Convolutional Codes From an Algebraic Geometric perspective

José Ignacio Iglesias Curto

joint works with
J. M. Muñoz Porras, J. Á. Domínguez Pérez, G. Serrano Sotelo,
F. J. Plaza Martín, Á. Muñoz Castañeda
Universidad de Salamanca

Zurich - June 7, 2023

Reed-Solomon are AG codes

Let $\mathbb{F}_q = \{0, \alpha_1, \dots, \alpha_{q-1}\}$, $\alpha = (\alpha_1, \dots, \alpha_{q-1}) \in \mathbb{F}_q^{q-1}$ and the evaluation map

$$\begin{aligned} ev_\alpha : \mathbb{F}_q[x]_{<k} &\longrightarrow \mathbb{F}_q^{q-1} \\ p(x) &\longrightarrow (p(\alpha_1), \dots, p(\alpha_{q-1})) \end{aligned}$$

$RS_q(n = q-1, k) = \mathrm{Im}\ \alpha.$

Reed-Solomon are AG codes

Let $\mathbb{F}_q = \{0, \alpha_1, \ldots, \alpha_{q-1}\}$, $\alpha = (\alpha_1, \ldots, \alpha_{q-1}) \in \mathbb{F}_q^{q-1}$ and the evaluation map

$$\begin{aligned} ev_\alpha : \mathbb{F}_q[x]_{<k} &\longrightarrow \mathbb{F}_q^{q-1} \\ p(x) &\longrightarrow (p(\alpha_1), \ldots, p(\alpha_{q-1})) \end{aligned}$$

$RS_q(n = q-1, k) = \mathrm{Im}\ \alpha$.
$\alpha_1, \ldots, \alpha_{q-1}$ are the affine coordinates of the points in $\mathbb{A}^1 - P_0$
$\mathbb{F}_q[x]_{<k}$ are the rational functions over $\mathbb{P}^1$ with at most $k-1$ poles at P_∞ (and nowhere else)

Goppa codes

- X, irreducible smooth projective curve of genus g over $\mathbb{F}_q$
- $P_1, \ldots, P_n$, n **different** $\mathbb{F}_q$-rational points of X,
  $D = P_1 + \cdots + P_n$
- $G = \sum n_i Q_i - \sum n'_j Q'_j$ with $suppG \cap suppD = \emptyset$
- Riemann-Roch space associated to G

$$L(G) = \left\{ f \in \mathbb{F}_q(X) \,\middle|\, \begin{array}{l} \text{has zeroes at least at the points } Q'_j\text{, of order} \geq n'_j, \\ \text{has poles only at the points } Q_i\text{, of order} \leq n_i \end{array} \right\}$$

Goppa codes

- X, irreducible smooth projective curve of genus g over $\mathbb{F}_q$
- $P_1, \dots, P_n$, n **different** $\mathbb{F}_q$-rational points of X, $D = P_1 + \cdots + P_n$
- $G = \sum n_i Q_i - \sum n'_j Q'_j$ with $suppG \cap suppD = \emptyset$
- Riemann-Roch space associated to G

$$L(G) = \left\{ f \in \mathbb{F}_q(X) \,\middle|\, \begin{array}{l} \text{has zeroes at least at the points } Q'_j, \text{ of order} \geq n'_j, \\ \text{has poles only at the points } Q_i, \text{ of order} \leq n_i \end{array} \right\}$$

There is a morphism (injective if $degG \leq degD$)

$$\begin{aligned} \alpha : L(G) &\longrightarrow \mathbb{F}_q^n \\ f &\longrightarrow (f(P_1), \dots, f(P_n)) \end{aligned}$$

Goppa codes

- X, irreducible smooth projective curve of genus g over $\mathbb{F}_q$
- $P_1, \ldots, P_n$, n **different** $\mathbb{F}_q$-rational points of X, $D = P_1 + \cdots + P_n$
- $G = \sum n_i Q_i - \sum n'_j Q'_j$ with $suppG \cap suppD = \emptyset$
- Riemann-Roch space associated to G

$$L(G) = \left\{ f \in \mathbb{F}_q(X) \,\middle|\, \begin{array}{l} \text{has zeroes at least at the points } Q'_j \text{, of order} \geq n'_j, \\ \text{has poles only at the points } Q_i \text{, of order} \leq n_i \end{array} \right\}$$

There is a morphism (injective if $degG \leq degD$)

$$\begin{aligned} \alpha : L(G) &\longrightarrow \mathbb{F}_q^n \\ f &\longrightarrow (f(P_1), \ldots, f(P_n)) \end{aligned}$$

Definition

$Im\alpha$ is the Goppa code $\mathcal{C}(D, G)$.

