code, Constacyclic code, Finite ring

References

[1] DERTLI A., CENGELLENMIS Y., EREN S., On quantum codes obtained from cyclic codes over A_2. *International journal of quantum information* **13**(03), 1550031 (2015).

[2] DERTLI A., CENGELLENMIS Y., EREN S., Some results on the linear codes over the finite ring $F_2+v_1F_2+...+v_rF_2$. *International journal of quantum information* **14**(01), 1650012 (2016).

[3] GAO J., WANG Y., u-Constacyclic codes over $F_p + uF_p$ and their applications of constructing new non-binary quantum codes. *Quantum Inf. Process* **17**(4), (2018).

[4] KAI X., ZHU S., Quaternary construction of quantum codes from cyclic codes over $F_4 + uF_4$. *Int. J. Quantum Inform.* **9**, 689-700 (2011).

[5] QIAN J., Quantum codes from cyclic codes over $F_2 + vF_2$. *Journal of Inform.& computational Science* **16**(6), 1715-1722 (2013).

[1]Department of Mathematics
Ondokuz Mayıs University
Samsun, Turkey
abdullah.dertli@gmail.com

[2]Department of Mathematics
Trakya University
Edirne, Turkey
ycengellenmis@gmail.com

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Self-dual codes over chain rings

Simon Eisenbarth[1], **Gabriele Nebe**[1]

Let $\mathbb{F}$ be a finite field of characteristic p and $^- : \mathbb{F} \to \mathbb{F}$ be some automorphism of order one or two. A code C in $\mathbb{F}^n$ is called self-dual if it coincides with its dual code with respect to the standard Hermitian inner dot product

$$v \cdot w := \sum_{i=1}^{n} v_i \overline{w_i}.$$

In [4], upper bounds for the minimum distance of several families of self-dual codes were given. Self-dual codes which achieve those bounds are called extremal. In [1] and [2], a generel decomposition theory for self-dual codes over $\mathbb{F}$ admitting permutation automorphisms of order prime to p has been developed. This has been frequently used, for example to classify ternary extremal codes with an automorphism of prime order ≥ 5 (see [3], [5]). In a recent work (together with G. Nebe), we developed techniques to classify $\mathbb{F}$-linear, self-dual codes with an automorphism g of order $q = p^e$, where it can w.l.o.g. be assumed that $g \in S_n$.

The group ring $\mathbb{F}\langle g\rangle$ is an Artinian chain ring with ideals $\langle (1-g)^i\rangle,\ 0 \leq i \leq q$ and it carries a natural involution defined by

$$\overline{\sum_{i=0}^{q-1} \alpha_i g^i} := \sum_{i=0}^{q-1} \overline{\alpha_i} g^{-i}.$$

Our work focused on the case where g has no fix points on $\{1, \ldots, n = pt\}$ and C is a free $\mathbb{F}\langle g\rangle$-module. Then the map

$$\mathbb{F}^n \to \mathbb{F}\langle g\rangle^t, (c_1, \ldots, c_{pt}) \mapsto \left(\sum_{i=1}^{p} c_i g^{i-1}, \ldots, \sum_{i=1}^{p} c_{(t-1)p+i} g^{i-1} \right)$$

is a bijection between the self-dual codes in $\mathbb{F}^n$ and the self-dual codes in $\mathbb{F}\langle g\rangle^t$ with respect to an inner product defined in the next section. This motivated the analysis of the structure of self-dual codes over chain rings.

Let R be a commutative Artinian chain ring with 1 and let $^- : R \to R$ be an involution, i.e. a ring automorphism of order one or two. If $\mathfrak{m} \leq R$ denotes the maximal ideal of R, then $^-$ induces an involution of the residue field $\mathbb{F} = R/\mathfrak{m}$

which we again denote by $^-$. If this involution is the identity on the residue field, then there is $\epsilon \in \{1, -1\}$ such that $\overline{x} \equiv \epsilon x \pmod{Rx^2}$ for any generator x of $\mathfrak{m}$. If $^-$ has order 2 on $\mathbb{F}$ (which we refer to as the hermitian case) then by Hilbert 90 we may choose a generator x of $\mathfrak{m}$ such that $\overline{x} \equiv x \pmod{Rx^2}$. We fix such a generator x of the maximal ideal R such that

