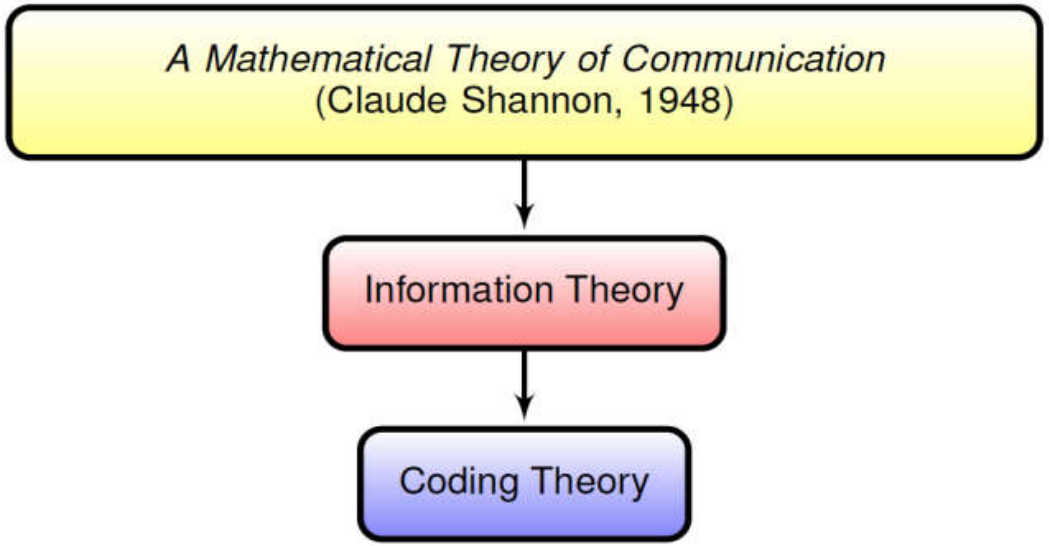
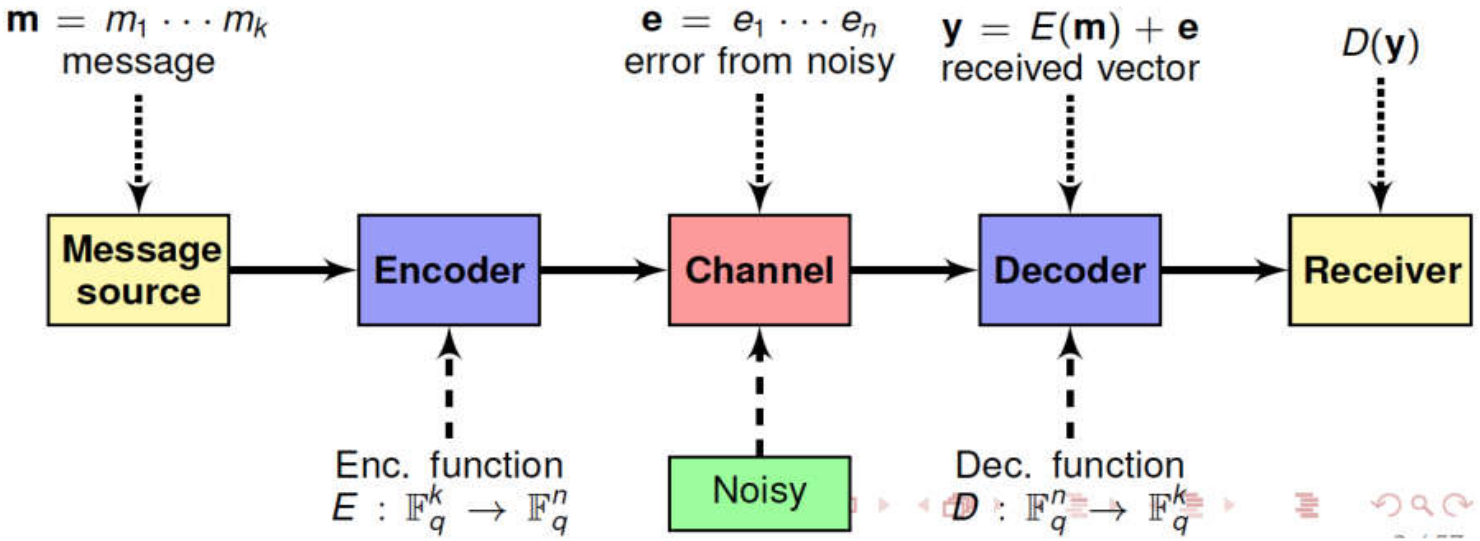
Groupes d'automorphisme des codes GRS et dérivés

Ousmane NDIAYE, LACGAA, DMI, UCAD

Codes linéaires

Claude Shannon
(1916-2001)





Codes linéaires: Généralités

▷ Le *poids de Hamming* d'un vecteur $\boldsymbol{x} \in \mathbb{F}_q^n$ est le nombre de positions non-nulles :

$$\mathsf{wt}(\boldsymbol{x}) = \Big|\{i \;\; / \;\; x_i \neq 0\}\Big|$$

▷ La *distance de Hamming* $\mathsf{dist}(\boldsymbol{x}, \boldsymbol{y})$ entre $\boldsymbol{x}$ et $\boldsymbol{y}$:

$$\mathsf{dist}(\boldsymbol{x}, \boldsymbol{y}) = \mathsf{wt}(\boldsymbol{x} - \boldsymbol{y})$$

▷ $\mathscr{C}$ est un *code linéaire* sur $\mathbb{F}_q$ de longueur n, de dimension k si $\mathscr{C}$ est un sous-espace vectoriel sur $\mathbb{F}_q^n$ de dimension k

▷ *Matrice génératrice* $\boldsymbol{G}$ de $\mathscr{C}$ est une matrice de taille $k \times n$ obtenue en prenant une base de $\mathscr{C}$

