Codes, Cryptology and Curves

Celebrating the influence of Ruud Pellikaan

March 7-8, 2019 @TUe, Eindhoven

Conference topics

Please join us in Eindhoven next March to celebrate Ruud's contribution to the fields of **Coding Theory, Cryptology and Curves (Algebraic Geometry)**. We encourage you to submit your contribution to this conference within those or related topics. A Special Issue of the journal **Designs, Codes and Cryptography** is being scheduled also on those topics in Honor of Ruud Pellikaan, please check the web page of the coference for further information.

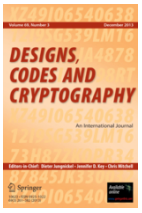
Scientific Committee

- **Peter Beelen** (Technical University of Denmark)
- **Olav Geil** (Aalborg University)
- **Relinde Jurrius** (The Netherlands Defence Academy)
- **Irene Márquez** (Universidad de La Laguna)
- **Edgar Martínez** (Universidad de Valladolid)
- **Tanja Lange** (Technische Universiteit Eindhoven)
- **Xin-Wen Wu** (Griffith University)

Organizing Committee

- **Tanja Lange** (Technische Universiteit Eindhoven)
- **Anita Klooster** (Technische Universiteit Eindhoven)
- **Relinde Jurrius** (The Netherlands Defence Academy)

Sponsors



TU/e Technische Universiteit Eindhoven University of Technology

Where innovation starts

Important dates

Deadline for abstract submission **Dec. 7, 2018**
Notification of Acceptance **Jan. 11, 2019**
Registration ends **Feb. 21, 2019**

More info:

http://www.singacom.uva.es/~edgar/CCC/

Codes, Cryptology and Curves

Celebrating the influence of R. Pellikaan

Preliminary Schedule

Thursday. March 7th, 2019

09:15–09:30	**Opening**	
09:30–10:30	**Inaugural lecture.**	Peter Beelen
10:30–11:00	**Break**	
11:00–11:30	**Classification of linear codes using canonical augmentation.**	I. Bouyukliev
11:30–12:00	**Characteristic vector and weight distribution of a linear code.**	S. Bouyuklieva
12:00–12:30	**Isometry-Dual Flags of AG Codes.**	M. Bras-Amorós
12:30–13:00	**Codes and Singularities.**	A. Campillo
13:00–14:00	**Lunch**	
14:00–14:30	**Improved constructions of quantum codes from the Hermitian curve.**	R.B. Christensen
14:30–15:00	**Surjective Encodings to (Hyper)Elliptic curves over Finite Fields**	M. Fadavi
15:00–15:30	**Computing Feng-Rao distances for AG codes.**	J.I. Farrán
15:30–16:00	**Break**	
16:00–16:30	**Quantum BCH and Reed-Solomon Entanglement-Assisted Codes.**	F.R. Fernandes Pereira
16:30–17:00	**Exploring the order domain conditions.**	O. Geil
14:30–15:00	**Codes, matroids, and their q-analogues**	R. Jurrius
	Dinner	

Friday. March 8th, 2019

09:30–10:00	**Construction of self-dual matrix codes.**	J.-L. Kim
10:00–10:30	**On the construction of high dimensional affine codes whose square code has designed minimum distance**	I. Márquez-Corbella
10:30–11:00	**Hamming and Simplex Codes for the Sum-Rank Metric**	U. Martínez-Peñas
11:00–11:30	**Break**	
11:30–12:00	**Vardøhus codes: Polar codes based on Castle curves.**	E. Martínez-Moro
12:00–12:30	**Twisted Hermitian codes in the McEliece cryptosystem.**	G.L. Matthews
12:30–13:00	**Locally Recoverable Algebraic Geometry codes.**	C. Munuera
13:00–14:00	**Lunch**	
14:00–14:30	**A new q-polynomial approach to cyclic and quasi-cyclic codes.**	F. Özdemir
14:30–15:00	**An extension of the Error Correcting Pairs algorithm**	I. Panaccione
15:00–15:30	**Reproducible Codes and Cryptographic Applications.**	P. Santini
15:30–16:00	**Farewell**	

Classification of linear codes using canonical augmentation

Iliya Bouyukliev

Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences, Veliko Tarnovo, Bulgaria

iliyab@math.bas.bg

Abstract. Classification of linear codes is an important task that affects the classification of other combinatorial structures such as finite geometries, combinatorial designs, etc. We propose a new algorithm for classification based on canonical augmentation.

The concept of canonical augmentation is introduced by Brandan McKey. It is a very powerful tool for classification of combinatorial structures. The canonical augmentation uses a canonical form to check the so called "parent test" and considers only objects that passed the test. Algorithms of this type have been used for classification of linear codes and before. The codes are represented by their generator matrix. To obtain generator matrices of all inequivalent codes of given length and dimension one begins from the empty set and constructs matrices column by column. In this way, to classify all linear $[n, k]$ codes, codes of the lengths $1, 2, \ldots, n$ and dimensions $\leq k$ are also constructed in the generation process.

We present a new algorithm of the same type but with a special modification which makes it much faster. Our algorithm also expands the matrices column by column but starts from the identity $k \times k$ matrix. So it constructs all inequivalent linear $[n, k]_q$ codes without getting codes of smaller dimensions. Restrictions on the dual distance, covering radius, minimal distance, etc. can be applied. The algorithm is included in the new version of the package Q-Extension. Using this software we classified and also proved the nonexistence of codes with given parameters over fields with 4, 5 and 7 elements. In this way, we solved some of the open problems presented in Code Tables: Bounds on the parameters of various types of codes: `http://www.codetables.de`.

The considered linear codes have parameters $[20+i, 13+i, 6]_4$, $[18+i, 7+i, 9]_4$, $[15+i, 4+i, 10]_5$, $[15+i, 5+i, 9]_5$, and $[14+i, 7+i, 7]_7$, $i \geq 0$. The result we obtain is that there are exactly two inequivalent $[20, 13, 6]_4$ codes, 10 inequivalent $[18, 7, 9]_4$ codes, 1628 inequivalent $[15, 4, 10]_5$ codes, and 4308 inequivalent $[15, 5, 9]_5$ codes. Further, we proved that codes with parameters $[21, 14, 6]_4$, $[19, 8, 9]_4$, $[16, 5, 10]_5$, $[16, 6, 9]_5$ and $[15, 8, 7]_7$ do not exist.

Joint work with Stefka Bouyuklieva (Faculty of Mathematics and Informatics, St. Cyril and St. Methodius University of Veliko Tarnovo, Bulgaria)
Partially funded by grant number DN 02/2/13.12.2016

Characteristic vector and weight distribution of a linear code

Stefka Bouyuklieva

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

stefka@ts.uni-vt.bg

Abstract. An algorithm for computing the weight distribution of a linear $[n, k]$ code over a finite field $\mathbb{F}_q$ is developed. The codes are represented by their characteristic vector with respect to a given generator matrix and a generator matrix of the k-dimensional simplex code $\mathcal{S}_k$.