- length($\mathcal{C}$)=n, bounded by the number of rational points in X
- $dim\,\mathcal{C} = dim L(G)$
  By Riemann-Roch Theorem,

$$dim\,\mathcal{C} \geq \deg(G) + 1 - g,$$

Goppa codes

Parameters

- length($\mathcal{C}$)=n, bounded by the number of rational points in X
- $dim\,\mathcal{C} = dimL(G)$
  By Riemann-Roch Theorem,

$$dim\,\mathcal{C} \geq \deg(G) + 1 - g,$$

If $\deg(G) > 2g - 2 \Rightarrow dim\,\mathcal{C} = \deg(G) + 1 - g$.

- length($\mathcal{C}$)=n, bounded by the number of rational points in X
- $dim\,\mathcal{C} = dimL(G)$
  By Riemann-Roch Theorem,
  $$dim\,\mathcal{C} \geq \deg(G) + 1 - g,$$
  If $\deg(G) > 2g - 2 \Rightarrow dim\,\mathcal{C} = \deg(G) + 1 - g$.
- According to the number of zeros in $suppD$ of $f \in L(G)$,
  $$d \geq n - \deg(G) \;\Rightarrow\; d + k \geq n + 1 - g$$
- By Singleton bound
  $$n - k + 1 - g \leq d \leq n - k + 1$$

Dual Goppa codes

- X, irreducible smooth projective curve of genus g over $\mathbb{F}_q$
- $P_1, \ldots, P_n$ n **different** $\mathbb{F}_q$-rational points of X,
  $D = P_1 + \cdots + P_n$
- $G = \sum n_i Q_i - \sum n'_j Q'_j$
- $\Omega(G) = \left\{ \omega \in \Omega_X \,\middle|\, \begin{array}{l} \text{has zeros at least at } Q_i\text{, of order} \geq n_i, \\ \text{has poles only at } Q'_j\text{, of order} \leq n'_j \end{array} \right\}$

Dual Goppa codes

- X, irreducible smooth projective curve of genus g over $\mathbb{F}_q$
- $P_1, \dots, P_n$ n **different** $\mathbb{F}_q$-rational points of X,
  $D = P_1 + \cdots + P_n$
- $G = \sum n_i Q_i - \sum n'_j Q'_j$
- $\Omega(G) = \left\{ \omega \in \Omega_X \left| \begin{array}{l} \text{has zeros at least at } Q_i \text{, of order} \geq n_i, \\ \text{has poles only at } Q'_j \text{, of order} \leq n'_j \end{array} \right. \right\}$

There is a morphism (injective if $\deg(G) > 2g - 2$)

$$\begin{array}{rcl} \beta : \Omega(G - D) & \longrightarrow & \mathbb{F}_q^n \\ \omega & \longrightarrow & (res_{P_1}(\omega), \dots, res_{P_n}(\omega)) \end{array}$$

Dual Goppa codes

- X, irreducible smooth projective curve of genus g over $\mathbb{F}_q$
- $P_1, \dots, P_n$ n **different** $\mathbb{F}_q$-rational points of X,
  $D = P_1 + \cdots + P_n$
- $G = \sum n_i Q_i - \sum n'_j Q'_j$
- $\Omega(G) = \left\{ \omega \in \Omega_X \,\middle|\, \begin{array}{l} \text{has zeros at least at } Q_i\text{, of order} \geq n_i, \\ \text{has poles only at } Q'_j\text{, of order} \leq n'_j \end{array} \right\}$

There is a morphism (injective if $\deg(G) > 2g - 2$)

$$\begin{aligned} \beta : \Omega(G - D) &\longrightarrow \mathbb{F}_q^n \\ \omega &\longrightarrow (res_{P_1}(\omega), \dots, res_{P_n}(\omega)) \end{aligned}$$

Definition

$\mathrm{Im}\ \beta$ is the dual Goppa code $\mathcal{C}^*(D, G)$.

