Codes and Rings: Theory and Practice

Patrick Solé

CNRS/LAGA

Paris, France, January 2017

Geometry of codes : the music of spheres

$R =$ a finite ring with identity.
A linear code of length n over a ring R is an $R-$submodule of R^n.
For historical reasons the ring R is called the alphabet and the elements of C codewords . We assume the existence of a metric d over R^n satisfying the three following axioms

1. (nonnegativity) $\forall x \in R^n \quad d(x,x) \geq 0,$
2. (symmetry) $\forall x, y \in R^n \quad d(x,y) = d(y,x),$
3. (triangle inequality) $\forall x, y, z \in R^n \quad d(x,z) \leq d(x,y) + d(y,z).$

Classical coding and the Hamming metric

Classical codes as used in Information transmission are the case of $R =$ a finite field and $d =$ Hamming metric

$$d_H(x, y) := \{j \in \{1, 2, \ldots, n\} \mid x_j \neq y_j\}.$$

Example :

$$d(00011, 11010) = 3$$

Alternative rings and metrics

$\mathbb{Z}_M$ Integers modulo M, Lee metric
Galois rings, chain rings, Frobenius rings,...
Notion of Gray map :

$$R \longrightarrow \mathbb{F}_q^N$$

Study of d induced by d_H on the right

The fundamental problem of coding theory

Sphere packing problem.
Study of the function $A_q(n, \delta)$, the maximum size of a code of length n over an alphabet of size q, such that the minimum pairwise distance between distinct codewords is at least δ.
Difficult in general...

Correlation of sequences

Let x, y denote two periodic sequences of period T with values in

$$\Omega_q := \{z \in \mathbb{C} \mid x^q = 1\}.$$

The *periodic correlation* at time lag ℓ say, of sequences x and y is defined as the hermitian scalar product over a period of x and y shifted ℓ times that is

$$\theta_{x,y}(\ell) := \sum_{j=0}^{T-1} x_j^* y_{j+\ell},$$

the indices being understood modulo T. When $x = y$ it is called autocorrelation and crosscorrelation when $x \neq y$. When $\ell = 0$ plainly, the correlation $\theta_{x,x}(0) = T$

Correlation of sequences : an extremal problem

Let $\mathcal{M}$ denote a family of M such sequences. Let θ_a denote the maximum modulus of correlation for all $x \in \mathcal{M}$ and $\ell \neq 0$. Similarly, let θ_c denote the maximum modulus of the crosscorrelation over all $M(M-1)$ pairs $x, y \in \mathcal{M}$ and all time lags ℓ. The least upper bound on the crosscorrelation θ_c and the nontrivial autocorrelation θ_a is usually denoted by

$$\theta_{\max} := \max(\theta_a, \theta_c).$$

Question Given $\theta_{\max}$, maximize M

Correlation of sequences : cyclic codes solution

Sidelnikov proved in 1971 that when M and T are both large and of the same order of magnitude then for ± 1-valued sequences we have

$$\theta_{\max} \geq \sqrt{2T},$$

while for all other sequences (i.e. $q > 2$) we can merely ascertain that

$$\theta_{\max} \geq \sqrt{T}.$$

The construction of Gold sequences (1978) relies on binary cyclic codes to show the bound is tight for $q = 2$.
Similarly, the construction of the sequences when $q = 4$ builds on certain families of $\mathbb{Z}_4$-cyclic codes to show the bound is tight for $q = 4$.(S. 1988).

Euclidean lattices

An n-dimensional lattice in $\mathbb{R}^n$ is a discrete $\mathbb{Z}$-module : imagine a big grid like $\mathbb{Z}^n$ for instance.
Lattices are useful in communications as group codes for the Gaussian channel (WiFi) and as codebooks for vector quantization (image processing).
There is a natural notion of dual L^* of a lattice, that is fundamental for physicists studying crystal diffraction, and for number theorists involved with modular forms.

$$L^* = \{y \in \mathbb{R}^n \mid \forall x \in L,\, x.y \in \mathbb{Z}\}.$$

The theta series counts lattice points of given norm.
The weight enumerator of a code is generating function for codewords of given weight.

$$\theta_L(q) = \sum_{x \in L} q^{x.x},\ W_C(x,y) = \sum_{c \in C} x^{n-w(c)} y^{w(c)}.$$

Codes vs lattices

Since the 1970's there is a dictionary between codes and lattices as shown in the following table :