We propose an algorithm for computing the weight distribution without listing all codewords. The linear codes here are represented by their characteristic vector χ. We obtain a vector whose coordinates are all non-zero weights in the code, by multiplying a special (recursively constructed) integer matrix by χ^{T}. The complexity for this multiplication is $O(kq^k)$, where k is the dimension of the considered code. The multiplication can be realized by a butterfly algorithm which is very fast in a parallel realization. The proposed algorithm is effective especially for codes with large length.

In the binary case, our approach is related to the Walsh-Hadamard transform, and so one can compute the weight distribution by using algorithms for fast Walsh transform which are easy for implementation. For codes over prime field with $p > 2$ elements we use an integer matrix of size $\theta(p, k) \times \theta(p, k)$ where $\theta(p, k) = \frac{p^k-1}{p-1}$. The weight distribution in this case can also be obtained by applying the generalized Walsh transform but then one has to use a $p^k \times p^k$ matrix. For codes over composite fields with $q = p^m$, $m > 1$, elements we use the trace map and take their images over the prime field $\mathbb{F}_p$.

We implemented the presented algorithm in a C/C++ program without special optimizations. Input data were randomly generated linear codes with lengths 300, 3000, 30000 and different dimensions over finite fields with 2, 3, 4, 5, and 7 elements. The results of our experiments show that the presented approach is faster for codes with large length. For example, calculating the weight distribution of codes with length 30000 with the presented algorithm is between 4 and 100 times faster (depending on the field) than the same calculation with the Magma software system.

Joint work with Iliya Bouyukliev and Paskal Piperkov (Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Veliko Tarnovo, Bulgaria) and Tatsuya Maruta (Department of Mathematical Sciences, Osaka Prefecture University, Sakai, Osaka 599-8531, Japan)

Partially funded by grant number DN 02/2/13.12.2016

Isometry-Dual Flags of AG Codes

Maria Bras-Amorós

Universitat Rovira i Virgili, Tarragona, Spain

maria.bras@urv.cat

Abstract. Consider a complete flag $\{0\} = C_0 < C_1 < \cdots < C_n = \mathbb{F}^n$ of one-point AG codes of length n over the field $\mathbb{F}$. A flag has the isometry-dual property if the given flag and the corresponding flag of dual codes are the same up to an invertible diagonal transformation. In [2] it is shown, for a curve of genus g, that a complete flag of one-point AG codes defined with a set of $n > 2g+2$ rational points is isometry-dual if and only if the code C_n in the flag has Goppa divisor of degree $n + 2g - 1$. Using a different proof, we extend this characterization to all sets of size $n \geq 2g + 2$. Moreover we show that this is best possible by giving examples of isometry-dual flags with $n = 2g + 1$ such that C_n has Goppa divisor of degree $n + 2g - 2$. We also prove a necessary condition, formulated in terms of maximum sparse ideals of a Weierstrass semigroup, under which a flag of punctured AG one-point codes inherits the isometry-dual property from the original unpunctured flag.

Let $\mathcal{X}$ be a smooth absolutely irreducible projective curve of genus g defined over the finite field $\mathbb{F}$. Let $P_1, \ldots, P_n$ and Q be distinct rational points on $\mathcal{X}$. For $D = P_1 + \cdots + P_n$, let $C_0 = C_L(D, -Q) = \{0\}$, and define a complete flag $\{0\} = C_0 < C_1 < \cdots < C_n = \mathbb{F}^n$ of one-point AG codes by choosing $m_1, \ldots, m_n$ minimal such that $C_i = C_L(D, m_i Q) \neq C_{i-1}$.

(Main Theorem) Let $m = m_n$. If the complete flag is isometry-dual then the following holds.

(a) If $m \geq 4g$, then $n = m - 2g + 1 \geq 2g + 1$.

(b) If $m = 4g - 1$, then either $n = 2g$ or $n = 2g + 1$.

(c) If $m \leq 4g - 2$, then $n \leq 2g$.

References

[1] Maria Bras-Amorós, Kwankyu Lee, and Albert Vico-Oton. New lower bounds on the generalized Hamming weights of AG codes. *IEEE Trans. Inform. Theory*, 60(10):5930–5937, 2014.

[2] Olav Geil, Carlos Munuera, Diego Ruano, and Fernando Torres. On the order bounds for one-point AG codes. *Adv. Math. Commun.*, 5(3):489–504, 2011.

[3] Carlos Munuera, and Ruud Pellikaan. Equality of geometric Goppa codes and equivalence of divisors. *Journal of Pure and Applied Algebra*, 90(3), 229–252, 1993.

Joint work with Euijin Hong (University of Illinois at Urbana-Champaign, USA) and Iwan Duursma (University of Illinois at Urbana-Champaign, USA)
Partially funded by 2017 SGR 00705, TIN2016-80250-R, NSF CCF-1618189

Codes and Singularities

Antonio Campillo

Mathematics Research Institute, IMUVA
University of Valladolid, Spain

campillo@agt.uva.es

For a given algebraic variety $\mathcal{X}$ over a finite field $\mathbb{F}$, a finite dimensional linear subspace L of $\mathbb{F}(\mathcal{X})$ and a finite set of rational P points of $\mathcal{X}$, the associated Evaluation Code $C = C(\mathcal{X}, L, P)$ is the image of the evaluation map of functions in L at the points in P. Algebraic geometry methods are classically available for studying those codes from the involved geometrical features. Their study becames specially succesful when the geometry of the data $\mathcal{X}, L, P$ allow to estimate the main parameters and give explicit expressions for their coding and decoding. This happens when $\mathcal{X}$ is a smooth projective curve or a toric variety among others.

Singularities are especially useful for some purposes. For instance, when the smooth curve $\mathcal{X}$ is the normalization of a singular proyective plane curve $\mathcal{Y}$, the parameters, coding and decoding of evaluation codes can be explicitly described by means of the classical Brill-Noether and Castelnuovo results. However, the evaluation is made on points P of $\mathcal{X}$ which are non singular points.

When the evaluation is made on singular points of algebraic varieties, the situation becomes even much more difficult. In fact, the complete information of the evaluation of a function at singular points includes an appropriated part of its Taylor expansion, which it is more than its single point evaluation. The main difficulty is that there are not general methods for estimating the minimal distance of the code, so one needs to find objects with really special geometric features.