Dual Goppa codes
Properties

- length($\mathcal{C}^*$)=n,
- $dim\,\mathcal{C}^* = dim\,\Omega(G-D)$
  By Riemann-Roch Theorem,

$$dim\,\mathcal{C} \geq n - \deg(G) - 1 + g,$$

Dual Goppa codes

Properties

- length($\mathcal{C}^*$)$=n$,
- $dim\,\mathcal{C}^* = dim\,\Omega(G - D)$
  By Riemann-Roch Theorem,

$$dim\,\mathcal{C} \geq n - \deg(G) - 1 + g,$$

If $\deg(G) < n \Rightarrow dim\,\mathcal{C} = n - \deg(G) - 1 + g.$

Dual Goppa codes

Properties

- length($\mathcal{C}^*$)=n,
- $dim\,\mathcal{C}^* = dim\,\Omega(G - D)$
  By Riemann-Roch Theorem,

$$dim\,\mathcal{C} \geq n - \deg(G) - 1 + g,$$

  If $\deg(G) < n \Rightarrow dim\,\mathcal{C} = n - \deg(G) - 1 + g$.
- By the number of poles of $\omega \in \Omega(G - D)$, we have

$$d \geq \deg(G) - 2g + 2 \;\Rightarrow\; d + k \geq n + 1 - g$$

Dual Goppa codes

Properties

- length($\mathcal{C}^*$)=n,
- $dim\,\mathcal{C}^* = dim\,\Omega(G-D)$
  By Riemann-Roch Theorem,
  $$dim\,\mathcal{C} \geq n - \deg(G) - 1 + g,$$
  If $\deg(G) < n \Rightarrow dim\,\mathcal{C} = n - \deg(G) - 1 + g$.
- By the number of poles of $\omega \in \Omega(G-D)$, we have
  $$d \geq \deg(G) - 2g + 2 \;\Rightarrow\; d + k \geq n + 1 - g$$
- By the Residues Theorem $\mathcal{C}^*(D,G) = \mathcal{C}^{\perp}(D,G)$.

Dual Goppa codes

Properties

- length($\mathcal{C}^*$)=n,
- $dim\, \mathcal{C}^* = dim\, \Omega(G-D)$
  By Riemann-Roch Theorem,
  $$dim\, \mathcal{C} \geq n - \deg(G) - 1 + g,$$
  If $\deg(G) < n \Rightarrow dim\, \mathcal{C} = n - \deg(G) - 1 + g$.
- By the number of poles of $\omega \in \Omega(G-D)$, we have
  $$d \geq \deg(G) - 2g + 2 \;\Rightarrow\; d + k \geq n + 1 - g$$
- By the Residues Theorem $\mathcal{C}^*(D,G) = \mathcal{C}^{\perp}(D,G)$.
- $\mathcal{C}^*(D,G) = \mathcal{C}(D, K + D - G)$.

Convolutional construction

Aim:

Develop an analogous construction for convolutional codes

Two possible (equivalent) settings

- CC as submodules over $\mathbb{F}_q[z]$
- CC as subspaces over $\mathbb{F}_q(z)$

Convolutional construction

Aim:
Develop an analogous construction for convolutional codes
Two possible (equivalent) settings

- CC as submodules over $\mathbb{F}_q[z]$
- CC as subspaces over $\mathbb{F}_q(z)$

CC as a free submodule of $\mathbb{F}_q[z]^n$

Block codes		Convolutional codes
subspaces over $\mathbb{F}_q$		submodules over $\mathbb{F}_q[z]$
X a curve over $\mathbb{F}_q$	$\rightsquigarrow$	X a family of curves parameterized by $\mathbb{A}^1$
n rational points	$\rightsquigarrow$	n sections of $X \to \mathbb{A}^1$
a divisor G	$\rightsquigarrow$	an invertible sheaf $\mathcal{L}$

