Algebraic constructions of codes in the sum-rank metric

Xavier Caruso

February 23, 2026

HAMMING DISTANCE

Ambient space: $E = K^n$ (K field)

Distance: $w(x_1, \dots, x_n) = \#\{i;\ x_i \neq 0\}$

Scalar product:

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$$

Cyclic codes

Definition: A code C is cyclic when:

$(x_1, \dots, x_n) \in C \Rightarrow (x_2, \dots, x_n, x_1) \in C$

A cyclic code corresponds to an ideal of $K[x]/(x^n-1)$

Reed-Solomon codes

k, n two integers with $k<n$

A RS code is the image of

$$K[x]_{<k} \longrightarrow K^n$$
$$P \longmapsto (P(a_1), \dots, P(a_n))$$

length $= n$
dimension $= k$
min. dist $= n-k+1$

(MDS)

Algebraic geometry codes

$\mathcal{C}$ algebraic curve over K

G divisor, $D_1, \dots, D_n$ points of

$$\mathcal{L}(G) \longrightarrow K^n$$

Riemann Roch space

$$P \longmapsto (P(D_1), \dots, P($$

length $= n$
dimension $\geq \deg G - g + 1$
min. dist $\geq n - \deg G$

SUM-RANK DISTANCE

Ambient space: $E = End(V)^s$ (K-linear)
$= End(L)^s$ (L-linear)

Distance: $w(F_1, \dots, F_s) = \sum_{i=1}^{s} \operatorname{rank}(F_i)$

Scalar product.

$$\langle F, G \rangle = Tr(F^* \circ G)$$

adjoint for a bilinear form on V
when $V = L$, we take $\langle x, y \rangle = Tr_{L/K}(xy)$

Definition: A code C is θ-cyclic when $(x_1, \dots, x_n) \in C$
$\Rightarrow (\theta(x_2), \dots, \theta(x_n), \theta(x_1)) \in C$

It's the same than an ideal in

$$L[X;\theta]/(X^n-1) \qquad (\text{assume } r \mid n)$$

$n=r$: $L[X;\theta]/(X^n-1) \simeq End(L)$

$n=2r$: $L[X;\theta]/(X^{2n}-1) \simeq End(L) \times End(L)$
if $\exists u \in L$ s.t $N_{L/K}(u) = -1$

Let $u_i : L \to L$ $(1 \leq i \leq n)$ be semi-linear endomorphisms (i.e. $u_i = c_i \theta$)

$$L[X;\theta]_{<k} \longrightarrow End(L)^s$$
$$P \longmapsto (P(u_1), \dots, P(u_s))$$

If $N_{L/K}(c_i)$ are pairwise distinct.

length $= rs$
dimension $= r \cdot k$
min. dist $= rs - k - 1$ [MSRD]

Martínez Peñas '18

$Y \to X$ Galois covering of curves with cyclic Galois group $<$

G divisor on Y, $D_1, \dots, D_s$ p

Also need a function x on X

$$\Lambda(G) \longrightarrow \prod_{i=1}^{s} End(V_i)$$
$$P \longmapsto (P(D_1), \dots, P(D_s))$$

where $P(D_i)$ is by def. P

dimension $\geq r \cdot \deg G - g_0 + 1$
min. dist $\geq rs - \deg G$

les

e C is cyclic when

$\Rightarrow (x_2, \dots, x_n, x_1) \in C$

corresponds to an

$]/(x^n-1)$

Reed-Solomon codes

k, n two integers with $k<n$

A RS code is the image of

$$K[X]_{<k} \longrightarrow K^n$$
$$P \longmapsto (P(a_1), \dots, P(a_n))$$

length = n
dimension = k
min. dist = $n-k+1$

(MDS)

Algebraic geometry codes

$\mathcal{C}$ algebraic curve over K

G divisor, $D_1, \dots, D_n$ points on $\mathcal{C}$

$$\mathcal{L}(G) \longrightarrow K^n$$
Riemann Roch space
$$P \longmapsto (P(D_1), \dots, P(D_n))$$

length = n
dimension $\geq \deg G - g + 1$
min. dist $\geq n - \deg G$

Ω-construction (duals of AG codes)

$$\Omega(D-G) \longrightarrow K^n$$
$$\omega \longmapsto \operatorname{res}_{D_i}(\omega)$$

(duality follows from residue formula)

length = n
dimension : complement of the dimension of AG
min. dist $\geq \deg G - (2g-2)$

Goppa codes

Let $g(x) \in \mathbb{F}_{q^e}[x]$, $a_i \in \mathbb{F}_{q^e}$

$$C = \left\{ (c_1, \dots, c_n) \in \mathbb{F}_q^n \text{ t.q. } \sum_{i=1}^{n} \frac{c_i}{x-a_i} \equiv 0 \pmod{g} \right\}$$

NB: It's a particular case of the Ω-construction (more exactly a subfield subcode)

Property: When $q=2$, improvement on the minimal distance!