Such special situation occurs when the set P is the singular subscheme of a foliations which isolated singularities of arbitrary degree r foliations by curves over the n-dimensional projective scheme over $\mathbb{F}$. Results by Campillo-Olivares show that, when $r > 2$, the foliation is determined by their singular subscheme and that P have very special geometric properties rather similar to those of the whole projective spaces. It allows to construct interesting examples of such P for many values of r inside a projective space of characteristic p, for many values of r and p. The evaluation codes of complete evaluation of polynomials of such P can be explicitly described and their parametes can be estimated. These result extend those proved by Campillo-Farran-Pisabarro for the special case of $n = 2$ and the singularities P reduced (say, counted one each of them).

Joint work with J. I. Farrán (Mathematics Research Institute, IMUVA, University of Valladolid)

Improved constructions of quantum codes from the Hermitian curve

René Bødker Christensen

Aalborg University

rene@math.aau.dk

Abstract. Ruud Pellikaan and coauthors in *Handbook of Coding Theory* introduced the order bound for a family of codes described in terms of their parity check matrices. This bound furthermore implies a method for improving the parameters. The bound was later enhanced to also work for primary codes. In this work, we employ the above methods to construct improved quantum codes from the Hermitian curve.

The CSS construction translates a pair of nested linear codes $C_2 \subsetneq C_1 \subseteq \mathbb{F}_q^n$ into a quantum code with parameters $[[n, k, d_z/d_x]]_q$ where d_z is the minimum distance related to phase-shift errors and d_x is the minimum distance related to bit-flip errors. Here, $k = \dim C_1 - \dim C_2$ is the codimension of C_1 and C_2, and $d_z = d(C_1, C_2)$ and $d_x = d(C_1^\perp, C_2^\perp)$ are given by the relative distances of the codes and their duals. When $d_z \neq d_x$, we speak of asymmetric quantum codes. In some situations, however, we are not interested in distinguishing between the two types of errors. In this case, we let $d = \min\{d_z, d_x\}$, and write the corresponding code parameters as $[[n, k, d]]_q$. Given appropriate codes $C_2 = C_1^\perp \subsetneq C_1 \subsetneq C_0$, the Steane enlargement method produces an $[[n, k, \geq d]]_q$ quantum code where $k = 2\dim C_1 - n + (\dim C_0 - \dim C_1)$ and $d = \min\{d(C_1), (1 + \frac{1}{q})d(C_0)\}$.

In this work, we apply the CSS construction and Steane's enlargement to codes constructed from the Hermitian curve. For the CSS construction we consider two cases. Namely, Case 1 where C_1 is an order bound improved code, and C_2 is the dual of an order bound improved code; and Case 2 where both C_1 and C_2 are ordinary one-point algebraic geometric codes, but at least one of the relative distances exceeds the corresponding non-relative one. In Case 3 we apply Steane's enlargement to order bound improved codes C_1 and C_0 (where of course $C_1^\perp \subsetneq C_1$). Doing this, we obtain very good quantum codes. Closed formula expressions for and estimates on the parameters of the codes are provided along with tables demonstrating the advantage of the construction. Here, we list only a few samples of code parameters.

Case 1	**Case 2**	**Case 3**
$[[27, 2, 23/2]]_9$	$[[27, 1, 20/4]]_9$	$[[27, 11, 7]]_9$
$[[27, 6, 12/6]]_9$	$[[64, 1, 46/9]]_{16}$	$[[64, 60, 3]]_{16}$
$[[27, 11, 11/3]]_9$	$[[64, 4, 49/4]]_{16}$	$[[64, 36, 10]]_{16}$
$[[64, 18, 36/4]]_{16}$	$[[125, 2, 86/20]]_{25}$	$[[125, 91, 11]]_{25}$
$[[125, 80, 28/5]]_{25}$	$[[125, 3, 91/15]]_{25}$	$[[125, 117, 4]]_{25}$

Table 1: Sample parameters for quantum codes in each of the cases 1, 2, and 3.

Joint work with Olav Geil (Aalborg University)

Surjective Encodings to (Hyper)Elliptic curves over Finite Fields

Mojtaba Fadavi, Reza Rezaeian Farashahi

Isfahan University of Technology

mfadavi88@gmail.com, farashahi@cc.iut.ac.ir

In this talk, we will propose a general method for constructing surjective encoding function to varieties with special features. Let H be a hyperelliptic curve of genus $g \geq 1$ over an odd characteristic finite field $\mathbb{F}_q$ given by the equation $y^2 = f(x)$. Let $\mathcal{J}$ be the Jacobian variety of H over $\mathbb{F}_q$. We will introduce different deterministic surjective encoding algorithms from $\{0,1\} \times \mathbb{F}_q$ to $H(\mathbb{F}_q)$, where $g = 1, 2$. In particular, if H is an elliptic curve over the finite field $\mathbb{F}_q$ and $\mathfrak{s} : \{0,1\} \times \mathbb{F}_q \to H(\mathbb{F}_q)$ is our proposed surjective encoding function. Then, the random variable $\chi : E(\mathbb{F}_q) \to \mathbb{N}$, where $\chi(P) = \#\mathfrak{s}^{-1}(P)$ for any $P \in E(\mathbb{F}_q)$, has a smaller mean and variance in comparison to the other known encoding functions. In addition, we construct a surjective encoding function from $\{0,1\}^2 \times (\mathbb{F}_q)^2$ to the Jacobian variety of genus 2 hyperelliptic curve H. The idea is extended to higher genus hyperelliptic curves to construct a surjective encoding function $\mathfrak{s} : \{0,1\}^g \times (\mathbb{F}_q)^g \to \mathcal{J}(\mathbb{F}_q)$. The rejection sampling technique may be used to provide a uniform distribution on $\{0,1\}^g \times (\mathbb{F}_q)^g$ from the uniform distribution on $J(\mathbb{F}_q)$.

Let $\psi : \mathbb{F}_q \to H(\mathbb{F}_q)$ be an encoding and consider the function $\mathfrak{f}^{\otimes s} : (\mathbb{F}_q)^s \to \mathcal{J}(\mathbb{F}_q)$ where

$$\mathfrak{f}^{\otimes s}(u_1, \ldots, u_s) = \psi(u_1) + \ldots + \psi(u_s).$$

Farashahi et al. in [1] proved that for $s \geq g + 1$, the distribution defined by $\mathfrak{f}^{\otimes s}$ on $J(\mathbb{F}_q)$ is statistically indistinguishable from the uniform distribution if the encoding ψ is well-distributed. For instance, for genus 2 hyperelliptic curves $\mathfrak{f}^{\otimes 3}$ is well-distributed. They also showed that if ψ is a well-distributed encoding, then for $s > 2g$, all divisors $D \in J(\mathbb{F}_q)$ have the same number of pre-images by $\mathfrak{f}^{\otimes s}$ up to negligible deviation, so $\mathfrak{f}^{\otimes s}$ is surjective.