$$\overline{x} \equiv \epsilon x \pmod{Rx^2}$$

with $\epsilon = 1$ in the Hermitian case. Let $a \in \mathbb{N}_0$, such that

$$R \supset Rx \supset Rx^2 \supset \cdots \supset Rx^{a+1} = \{0\}$$

is the complete chain of ideals in R. Then all indecomposable R-modules are of the form

$$S_b := Rx^b \text{ for some } 0 \leq b \leq a$$

where $S_0 = R$ is the free module of rank 1 and S_a is the unique simple R-module. To consider codes let $t \in \mathbb{N}$ and

$$V := R^t = \{(v_1, \ldots, v_t) \mid v_i \in R\}$$

denote the free R-module of rank t. We define the $^-$-Hermitian standard inner product

$$\langle \cdot, \cdot \rangle : V \times V \to R, \langle v, w \rangle := \sum_{j=1}^{t} v_j \overline{w_j}.$$

on V. We call an R-submodule C of V a code of length t (over R). Then by the theorem of Krull, Remak, Schmidt, there are unique $t_0, t_1, \ldots, t_a \in \mathbb{Z}_{\geq 0}$ such that

$$C = S_0^{t_0} \oplus S_1^{t_1} \oplus \cdots \oplus S_a^{t_a}.$$

Now let $C = C^\perp$ be a self-dual code of even length t which is a free R-module, i.e. $t_0 = t/2$ and $t_1 = \cdots = t_a = 0$. Then the subcodes

$$C^{(i)} := Cx^i$$

form the following chain:

$$V = R^t \supset {C^{(a)}}^\perp \supset \cdots \supset {C^{(1)}}^\perp \supset C = C^\perp \supset C^{(1)} \supset \cdots \supset C^{(a)} \supset \{0\}.$$

We now want to iteratively construct the codes $C^{(a)}, C^{(a-1)}, \ldots, C$, starting with the socle $soc(C) = C^{(a)}$.

The multiplication by x^a defines an isomorphism between the residue field and the socle of R, and the map

$$\varphi : \mathbb{F} = R/Rx \xrightarrow{\sim} Rx^a = S_a, r + Rx \mapsto rx^a$$

can be naturally extended to the socle $soc(V) = Vx^a$ of V, i.e.

$$\pi : soc(V) \to \mathbb{F}^t, (v_1, \ldots, v_t) \mapsto (\varphi^{-1}(v_1), \ldots, \varphi^{-1}(v_t))$$

is an $\mathbb{F}$-linear isomorphism.
In our initial setting, this means that the fixcode of g is generated by some matrix

$$M \otimes \begin{pmatrix} 1 & \ldots & 1 \end{pmatrix},$$

where M generates a self-dual code in $\mathbb{F}^t$ with respect to the standard Hermitian inner product. Using the classification of self-dual codes of moderat lengths, one can therefore find all possibilities for $C^{(a)}$.

For the iteration process, let $0 \leq i < a$ and fix some $C^{(i+1)}$. We want to find all admissible $C^{(i)}$, i.e. all codes D which are self-orthogonal and $Dx = C^{(i+1)}$. We put

$$W_i := {C^{(i+1)}}^{\perp} x^i / C^{(i+1)} \cong \mathbb{F}^t$$

and define

$$(\cdot, \cdot)_i : W_i \times W_i \to \mathbb{F}, (Ax^i, Bx^i)_i := \varphi^{-1}(\langle A, B \rangle x^i).$$

Then $(\cdot, \cdot)_i$ is a well-defined, non-degenerate inner product which is Hermitian in the Hermitian case and $\epsilon^{(i+a)}$-symmetric bilinear otherwise.
With respect to this inner product, $X_i := (soc(V) + C^{(i+1)})/C^{(i+1)} \leq W_i$ is self-dual code $(W_i, (\cdot, \cdot)_i)$. Moreover, $C^{(i)}/C^{(i+1)}$ is a self-dual code as well that complements X_i, i.e.

$$W_i = C^{(i)}/C^{(i+1)} \oplus X_i.$$

By constructing all complements of X_i, we can find all lifts of $C^{(i+1)}$.