$\mathbb{F}_2^n$	$\mathbb{R}^n$
Hamming distance	Euclidean distance
minimum distance	norm
dimension	determinant
Weight enumerator	Theta function
Mac Williams relations	Poisson Jacobi formula
Self-dual codes	Unimodular Lattices

Construction A

This analogy is materialized by construction A which associates to a binary code C a lattice $A(C)$ through the following formula :

$$\sqrt{2}A(C) = C + 2\mathbb{Z}^n := \bigcup_{c \in C} (c + 2\mathbb{Z}^n).$$

This construction builds unimodular lattices (lattices equal to their duals) from self-dual codes.
The theta series of $A(C)$ can be computed by substituting for the variables x, y in the weight enumerator $W_C(x, y)$ the one-dimensional theta series corresponding to $\mathbb{Z}$ and $\mathbb{Z} + \frac{1}{2}$.

Constructing the Leech lattice by $\mathbb{Z}_4$-codes

The Leech lattice is a very symmetric unimodular lattice in dimension 24 : Conway three sporadic simple groups are involved in its automorphism group.
There is a construction A modulo 4.

$$2A(C) = C + 4\mathbb{Z}^n := \bigcup_{c \in C} (c + 4\mathbb{Z}^n).$$

Take C to be a special self-dual $\mathbb{Z}_4$-code above the Golay code in length 24 to get the Leech lattice.(Bonnecaze, S. 1995).

MacWilliams formula

The weight enumerator W_c of a *linear* code C and the weight enumerator of its dual $C^\perp$ are related by

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x+y, x-y).$$

This is proved by Fourier analysis on the group $(\mathbb{F}_q^n, +)$ and requires linearity of C.

Hamming vs Simplex

A simple example of dual pair of codes is the Hamming code H_m a ("big")$[n = 2^m, n - m - 1, 4]$ code with dual is the ("small") $[2^m, m + 1, 2^{m-1}]$ first order Reed Muller R_m . The matrix

$$\mathcal{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \end{bmatrix},$$

where $n = 2^m - 1$, and α is a root of an irreducible polynomial, is both a generator matrix for R_m and a parity check matrix for $H_m = Ker(\mathcal{H})$.
The small code R_m has the simple weight distribution

$$W_{R_m}(x, y) = x^n + y^n + (2n - 2)(xy)^{n/2}.$$

The Kerdock Preparata enigma

In the 1970's was found two infinite families of nonlinear codes, Kerdock (low rate) and Preparata (high rate) which are MacWilliams dual of each other.
For instance the intersection of the two families is the formally self-dual Nordstrom-Robinson code of parameters $(16, 2^8, 6)$.
William Kantor declared that "it was merely a coincidence."

The Gray map trick

A well-known trick in modulation theory to address the 4-PSK constellation consists of using the so-called Gray map . This is a map from $\mathbb{Z}_4$ to $\mathbb{F}_2^2$ defined by

$$0 \to 00, 1 \to 01, 2 \to 11, 3 \to 10,$$

and extended to a map from $\mathbb{Z}_4^n$ to $\mathbb{F}_2^2$ in the natural way.
The key property, is that the map

$$\phi : (\mathbb{Z}_4^n, \textit{Lee distance}) \to (\mathbb{F}_2^{2n}, \textit{Hamming distance})$$

is an isometry of metric spaces.
For graph theorists : the 4-cycle is a Cayley graph for two different groups : Klein-4 and the cyclic group of order 4.

The Kerdock Preparata enigma : solution

Using a matrix similar to the one used for Hamming and Reed-Muller code

$$\mathcal{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \end{bmatrix},$$

where α lives in a Galois ring , a ring extension of $\mathbb{Z}_4$, it is possible to construct a pair of dual $\mathbb{Z}_4$-codes the Gray map image of which has the same weight enumerator as the Kerdock and Preparata codes respectively. (Hammons, Kumar, Calderbank, Sloane and S. 1994).
Further these codes are better than linear codes of the same length and minimum distance.

The two ways to mix rings and codes

The obvious way is to assume a ring structure on the alphabet.
The other way is to use the code symmetry to give it an algebraic structure of ring or module.

Example 1 : C is a cyclic code of length n over F if it is invariant under the shift T that is $TC \subseteq C$.
$T : (x_1, \ldots, x_n) \mapsto (x_n, x_1, \ldots, x_{n-1})$.
Then C is an ideal in the polynomial ring $R = F[x]/(x^n - 1)$.
(Note that $T^n = 1$.)