From the surjective encoding function $\mathfrak{s}$, we propose a function $\mathfrak{g}^{\otimes s} : \{0,1\}^g \times (\mathbb{F}_q)^s \to \mathcal{J}(\mathbb{F}_q)$ where

$$\mathfrak{g}^{\otimes s}(i, u_1, \ldots, u_s) = \mathfrak{s}(i, u_1, \ldots, u_g) + \psi(u_{g+1}) + \ldots + \psi(u_s),$$

and $s \geq g + 1$. It can be shown that the distribution defined by $\mathfrak{g}^{\otimes s}$ on $J(\mathbb{F}_q)$ is statistically indistinguishable from the uniform distribution assuming ψ is well-distributed.

References

[1] Farashahi, R. R., Fouque, P.-A., Shparlinski, I., Tibouchi, T., Voloch F.: Indifferentiable deterministic hashing to elliptic and hyperelliptic curves. Mathematics of Computation, volume 82, pp. 491–512 (2013)

Computing Feng-Rao distances for AG codes

José I. Farrán

Universidad de Valladolid

jifarran@eii.uva.es

Abstract. The weight hierarchy of one-point algebraic geometry codes can be estimated by the generalised order bounds, also called generalised Feng-Rao distances. This talk shows a general view of the main results obtained during the last years, with special focus on the asymptotic behaviour of the order bounds and some particular cases of Weierstrass semigroups.

The order bound distance was introduced by Feng and Rao for the decoding of one-point algebraic geometry codes (AG codes in short) up to half the Feng-Rao distance. In particular, such distance is a lower bound for the minimum distance of these codes. The computation of the Feng-Rao distance involves combinatorics on a certain Weierstrass semigroup of the underlying curve. The first interesting results were given by Kirfel and Pellikaan for telescopic semigroups. Other results were obtained later for symmetric, acute and Arf semigroups, among others.

On the other hand, the generalised order bounds were proven by Heijnen and Pellikaan to be also lower bounds for the generalised Hamming weights. These generalised Feng-Rao distances are far harder to deal, and very few results have been obtained in this direction. First Farrán and Munuera proved that they have a similar Goppa-like lower bound, for some constants that were called Feng-Rao numbers. After this work some papers were addressed to compute the Feng-Rao numbers for semigroups with two generators, telescopic semigroups, semigroups generated by intervals, and inductive semigroups. For Arf semigroups, it is possible to compute precisely the second Feng-Rao distance in the whole range, generalising the results for the classical Feng-Rao distance.

Joint work with Antonio Campillo (Universidad de Valladolid), Manuel Delgado (Universidade do Porto), Pedro A. García-Sánchez (Universidad de Granada), David Llena (Universidad de Almería), Carlos Munuera (Universidad de Valladolid), and Benjamín A. Heredia (Universidade de Lisboa)

Partially funded by MTM2015-65764-C3-1-P (MINECO/FEDER)

Quantum BCH and Reed-Solomon Entanglement-Assisted Codes

Francisco Revson Fernandes Pereira

Department of Mathematics and Computing Science, Eindhoven University of Technology,
P.O. Box 513, 5600 MB Eindhoven, The Netherlands

f.r.fernandes.pereira@tue.nl

Abstract. Quantum error correcting codes play the role of suppressing noise and decoherence in quantum systems by introducing redundancy. Some resources can be used to improve the parameters of these codes, e.g., entanglement. Such codes are called entanglement-assisted quantum (QUENTA) codes. In this paper, it is shown a general method to construct QUENTA codes via cyclic codes. Afterwards, the method is applied to BCH and Reed-Solomon codes, resulting in new families of QUENTA codes, where one of them has maximal entanglement and maximal distance separability.

It is generally accepted that the prospect of practical large-scale quantum computers and the use of quantum communication are only possible with the implementation of quantum error correcting codes. Quantum error correcting codes play the role of suppressing noise and decoherence by introducing redundancy. The capability of correcting errors of such codes can be improved if it is possible to have pre-shared entanglement states. This class of codes is known as Entanglement-Assisted Quantum (QUENTA) codes. Additionally, it is possible to show that they can achieve the hashing bound and violate the quantum Hamming bound. The stabilizer formalism of QUENTA codes was created by Brun *et al.* in 2014, where they showed that QUENTA codes paradigm does not require dual-containing constraint as standard quantum error-correcting code does.

After this paper of Brun *et al.*, many works have focused on the construction of QUENTA codes based on classical linear codes. However, the analysis of q-ary QUENTA codes was taken into account only recently. The majority of them utilize constacyclic codes or negacyclic codes as the classical counterpart. However, little attention has been paid to maximal entanglement QUENTA codes. Using the well-known class of cyclic code, we describe a method to construct QUENTA codes that have maximal entanglement. This results in quantum codes with better parameters when compared with the ones in the literature and codes that are good candidates to achieve the hash bound.

First of all, we show that amount of entanglement in a QUENTA code is related to the intersection of the two codes used in the construction. With this characterization and after showing that intersecting two cyclic codes gives us another cyclic code, a few families of QUENTA codes are constructed via BCH and Reed-Solomon codes. In addition, it is showed that one of the families has maximal entanglement and maximal distance separable. In the end, some numerical examples are given and comparisons with the best quantum codes in the literature are done.

Joint work with Ruud Pellikaan (Eindhoven University of Technology, The Netherlands)
Partially funded by the Brazilian funding agencies CNPq (201223/2018-0)

Exploring the order domain conditions

Olav Geil

Aalborg University

olav@math.aau.dk

Abstract. Ruud Pellikaan in *On the Existence of Order Functions* (and independently Shinji Miura) showed how to represent any union $\cup_{m=0}^{\infty}\mathcal{L}(mQ)$ as a quotient ring $\mathbb{F}[X_1,\ldots,X_m]/I$, where m is the number of generators of the corresponding Weierstrass semigroup, and where I satisfies some simple conditions. Here, Q is a rational place. Using this description we conduct computer searches for curves with given Weierstrass semigroups and with many rational places.

Consider an algebraic function field over K of transcendence degree 1. Let Q be a rational place and denote by m the minimal number of generators of the corresponding Weierstrass semigroup $\Gamma = \langle w_1,\ldots,w_m\rangle$. Then there exists an ideal $I \subseteq K[X_1,\ldots,X_m]$ such that $\cup_{m=0}^{\infty}\mathcal{L}(mQ) \simeq K[X_1,\ldots,X_m]/I$ and such that I satisfies

1. There exists a Gröbner basis $\{G_1,\ldots,G_s\}$ of I such that each polynomial has exactly two monomials of highest weight in its support. Here, the weight is defined by $w(X_1^{i_1}\cdots X_m^{i_m}) = w_1i_1+\cdots+w_mi_m$.
2. The set $\{M \mid M \text{ is a monomial, } M \notin \mathrm{lm}(I)\}$ does not possess two monomials of the same weight.