Le décodeur $\gamma_{\boldsymbol{G}}$ *corrige* t erreurs ssi $\forall \boldsymbol{e} \in \mathbb{F}_q^n$ et $\forall \boldsymbol{m} \in \mathbb{F}_q^k$, on a :

$$\mathsf{wt}(\boldsymbol{e}) \leq t \quad \Longrightarrow \quad \gamma_{\boldsymbol{G}}\Big(\boldsymbol{m} \times \boldsymbol{G} \oplus \boldsymbol{e}\Big) = \boldsymbol{m}.$$

▷ La *distance minimale* $\mathsf{dist}(\mathscr{C})$ de $\mathscr{C}$ est définie par :

$$\mathsf{dist}(\mathscr{C}) = \min_{x \in \mathscr{C} - \{\mathbf{0}\}} \mathsf{wt}(\boldsymbol{x})$$

▷ *Paramètres* d'un code linéaire $[n, k, d]_q$

- n : longueur
- k : dimension
- d : distance minimale

Capacité de correction :
du code $\mathcal{C}$ de paramètres $[n, k, d]_q$ est l'entier t tel que $t = \lfloor \frac{d-1}{2} \rfloor$.
Pourquoi ?

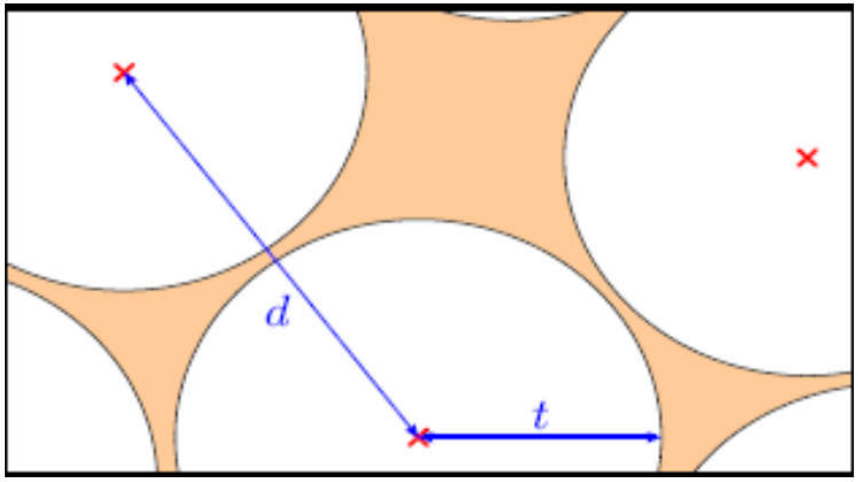


FIGURE 2 – Distance minimale d et capacité de correction t

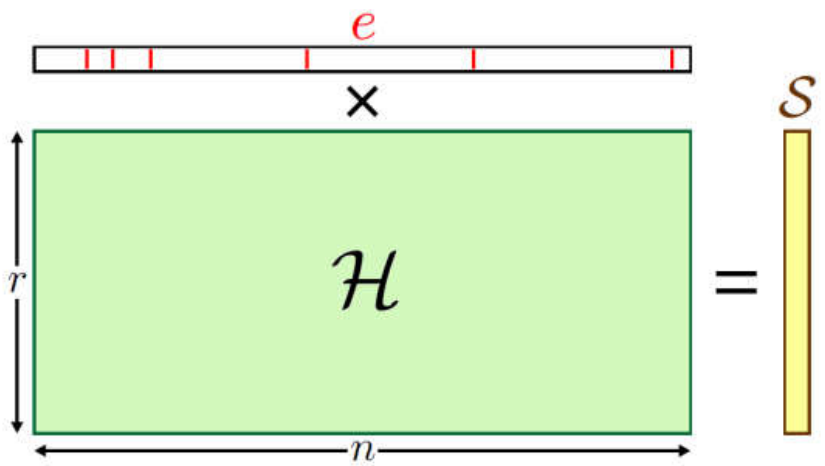
Soit C un $[n, k, d]_q$-code de matrice génératrice $\boldsymbol{H}$ alors il existe
$\boldsymbol{C^{\perp}} = \{\boldsymbol{x} \in \boldsymbol{F_q^n} \mid \forall\, \boldsymbol{y} \in \boldsymbol{C}\colon\ \boldsymbol{x}.\boldsymbol{y} = \boldsymbol{0}\}$=$\{\boldsymbol{x} \in \boldsymbol{F_q^n} \mid \boldsymbol{H}.\boldsymbol{x^t} = \boldsymbol{0}\}$ est un code de longueur n et de dimension $\boldsymbol{n - k}$. $\boldsymbol{H}$ est appelé matrice de parité de $\boldsymbol{C^{\perp}}$

Cryptographie à base de codes

Données. $\begin{cases} \mathcal{H} & : & \text{matrice de taille } r \times n \\ \mathcal{S} & : & \text{vecteur de } \mathbb{F}_q^r \\ t & : & \text{entier} \end{cases}$

Problème.

Existe-t-il e vecteur de $\mathbb{F}_q^n$ **de poids** t tel que : $\mathcal{H}^t e = \mathcal{S}$?



Problème $\mathcal{NP}$-complet
E.R. Berlekamp, R.J. McEliece et H.C. Van Tilborg.
On the inherent intractability of certain coding problems. IEEE Transactions on Information Theory, 24(3), mai 1978.

Cryptosystème de McEliece

Données privées.

$\mathcal{G}$: matrice génératrice d'un code $\mathcal{C}$ que l'on sait décoder
P : matrice de permutation de taille $n \times n$
Q : matrice inversible de taille $k \times k$
$\gamma_{\mathcal{G}}$: algorithme de décodage jusqu'à $\frac{d}{2}$ erreurs

Données publiques.

$\mathcal{G}' \stackrel{\text{déf}}{=} Q\mathcal{G}P$
t : entier $< \frac{d}{2}$

Chiffrement

Soit m le message clair que l'on veut envoyer

1. choisir e une erreur aléatoire de poids t ;
2. calculer $c' = m\mathcal{G}' \oplus e$;

- c' est le texte chiffré.