The evaluation map

Let us recall how the evaluation map is defined:
Let D be a divisor over X. We have an exact sequence

$$0 \longrightarrow \mathcal{O}_X(-D) \longrightarrow \mathcal{O}_X \longrightarrow \mathcal{O}_D \longrightarrow 0\,,$$

where $\mathcal{O}_D \simeq \mathbb{F}_q^n$.
G a divisor with $suppG \cap suppD = \emptyset$, $\mathcal{O}_X(G)$ invertible sheaf.
By tensoring by $\mathcal{O}_X(G)$ and taking global sections we have

$$0 \longrightarrow H^0(X, \mathcal{O}_X(G-D)) \longrightarrow H^0(X, \mathcal{O}_X(G)) \equiv L(G) \xrightarrow{\alpha} \mathbb{F}_q^n \longrightarrow \dots$$

- $X \xrightarrow{\pi} \mathbb{A}^1$ a family of curves parameterized by $\mathbb{A}^1$.
- $p_i := \mathbb{A}^1 \to X$, $1 \leq i \leq n$, different sections of π,
  $D = p_1(\mathbb{A}^1) \cup \ldots \cup p_n(\mathbb{A}^1)$, a Cartier divisor on X.
- $\mathcal{L}$ an invertible sheaf over X.

- $X \xrightarrow{\pi} \mathbb{A}^1$ a family of curves parameterized by $\mathbb{A}^1$.
- $p_i := \mathbb{A}^1 \to X$, $1 \leq i \leq n$, different sections of π,
  $D = p_1(\mathbb{A}^1) \cup \ldots \cup p_n(\mathbb{A}^1)$, a Cartier divisor on X.
- $\mathcal{L}$ an invertible sheaf over X.

We have

$$0 \longrightarrow \mathcal{L}(-D) \longrightarrow \mathcal{L} \longrightarrow \mathcal{O}_D \otimes \mathcal{L} \simeq \mathcal{O}_D \longrightarrow 0\,,$$

and by taking global sections

$$0 \longrightarrow H^0(X, \mathcal{L}(-D)) \longrightarrow H^0(X, \mathcal{L}) \xrightarrow{\alpha} H^0(X, \mathcal{O}_D) \longrightarrow \ldots,$$

There are (non-canonical, in general) isomorphisms

$$\phi : H^0(X, \mathcal{O}_D) \xrightarrow{\sim} \mathbb{F}_q[z]^n$$

Definition

The convolutional Goppa code defined by $\mathcal{L}, D, \phi$ is the submodule $\mathcal{C}(\mathcal{L}, D, \phi) = \mathrm{Im}\ \phi \circ \alpha$ with

$$H^0(X, \mathcal{L}) \xrightarrow{\alpha} H^0(X, \mathcal{O}_D) \xrightarrow{\phi} \mathbb{F}_q[z]^n$$

There are (non-canonical, in general) isomorphisms

$$\phi : H^0(X, \mathcal{O}_D) \xrightarrow{\sim} \mathbb{F}_q[z]^n$$

Definition

The convolutional Goppa code defined by $\mathcal{L}, D, \phi$ is the submodule $\mathcal{C}(\mathcal{L}, D, \phi) = \mathrm{Im}\ \phi \circ \alpha$ with

$$H^0(X, \mathcal{L}) \xrightarrow{\alpha} H^0(X, \mathcal{O}_D) \xrightarrow{\phi} \mathbb{F}_q[z]^n$$

Further, we may consider a subspace $\Gamma \subseteq H^0(X, \mathcal{L})$.

Definition

The convolutional Goppa code defined by Γ, D, ϕ is the submodule $\mathcal{C}(\Gamma, D, \phi) = \mathrm{Im}\ \phi \circ \alpha|\Gamma$.