In the other direction any such description defines a union of $\mathcal{L}$-spaces as above or a subalgebra thereof. If (and only if) the curve is non-singular (which is checked by considering the derivatives of the generators) then equality holds. In such a description there is a one-to-one correspondence between the rational places different from Q and the affine roots of I.

Using a computer program we investigate for different semigroups with not too many gaps (i.e. small genus) what is the maximal number of rational places.

It is interesting to note that the Goppa bound works for the corresponding evaluation codes also if the generating set $\{G_1,\ldots,G_s\}$ is not a Gröbner basis. This suggests to speed up the program by avoiding the test, rephrasing of course the problem slightly.

The search can be enhanced to investigate similar questions for order domains of higher transcendence degree over a finite field. Here, we do not have the Hasse-Weil bound for comparison, but can instead employ the footprint bound from Gröbner basis theory.

Joint work with Kasper Halbak Christensen (Aalborg University)

Codes, matroids, and their q-analogues

Relinde Jurrius

The Netherlands Defence Academy

rpmj.jurrius@mindef.nl

Abstract. Over the last decades, many have studied the relation between linear codes and matroids. One link between the two objects goes via the extended weight enumerator of a code and the Tutte polynomial of the corresponding matroid. The recent interest in network coding leads to the question if this link has a q-analogue. In this talk I will report on the ongoing quest for the q-analogues of matroids, the Tutte polynomial, and their link with network coding.

Greene was the first to notice that the weight enumerator of a linear code is defined by the Tutte polynomial of the matroid corresponding to the code. In my PhD thesis under supervision of Ruud Pellikaan, I studied a generalisation of the weight enumerator, the *extended weight enumerator*. This polynomial defines the Tutte polynomial of the corresponding matroid, leading to a two-way equivalence between the two polynomials.

In the last decade the focus in coding theory shifted to network coding, where communication is not over a single channel but over a network. Accelerated by the COST action "Random network coding and designs over $GF(q)$", codes with respect to the rank metric attracted a lot of attention. One can see these codes as a q-analogue of codes with respect to the Hamming metric. A q-analogue is, roughly speaking, what happens if we generalise from sets to subspaces.

Ruud and I started working on the q-analogue of the weight enumerator and its generalisations. The first results on the *rank weight enumerator* went very smoothly, and it seemed that a lot of results in classical coding theory were just waiting for a straightforward q-analogue. Quit soon we started fantasising about the q-analogues of matroids, the Tutte polynomial, and their link with the rank weight enumerator.

Unfortunately, q-analogues turned out not to be as straightforward as we initially thought. With this talk I hope to argue that this makes the topic in fact much more interesting. I will describe how we came to a sensible definition of the q-analogue of a matroid, how this links to earlier work of Henry Crapo, and what the next open problems in this subject are.

Joint work with Ruud Pellikaan (Eindhoven University of Technology) and Henry Crapo (Les Moutons Matheux, La Vaquerie).

Construction of self-dual matrix codes

Jon-Lark Kim

Sogang University

jlkim@sogang.ac.kr

Abstract. Matrix codes over a finite field $\mathbb{F}_q$ are linear codes defined as subspaces of the vector space of $m \times n$ matrices over $\mathbb{F}_q$. They are closely related to rank metric linear codes. In this paper, we show how to obtain self-dual matrix codes from a self-dual matrix code of smaller size using a method we call the building-up construction. We show that every self-dual matrix code can be constructed using this building-up construction. Using this, we classify, that is, we find a complete set of representatives for the equivalence classes of self-dual matrix codes of small sizes. In particular we have classifications for self-dual matrix codes of sizes 2×4, 2×5 over $\mathbb{F}_2$, of size 2×3, 2×4 over $\mathbb{F}_4$, of size 2×2, 2×3 over $\mathbb{F}_8$, and of size 2×2, 2×3 over $\mathbb{F}_{13}$, all of which have been left open from K. Morrison's classification.

We can define a generator matrix for matrix codes using the correspondence with linear block codes. Using this definition, we introduce the *building-up construction of self-dual matrix codes* and show that every self-dual matrix code is obtained this way. Thus, using this construction and the notion of equivalence for matrix codes given in [2], we have a new technique to classify self-dual matrix codes, different from what was done in [2] and add new results, as well. The classification is summarized on the table below.

Table 1: The number of inequivalent self-dual matrix codes of small sizes over the finite field $\mathbb{F}_q$ where $q = 2, 3, 4, 5, 8, 9, 13$. Values marked with $*$ and $**$ are the same values given in [2] and [1], respectively. Values in bold are new classifications which were previously unknown.

Size	$\mathbb{F}_2$	$\mathbb{F}_3$	$\mathbb{F}_4$	$\mathbb{F}_5$	$\mathbb{F}_8$	$\mathbb{F}_9$	$\mathbb{F}_{13}$
2×2	2^*	1^*	3^*	2^*	**5**	2^{**}	**2**
2×3	5^*		**5**	7^*	**5**	7^{**}	**7**
2×4	**20**	13^*	**36**	24^*			
2×5	**22**						
4×3	**442**						

References

[1] K. Morrison. *Equivalence and duality for rank-metric and matrix codes.* The University of Nebraska-Lincoln, 2012.

[2] K. Morrison. An enumeration of the equivalence classes of self-dual matrix codes. *Advances in Mathematics of Communications*, 9(4):415 – 436, May 2015.

Joint work with Lucky Galvez (Sogang University)
J.-L. Kim was supported by Basic Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF- 2016R1D1A1B03933259)

On the construction of high dimensional affine codes whose square code has designed minimum distance

Ignacio García-Marco[1], Irene Márquez-Corbella[1] and Diego Ruano[2]

[1]Universidad de La Laguna and [2]Universidad de Valladolid

iggarcia@ull.es, imarquec@ull.es, diego.ruano@uva.es

Abstract. Given a linear code C, we define its square code C^{*2} as the span of all component-wise products of two elements of C. Our purpose with this work is to answer the following question: which families of affine codes have simultaneously high dimension and high minimum distance of C^{*2}? This work is a tribute to the work of Pellikaan whose contributions to the notion of component-wise products of codes are beyond question. Indeed, he introduced this notion in coding theory for decoding in the 90's.