Example 2 : C is a quasi-cyclic code of length n and index p over F if it is invariant under T^p that is $T^p C \subseteq C$.
Then C is an R-module, a submodule of $R^{n/p} \Rightarrow$ 5 papers with S. Ling.

Quasi-cyclic codes : background

A linear code over $\mathbb{F}_q$ is called a quasi-cyclic (QC) code of index ℓ if it is closed under shifting codewords by ℓ units, and ℓ is the smallest positive integer with this property.

So, cyclic codes amount to the special case $\ell = 1$.

Let C be a QC code of length $m\ell$, index ℓ over $\mathbb{F}_q$.

If we let $R := \mathbb{F}_q[x]/\langle x^m - 1\rangle$, then the code C can be viewed as an R-module in R^ℓ

Here is a duality-driven factorization into irreducible polynomials in $\mathbb{F}_q[x]$

$$x^m - 1 = g_1 \cdots g_s h_1 h_1^* \cdots h_t h_t^*.$$

where g_i's are self-reciprocal and h_j^* denotes the reciprocal of h_j.

Quasi-cyclic codes : CRT I

$$\left(\bigoplus_{i=1}^{s} \mathbb{F}_q[x]/\langle g_i \rangle\right) \oplus \left(\bigoplus_{j=1}^{t} \left(\mathbb{F}_q[x]/\langle h_j \rangle \oplus \mathbb{F}_q[x]/\langle h_j^* \rangle\right)\right)$$

$$= \left(\bigoplus_{i=1}^{s} \mathbb{F}_q(\xi^{u_i})\right) \oplus \left(\bigoplus_{j=1}^{t} \left(\mathbb{F}_q(\xi^{v_j}) \oplus \mathbb{F}_q(\xi^{-v_j})\right)\right).$$

We let $G_i = \mathbb{F}_q[x]/\langle g_i \rangle$, $H_j' = \mathbb{F}_q[x]/\langle h_j \rangle$ and $H_j'' = \mathbb{F}_q[x]/\langle h_j^* \rangle$ for simplicity. The map that sends $a(x) \in R$ to the decomposition can be thought of as projections mod each irreducible factor or as follows :

$$a(x) \mapsto \left(\bigoplus_{i=1}^{s} a(\xi^{u_i})\right) \oplus \left(\bigoplus_{j=1}^{t} \left(a(\xi^{v_j}) \oplus a(\xi^{-v_j})\right)\right).$$

Quasi-cyclic codes : CRT II

This decomposition naturally extends to R^ℓ and then $C \subset R^\ell$ decomposes as

$$C = \left(\bigoplus_{i=1}^{s} C_i \right) \oplus \left(\bigoplus_{j=1}^{t} \left(C'_j \oplus C''_j \right) \right),$$

where each component code is a length ℓ linear code over the base field (G_i, H'_j or H''_j) it is defined on.
Note that since the degree of h_j and h_j are the same, H'_j is abstractly field isomorphic to H''_j.
Component codes C_i, C'_j, C''_j are called the constituents of C.

Quasi-cyclic codes : duality

The (Euclidean) dual in $\mathbb{F}_q^{m\ell}$ of C is of the form

$$C^{\perp} = \left(\bigoplus_{i=1}^{s} C_i^{\perp_h} \right) \oplus \left(\bigoplus_{j=1}^{t} \left(C_j''^{\perp_e} \oplus C_j'^{\perp_e} \right) \right).$$

Note the swap between $'$ and $''$
Here, $\perp_h$ denotes the Hermitian dual on $G_i^{\ell} = \mathbb{F}_q(\xi^{u_i})^{\ell}$
Definition of the Hermitian inner product of
$\vec{c} = (c_1(\xi^{u_i}), \ldots, c_{\ell}(\xi^{u_i})), \vec{d} = (d_1(\xi^{u_i}), \ldots, d_{\ell}(\xi^{u_i})) \in \mathbb{F}_q(\xi^{u_i})^{\ell}$,
where $c_b(x), d_b(x) \in R$ for all $1 \leq b \leq \ell$, is :

$$\langle \vec{c}, \vec{d} \rangle := \sum_{b=1}^{\ell} c_b(\xi^{u_i}) d_b(\xi^{-u_i}).$$

