

Coding theory over fields

Patrick Solé

ICS, UMR 6070, Université de Nice Sophia antipolis

Conference Non Commutative Rings June 09

Shannon Paradigm

In 1948, Claude Sannon (Bell Labs) published "A mathematical theory of Communication", dealing with the problem of **digital communication** in presence of natural noise between a source of messages and a receiver.

- 1 message $m \in \mathbb{F}_2^k$ is
- 2 encoded as a string (**codeword**) $c \in \mathbb{F}_2^n$ with $n > k$
- 3 sent on a **channel** where it is
- 4 corrupted by an **error word** $e \in \mathbb{F}_2^n$
- 5 received as $y = c + e$
- 6 decoded as \hat{m}

The **code** is the set of all codewords generated by all possible messages.

The integer n is called the **length** of the code and the ratio k/n its **transmission rate** .

Channels in practice

There are two kinds

- **space** channel
 - telephone line
 - radio
- **time** channels
 - CD, DVD
 - mass memories
 - flash memories

Shannon theorem

Shannon proved that as long as the transmission rate k/n is less than the **capacity of a channel**, given ϵ there are long codes (ie with n large) such that the probability that $m \neq \hat{m}$ is $< \epsilon$

The proof is probabilistic and non constructive :=((

The aim of **algebraic** coding theory is to construct **effectively** good codes, by assuming some algebraic structure on the code.

One method is to replace bits by elements of a ring (**the alphabet**) and assume the code is a module over that ring.

Another method is to assume some symmetry (**cyclicity, quasicyclicity**) that can be expressed by an ideal or module structure of the code over some auxiliary ring.

Advertisement

The Proceedings of the CIMPA summer school on **Codes over rings** (Ankara 2008) are to be published next Fall by World Scientific.

A tentative table of contents is

- 1 Preface
- 2 S. Boztas, U. Parampalli, Partial correlation of sequences and their applications
- 3 H.Q. Dinh, S.R. Lopez-Permouth, S. Szabo, A survey on cyclic and negacyclic codes over finite chain rings
- 4 T. Honold, I. Landgev, Linear Codes over Finite Chain Rings and Projective Hjelmslev Geometries
- 5 J. Wood, Foundations of linear codes defined over finite modules : the extension theorem and the MacWilliams identities

Linear codes over finite fields

A linear code C of length n over \mathbb{F}_q is an \mathbb{F}_q vector subspace of \mathbb{F}_q^n

The **dimension** of such a code usually denoted by k is its dimension as an \mathbb{F}_q vector space

The parameters of a code are denoted by $[n, k]_q$.

The code is specified by a basis of the space. A matrix of size k by n with rows these vectors is called a **generator** matrix.

$$C = \{uG \mid u \in \mathbb{F}_q^k\}$$

The **parity check** matrix H of a code is any $n - k$ by n matrix such that $C = \text{Ker}(H)$ or in other words

$$C = \{x \in \mathbb{F}_q^n \mid Hx^T = 0\}$$

The row span of H is a code of dimension $n - k$ denoted by C^\perp and called the **dual** code.

The parity check code

It is the dual code of the preceding.

It is a high rate code that can detect one error but correct none .

Anecdote : It is because Hamming an office mate of Shannon in the 40's was tired to have stalled programs over the week end by a failed parity check that he invented the Hamming codes that can correct one error.

Distance and Weight

The **Hamming weight** $w_H(x)$ of $x \in \mathbb{F}_q^n$ is the number of entries where $x \neq 0$.

The **Hamming distance** $d_H(x, y)$ of two vectors $x, y \in \mathbb{F}_q^n$ is $w_H(x - y)$.