Component-wise products of linear codes have been used to decode linear codes and to attack some variants of the McEliece cryptosystem, but it has also been used for secure multiparty computation that studies the case where a group of persons, each holding an input for a function, wants to compute the output of the function, without having each individual reveal his or her input to the other parties. Multi-party computation is possible from secret sharing schemes, and hence from coding theory. One of the best known protocols is MiniMac, which uses a linear binary code C, which should prevent cheating. The probability that a cheating player is caught depends on the minimum distance of the square of a linear code, denoted by $d(C^{*2})$, meaning that a high distance on the square will give a higher security. Simultaneously, it would be beneficial to have a high dimension on the code C to reduce the communication cost. Additionally, if the minimum distance of the dual of C and $d(C^{*2}) \geq t+2$, then C can be used to construct a t-strongly multiplicative secret sharing scheme (SSS). Such a SSS is enough to construct an information theoretic secure secret sharing scheme if at most t players are corrupted. These applications show the importance of finding linear codes, where both the code itself and the square has good parameters. Or maybe, to be more specific, that $\dim(C)$, $d(C^{\perp})$, and $d(C^{*2})$ are simultaneously high relative to the length of the codes.

Given $A \subset \mathbb{N}^n$, the affine code C_A is the image of the morphism that evaluates the polynomials in $\mathbb{F}_q[A] = \mathbb{F}_q[\mathbf{x}^\alpha \,|\, \alpha \in A]$ in all the points of $\mathbb{F}_q^n$. Given $d \in \mathbb{Z}^+$, in this work we propose a method to obtain an affine code C satisfying that $d(C^{*2}) \geq d$ and such that $\dim(C)$ is considerably high. Our method receives as input a value $d \in \mathbb{Z}^+$ and starts by considering an affine code C_B such that $d(C_B) \geq d$, say for example, a hyperbolic code with minimum distance at least d. Then, by means of convexity arguments, we build a set $A \subset \mathbb{N}^m$ such that the Minkowski sum $A + A$ is contained in B. The latter condition implies that $d(C_A^{*2}) \geq d(B) \geq d$. Remarkably, in many cases our approach builds a code C such that $d(C^{*2}) \geq d$ and $\dim(C) \geq \dim(D)$ for any code D from the family of weighted Reed-Muller and hyperbolic codes satisfying that $d(D^{*2}) \geq d$.

Partially funded by the Spanish Ministry of Economy/FEDER: grants MTM2015-65764-C3-2-P, MTM2015-69138-REDT, MTM2016-78881-P, MTM2016-80659-P and RYC-2016-20208 (AEI/FSE/UE).

Vardøhus codes: Polar codes based on Castle curves

Edgar Martínez-Moro

Institute of Mathematics
University of Valladolid

edgar.martinez@uva.es

Abstract. In this contribution we explore the idea of employing algebraic geometric codes to produce kernels of polar codes. The idea is not new and it can be find in [1] and the references therein. Castle curves and Castle codes [2] seem to be well suited for the desing of such kernels.

Based on the definition of additive channels over the alphabeth $\mathbb{F}_q$ (the finite field of $q = p^r$ elements with p a prime number) we analyze the properties of polar codes whose kernel is given by codes over pointed curves $(\mathcal{X}, Q)$. We defined the concept of extrict decreasing code that allows us to control some parameters of the code. It turns that for the case of Castle curves the kernel associate to its dual is isometric to a extrict decreasing code. This fact allows us to control new kernels obtained by punturing the code.

References

[1] Anderson, S. E., & Matthews, G. L. (2014). Exponents of polar codes using algebraic geometric code kernels. Designs, codes and cryptography, 73(2), 699–717.

[2] C. Munuera, A. Sepulveda, F. Torres (2008), Algebraic geometry codes from Castle curves, in: A. Barbero (Ed.), Coding Theory and Applications, in: Lecture Notes in Comput. Sci., vol. 5228, Springer-Verlag, Berlin, pp. 117–127.

Joint work with Eduardo Camps and Eliseo Sarmiento (IPN, México)
Partially funded by Spanish Research Council grant MTM2015-65764-C3-1-P and CONACYT (México)

Hamming and Simplex Codes for the Sum-Rank Metric

Umberto Martínez-Peñas

Dept. of Electrical & Computer Engineering, University of Toronto

umberto@ece.utoronto.ca

Abstract. Sum-rank Hamming codes, with minimum sum-rank distance 3, are introduced, together with their duals, called sum-rank simplex codes. It is shown that sum-rank isometric classes of sum-rank Hamming codes are in bijective correspondence with maximum-size partial spreads. It is also shown that sum-rank Hamming codes are perfect codes for the sum-rank metric. This is in contrast with the rank-metric case, where no non-trivial perfect codes exist. Finally, bounds on the minimum sum-rank distance of sum-rank simplex codes are given based on known upper bounds on the size of partial spreads.

Let $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ be an extension of finite fields. For numbers ℓ, N and $n = \ell N$, we may define the sum-rank weight of $\mathbf{c} = (\mathbf{c}^{(1)}, \mathbf{c}^{(2)}, \dots, \mathbf{c}^{(\ell)}) \in \mathbb{F}_{q^m}^n$ by $\mathrm{wt}_{SR}(\mathbf{c}) = \sum_{i=1}^{\ell} \mathrm{wt}_R(\mathbf{c}^{(i)})$, where wt_R denotes rank weight. The sum-rank metric is then defined by $\mathrm{d}_{SR}(\mathbf{c}, \mathbf{d}) = \mathrm{wt}_{SR}(\mathbf{c} - \mathbf{d})$. This metric measures the error-correction capability of codes in multishot network coding, and gives an estimate on the global erasure correction capability of locally repairable codes. Furthermore, it recovers the Hamming metric when $N = 1$ and it recovers the rank metric when $\ell = 1$.

For $m = 1$ and fixed N, we define *sum-rank Hamming codes* as linear codes $\mathcal{C} \subseteq \mathbb{F}_q^n$ with minimum sum-rank distance $\mathrm{d}_{SR}(\mathcal{C}) = 3$ and maximum possible length $n = \ell N$. Such codes are given by parity check matrices of the form

$$H = (H_1, H_2, \dots, H_\ell) \in \mathbb{F}_q^{r \times n},$$

where $\mathcal{H}_i \cap \mathcal{H}_j = \{\mathbf{0}\}$ if $i \neq j$, being $\mathcal{H}_i \subseteq \mathbb{F}_q^r$ the column space of $H_i \in \mathbb{F}_q^{r \times N}$. Thus $\{\mathcal{H}_1, \mathcal{H}_2, \dots, \mathcal{H}_\ell\}$ forms a maximum-size partial N-spread in $\mathbb{F}_q^r$. Note that classical Hamming codes are recovered by choosing $N = 1$, in which case $\{\mathcal{H}_1, \mathcal{H}_2, \dots, \mathcal{H}_\ell\}$ forms the $(r-1)$-dimensional projective space.

If N divides r, it was shown by Beutelspacher that a maximum-size partial spread has size

$$\ell = \frac{q^r - 1}{q^N - 1}.$$

In such a case, sum-rank Hamming codes have length $n = N\frac{q^r-1}{q^N-1}$, dimension $k = N\frac{q^r-1}{q^N-1} - r$ and minimum sum-rank distance 3. By computing the size of a ball of sum-rank radius 1, we may check that these sum-rank Hamming codes are *perfect codes* for the sum-rank metric.