Déchiffrement

1. calculer $c'P^{-1} = (mQ)\mathcal{G} \times PP^{-1} \oplus eP^{-1}$;
- eP^{-1} est de poids t et $(mQ)\mathcal{G}$ est un mot du code ;
2. à l'aide de $\gamma_{\mathcal{G}}$ on décode et on retrouve $(mQ)\mathcal{G}$;
3. prendre les k premiers bits de $(mQ)\mathcal{G}$, que l'on note $\tilde{m}$.
- on obtient alors $\tilde{m} = mQ$ car $\mathcal{G}$ a été prise sous forme systématique.
4. calculer $\tilde{m}Q^{-1} = (mQ)Q^{-1}$ pour obtenir m.

Avantages:
-Très efficace
-Sécurité théorique Prouvée par réduction aux problèmes NP-Complets
-Résistant à tous les algorithmes quantiques ,
Inconvénient: Très grande taille de la clé publique.
Solutions: trouver des codes à matrice génératrice redondante

GRS codes

- Soit $\alpha = (\alpha_1, \dots, \alpha_n)$ où les α_i sont des éléments distincts deux de K^n, $\beta = (\beta_1, \dots, \beta_n)$ un n-uplet d'éléments non nuls de K^n et $1 \leq k \leq n-1$. Alors le code de Reed-Salomon Généralisé $GRS_k(\alpha, \beta)$ est défini par

$$GRS_k(\alpha, \beta) = \left\{ \left(\beta_1 P(\alpha_1), \dots, \beta_n P(\alpha_n) \right) : P \in K[X]_{k-1} \right\}$$

qui est un code $[n, k]$ sur K.

$$K[X]_{k-1} \to GRS_k(\alpha, \beta) : P \to \left(\beta_1 P(\alpha_1), \dots, \beta_n P(\alpha_n) \right)$$

$L = \{\alpha_1, \dots, \alpha_n\}$ est appelé support du code $GRS_k(\alpha, \beta)$

$$G = \begin{pmatrix} \beta_1 \alpha_1^0 & \cdots & \beta_n \alpha_n^0 \\ \vdots & \ddots & \vdots \\ \beta_1 \alpha_1^{k-1} & \cdots & \beta_n \alpha_n^{k-1} \end{pmatrix}$$ est une matrice génératrice de $GRS_k(\alpha, \beta)$.

Code de Cauchy

Il est possible de générer les code GRS par les code de Cauchy définit sur la droite projective $P^1(K) = \overline{K} = K \cup \{\infty\}$ et donc tout code $GRS_k(\alpha, y)$ est Code de Cauchy $C_k(\alpha, y)$ avec $P \in K[X, Y]_{k-1}$ de ensemble des polynômes homogènes de $degré = k - 1$

Codes GRS et codes dérivés

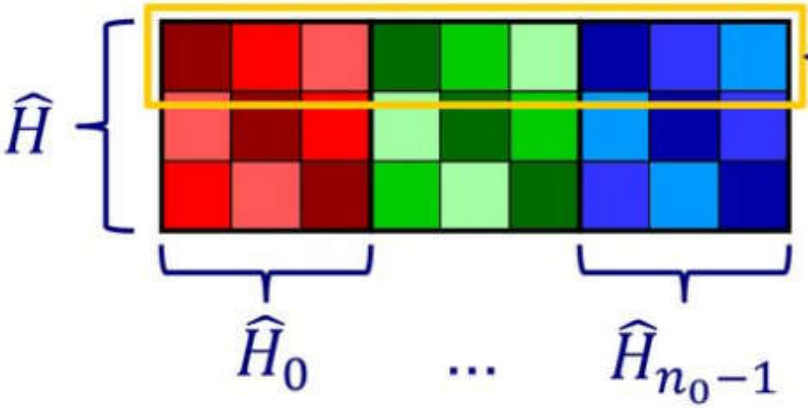
- Code Alternant: Soit $\alpha = (\alpha_1, \dots, \alpha_n)$ où les α_i sont des éléments distincts deux de K^n,
  $\beta = (\beta_1, \dots, \beta_n)$ un n-uplet d'éléments non nuls de K^n et $1 \leq k \leq n-1$. Alors le code Alternant $A_k(\alpha, \beta)$ est le code de longueur n sur $F = GF(p)$ avec p caractéristique de K de matrice de Parité

$$V_{n,k}(\alpha, \beta) = \begin{pmatrix} \beta_1 \alpha_1^0 & \cdots & \beta_n \alpha_n^0 \\ \vdots & \ddots & \vdots \\ \beta_1 \alpha_1^{k-1} & \cdots & \beta_n \alpha_n^{k-1} \end{pmatrix}$$

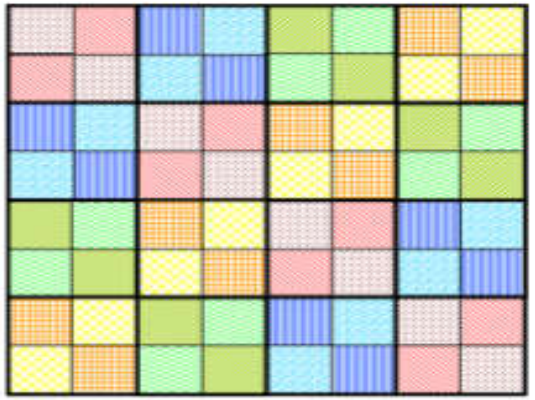
- $G_k(\alpha, \beta)$ est le code de Goppa de longueur n sur $F = GF(p)$ ssi $G_k(\alpha, \beta)$ un code alternant et qu'il existe un polynôme $g \in K[X]$ tel que $\forall\, i \in [\![1 \dots n]\!],\ \beta_i = g(\alpha_i)^{-1}$.