This theory has been used to show in an exhaustive search that every extremal ternary code of length 36 with an automorphism of order 3 is isomorphic to the Pless Code P_{36}, strengthening the result given in [3].

Keywords: Self-dual codes, automorphisms, chain ring

References

[1] W. C. HUFFMAN, On the [24,12,10] quaternary code and binary codes with an automorphism having two cycles. *IEEE Trans. Inform. Theory* **34**(3), 486–493 (1988).

[2] W. C. HUFFMAN, On extremal self-dual quaternary codes of lengths 18 to 28. I. *IEEE Trans. Inform. Theory* **36**(3), 651–660 (1990).

[3] W. C. HUFFMAN, On Extrema1 Self-Dual Ternary Codes of Lengths 28 to 40. *IEEE Transactions on Information Theory* **38**(4), 1395–1400 (1992).

[4] C. L. MALLOWS; N. J. A. SLOANE, An upper bound for self-dual codes. *Information and Control* **22**(2), 188–200 (1973).

[5] G. NEBE, On Extremal Self-Dual Ternary Codes of Length 48 *International Journal of Combinatorics* **2012**, (2012).

[1]Lehrstuhl D für Mathematik
RWTH Aachen University
52056 Aachen, Germany
simon.eisenbarth@rwth-aachen.de

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Constacyclic and Cyclic Codes over the Class of Finite Rings $\mathbb{F}_{2^k} + u\mathbb{F}_{2^k} + u^2\mathbb{F}_{2^k} + v\mathbb{F}_{2^k}$

G.Gozde GUZEL[1], **Abdullah DERTLI**[2], **Yasemin CENGELLENMIS**[3]

In this paper, a new class of finite rings includes the finite ring which is presented in [9] is given. It is shown that these rings are semilocal, principally ideal and Frobenious rings. It is studied the units and the ideals of the ring. It is introduced a Gray map on it. The Gray images of both cyclic and $(1 + u)$-constacyclic codes over the finite ring are obtained.

Keywords: Gray map, Cyclic codes, Quasicyclic codes

References

[1] M.C.V. AMARRA, AND F.R. NEMENZO, On $(1 - u)-$ cyclic codes over $F_{p^k} + uF_{p^k}$,*Appl. Math. Lett.*, **21**, 1129–1133, (2008).

[2] N. AYDIN, Y.CENGELLENMIS, A. DERTLI, On some constacyclic codes over $Z_4[u]/(u^2 - 1)$, their Z_4 images, and new codes, *Des. Codes Cryptogr.*, DOI 10.1007/s10623-017-0392-y, (2017).

[3] I.F.BLAKE, Codes over certain rings, *Inform. Control*, **20**, 396–404, (1972).

[4] I.F.BLAKE, Codes over integer residue rings, *Inform. Control*, **29**, 295–300,(1975).

[5] Y. CENGELLENMIS, On $(1 - u^m)-$cyclic codes over $F_2 + uF_2 + u^2F_2 + ... + u^mF_2$, *International Journal of Contemporary Math. Sci.*, **4** 987–992, (2009).

[6] A. DERTLI, Y. CENGELLENMIS, On $(1+u)-$cyclic and cyclic codes over $F_2 + uF_2 + vF_2$, *European J. of Pure and Applied Math.*, **9**, 305–313, (2016).

[7] S.T. DOUGHERTY, E.SALTURK, Constacyclic codes over local rings of order 16, to be submitted.

[8] J. GAO, Linear codes and $(1 + uv)-$constacyclic codes over $R[v]/(v^2 + v)$, *IEICE Transactions on Fundamentals* , **E98-A**, 1044–1048,(2015).

[9] GUZEL G.G., DERTLI A., CENGELLENMIS Y., The $(1 + u^2)-$ constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + v\mathbb{F}_2$, to be submitted.

[10] A.R. HAMMONS JR., P.V.KUMAR, A.R.CALDERBANK, N.J.A. SLOANE, P. SOLÉ, *The Z_4- linearity of Kerdock, Preparata, Goethal, and related codes*, IEEE Trans. Inform. Theory, **40**, 301–319, (1994).

[11] X.KAI, S.ZHU, L. WANG, A family of constacyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$, J Sysst Sci Complex,**25**, 1032–1040,(2012).