Quasi-cyclic codes : concatenation I

For $i \in \{1, \ldots, s\}$, let θ_i be the generating primitive idempotent for the q-ary minimal cyclic code of length m, whose check polynomial is $g_i(x)$. This cyclic code $\langle \theta_i \rangle$ is $\simeq$ to the field G_i. Similarly, let θ'_j and θ''_j denote the primitive idempotents attached in the same way to the fields H'_j and H''_j (for $1 \leq j \leq t$). By Jensen's work , it was shown in Gueneri-Ozbudak that the QC code C above also has a concatenated decomposition

$$C = \left(\bigoplus_{i=1}^{s} \langle \theta_i \rangle \square \mathfrak{C}_i \right) \oplus \left(\bigoplus_{j=1}^{t} \left(\langle \theta'_j \rangle \square \mathfrak{C}'_j \right) \oplus \left(\langle \theta''_j \rangle \square \mathfrak{C}''_j \right) \right),$$

where the outer codes $\mathfrak{C}_i, \mathfrak{C}'_j, \mathfrak{C}''_j$ are length ℓ linear codes over G_i, H'_j, H''_j, respectively, and where $\square$ denotes standard concatenation.

Quasi-cyclic codes : concatenation II

The key fact is that the outer codes coincide with the constituents in the CRT decomposition :
$\mathfrak{C}_i = C_i, \mathfrak{C}'_j = C'_j, \mathfrak{C}''_j = C''_j$ for all i, j. The converse statement holds as well. Namely, if you start with arbitrary length ℓ outer codes (constituents) over the fields G_i, H'_j, H''_j and form the concatenation above, the resulting code is a length $m\ell$, index ℓ QC code over $\mathbb{F}_q$.

Skew polynomial rings

For a finite field $\mathbb{F}_q$ and θ an automorphism of $\mathbb{F}_q$ we consider the ring

$$R = \mathbb{F}_q[X;\theta] = \{a_n X^n + \cdots + a_1 X + a_0 | a_i \in \mathbb{F}_q, n \in N\}.$$

This is the set of formal polynomials where the coefficients are written on the left of the variable X.

Addition is defined to be the usual addition of polynomials

Multiplication is defined by the commutation rule $\{X \cdot a = \theta(a)X \in \mathbb{F}_q\}$, extended to all elements of R by associativity and distributivity.

Left and right gcds and lcms exist in R and can be computed using the left and right Euclidean algorithm.

Over finite fields skew polynomial rings are also known as linearized polynomials .

Skew cyclic codes : ideal definition

By analogy with cyclic codes define a skew cyclic code over a finite field F as an ideal in the quotient of the skew polynomial ring $R = F[\theta, x]$ by one of its ideal I.
For the quotient to retain the structure of a ring it is necessary for I to be two-sided.
Advantage over classical cyclic codes : Because factorization in R is not unique, many more codes for given length.
We will focus on two special cases :

1. If $f \in Z(\mathbb{F}_q[X, \theta])$, then we call the θ-code corresponding to the left ideal $(g)/(f)$ a **central** θ-code.
2. If the order of θ divides n and $f = X^n - 1$, then we call the θ-code. corresponding to the left ideal $(g)/(X^n - 1)$ a θ-**cyclic** code.

Skew cyclic codes : module definition

Let F denote a finite field of characteristic p and size $q = p^a$. Let σ denote an element of its Galois group, of order r, so that r divides a. If $a = rm$, then the fixed field of σ has order $Q = p^m$. By a module skew code of length n we shall mean a left submodule of the left R-module $R_f = R/Rf$ where $f \neq 0$ is arbitrary of degree n. Since R is left euclidean it is easy to see that such a submodule is of the form Rg/Rf, where g right divides f.

Advantage over ideal skew cyclic codes : More codes, more chances to find better codes.

Skew cyclic codes are good

Let C_n be a sequence of codes of length n, dimension k_n, and minimum distance d_n over F. The asymptotic rate ρ of the family is defined as

$$\rho = \limsup_{n\to\infty} \frac{k_n}{n}.$$

The asymptotic relative distance δ is defined as

$$\delta = \limsup_{n\to\infty} \frac{d_n}{n}.$$

A family of codes is said to be good if $\rho\delta > 0$.
It can be shown, by varying the f that skew module codes are good (Leroy, S. 2015).

Conclusion and perspectives

If you have liked this talk please buy my book ! ! ! !

M. Shi, A. Alahmadi, P. Solé,
Codes and Rings : Theory and Practice,
Academic Press, to appear in 2017.
More resuls on

- local rings, Galois rings, chain rings, Frobenius rings, . . .
- Lee metric, homogeneous metric, rank metric, RT-metric, . . .
- Quasi-twisted codes, consta-cyclic codes, skew-cyclic codes. . .