Codes algébriques structurés

- **Codes cycliques (quasi-)∩ Aternant**



- **Codes dyadiques (quasi-)∩ Aternant**



Besoin de connaitre le groupe de Permutation pour une construction efficace de ces codes !

Attaques Algébriques: McEliece(78)

- $G = Q \cdot V_{n,k}(\alpha, y) \cdot P = Q \cdot \begin{pmatrix} \beta_{1\alpha_1^0} & \cdots & \beta_{n\alpha_n^0} \\ \vdots & \ddots & \vdots \\ \beta_1 \alpha_1^{k-1} & \cdots & \beta_n \alpha_n^{k-1} \end{pmatrix} \cdot P$ est une matrice génératrice d'un code alternant équivalent. Donc il exist $H = V_{n,t}(x, y)$ tel que $HG^{\mathbf{t}} = 0_{t,k}$

$\mathrm{McE}_{n,k,t}(\boldsymbol{X}, \boldsymbol{Y})=$

$$\begin{cases} \vdots \\ g_{i,0} Y_0 X_0^j + \ldots + g_{i,n-1} Y_{n-1} X_{n-1}^j = 0 \text{ with } \begin{cases} i \in \{0, \ldots, k-1\} \\ j \in \{0, \ldots, t-1\} \end{cases} \\ \vdots \end{cases}$$

Premier niveau de sécurité $q = 2^{10}, n = 1024, t = 50$ et $k \geq 524$.
Soit plus de **26200 équations non-linéaires et 2048 inconnus**

Bases de Groebner → **Besoin du groupe de Permutation pour réduire les variables**

- ***Espaces Projectifs***
  Soit K un corps fixé et n un entier fixé $(char(K) \neq 0)$. Posons $E = K^{n+1}$ un espace vectoriel de dimension n+1 sur K. Notons pour tout $x \in E$ de coordonnées affines $(x_0, \dots, x_n)$.

Définition: soit R une relation d'équivalence sur $E - \{0\}$:

$$xRy \leftrightarrow \exists\, \alpha \in K^* : y = \alpha x$$

Définition: L'espace projectif associé à E noté P(E) est l'ensemble quotient de $E - \{0\}$ par la relation R. Noté aussi $P^n(K)$.

Définition: Soit F un sous-espace de E de dimension $m + 1$, alors l'image de F par la projection canonique induite par R est définie comme sous espace projectif de $P(E)$ de dimension m noté $\overline{F} = P(F)$

- **Lien Affine-projectif**

Soit H un hyperplan vectoriel de $E \equiv K^{n+1}$ d'équation $x_0 = 0$ et $\overline{H}$ l'hyperplan projectif associé à H et posons $U = P^n(K) - \overline{H}$. Alors nous avons une bijection entre

$$\varphi\colon U \to K^n : \overline{x} = \overline{\alpha(x_0, \dots, x_n)} \to \left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right)$$

Donc L'image de $\overline{x}$ ne dépend pas du système de coordonnées homogène fixé. L'application φ est une bijection de réciproque

$$(y_1, \dots, y_n) \to \overline{(1, y_1, \dots, y_n)}$$

Cette bijection permet de décrire $P^n(K) = U \cup \overline{H} = K^n \cup \overline{H}$

On dira que l'espace affine de dimension finie K^n est plongé dans l'espace projectif $P^n(K)$ de même dimension. Un point de K^n est appelé est dit point à **distance finie** et un point de $\overline{H}$ est dit point à l'**infini**

- ***La Droite Projective***

Posons $E = K^2$ *et* $H = \{(x_0, x_1) \in K^2 : x_1 = 0\}$ *comme hyperplan à l'infini . Comme tous les élément de* H *sont colinéaire alors* $\overline{H}$ *est réduit à un seul élément noté* $\infty = \overline{(1,0)}$ *. Donc le plongement de* K *sur* $P^1(K)$ *se traduit par* $x \to \overline{(x,1)}$ *donc* $P^1(K) = K \cup \{\infty\}$

Homographie d'espace projectif

Soit E_1 et E_2 deux K-espaces vectoriel et $f : E_1 \to E_2$.

f envoie les droites de $(\mathrm{E}_1 \backslash Kerf) \cup \{0\}$ sur des droites de E_2.

f induit une application $P(f) = \overline{f} : P(E_1) \backslash \mathrm{P}(Kerf) \to P(E_2)$ telle que le diagramme suivant soit commutatif:

Remarque : $\overline{f \circ g} = \overline{f} \circ \overline{g}$

- ***Définition***: Soit $P(E_1)$ et $P(E_2)$ deux espace projectifs. Un morphisme d'espace projectif est une application $\varphi: P(E_1)\backslash \mathrm{P}(F) \to P(E_2)$ où $P(F)$ est un sous espace projectif de $P(E_1)$ tel qu'il $f \in L(E_1, E_2)$ et $F = Kerf(f)$ et $\varphi = \overline{f}$
- Si de plus $E_1 = E_2$ et $f \in GL(E)$ alors $\varphi = \overline{f}$ est appelé homographie. L'ensemble des homographie forme un groupe noté $PGL(E)$
- ***Proposition***:$\overline{f} = \overline{g}$ si et seulement si $\exists\ \lambda \in K^*$ tel que $f = \lambda g$
  - Si $f = \lambda g$ alors $f(x) = \lambda g(x) = g(\lambda x)$ donc $\overline{f(x)} = \overline{g(\lambda x)} = \overline{g(x)}$ donc $\overline{f} = \overline{g}$
  - Si $\overline{f} = \overline{g}$ alors $\ker(f) = Ker(g)$ et $Im(f) = Im(g)$.
    Soit H le supplémentaire de $\ker(f)$ alors $f_H, g_H: H \to Imf$ sont des isomorphismes et $\overline{f_H} = \overline{g_H}$ donc$\overline{f_H}^{-1} \circ \overline{g_H} = id_{P(H)}$ donc une homothétie ie $\exists\ \lambda \in K^*$ tel que $f_H^{-1} \circ g_H = \lambda Id_H$ donc $f = \lambda g$

- *Propriétés:*
  - *Le groupe des homographies $PGL(E)$ est transitif sur $P(E)$*
  - Les homographies de $P^1(K) = P(K^2)$ sont des applications de la forme

$$\overline{f}: P^1(K) \backslash \mathrm{Ker}(f) \to P^1(K)$$

$$x \to \frac{a_1 x + b_1}{c_1 x + d_1}$$

$\overline{f}$ homographie alors $f = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K^2)$ tel que $ad - cb \neq 0$.