The Hamming distance satisfies **the triangle inequality** namely

$$d_H(x, y) \leq d_H(x, z) + d_H(z, y)$$

The **sphere** of radius r about x is defined as

$$B_x(r) = \{y \in \mathbb{F}_q^n \mid d_H(x, y) \leq r\}$$

Minimum distance and error correction capacity

The **Minimum distance** $d_H(C)$ of a code C is defined as

$$d_H(C) = \min\{d_H(x, y) \mid x \neq y \in C\}$$

The **error correcting capacity** a.k.a **packing radius** is then

$$t(C) := \lfloor \frac{d_H(C) - 1}{2} \rfloor$$

The triangle inequality shows that the spheres of radius t about codewords are pairwise disjoint. Therefore all received words corrupted by $\leq t$ errors are at distance at most t of **at most one** codeword :

nearest neighbor decoding if at all possible gives a unique result.

The parameters of a code are compactly denoted by $[n, k, d]_q$.

Fundamental Problem

Let $B_q(n, d)$ denote the largest size of an $[n, k, d]_q$ code.

Given n, d one would like this function to be as large as possible to send as **many messages** as possible.

Given n and k one would like to d to be as large as possible to correct as **many errors** as possible.

There is a trade-off between these two conflicting requirements. Determining $B_q(n, d)$ is the so called **fundamental problem** of coding theory.

The repetition and parity check codes are two optimal codes at each end of the spectrum, showing that, respectively

$$B_2(n, 2) = n - 1 \text{ and } B_q(n, n) = q.$$

See www.codetables.de for a table of **record holders**!

Sphere packing and sphere covering bounds

The notion of packing radius shows by enumeration that

$$B_q(n, d) \leq \frac{q^n}{\#B_0(t)} = \frac{q^n}{\sum_{j=0}^t \binom{n}{j} (q-1)^j}.$$

The notion of **covering radius** shows that (**Gilbert bound**) there are codes as good as

$$B_q(n, d) \geq \frac{q^n}{\#B_0(d-1)} = \frac{q^n}{\sum_{j=0}^{d-1} \binom{n}{j} (q-1)^j}$$

Cyclic codes over fields

Let T denote the shift operator over \mathbb{F}_q^n .

$$T((c_0, \dots, c_{n-1})) := (c_{n-1}, c_0, \dots, c_{n-2})$$

A code C is said to be **cyclic** if it linear and wholly invariant under the shift $T(C) \subseteq C$.

The **polynomial representation** of cyclic codes is the generating function approach as defined by

$$c(x) := c_0 + c_1x + \dots + c_{n-1}x^{n-1}$$

It is immediate to see that a code is cyclic iff its polynomial representation is an ideal of the ring

$$R_n(q) := \mathbb{F}_q[x]/(x^n - 1).$$

Algebraic structure of cyclic codes

The ring $R_n(q)$ is **principal**.

If C is cyclic then there exists a unique monic polynomial of lowest degree g such that $C = \langle g \rangle$.

It can be shown that g divides $x^n - 1$ and that $\dim(C) = n - \deg(g)$.

The dual of a cyclic code is also cyclic, with generator the (normalized) reciprocal of $(x^n - 1)/g$.

Conclusions

- To understand the structure of cyclic codes we need to understand the structure of the ring $R_n(q)$
- To generate all cyclic codes of length n we need to factorize $x^n - 1$

This philosophy will remain when replacing \mathbb{F}_q by a more complex ring!

Factorizing $x^n - 1$

If $(n, q) = 1$ all the roots of $x^n - 1$ over \mathbb{F}_q are simple.

The roots of $x^n - 1$ are powers of α where α is a primitive root of unity of order n in a large enough extension of \mathbb{F}_q .

To be precise \mathbb{F}_{q^t} where t is the order of q modulo n

Define the q -cyclotomic classes as the orbits of \mathbb{Z}_n under the permutation $x \mapsto qx$

There is a one to one correspondence between such orbits and irreducible factors of $x^n - 1$,

$$C \leftrightarrow \prod_{i \in C} (x - \alpha^i)$$

Example : Take $n = 7$ and $q = 2$. The classes are

$$\{0\}, \{1, 2, 4\}, \{3, 5, 6\},$$

corresponding to factors $(x + 1)$, $(x^3 + x + 1)$, $(x^3 + x^2 + 1)$

Roots and minimum distance

There are many bounds on the **minimum distance** of C as a function of the roots of g .