[12] S. KARADENIZ, B. YILDIZ, $(1 + v)-$constacyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$, Journal of Franklin Ins., **348**, 2625–2632, (2011).

[13] D. LIAO, Y. TANG, A class of constacyclic codes over $R+vR$ and its Gray image, Int. J. Communications, Network and System Sciences, **5**, 222–227,(2012).

[14] J.F. QIAN, L.N.ZANG, S.X. ZHU, $(1+u)-$constacyclic and cyclic codes over $F_2 + uF_2$, Appl. Math. Lett., **19**, 820–823, (2006).

[15] J.F. QIAN, L.N.ZANG, S.X. ZHU, Constacyclic and cyclic codes over $F_2 + uF_2 + u^2F_2$, IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, **E89-A(6)**, 1863–1865, (2006).

[16] S. ZHU, L. WANG, A class of constacyclic codes over $F_p + vF_p$ and its Gray image , Discrete Mathematics, **311**, 2677–2682,(2011).

[1]Ipsala Vocational College
Trakya University
Edirne, Turkey
ggozdeguzel@gmail.com

[2]Department of Mathematics, Faculty of Arts and Sciences
Ondokuz Mayis University
Samsun,Turkey
abdullah.dertli@gmail.com

[3]Department of Mathematics, Faculty of Science
Trakya University
Edirne, Turkey
ycengellenmis@gmail.com

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Cyclic structures in convolutional codes and free distance*

José Gómez-Torrecillas[1], **F. J. Lobillo**[1], **Gabriel Navarro**[2]

The results of this talk are included in [6].

A rate k/n convolutional code $\mathcal{C}$ over a finite field $\mathbb{F}$ can be modeled as a rank k direct summand of $\mathbb{F}[z]^n$, i.e. $\mathcal{C} = \mathrm{im}(\cdot G)$ where $G = \sum_{i=0}^{m} z^i G_i \in \mathcal{M}_{k\times n}(\mathbb{F}[z])$ is basic. One of the main parameters of convolutional codes is the free distance, which is directly related with the correction capability of a convolutional code. The free distance is defined as

$$\mathrm{d}_{\mathsf{free}}(\mathcal{C}) = \min\left\{\mathrm{w}_{\mathsf{H}}(f) : f \in \mathcal{C}, f \neq 0\right\},$$

see [7, Ch. 3], where the Hamming weight of a polynomial over $\mathbb{F}^n$ is the coefficient-wise extension of the Hamming weight in $\mathbb{F}^n$. The free distance of a convolutional code can be calculated computing the classic associated column and row distances until they coincide. Both sequences must be computed since there is not regularity in their respectively increase and decrease.

Cyclic structures on convolutional codes can be provided enriching the algebraic structure of $\mathbb{F}^n$. Concretely, let A be an n-dimensional $\mathbb{F}$-algebra, $\sigma : A \to A$ an $\mathbb{F}$-automorphism and $\mathfrak{v} : A[z;\sigma] \to \mathbb{F}^n[z]$ the canonical isomorphism associated to a fixed basis of A. A convolutional code $\mathcal{C}$ is said to be skew cyclic, see [2], if $\mathcal{C} = \mathfrak{v}(I)$ for some left ideal $I \leq A[z;\sigma] = R$. If, in addition, I is a direct summand as left ideal, i.e. $I = R(1-e) = \mathrm{Ann}_R^{\ell}(e)$ for some idempotent $e = \sum_{i=0}^{m} z^i e_i \in R$, then $\mathcal{C}$ is called an idempotent convolutional code, see [4, 5].

Let

$$E_k^c = \left[\sigma^{-j}(e_{j-i})\right]_{0\leq i,j\leq k} \in \mathcal{M}_{k+1}(A).$$

We introduce the kth cyclic column distance of $\mathcal{C}$ as

$$\delta_k^c = \min\left\{\mathrm{w}(a_0,\ldots,a_k) \mid (a_0,\ldots,a_k) \in \ker(\cdot E_l^c), a_0 \neq 0\right\}.$$