Par convention $\frac{1}{0} = \infty$

- $f(x,1) = (ax + b, cx + d)$
  - si $cx + d \neq 0$ alors $\overline{f(x,1)} = \overline{(\frac{ax+b}{cx+d}, 1)}$
  - si $cx + d = 0$, $\overline{f(x,1)} = \overline{(ax + b, 0)} = \overline{(1,0)} = \infty$
- et $f(1,0) = (a,c) = (1,0)\ ou\ (\frac{a}{c}, 1)$

Centres des groupe linéaire ($\mathrm{E} = K^n$)

- Le centre Z de $GL(E)$ est formé des homothéties. Il est donc isomorphe à $K^* Id_E = K^*$.
- $SL_n(K) = Ker(det)\ alors\ GL(E)$ est isomorphe à $SL(E) \rtimes K^*$.

- Le centre de $SL(E)$ est égal à $Z \cap SL(E) = (K^* Id_E) \cap SL(E)$. Il est isomorphe au sous-groupe des racines $n^{ième}$ de l'unité dans K: $U_n(K)$.

- Proposition : $PGL(E) = GL(E)/(K^* Id_E)$
  - Π: $GL(E) \to PGL(E)$ est un morphisme de groupe dont le noyau est formé par les homothéties de $\boldsymbol{E}$
- *On note $PSL_n(K)$ l'image du groupe spécial linéaire $SL_n(K)$ par la projection $GL_n(K) \to PGL_n(K)$. $PSL_n(K)$* est obtenu comme le quotient de $SL_n(K)$ par le sous-groupe des racines $n^{ième}$ de l'unité dans K (son centre).

- *Proposition:* $PSL_n(K) \cong$ Z.$SL_n(K)$/Z avec $Z = Z(GL(E))$

Groupes semi-linéaires

- On définit le groupe général semi-linéaire sur $\mathrm{E} = K^n$:

$$\Gamma L_n(K) = GL_n(K) \rtimes Gal(K)$$

- On définit le groupe projectif semi-linéaire sur $\mathrm{E} = K^n$:

$$P\Gamma L_n(K) = PGL_n(K) \rtimes Gal(K)$$

- où $\forall F = (f, \gamma) \in P\Gamma L_n(K)$, $z \in \overline{K}$ $F(z) = f(\gamma(z))$ et $\gamma(\infty) = \infty$.
- Le groupe affine $Aff_n(K)$ est un prolongement de $GL_n(K)$ par le groupe K^n . Il peut être écrit en tant que produit semi - direct :

$$Aff_n(K) = AGL_n(K) = GL_n(K) \ltimes K^n$$

- Le groupe affine Projectif $\mathrm{P}Aff_n(K)$ est un prolongement de $\mathrm{P}GL_n(K)$ par le groupe K^n . Il peut être écrit en tant que produit semi - direct :

$$PAff_n(F) = PAGL_n(K) = PGL_n(K) \ltimes K^n$$

Sous-groupes dérivés

- $GL_n(F_2) \cong SL_n(F_2) \cong PSL_n(F_2) \cong PGL_n(F_2)$
- $GL_2(F_2) \cong S_3$
- Pour $n \neq 2$ ou $K \neq F_2$ alors on a $D(GL(E)) = SL(E)$.
- Pour $n = 2$ et $K = F_2$ alors on a $D\left(GL_2(F_2)\right) \cong A_3$
- Pour $n \neq 2$ ou $K \neq F_2, F_3$, on a $D(SL(E)) = SL(E)$
- Pour n = 2
  - Si $K = F_2$, on a $D\left(SL_2(F_2)\right) \cong A_3$, et on a aussi $SL_2(F_2) \cong S_3$.
  - Si $K = F_3$, on a $D\left(SL_2(F_3)\right) \cong H_8$, et on a aussi $SL_2(F_3) \cong H_8 \ \therefore Z/3Z$.
  - .

- Si $K = F_q$ un corps fini de cardinal q
  - $\left|P^n(F_q)\right| = |K^n \cup K^{n-1} \cup \cdots \cup K \cup \{\infty\}| = q^n + q^{n-1} + \cdots + q + 1$
    - Plongement des Espaces affines
  - $\left|GL_n(F_q)\right|$=$(q^n - 1)(q^n - q)(q^n - q^2) \ldots (q^n - q^{n-1})$
    - Il suffit de compter de nombre de bases possible
  - $\left|SL_n(F_q)\right|$=$\left|PGL_n(F_q)\right| = (q^n - 1)(q^n - q)(q^n - q^2) \ldots (q^n - q^{n-2})q^{n-1}$
    - Pour $PGL_n(F_q)$ il suffit d'utiliser $PGL(E) = GL(E)/(K^* Id_E)$
    - Pour $\left|SL_n(F_q)\right| = |Ker(det)| = \frac{\left|GL_n(F_q)\right|}{|F_q^*|}$
  - $\left|PSL_n(F_q)\right| = \frac{|SL_n(F_q)|}{|U_n(F_q)|} = \frac{|SL_n(F_q)|}{PGCD(n,q-1)}$

Définition: Groupe de Hamming de K^n

Le groupe de Hamming de K^n est l'ensemble des applications semi-linéaires note H de K^n dans lui même qui préservent la distance de Hamming.