Finally, define s*um-rank simplex codes* as duals of sum-rank Hamming codes. It can be shown that the non-zero components of their codewords correspond to certain (possibly not maximum-size) partial spreads. By applying known bounds on the maximum size of a partial spread, the minimum sum-rank distance of sum-rank simplex codes can be lower bounded.

Funded by The Independent Research Fund Denmark (Grant No. DFF-7027-00053B).

Twisted Hermitian codes in the McEliece cryptosystem

Gretchen L. Matthews

Virginia Tech

gmatthews@vt.edu

Abstract. We define twisted Hermitian codes based on one-point Hermitian codes and strongly inspired by the twisted Reed-Solomon codes described by Beelen, Puchinger, and Nielsen. We demonstrate that these new codes can have high-dimensional Schur squares, and we identify a subfamily of multi-twisted Hermitian codes that achieves a Schur square dimension close to that of a random linear code. Codes of this subfamily are resistant to Schur square distinguishing when implemented within the McEliece cryptosystem where as one-point Hermitian codes are not, as recently demonstrated by Couvreur, Márquez-Corbella, and Pellikaan.

Many variants of the McEliece cryptosystem have been introduced which use different families of linear codes than the original Goppa codes. Additional structure can lead to a reduction in key size but often at the cost of introducing vulnerabilities that allow an attacker to extract identifying characteristics of the underlying code from the public-key matrix; see, for instance, the recent work by Couvreur, Márquez-Corbella, and Pellikaan on algebraic geometry codes. Schur square distinguishing is effective against one-point Hermitian codes by exploiting the low Schur square dimension of one-point Hermitian codes. To retain many desirable qualities of one-point Hermitian codes while fortifying a Hermitian-based McEliece variant, we introduce a new family of codes called twisted Hermitian codes. These codes are based on one-point Hermitian codes and strongly inspired by the twisted Reed-Solomon code described by Beelen, Puchinger, and Nielson. Hermitian codes have an advantage over Reed-Solomon codes in that longer codes can be obtained over smaller alphabets; for instance, to obtain a Reed-Solomon code of length 4096, one must use an alphabet of size 4096 whereas a Hermitian code of the same length only requires an alphabet size of 256. Twisted Hermitian codes can have a large Schur square, which safeguards against the efficacy of Schur square distinguishing attack. We construct a subfamily of multi-twisted Hermitian codes that achieves a Schur square dimension approaching that of a random linear code. The security of the new code against Schur square distinguishing may be interesting for code-based cryptography.

Joint work with Austin Allen (Carnegie Mellon University), Keller Blackwell (University of South Florida), Olivia Fiol (Vassar College), Rutuja Kshirsagar (Virginia Tech), Bethany Matsick (Liberty University), and Zoe Nelson (Oglethorpe University).
Partially funded by NSF DMS-1403062, -1547399, and -1855136.

Locally Recoverable Algebraic Geometry codes

Carlos Munuera

Universidad de Valladolid

cmunuera@arq.uva.es

Abstract. A Locally Recoverable code is an error-correcting code such that any erasure in a single coordinate of a codeword can be recovered from a small subset of other coordinates. We study Locally Recoverable Algebraic Geometry codes arising from certain curves defined by equations with separated variables. The recovery of erasures is obtained by means of Lagrangian interpolation in general, and simply by one addition in some particular cases.

Locally Recoverable (LRC) codes were introduced motivated by the use of coding techniques applied to distributed and cloud storage systems. Roughly speaking, local recovery techniques enable us to repair lost encoded data by a local procedure, that is by making use of small amount of data instead of all information contained in a codeword.

Let $\mathcal{C}$ be a linear code of length n, dimension k and minimum distance d over the field $\mathbb{F}_q$. A coordinate $i \in \{1, \ldots, n\}$ is *locally recoverable with locality* r if there is a *recovery set* $R_i \subseteq \{1, \ldots, n\}$ with $i \notin R_i$ and $\#R_i = r$, such that for any two codewords $\mathbf{u}, \mathbf{v} \in \mathcal{C}$, whenever $\pi_i(\mathbf{u}) = \pi_i(\mathbf{v})$ we have $u_i = v_i$, where π_i is the projection on the coordinates of R_i. Under this condition, an erasure at position i of $\mathbf{v}$ can be recovered by using the information given by the coordinates of $\mathbf{v}$ with indices in R_i. The code $\mathcal{C}$ is *locally recoverable with locality* r if any coordinate is locally recoverable with locality at most r.

RS codes have the largest possible locality $r = k$. A variation of RS codes for local recoverability purposes was introduced by Tamo and Barg. These so-called LRC RS codes can have much smaller locality than RS codes. Its length is smaller than the size of $\mathbb{F}_q$. This is a usual fact: for most known optimal codes, the cardinality of the ground field $\mathbb{F}_q$ is larger than the code length n. Then the use of such codes for parctical applications rely on alphabets of large size, what limits its usefulness. Thus the search for long optimal codes has become a challenging problem. A method to obtain long codes is to consider codes from algebraic curves with many rational points. In this way the above construction of LRC RS codes was extended by Barg, Tamo and Vladut to the *LRC Algebraic Geometry (LRC AG) codes*, obtaining larger LRC codes.

In this article we study LRC AG codes coming from curves defined by equations with separated variables $A(Y) = B(X)$, paying special attention to the case in which the degrees of $A(Y)$ and $B(X)$ are coprime. We study also the generalized Hamming weights of these codes, and show how in some special cases the recovery can be done simply by one addition.

Joint work with Wanderson Tenório (Universidade Federal de Mato Grosso) and Fernando Torres (Universidade de Campinas).

Partially founded by grants MTM2015-65764-C3-1-P MINECO/FEDER; and 201584/2015-8, 159852/2014-5, 310623/2017-0 from CNPq-Brazil.

A new q-polynomial approach to cyclic and quasi-cyclic codes

Funda Özdemir

İstinye University

funda.ozdemir@istinye.edu.tr

Abstract. A q-polynomial approach to cyclic codes was introduced by Ding and Ling [D-L]. In this work, we present an alternative q-polynomial approach to cyclic and quasi-cyclic codes.