The main result of this talk is

Theorem. *Let A be an n-dimensional $\mathbb{F}$-algebra and let σ be an isometry on A with respect to a fixed basis. Let $R = A[z;\sigma]$ and $\mathfrak{v} : R \to \mathbb{F}^n[z]$. Let $\mathcal{C} = \mathfrak{v}(\mathrm{Ann}_R^{\ell}(e))$ for some idempotent $e = \sum_{i=0}^{m} z^i e_i \in R$. Let E_k^c and δ_k^c be as before. Then $\delta_k^c \leq \delta_{k+1}^c \leq \mathrm{d}_{\mathsf{free}}\mathcal{C}$. If $\delta_k^c = \delta_{k+m}^c$, then $\mathrm{d}_{\mathsf{free}}(\mathcal{C}) = \delta_k^c$.*

The theorem allows to compute the free distance by using the cyclic column distance sequence. No row distance is needed.

*Research partially supported by grant MTM2016-78364-P from Agencia Estatal de Investigación and from FEDER.

Keywords: Cyclic convolutional code, Free distance

References

[1] S. Estrada, J. R. García-Rozas, J. Peralta, and E. Sánchez-García. 2008. Group convolutional codes. *Advances in Mathematics of Communications* 2, 1 (2008), 83–94. https://doi.org/10.3934/amc.2008.2.83

[2] H. Gluesing-Luerssen and W. Schmale. 2004. On Cyclic Convolutional Codes. *Acta Applicandae Mathematicae* 82, 2 (2004), 183–237. https://doi.org/10.1023/B:ACAP.0000027534.61242.09

[3] J. Gómez-Torrecillas, F. J. Lobillo, and G. Navarro. 2016a. Convolutional codes with a matrix-algebra word ambient. *Advances in Mathematics of Communications* 10, 1 (2016), 29–43.

[4] J. Gómez-Torrecillas, F. J. Lobillo, and G. Navarro. 2017b. Ideal codes over separable ring extensions. *IEEE Transactions on Information Theory* 63, 5 (May 2017), 2796 – 2813. https://doi.org/10.1109/TIT.2017.2682856

[5] J. Gómez-Torrecillas, F. J. Lobillo, and G. Navarro. 2017a. Computing separability elements for the sentence-ambient algebra of split ideal codes. *Journal of Symbolic Computation* 83 (2017), 211–227.

[6] J. Gómez-Torrecillas, F. J. Lobillo, and G. Navarro. 2018. Computing free distances of idempotent convolutional codes. In *Proceedings of the 2018 ACM on International Symposium on Symbolic and Algebraic Computation (ISSAC '18)*. ACM, New York, NY, USA.

[7] R. Johannesson and K. Sh. Zigangirov. 1999. *Fundamentals of Convolutional Coding*. Wiley-IEEE Press. http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0780334833,miniSiteCd-IEEE2.html

[8] S. R. López-Permouth and S. Szabo. 2013. Convolutional codes with additional algebraic structure. *Journal of Pure and Applied Algebra* 217, 5 (2013), 958 – 972. https://doi.org/10.1016/j.jpaa.2012.09.017

[9] P. Piret. 1976. Structure and constructions of cyclic convolutional codes. *IEEE Transactions on Information Theory* 22, 2 (1976), 147–155. https://doi.org/10.1109/TIT.1976.1055531

[1]CITIC and Department of Algebra
University of Granada
E18071 Granada
Spain
gomezj@ugr.es
jlobillo@ugr.es

[2]CITIC and Department of Computer Science and Artificial Intelligence
University of Granada
E18071 Granada
Spain
gnavarro@ugr.es

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Generalized Hamming Weights of Binary Linear Codes

I. Márquez-Corbella[1], **E. Martínez-Moro**[2]

We can associate to each linear code $\mathcal{C}$ defined over a finite field the matroid $M[H]$ of its parity check matrix H. For any matroid M one can define its generalized Hamming weights which are the same as those of the code $\mathcal{C}$. In [1] the authors show that the generalized Hamming weights of a matroid are determined by the $\mathbb{N}$-graded Betti numbers of the Stanley-Reisner ring of the simplicial complex whose faces are the independent set of M. In this talk we go a step further. Our practical results indicate that the generalized Hamming weights of a linear code $\mathcal{C}$ can be obtained from the monomial ideal associated with a test-set for $\mathcal{C}$. Moreover, recall that in [2] we use the Gröbner representation of a linear code $\mathcal{C}$ to provide a test-set for $\mathcal{C}$.