Proposition: $\mathbf{H} \cong \boldsymbol{H_n(K)} = (\boldsymbol{K}^*)^{\boldsymbol{n}} \rtimes (\boldsymbol{S_n} \times \boldsymbol{Gal(K)})$ où $(\boldsymbol{K}^*)^{\boldsymbol{n}}$ est le groupe produit, $\boldsymbol{Gal(K)}$ le groupe des automorphisme de $\boldsymbol{K}$ sur son corps primitif.

$(\boldsymbol{S_n} \times \boldsymbol{Gal(K)})$ agit sur $(\boldsymbol{K}^*)^{\boldsymbol{n}}$ par $(\sigma, \gamma)d = e$ tq $e_i = \gamma(d_{\sigma^{-1}(i)})$

Loi du groupe $\boldsymbol{H_n(K)}$: $(c, \sigma, \gamma) * (d, \tau, \delta) = (e, \sigma\tau, \gamma\delta)$ tq $e_i = c_i\gamma(d_{\sigma^{-1}(i)})$

L'isomosphisme est défini par:$(c, \sigma, \gamma) \to S$ tel $S(x)_i = c_i\gamma(x_{\sigma^{-1}(i)})$

Definition: Le groupe d'automorphisme d'un code C de longueur n, $Aut(C) \leq H(n, K)$, est l'ensemble des element de $H(n, K)$ qui laissent invariant C.

Définition: Groupe de Permutation d'un Code C. L'image du morphisme

$$Aut(C) \to S_n : (c, \sigma, \gamma) \to \sigma$$

Est appelé le groupe de permutation de C note $Per(C)$

- Proposition:

$$Aut(C) = Aut(C^{\tau})$$
$$Per(C) = Per(C^{\tau})$$

- Theorem:

Soit C un code $de\ Cauchy$ de longueur n et de dimension k alors :

- Si $k = 1\ ou\ k = n - 1$ alors $Aut(C) \cong (K^{*} \rtimes Gal(K)) \times S_n$

Preuve: Posons $k = 1$ Le morphisme $(K^{*} \rtimes Gal(K)) \times S_n \rightarrow Aut(C_k(\alpha, y))$

$$(\lambda, \gamma, \sigma) \rightarrow (c, \gamma, \sigma)$$

Tel que $c_i = \frac{\lambda y_i}{\gamma(y_{\sigma^{-1}(i)})}$. Soit x ∈ $C_k(\alpha, y)$ alors il existe un polynôme P de degré < 1 tel que $\mathrm{x} = \left(y_1 P(\alpha_1), \dots, y_n P(\alpha_n)\right) = \mu(y_1, \dots, y_n)$.

Posons $(c, \gamma, \sigma)(x) = e$ alors

$e_i = c_i \gamma\left(x_{\sigma^{-1}(i)}\right) = \frac{\lambda y_i}{\gamma(y_{\sigma^{-1}(i)})} \gamma\left(\mu y_{\sigma^{-1}(i)}\right) = \lambda\gamma(\mu) y_i$ donc e est l'évaluation du polynôme constant $Q(X) = \lambda\gamma(\mu)$ donc $(c, \gamma, \sigma)(x) \in C_k(\alpha, y)$.

Pour $2 \leq k \leq n-2$

- Pour étudier ces codes nous allons plongés les GRS dans la famille des Cauchy.
- Tout Point non nul du plan 2D peut etre représenté par ses coordonnées polaire (module, tangente)

$$K^2 - \{0\} \to K^* \times \overline{K}$$

$$(u, v) \quad \to \Pi(u, v) = \begin{cases} (v, \frac{u}{v}), & v \neq 0 \\ (u, \infty), & v = 0 \end{cases}$$

Comme $GL_2(K)$ agit sur $K^2 - \{0\}$ alors il est possible de définir une action via Π sur $K^* \times \overline{K}$ tq $\forall\ (\lambda, z) \in K^* \times \overline{K}$ et $f = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$ alors

$$\Pi \circ f \circ \Pi^{-1}(\lambda, z) = \begin{cases} \left(\lambda(cz+d), \frac{az+b}{cz+d}\right) \ si\ z \neq \infty\ et\ cz+d \neq 0 \\ \left(\lambda \frac{ad-bc}{-c}, \frac{az+b}{cz+d} = \infty\right) si\ z \neq \infty\ et\ cz+d = 0 \\ \left(\lambda c, \frac{a}{c}\right)\ si\ z = \infty\ et\ c \neq 0 \\ (\lambda a, \infty)\ si\ z = \infty\ et\ c = 0 \end{cases}$$

$\forall\ z \in \overline{K}$, en fixant $\lambda = 1$ et $\Pi = (\Pi_1, \Pi_2)$, on définit avec f $\in GL_2(K)$ deux applications

$\theta_1(f,z) = \Pi_1 \circ f \circ \Pi^{-1}(1,z) \in K^*$ et $\theta_2(f,z) = \Pi_2 \circ f \circ \Pi^{-1}(1,z) = \frac{az+b}{cz+d} = \bar{f}(z)$

Remarque: $\theta_1(\lambda f, z) = \lambda \theta_1(f,z)$, $\theta_1(id,z) = 1$ *et* $\theta_1(fg,z) = \theta_1(f, g(z)) \cdot \theta_1(g,z)$

- *On définit une action de* $GL_2(K)$ *sur* $K[X,Y]_k$ *par* $(fP)(X,Y) = P(AX+BY, CX+DY)$ *tq*

$$f^{-1} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

$Théorème$: $(f^{-1}P)(z) = \theta_1(f,z)^k P(f(z))$ *on pose* $P(z) = P(\Pi^{-1}(1,z))$