The so called BCH bound states that if the exponents of the roots contain s consecutive residues modulo n , then $d \geq s + 1$. The proof is based on the evaluation of the van der Monde determinant.

Example : Take $n = 7$ and $q = 2$. The generator $(x + 1)(x^3 + x^2 + 1)$ contains roots corresponding to 5, 6, 0. And yes the distance is 4 (even part of the Hamming code).

Hamming code

Let $q = 2$ and $n = 2^m - 1$. Choose g to be an irreducible primitive polynomial. Its roots contain $\{\alpha, \alpha^2\}$. Hence $d \geq 3$, by the BCH bound. It can be shown that $d = 3$.

In fact $n - k = m$ and therefore $2^{n-k} = 2^m = n + 1$, showing that the code meets the Hamming bound with equality.

Such a code is called **perfect**.

The parameters of linear perfect codes over finite fields were classified in the 70's

- repetition codes $[2m + 1, 1, m]_2$
- Hamming codes $[\frac{q^m - 1}{q - 1}, n - m, 3]_q$
- binary Golay code $[23, 12, 7]_2$
- ternary Golay code $[11, 6, 5]_3$

The last two are cyclic.

The classification of codes is open for non necessary linear codes.

The classification of parameters is totally open for non prime powers alphabets.

Reed Solomon code

Let $n = q - 1$, so that, by Fermat little Theorem, $x^n - 1$ factors completely over $\mathbb{F}_q[x]$.

Take

$$g = \prod_{i=1}^s (x - \alpha^i),$$

a polynomial with coefficients in \mathbb{F}_q

By the BCH bound $d \geq s + 1 = n - k + 1$.

But looking at the rank of a parity check matrix we see that $d \leq n - k + 1$. (Singleton bound)

So $d = n - k + 1$.

Such a code is called **MDS** for maximum distance separable.

Convolutional codes vs block codes

Block codes are used in groups of n symbols comprising k information symbols.

This requires **synchronization** between source and receiver

Think of a **convolutional** encoder as a linear transform that turns k streams of information symbols into n streams of encoded symbols.

There are universal graph theoretic algorithms to decode convolutional codes.

In some cases these algorithms allow self synchronization.

Convolutional Codes : algebraic structure

A convolutional code of rate k/n over a field F is a block code of length n and k generators over a ring R of generating functions with coefficients in F and indeterminate D , say

This is the D -transform representation of a linear **system** over F with k inputs and n outputs. In the past various schools have used various conventions :

- $R = F(D)$ (rational functions for Massey)
- $R = F[[D]]$ (formal power series for van Lint)
- $R = F[D]$ (polynomials for Rosenthal and behaviorists)

In this talk we shall adopt $R = F[D]$ and $F = \mathbb{F}_2$

Convolutional Codes : metric structure

The Hamming weight w over F is extended additively to polynomials

If $f = f_0 + \dots + f_d D^d$ then $w(f) := w(f_0) + \dots + w(f_d)$

and componentwise to vectors in polynomials

The free distance $d_f(C)$ of a convolutional code C is the minimum Hamming weight of a nonzero codeword

Fundamental problem : Given n, k what is the largest d_f of an $[n, k]$ convolutional code?