There are (non-canonical, in general) isomorphisms

$$\phi : H^0(X, \mathcal{O}_D) \xrightarrow{\sim} \mathbb{F}_q[z]^n$$

Definition

The convolutional Goppa code defined by $\mathcal{L}, D, \phi$ is the submodule $\mathcal{C}(\mathcal{L}, D, \phi) = \mathrm{Im}\ \phi \circ \alpha$ with

$$H^0(X, \mathcal{L}) \xrightarrow{\alpha} H^0(X, \mathcal{O}_D) \xrightarrow{\phi} \mathbb{F}_q[z]^n$$

Further, we may consider a subspace $\Gamma \subseteq H^0(X, \mathcal{L})$.

Definition

The convolutional Goppa code defined by Γ, D, ϕ is the submodule $\mathcal{C}(\Gamma, D, \phi) = \mathrm{Im}\ \phi \circ \alpha|\Gamma$.

The dual convolutional Goppa codes are obtained analogously.

	Block codes	Convolutional codes
Subspaces over	$\mathbb{F}_q$	$\mathbb{F}_q(z)$
A curve over	$\mathbb{F}_q$	$\mathbb{F}_q(z)$
n **different** points	$\mathbb{F}_q$-rational	$\mathbb{F}_q(z)$-rational

- Simpler tools
- The submodule approach yields this one by taking the fiber at the generic point
- Not every curve over $\mathbb{F}_q(z)$ extends to a family parameterized by $\mathbb{A}^1$
- The submodule approach allows characterization of basic matrices

Convolutional Goppa codes

$\mathbb{F}_q(z)$-vector subspaces

- X, irreducible smooth projective curve of genus g over $\mathbb{F}_q(z)$
- $P_1, \ldots, P_n$, n **different** $\mathbb{F}_q(z)$-rational points of X,
  D the divisor $D = P_1 + \cdots + P_n$
- $G = \sum n_i Q_i - \sum n'_j Q'_j$ another divisor in X with
  $suppG \cap suppD = \emptyset$

  $L(G)$ the $\mathbb{F}_q(z)$-vector space of global sections of $\mathcal{O}_X(G)$

Convolutional Goppa codes

$\mathbb{F}_q(z)$-vector subspaces

- X, irreducible smooth projective curve of genus g over $\mathbb{F}_q(z)$
- $P_1, \ldots, P_n$, n **different** $\mathbb{F}_q(z)$-rational points of X,
  D the divisor $D = P_1 + \cdots + P_n$
- $G = \sum n_i Q_i - \sum n'_j Q'_j$ another divisor in X with $suppG \cap suppD = \emptyset$

  $L(G)$ the $\mathbb{F}_q(z)$-vector space of global sections of $\mathcal{O}_X(G)$

If $degG \leq degD$, there exists an injective morphism

$$\begin{aligned} \alpha : L(G) &\longrightarrow \mathbb{F}_q(z)^n \\ s &\longmapsto (s(P_1), \ldots, s(P_n)) \end{aligned}$$

Definition

$Im\alpha \cap \mathbb{F}_q[z]^n$ is the convolutional Goppa code $\mathcal{C}(D, G)$.

Convolutional Goppa codes

$\mathbb{F}_q(z)$-vector subspaces

- X, irreducible smooth projective curve of genus g over $\mathbb{F}_q(z)$
- $P_1, \ldots, P_n$, n **different** $\mathbb{F}_q(z)$-rational points of X,
  D the divisor $D = P_1 + \cdots + P_n$
- $G = \sum n_i Q_i - \sum n'_j Q'_j$ another divisor in X with
  $suppG \cap suppD = \emptyset$

  $L(G)$ the $\mathbb{F}_q(z)$-vector space of global sections of $\mathcal{O}_X(G)$

If $degG \leq degD$, there exists an injective morphism

$$\begin{aligned} \alpha : L(G) &\longrightarrow \mathbb{F}_q(z)^n \\ s &\longmapsto (s(P_1), \ldots, s(P_n)) \end{aligned}$$

Definition

$Im\alpha \cap \mathbb{F}_q[z]^n$ is the convolutional Goppa code $\mathcal{C}(D, G)$.

The dual construction is carried out in the same way.

- Riemann-Roch Theorem and Residues Theorem are of application in this setting.
- Parameters:
  - length($\mathcal{C}$)=length($\mathcal{C}^*$)=n
  - If $2g - 2 < \deg(G) < n$

$$dim\, \mathcal{C} = \deg(G) + 1 - g$$
$$dim\, \mathcal{C}^* = n - \deg(G) - 1 + g$$

  - The free distances are loosely bounded by the number of zeros/poles.