- $Théorème$: soit $2 \leq k \leq n-2$ alors $C_k(\alpha, y) = C_k(\beta, v)$ si et seulement $\exists\, f \in GL_2(K), \lambda \in K^*;\ \beta_i = \bar{f}(\alpha_i)$ et $\mathrm{v_i} = \lambda y_i \theta_1(f, \alpha_i)^{k-1}$
  - D'après ce Théorème le groupe de Permutation(linéaire) de $C_k(\alpha, y)$ est lié $\mathrm{P}GL_2(K)$
- Activités: Soit le groupe $G(K) = (K^* \times GL_2(K)) \rtimes Gal(K)$ défini par la cette loi $(\lambda, f, \gamma)(\mu, g, \delta) = (\lambda\gamma(\mu), f\gamma(g), \gamma\delta) \in G(K)$

  on peut définir un sous groupe de G(K) relativement à une famille d'élément L : $G(K)_L = \{(\lambda, f, \gamma) \in G(K): \bar{f}\big(\gamma(L)\big) = L\}$
- Théorème[BERGER]: soit $C_k(\alpha, y)$ $(2 \leq k \leq n-2)$ un code de Cauchy. L'application

$$\phi:\ G(K)_y \to H_n(K)$$

$$(\lambda, f, \gamma) \to (c, \sigma, \gamma)$$

Telle que $\bar{f}\big(\gamma(\alpha_i)\big) = \alpha_{\sigma(i)}$ et $c_i = \frac{\lambda y_i \theta_1(f^{-1}, \alpha_i)^{k-1}}{\gamma(y_{\sigma^{-1}(i)})}$, définit un morphisme de groupe, $Ker\phi = \left\{\left(\mu^{k-1}, \mu Id, Id\right), \mu \in K^*\right\}$ et $Im\phi = Aut(C_k(\alpha, y))$

- Soit $(c,\sigma,\gamma) \in H_n(K)$ et $x = \left(y_i P(\alpha_i)\right)_{i=1\dots n}$ alors

$$(c,\sigma,\gamma)\left(\left(y_i P(\alpha_i)\right)_{i=1\dots n}\right) = \left(c_i \gamma(y_{\sigma^{-1}(i)} P\left(\alpha_{\sigma^{-1}(i)}\right))\right)_{i=1\dots n} =$$
$$\left(c_i \gamma(y_{\sigma^{-1}(i)}) \gamma(P\left(\alpha_{\sigma^{-1}(i)}\right))\right)_{i=1\dots n}$$

$v_i = c_i \gamma(y_{\sigma^{-1}(i)})$ et $\gamma\left(P\left(\alpha_{\sigma^{-1}(i)}\right)\right) = (\gamma P)(\gamma(\alpha_{\sigma^{-1}(i)}))$ donc on pose $\mathrm{Q} = \gamma P$ en appliquant γ à chaque coefficient et $\beta_i = \gamma(\alpha_{\sigma^{-1}(i)})$.

Ce qui implique $(c,\sigma,\gamma)\left(\left(y_i P(\alpha_i)\right)_{i=1\dots n}\right) = \left(\left(v_i Q(\beta_i)\right)_{i=1\dots n}\right) \in C_k(\beta, v)$,

$(c,\sigma,\gamma) \in Aut(C_k(\alpha,y))$ sssi $C_k(\alpha,y) = \mathrm{C_k}(\beta,v)$, ssi $\exists\, f \in GL_2(K)$; $\beta_i = \mathrm{f}(\alpha_i)$ et $\mathrm{v_i} = \lambda y_i \theta_1(f^{-1},\alpha_i)^{k-1}$ ssi $f\left(\gamma(\alpha_i)\right) = \alpha_{\sigma(i)}$ et $c_i = \frac{\lambda y_i \theta_1(f^{-1},\alpha_i)^{k-1}}{\gamma(y_{\sigma^{-1}(i)})}$.

$$Aut(C_k(\alpha,y)) \cong G(K)_L / \left\{\left(\mu^{k-1}, \mu Id, Id\right), \mu \in K^*\right\}$$

- Qu'en est-il du groupe de Permutation de $\mathrm{Per}(C_k(\alpha, y)) \leq Aut(C_k(\alpha, y))$?

D'après le morphisme du théorème précédent($\bar{f}\big(\gamma(\alpha_i)\big) = \alpha_{\sigma(i)}$) il est possible d'extraire le groupe de Permutation de $P\Gamma L_2(K) = PGL_2(K) \rtimes Gal(K)$

$Corollaire$: soit $2 \leq k \leq n-2$ alors l'application

$$P\Gamma L_2(K)_L = \{F \in P\Gamma L_2(K) : F(L) = L\} \to Per(C_k(\alpha, y))$$
$$F \to \sigma$$

Telle que $F(\alpha_i) = \alpha_{\sigma(i)}$, alors est morphisme surjectif.

Dans la suite posons $\mathrm{K} = F_q$, $q = p^m$

$$Gal(K) = \{x \to x^{pi}\} = \mathrm{Gal}(\mathrm{F_{p^m}}, \mathrm{F_p}) \cong (\frac{\mathrm{Z}}{\mathrm{mZ}}, +) \text{ cyclique}$$

- $Corollaire$: Si $Card(y) > p^l$ avec l le plus grand diviseur proper de m. Alors le morphisme précédent devient un isomorphisme et
  - $Per\big(C_k(\alpha, y)\big) = D_{2(q-1)} \rtimes Gal(K)$ si $y = K^*$, avec $D_{2(q-1)} =< \left\{z \to \theta z,\ z \to \frac{1}{z}\right\} >$ avec θ un élément primitif de K.
  - $Per\big(C_k(\alpha, y)\big) = Aff(1, K) \rtimes Gal(K)$ si $y = K,\ Aff(1, K) = \{z \to az + b; a \in K^* \ et\ b \in K\}$
  - $Per\big(C_k(\alpha, y)\big) = PGL_2(K) \rtimes Gal(K)$ si $y = \overline{K}$

- $En\ caractéristique\ 2$, $Aut(C_k(\alpha, y))$ peut être décrit par un sous groupe de $\mathrm{A}\Gamma L_2(K) = \Gamma L_2(K) = GL_2(K) \rtimes Gal(K)$.