Codes, Invariants, Modular forms : Motivation

In 1972 Broué and Enguehard derived an algebra isomorphism between

The ring $M_{4*}(PSL(2, \mathbb{Z}))$ of modular forms of weight multiple of 4

and

The ring of invariants that contain the weight enumerators of Type II codes

Recent results

In the 90's there has been a renaissance of that kind of problem for two reasons

New **alphabets** for the codes : codes over rings

New **weight enumerators** : Lee weight, multiple weight, split weight

As a result connections with more types of modular forms appear :

Hilbert, Siegel, Jacobi, half integral weight

in the work of many authors :

Bannai, Choie, Chua, Duke, Ebeling, Hirzebruch, Nebe, Runge, S., Ozeki, Vardi, etc

In the current talk I cannot develop the MF aspect but I will review the classical material for codes over fields

Type II codes

A binary code of length n and dimension k is a k -dimensional \mathbb{F}_2 -subspace of \mathbb{F}_2^n .

The dual of a code is wrt the standard Euclidean product $\sum_i x_i y_i$.

$$C^\perp = \{y \in \mathbb{F}_2^n, \forall x \in C, x \cdot y = 0\}.$$

A code is self-dual if equal to its dual.

It is Type II iff it is self-dual and each of its vectors contains w ones with w a multiple of 4.

Example : $R_2 := \{00, 11\}$. is self dual but not Type II.

Property : Type II codes only exist in lengths multiple of 8.

Weight Enumerators

If z is a binary vector denote by z_0 (resp. z_1) the number of zeroes (resp. number of ones) in its entries.

The (Hamming) **Weight Enumerator** of a code C is the homogeneous polynomial in two variables of total degree n

$$W_C(x, y) = \sum_{c \in C} x^{c_0} y^{c_1}.$$

Example : $W_{00,11}(x, y) = x^2 + y^2.$

A finite group of order 192

Let G_{II} denote the matrix group $\langle M, N \rangle$, where

$$M = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad N = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}.$$

Key fact If C is a type II code, its weight enumerator is invariant under G_{II} by linear action

M invariance expresses self-duality (fixed point of MacWilliams transform)

N invariance expresses Type II property

Example : $W_C(x, y) = x^2 + y^2$, is M -invariant but not N -invariant

Gleason Theorem (ICM 1970)

Define

$$\psi_8(x, y) = x^8 + y^8 + 14x^4y^4, \quad \nu_{24} = x^4y^4(x^4 - y^4)^4$$

The weight enumerator of a Type II code of weight $8n$ is a polynomial in ψ_8 and ν_{24} .

$$W_C = \sum_{j=0}^{\lfloor n/3 \rfloor} a_j \psi_8^{n-3j} \nu_{24}^j,$$

for some (unique) scalars a_j .

In other words, the algebra of invariants of G_{II} is generated by ψ_8, ν_{24} .

$$\mathbb{C}[x, y]^{G_{II}} = \mathbb{C}[\psi_8, \nu_{24}].$$

Lattices

Let (v_1, \dots, v_n) be a basis of \mathbb{R}^n

A **Lattice** Λ is defined as

$$\Lambda := \left\{ \sum_{i=1}^n \lambda_i v_i \mid \lambda_i \in \mathbb{Z} \right\}$$

Its main measurements are
fundamental parallelotope, fundamental volume, packing radius ρ ,
covering radius R .

The **dual** Λ^* of a lattice Λ is

$$\Lambda^* := \{y \in \mathbb{R}^n \mid \forall x \in \Lambda \ x \cdot y \in \mathbb{Z}\}$$

A lattice is **unimodular** if it is equal to its dual.

Lattices and Modular forms

Define the **theta series** of the lattice L by

$$\theta_L(q) = \sum_{v \in L} q^{v \cdot v},$$

where $q = \exp(\pi\sqrt{-1}\tau)$, and $\Im(\tau) > 0$. Recall the generators S, T of $PSL(2, \mathbb{Z})$

$$S : \tau \mapsto -1/\tau, \quad T : \tau \mapsto \tau + 1.$$

key fact : If $L \subseteq \mathbb{R}^n$ is unimodular even its theta series is a modular form of weight $n/2$ and principal character