---

e C is θ-cyclic

$\in C$

$z_2), \dots, \theta(z_n), \theta(z_n)) \in C$

n an ideal in

(assume $r|n$)

$\simeq End(L)$

$\simeq End(L) \times End(L)$

s.t. $N_{L/K}(u) = -1$

Let $u_i : L \to L$ $(1 \leq i \leq n)$ be semi-linear endomorphisms (i.e. $u_i = c_i \theta$)

Manbinq Peng '18

$$L[X;\theta]_{<k} \longrightarrow End(L)^s$$
$$P \longmapsto (P(u_1), \dots, P(u_s))$$

If $N_{L/K}(c_i)$ are pairwise distinct.

length = rs
dimension = $r \cdot k$
min. dist = $rs-k-1$ [MSRD]

Berardini, C. '25

Y Galois covering of curves with cyclic Galois group $\langle \theta \rangle$
$\downarrow$
X

G divisor on Y, $D_1, \dots, D_s$ points on X

Also need a function x on X

$$\Lambda(G) \longrightarrow \prod_{i=1}^{s} End(V_i)$$
$$P \longmapsto (P(D_1), \dots, P(D_s))$$

where $P(D_i)$ is by def. $P \bmod D_i$.

dimension $\geq r \cdot \deg G - g_D + 1$
min. dist $\geq rs - \deg G$

Berardini, C., Drain (coming soon)

$$\left(D = \frac{K(Y)[X;\theta]}{X^r - x} \right)$$

$\Omega_D = D \otimes_K \Omega_K$ (differentials)

$$\Omega_D(D-G) \longrightarrow \prod_{i=1}^{s} End(V_i)$$
$$\omega \longmapsto (\operatorname{res}_{D_i} \omega) = g_i(D_i) \text{ where } \omega = g_i \frac{dt_i}{t_i}$$

min. dist $\geq r \cdot \deg G - (2g_D - 2)$

Wang '18
Gomez, Lobillo, Navarro '23

More or less same definition.

Project:

- rewrite in the algebraic geometry language
- prove an improvement in some cases (I suspect $r = g-1$)

SUM-RANK

Ambient space:

$$E = M_r(K)^s = \mathrm{End}_K(V)^s$$

(K-linear case)

or $E = \mathrm{End}_K(L)^s$ (L-linear case)

where L/K is a finite extension

Distance:

$$w(P_1, \dots, P_s) = \sum_{i=1}^{s} \mathrm{rank}(P_i)$$

A code is a K-subspace (or L-subspace) of E

By definition:

(n) length = sr^2

(k) dimension = $\dim_K C$

(d) min. dist = $\min\{w(P) : P \in C\}$

Singleton bound:

$$\frac{k}{r} + d \leq \frac{n}{r} + 1$$

Duality:

On $M_r(K)$, we have the classical pairing:

$$\langle A, B \rangle = \mathrm{Tr}({}^tA \cdot B)$$

(it's just the scalar product entrywise)

Reformulation in terms of $\mathrm{End}_K(V)$:

We need a bilinear form on V

Then we define:

(adjoint): For $P: V \to V$, it is $P^*: V \to V$ defined by $\langle P^*(x), y \rangle = \langle x, P(y) \rangle$

(pairing): $\langle P, g \rangle = \mathrm{Tr}(P^* \circ g)$

When $V = L$, we take the bilinear form:

$$\langle x, y \rangle = \mathrm{Tr}_{L/K}(xy)$$

Skew polynomials

We want an evaluation that produces endomorphisms... so we shall evaluate at endomorphisms.

Just considering $K[x] \to \mathrm{End}_K(V)$

$$P \mapsto P(u)$$

is not enough to get something interesting.

Instead, we consider in addition scalar multiplications by L; this leads to introducing $L[X;\theta] = \{\sum a_i X^i\}$ with multiplication given by the rule:

$$X \cdot a = \theta(a) X$$

If $u: L \to L$ is semi-linear, i.e satisfies $u(ax) = \theta(a)\, u(x)$, then $P(u)$ makes sense for $P \in L[X;\theta]$.