Our results are still a work in progress, but its applications to Coding Theory and Cryptography are of great value.

Keywords: Generalized Hamming Weights, Test Set

References

[1] J. T. Johnsen and H. Verdure. *Hamming weights and Betti numbers of Stanley–Reisner rings associated to matroids*. Applicable Algebra in Engineering, Communication and Computing. 24(1): 73-93, 2013.

[2] I. Márquez-Corbella, E. Martínez-Moro and E. Suárez-Canedo. *On the ideal associated to a linear code*. Advances in Mathematics of Communications (AMC). 10(2): 229-254, 2016.

[1]Department of Mathematics, Statistic and O. Research
University of La Laguna, Spain
imarquec@ull.edu.es

[2]Mathematics Research Institute
University of Valladolid, Castilla, Spain
edgar.martinez@uva.es

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

On additive cyclic codes over chain rings

E. Martínez-Moro[1], **K. Otal**[2] and **F. Özbudak**[2]

Additive codes are a direct and useful generalization of linear codes, and they have applications in quantum error correcting codes. There are several studies using different approaches on them and their applications. On the other hand cyclic codes are one of the most attractive code families thanks to their rich algebraic structure and easy implementation properties. In this talk we will investigate the structure of Additive cyclic codes over finite (commutative) chain rings. When we focus on non-Galois finite commutative chain rings, we observe two different kinds of additivity. One of them is a natural generalization of precedding studies whereas the other one has some unusual properties especially while constructing dual codes. We interpret the reasons of such properties and illustrate our results giving concrete examples.

Keywords: Cyclic codes, Additive codes, Codes over rings

References

[1] EDGAR MARTÍNEZ-MORO,KAMIL OTAL,FERRUH ÖZBUDAK, Additive cyclic codes over finite commutative chain rings. *Discrete Mathematics* **(341-7)**, 1873–1884 (2018).

[1]Mathematics Research Institute
University of Valladolid, Castilla, Spain
edgar.martinez@uva.es

[2]Department of Mathematics and Institute of Applied Mathematics
Middle East Technical University, Ankara, Turkey
kamil.otal@gmail.com
ozbudak@metu.edu.tr

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

On varieties and codes defined by quadratic equations

Ruud Pellikaan[1]

We will review the work on algebraic geometry codes $\mathcal{C} = \mathcal{C}_L(\mathcal{X}, P, E)$ that have a unique representation $(\mathcal{X}, P, E)$, where $\mathcal{X}$ is an algebraic curve, P is an n-tuple of mutually distinct points and E is a divisor. See [1, 2, 4, 5]. As a consequence algebraic geometry codes with certain parameters are not secure for the code based McEliece public crypto system.

One of the key ingredients of these results is the classical fact that certain curves embedded in projective space are defined by quadratic equations. We consider generalizations to higher dimensional varieties [6] and order domains [3] and their corresponding codes.

Keywords: McEliece public crypto system, algebraic geometry codes

References

[1] A. Couvreur, I. Márquez-Corbella and R. Pellikaan, "Cryptanalysis of public-key cryptosystems that use subcodes of algebraic geometry codes". In *Coding theory and applications*, pp. 133—140, CIM Ser. Math. Sci., 3, Springer, Cham, 2015.

[2] A. Couvreur, I. Márquez-Corbella and R. Pellikaan, "Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes". IEEE Trans. Inform. Theory vol. 63, pp. 5404—5418, 2017.

[3] O. Geil and R. Pellikaan, "On the structure of order domains". Finite Fields Appl. vol. 8, pp. 369-–396, 2002.

[4] I. Márquez-Corbella, E. Martínez-Moro and R. Pellikaan, "On the unique representation of very strong algebraic geometry codes". Designs, Codes and Cryptography, vol.70, pp. 215—-230, 2014.

[5] I. Márquez-Corbella, E. Martínez-Moro, D. Ruano and R. Pellikaan, "Computational aspects of retrieving a representation of an algebraic geometry code", J. Symbolic Comput. vol. 64, pp. 67—87, 2014.

[6] D. Mumford, "Varieties defined by quadratic equations". In: *Questions on Algebraic Varieties*, C.I.M.E., III Ciclo, Varenna, 1969, pp. 29—100. Edizioni Cremonese, Rome 1970.