Hecke Theorem

Define the Eisenstein series of weight 4 and the cusp form of weight 12

$$E_4 = 1 + 240 \sum_{m=1}^{\infty} \sigma_3(m) q^m, \quad \Delta = q^2 \prod_{m=1}^{\infty} (1 - q^{2m})^{24}.$$

The weight enumerator of a unimodular even lattice of dimension $8n$ is a polynomial in E_4 and Δ .

$$W_C = \sum_{j=0}^{\lfloor n/3 \rfloor} a_j E_4^{n-3j} \Delta^j,$$

for some (unique) scalars a_j . In other words

$$M_{4*}(PSL(2, \mathbb{Z})) = \mathbb{C}[E_4, \Delta]$$

Dictionary

| | |
|---|------------------------|
| Lattices | Codes |
| \mathbb{R}^n | \mathbb{F}_2^n |
| Euclid | Hamming |
| unimodular | self-dual |
| unimodular even | Type II |
| theta series | weight enumerator |
| $PSL(2, \mathbb{Z}) = \langle S, T \rangle$ | $\langle M, N \rangle$ |
| Hecke theorem | Gleason theorem |
| modular forms | invariant theory |
| E_4 | ψ_8 |
| Δ | ν_{24} |

Construction A

Given an additive code C of length n over \mathbb{Z}_m **construction A** builds a lattice $A(C)$ by the rule

$$\sqrt{m}A(C) = C + m\mathbb{Z}^n$$

$\sqrt{m}A(C)$ is the inverse image of reduction mod m in \mathbb{Z}^n

The **fundamental volume** is $m^{n/2}/|C|$

The **packing radius** is determined by the minimum Hamming distance ($m = 2$)

or the minimum Euclidean distance ($m = 4$)

$A(C)$ is **unimodular** iff C is self-dual

$A(C)$ is **even** iff the euclidean weights of C are multiples of $2m$

Partial explanation of the dictionary

Define two Jacobi theta null werte

$$\theta_3 = \sum_{n \in \mathbb{Z}} q^{n^2}$$

$$\theta_2 = \sum_{n \in \mathbb{Z}} q^{(n+1/2)^2}$$

Then the theta series of the lattice $A(C)$ is

$$W_C(\theta_3, \theta_2).$$

Example : if C is the unique Type II code of length 8 then $A(C)$ is the unique unimodular even lattice of dimension 8, the root lattice E_8 .

$$E_4 = \theta_{E_8} = \psi_8(\theta_3, \theta_2),$$

with $\psi_8(x, y) = x^8 + y^8 + 14x^4y^4$.

Broué- Enguehard map

The map $BE : f \mapsto f(\theta_3, \theta_2)$ is an algebra isomorphism from the invariant ring of G_{II} onto the ring of modular forms of weight multiple of four $M_{4^*}(PSL(2, \mathbb{Z}))$, which maps ψ_8 on E_4 and ν_{24} on Δ .

That $BE(f)$ is a modular form comes from the transformation law of Jacobi thetas combined with the group laws

The map is one to one because both algebras are free on two generators

Of course many invariants of G_{II} are not weight enumerators : an example is Δ .

Ozeki extension

The map $BE : f \mapsto f(\theta_3, \theta_2)$ is an algebra isomorphism from a ring of relative invariants of G_{II} onto the ring of modular forms of even weight $M_{2*}(PSL(2, \mathbb{Z}))$, which maps ψ_8 on E_4 and k_{12} on E_6 .

Here $k_{12} = x^{12} - 33(x^8y^4 + x^4y^8) + y^{12}$, is an invariant occurring in Felix Klein's work on the **icosahedron**

The ring of relative invariants is free on two generators ψ_8 and k_{12}

Conclusion : codes and rings

There are many aspects in coding theory : combinatorial, probabilistic, algebraic

Algebra is mostly useful in explicit constructions

Ring theory in particular occurs in relation with **cyclic codes**

It can also be used to determine the structure of certain ring of polynomial invariants containing **weight enumerators**