- Riemann-Roch Theorem and Residues Theorem are of application in this setting.
- Parameters:
  - length($\mathcal{C}$)=length($\mathcal{C}^*$)=n
  - If $2g - 2 < \deg(G) < n$

$$dim\,\mathcal{C} = \deg(G) + 1 - g$$
$$dim\,\mathcal{C}^* = n - \deg(G) - 1 + g$$

  - The free distances are loosely bounded by the number of zeros/poles.
- $\mathcal{C}^*(D, G) = \mathcal{C}^{\perp}(D, G)$

An example over an elliptic curve

- X the curve $y^2 + zxy + y = x^3 + x^2$ over $\mathbb{F}_2(z)$
- $D = P_1 + P_2 + P_3 + P_4$ with

$$\begin{array}{cc} P_1 = (1+z, z) & P_2 = (1+z, 1+z^2) \\ P_3 = (\frac{1+z^3}{z^2}, \frac{1+z^3+z^4+z^5}{z^3}) & P_4 = (\frac{1+z^3}{z^2}, \frac{1+z^2+z^4}{z^3}) \end{array}$$

- $G = 3P_\infty - P_0$
  $L(G) = \langle x, y \rangle = \left\langle \frac{z^2}{1+z} x \, , \, zy + \frac{1+z+z^2}{1+z} x \right\rangle.$

An example over an elliptic curve

- X the curve $y^2 + zxy + y = x^3 + x^2$ over $\mathbb{F}_2(z)$
- $D = P_1 + P_2 + P_3 + P_4$ with

$$\begin{array}{cc} P_1 = (1+z, z) & P_2 = (1+z, 1+z^2) \\ P_3 = (\frac{1+z^3}{z^2}, \frac{1+z^3+z^4+z^5}{z^3}) & P_4 = (\frac{1+z^3}{z^2}, \frac{1+z^2+z^4}{z^3}) \end{array}$$

- $G = 3P_\infty - P_0$
  $L(G) = \langle x, y \rangle = \left\langle \frac{z^2}{1+z} x \, , \; zy + \frac{1+z+z^2}{1+z} x \right\rangle$.

$\mathcal{C}(D, G)$ is generated by

$$\begin{pmatrix} z^2 & z^2 & 1+z+z^2 & 1+z+z^2 \\ 1+z & 1+z^2+z^3 & 1+z+z^3 & 0 \end{pmatrix}$$

$\mathcal{C}(D, G)$ has parameters $[n, k, \delta, m, d_{free}] = [4, 2, 5, 3, 8]$ reaching the Griesmer bound.

Convolutional vs Block

On the one (adverse) side

- Convolutional construction is far more complex
- Distance issues: free distance cannot be related to zeroes of functions
- Decoding via an evaluator polynomial cannot be (straightforwardly) applied

On the other (favorable) one

- many optimal constructions on curves with low genus
- curves over $\mathbb{F}_q(z) \to$ infinitely many rational points
- also block codes can be constructed in this way

AG structure of any code

Block codes

- R. Pellikaan et al. ("Which linear codes are algebraic geometric?")

Every code may be given a certain algebraic geometric structure over a curve with sufficiently many points (high genus)

AG structure of any code

Block codes

- R. Pellikaan et al. ("Which linear codes are algebraic geometric?")

Every code may be given a certain algebraic geometric structure over a curve with sufficiently many points (high genus)

Convolutional codes

- Every code may be given a certain algebraic geometric structure over $\mathbb{P}^1$ (and any other curve)
- Characterization of codes with complete Goppa structure over $\mathbb{P}^1$, elliptic and hiperelliptic curves.
- Explicit constructions
- Characterization of MDS codes of rate $1/n$.

Conclusions

Much has been done

- AG constructions work for CC
- explicit examples of optimal codes can be easily obtained
- characterizations over curves with low genus and codes of low rates

and much remains to be done

- characterization of the free distance
- decoding algorithms
- more general characterizations

Thank you!