[1]Department of Mathematics and Computing Science
Technical University of Eindhoven
g.r.pellikaan@tue.nl

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Computer algebra tales on Goppa codes and McEliece cryptography

Narcís Sayols[1], **Sebastià Xambó-Descamps**[2]

Abstract

The fourty-year old McEliece public-key crypto-system is revisted with the help of recently developed resources: an improved Peterson-Gorenstein-Zierler decoder for alternant error-correcting codes; PyECC, a purely Python CAS; a package of PyECC functional utilities for the computations involved in defining, coding and decoding error-correcting codes; a web page with free-access to the materials generated by the project.

Keywords: Error-correcting codes, Classical Goppa codes, Post-quantum cryptography

One of the motivations for this work was the development of a purely Python CAS environment to cover the computational needs of a book such as [11] and the confidence gained in implementing decoders like the old Peterson-Gorenstein-Zierler [7, 3, 8], including the improvements presented in [2], and the computations for [5]. Further developments led to the CAS system that is now available at https://mat-web.upc.edu/people/sebastia.xambo/PyECC.htmlPyECC. The revisiting of the McEliece public-key crypto-system [4], which is based in a class of binary classical Goppa codes, was a further test of these tools. One friendly feature of the environment is the availability of the source code through Jupyter notebooks.*

The main purpose of our talk is to present an overview of those developments and will be structured as follows: A brief introduction to Goppa codes, particularly to their decoding (see [11, 2]); a detailed description of the McEliece system [4] and analysis of its security levels (see [1, 6]); a report on the structure and functionality of PyECC, with emphasis on the utilities needed for the implementation of that system.

References

[1] D. J. Bernstein, T. Lange, and C. Peters. Attacking and defending the McEliece cryptosystem. In PQCrypto '08: Proceedings of the 2nd International Workshop on Post-Quantum Cryptography, Lecture Notes in Computer Science, pages 31-46. Springer, 2008.

*http://jupyter.org/

[2] R. Farré, N. Sayols, and S. Xambó-Descamps. On the PGZ decoding algorithm for alternant codes. arXiv:1704.05259, 2017.

[3] D. Gorenstein and N. Zierler. A class of error-correcting codes in p^m symbols. *J. Soc. Ind. Appl. Math.* 9(2):207–214, 1961.

[4] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory, 1978. Jet Propulsion Laboratory DSN Progress Report 42-44. URL: `http://ipnpr.jpl.nasa.gov/progressreport2/42-44/44N.PDF`.

[5] S. Molina, N. Sayols, S. Xambó-Descamps. A bootstrap for the number of $\mathbb{F}_{q^m}$-rational points on a curve over $\mathbb{F}_q$. https://arxiv.org/pdf/1704.04661.pdfarXiv

[6] R. Niebuhr. *Attacking and Defending Code-based Cryptosystems*. https://d-nb.info/1106116461/34PhD thesis, 2012.

[7] W. W. Peterson. Encoding and error-correction procedures for the Bose-Chaudhuri codes. *IRE Transactions on Information Theory*, IT-6:459-470, 1960.

[8] W. W. Peterson and E. J. Weldon. *Error-Correcting codes*. MIT Press (2nd edition), 1972.

[9] J. Rué, S. Xambó-Descamps. Introducció matemàtica a la computació quàntica, *Butlletí de la Societat Catalana de Matemàtiques*, 28/2 (2013), 183-231.

[10] N. Sayols and S. Xambó-Descamp. A Python package for the construction, coding and decoding of error-correcting codes. https://mat-web.upc.edu/people/sebastia.xambo/PyECC.htmlPyECC, 2017.

[11] S. Xambó-Descamps. *Block error-correcting codes: a computational primer*. Univesitext. Springer, 2003.