Let $\mathbb{F}_q$ be the finite field with q elements, and $\mathbb{F}_{q^n}$ be the extension field of degree $n > 1$ over $\mathbb{F}_q$. Let $\mathcal{B} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ be a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ for a normal element $\alpha \in \mathbb{F}_{q^n}^*$. The following map is an $\mathbb{F}_q$-linear isomorphism.

$$\begin{array}{rcl} \phi_{\mathcal{B}} : \mathbb{F}_{q^n} & \longrightarrow & \mathbb{F}_q^n \\ v_0\alpha + v_1\alpha^q + \cdots + v_{n-1}\alpha^{q^{n-1}} & \mapsto & (v_0, v_1, \ldots, v_{n-1}). \end{array}$$

We call $V \subseteq \mathbb{F}_{q^n}$ q-invariant if $V = V^q$, i.e. V is mapped onto itself by the Frobenius automorphism. Taking q-th power of $v \in \mathbb{F}_{q^n}$ corresponds to a cyclic shift of $\vec{v} \in \phi_{\mathcal{B}}(V)$. Hence, V is a q-invariant $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^n}$ if and only if $\phi_{\mathcal{B}}(V)$ is a linear cyclic code of length n over $\mathbb{F}_q$.

The following theorem shows our correspondence between q-polynomials and cyclic codes. This is different from Theorem 4.10 in [D-L].

Theorem 0.1.

(i) Let $L(x) \in \mathbb{F}_q[x]$ be a q-polynomial of degree q^k which splits in $\mathbb{F}_{q^n}$ and let $V \subseteq \mathbb{F}_{q^n}$ be the set of roots of $L(x)$. Then $\phi_{\mathcal{B}}(V)$ is a q-ary $[n,k]$-cyclic code.

(ii) For every q-ary $[n,k]$-cyclic code, there exists a q-polynomial of degree q^k over $\mathbb{F}_q$ splitting in $\mathbb{F}_{q^n}$.

Using the relation in the Theorem, we can construct optimal cyclic codes. We also obtain a characterization of linear complementary dual (LCD) cyclic codes in terms of q-polynomials. Let us recall that an LCD code is a linear code which intersects its dual trivially.

Theorem 0.2. *Let $A(x) \in \mathbb{F}_q[x]$ be the q-polynomial, splitting in $\mathbb{F}_{q^n}$, of a q-ary $[n,k]$-cyclic code C and $B(x) \in \mathbb{F}_q[x]$ be the q-polynomial, splitting in $\mathbb{F}_{q^n}$, of $C^\perp$. Assume that $(n,q) = 1$. Then C is LCD if and only if $A(x) \circ B(x) = x^{q^n} - x$.*

We also generalize our results to quasi-cyclic codes.

[D-L] C. Ding and S. Ling, "A q-polynomial approach to cyclic codes", *Finite Fields Appl.*, vol. 20, 1-14, 2013.

Joint work with Cem Güneri (Sabancı University) and Ferruh Özbudak (Middle East Technical University).

An extension of the Error Correcting Pairs algorithm

Isabella Panaccione and Alain Couvreur

INRIA & CNRS UMR 7161, Laboratoire LIX, Université Paris-Saclay

isabella.panaccione@inria.fr, alain.couvreur@lix.polytechnique.fr

Abstract. In this talk we present a "power" extension of the Error Correcting Pairs algorithm for Reed-Solomon codes. If ℓ is the power we choose, we get for $\ell = 2$ an algorithm whose decoding radius equals that of the Power Decoding algorithm.

It is known that several algorithms have been designed in order to decode Reed-Solomon codes. In particular Berlekamp-Welch algorithm and the Error Correcting Pairs algorithm are two classical algorithms which correct up to $\frac{d-1}{2}$ errors.

Berlekamp-Welch algorithm can be extended to algorithms correcting beyond half the minimum distance. On the one hand Sudan algorithm and Guruswami-Sudan algorithm are deterministic and return the list L of all possible solutions (note that in the typical situation $|L| = 1$). On the other hand, the Power Decoding algorithm has the same decoding radius as Sudan algorithm, is quicker but may fail (it gives one solution or zero).

The Error Correcting Pairs algorithm behave slightly differently, since it mainly consists in localizing errors. After that, decoding boils down to elementary linear algebra. The advantage of this algorithm is that it can also be applied to some cyclic codes. It would be then interesting to have an extension of the Error Correcting Pairs algorithm correcting more than half the minimum distance.

We propose then a "power" generalisation of the Error Correcting Pairs algorithm. In order to do that, as for the Power Decoding algorithm, we start by considering more subproblems (each of them given by a power of the main one) at the same time. Though, while for the Power Decoding algorithm the condition to have a solution depends on the dimension of a linear system solution space, for the Power Error Correcting Pairs algorithm, it depends on the nullity of the intersection of some spaces.

Reproducible Codes and Cryptographic Applications

Paolo Santini

Università Politecnica delle Marche

p.santini@pm.univpm.it

Abstract. In this work we study structured linear block codes, starting from well-known examples and generalizing them to a wide class of codes that we call *reproducible codes*. These codes have the property that they can be entirely generated from a small number of signature vectors, and consequently admit matrices that can be described in a very compact way. We then show some cryptographic applications of this class of codes and explain why the general framework we introduce may pave the way for future developments of code-based cryptography.

The importance of code-based cryptography, one of the most important areas in Post-Quantum Cryptography, has risen dramatically in modern times, and code-based primitives are at the basis of many candidates for the Post-Quantum Standardization call recently launched by NIST. The use of structured codes is the preferred solution to deal with the main inherent issue of code-based cryptography, namely the large size of public keys. Unfortunately, this also has a long history of successful cryptanalysis, mainly due to the fact that structure is traditionally added to codes with existing algebraic properties (e.g. Goppa, GRS), and this gives way to structural attacks. *Sparse-matrix* codes such as LDPC and MDPC have no inherent algebraic structure, depending only on the sparsity of their defining matrix, and thus give way to no such attacks. Moreover, these codes are efficiently decodable and simple to describe and generate, therefore constituting a very promising candidate for McEliece-like schemes with compact keys. However, schemes based on sparse-matrix codes currently suffer from issues related to the decoding algorithm, namely a non-trivial decoding failure rate (DFR), which leads to reaction attacks and severely limits their potential. The contribution of our work is two-fold: first, we introduce a definitional framework which captures the generic idea of a code admitting matrices that can be entirely described by a subset of their rows. To the best of our knowledge, it is the first time such a broad concept is introduced and studied in its entirety. We show that all the existing constructions of structured codes (cyclic, quasi-cyclic, dyadic etc.) are in fact but a special case of our general formulation – in particular, corresponding to the simplest case where the codes are "reproduced" via permutations applied to a single row. We then explain how it is possible to strongly generalize existing constructions by relaxing the choice of the signature set and related family of linear transformations. As an additional contribution, we point out that our work also presents tangible security advantages. For instance, stepping away from quasi-cyclicity means current reaction attacks are no longer applicable, and hinders other attacks (e.g. DOOM) that benefit from the extreme regularity of this type of structure.

Joint work with Edoardo Persichetti (Florida Atlantic University) and Marco Baldi (Università Politecnica delle Marche)