[12] S. Xambó-Descamps, N. Sayols. Alternant codes and the McEliece cryptosystem. https://mat-web.upc.edu/people/sebastia.xambo/PyECC/s-CryptoLleida-7-10-2017.pdfpdf

[1]Departament d'Enginyeria de Sistemes, Automàtica i Informàtica Industrial
Universitat Politècnica de Catalunya
Jordi Girona, 1-3. K2M
narcissb@gmail.com

[2]Department de Matemàtiques
Universitat Politècnica de Catalunya
Jordi Girona, 1-3. Omega
sebastia.xambo@upc.edu

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

On the rank and kernel of new HFP-codes

E. Suárez-Canedo[1]

Hadamard codes with a subjacent group structure were principally studied from the point of view of cocyclic Hadamard matrices, Hadamard groups, and relative difference sets [1, 2, 3]. Propelinear codes, introduced in 1989 [4], also played an important role on the computation of Hadamard codes; indeed, they allow to classify Hadamard codes with a subjacent $\mathbb{Z}_2\mathbb{Z}_4$ and $\mathbb{Z}_2\mathbb{Z}_4Q_8$ group structure attending to the values of the rank and dimension of the kernel [5]. In [6] we define the family of HFP-codes and we prove the equivalences between them and Hadamard groups. Furthermore, constructions on HFP-codes with a subjacent $C_n \times Q_8$ and the dicyclic Q_{8n} group structure appear in [7, 8]. Now we classify new families of HFP-codes attending to the values of the rank and dimension of the kernel.

Keywords: Rank, kernel, HFP-codes.

References

[1] A. T. BUTSON, *Generalized Hadamard matrices,* Proc. Amer. Math. Soc., vol. 13, pp. 894-898, 1962.

[2] K. J. HORADAM, W. DE LAUNEY, *Generation of cocyclic Hadamard matrices,* Research Report No. 2, Mathematics Department, RMIT, March 1993.

[3] N. ITO, *On Hadamard groups,* J. Algebra 168, pp. 981-987, 1994.

[4] J. RIFÀ, J. M. BASART, L. HUGUET, *On Completely regular propelinear codes,* AAECC-6 Proc. of the 6th International Conference, on Appl. Algebra, Alg. Algorithms and Error-Correcting Codes, pp. 341-355, 1989.

[5] A. DEL RIO, J. RIFÀ, *Families of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes,* IEEE Trans. Inf. Theory, vol. 59, no. 8, pp. 5140–5151, 2013.

[6] J. RIFÀ, E. SUÁREZ-CANEDO, *About a class of Hadamard propelinear codes,* Electron. Note Discr. Math., vol. 46, pp. 289-296, 2014.

[7] J. RIFÀ, E. SUÁREZ-CANEDO, *Kronecker sums to construct Hadamard full propelinear codes,* Proc. of the 21-st Conference on applications of Computer Algebra (ACA15), Kalamata, Greece, pp. 135-139, 20-23 July 2015.

[8] J. RIFÀ, E. SUÁREZ-CANEDO, *Hadamard full propelinear codes of type Q; rank and kernel,* E. Des. Codes Cryptogr. (2017). https://doi.org/10.1007/s10623-017-0429-2

[1]Departament d'Enginyeria de la Informació i les Comunicacions
Universidad Autónoma de Barcelona, Spain
emiliosuarezcanedo@gmail.com

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Satisfiability modulo theory in finding the distance distribution of binary constrained arrays

Putranto Utomo[1]

Despite of the hardness of finding the distance distribution of a code, it is one of the important topics in coding theory. By knowing the distance distribution of a code, we can measure the performance of the code.

The development in satisfiability (SAT) theory has been improved recently. The modern SAT solver is performing much better in terms of computational efficiency. Unfortunately not all problems could easily be expressed as a propositional satisfiability problem, and some could lead to a very complex representation. This problem gives rise to a new topic called satisfiability modulo theory (SMT). The idea is to restrict the fragment of first order logic to some logical background theory. By doing this, it can solve more varied problems efficiently using the SAT solver engine.

The constrained system, especially the 1-D constraint, has proved to be beneficial for the magnetic tape recording. Recent developments in data recording technology allows us to store data in 2-D format, such as the holographic recording technology. However, in constrast with the constrained sequence, the theory is not yet well developed.

In this paper, we utilize the power of the SMT solver to find the distance distribution of 2-D binary constrained systems.

Keywords: Constrained arrays, Distance distribution

[1]Department of Mathematics and Computer Science
Eindhoven University of Technology
Posbus 513. 5600MB Eindhoven
p.h.utomo@tue.nl