$Corollaire$: en définissant $\Gamma L_2(K)_L = \{(f, \gamma) \in \Gamma L_2(K) : F(L) = L\}$

$$\phi : \Gamma L_2(K)_L \to Aut(C_k(\alpha, y))$$
$$(f, \gamma) \to (c, \sigma, \gamma)$$

Telle que $\bar{f}\big(\gamma(\alpha_i)\big) = \alpha_{\sigma(i)}$ et $c_i = \frac{\det(f)^{\frac{k}{2}} y_i \theta_1\left(f^{-1}, \alpha_i\right)^{k-1}}{\gamma\left(y_{\sigma^{-1}(i)}\right)}$, définit un isomorphisme de groupe.

$Ker\phi = \{(id_{GL_2(K)}, id_{Gal(K)})\}$ et $Im\phi = Aut\big(C_k(\alpha, y)\big) = \Gamma L_2(K)_L$

Résumé sur les groupe d'automorphisme de codes

- $\boldsymbol{H_n(K) = (K^*)^n \rtimes (S_n \times Gal(K))}$ est le groupe des automorphismes semi-linéaire isométrique (hamming) de K^n.
- $\boldsymbol{(S_n, \circ)}$ **et** $\boldsymbol{(K^{*n}, .)}$ sont des groups d'automosphisme(linéaire) sur l'espace vectoriel K^n préservant le poids de Hamming.
- $\boldsymbol{M_n(K) = (K^*)^n \rtimes S_n}$ est appelé le groupe monomial de matrice carrée d'ordre n sur K. $(c, \sigma) * (d, \tau) = (e, \sigma\tau)$ tq $e_i = c_i(d_{\sigma^{-1}(i)})$
- $\boldsymbol{Gal(K)}$ agit sur K^n comme une transformation semi-linéaire préservant le poids de Hamming.
- $\boldsymbol{Per(C) \leq S_n}$ qui laisse invariant le code C.
- $\boldsymbol{Aut_l(C) \leq M_n(K)}$ qui laisse C invariant. Groupe des automorphismes linéaire.
- $\boldsymbol{Aut_s(C) \leq H_n(K)}$ qui laisse C invariant. Groupe des automorphismes semi-linéaire.
- $\boldsymbol{Per_l(C) \leq Aut_l(C)}$ la projection de $\boldsymbol{Aut_l(C)}$ sur $S(C) = S_{|C|}$
- $\boldsymbol{Per_s(C) \leq Aut_s(C)}$ la projection de $\boldsymbol{Aut_s(C)}$ sur $S(C) = S_{|C|}$

- $K^* \times Per(C) \leq Aut_l(C) \leq Aut_s(C)$
- $Per(C) \leq Per_l(C) \leq Per_s(C)$

Alternant Codes

- Le code Alternant $A_k(\alpha, y)$ associé au code $C_k(\alpha, y)$ est définit par

$$A_k(\alpha, y) = C_k(\alpha, y)^{\perp} \cap F_p^n$$

- Le groupe de Hamming de F_p^n est isomorphe à

$$\boldsymbol{H_n(F_p) = (F_p{}^*)^n \rtimes S_n}$$

- Si $K = F_p$ alors $\boldsymbol{Aut_l(C) = Aut_s(C)}$, car $Gal(F_p) = Id_{F_p}$
- Si $K = F_2$ alors $Per(C) = \boldsymbol{Aut_s(C)}$
- $Proposition$: $Per(C) \leq Per(C^{\perp} \cap F_p^n)$
- $Proposition$: si $(c, \sigma, \gamma) \in \boldsymbol{Aut_s(C)}$ tel que $c = (\lambda, \dots, \lambda)$ alors $\sigma \in Per(C \cap F_p^n)$
  - Si $x \in C \cap F_p^n$ alors $(c, \sigma, \gamma)(x) = \lambda(x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)}) \in C$ donc $\sigma(x) = \lambda^{-1}(c, \sigma, \gamma)(x) \in C \cap F_p^n$

Codes Alternants cycliques

- D'après la proposition précédente, il est possible de construire des codes alternants ayant une structure particulière à partir du groupe d'automorphisme de son code GRS
- Un code C est cyclique si $Per(C)$ contient la permutation le n-cycle
$$\sigma = (1,2,3, \dots ., n)$$
- Un code de Cauchy induit une permutation σ sur le code alternant correspondant si et seulement si son groupe d'automorphisme contient une permutation de la forme $(\lambda \mathbf{1}, \sigma, \gamma)$
- ***Théorème*** : Un code alternant est cyclique induit $A_k(\alpha, y)$ si et seulement si
  - Il existe $F \in P\Gamma L(2, K)$ telle que $L = \{\alpha_1, \dots, \alpha_n\}$ soit l'orbite de α_1 par F

  Si $F = f \circ \gamma_{p^j}$ avec $f \in PGL(2, K)$ et $\gamma_{p^j} \in Gal_{F_p}(K)$, alors il existe $\lambda \in K^*$ tel que

  Tel que $y_{i+1} = \frac{\lambda y_i \theta_1(f^{-1}, \alpha_i)^{k-1}}{\left(y_{\sigma^{-1}(i)}\right)^{p^j}}$ et $y_{n+1} = y_1$

Classification des groupes d'automorphisme

- Proposition: Soit $L = \{\alpha_1, \dots, \alpha_n\}$ l'orbite de α_1 par une $F \in P\Gamma L(2, K)$ et h $\in$ $P\Gamma L(2, K)$ alors $h(L)$ est l'orbite de $h(\alpha_1)$ par $h \circ F \circ h^{-1}$

Cette proposition permet de classifier les Permutation de d'un code e cauchy par orbite sous l'action de conjugaison du $PGL(2, K)$ sur $P\Gamma L(2, K)$.

Théorème: à une conjugaison près avec $PGL(2, K)$, un élément $F(z) = \left(\frac{az+b}{cz+d}\right)^{p^j} \in P\Gamma L(2, K)$ est de l'une de ces forms: ($j \leq m$)

- Admet au moins trois point fixes alors $F(z) = z^{p^j}$
- Deux points fixes $F(z) = (az)^{p^j}$ et $a \neq z^{1-p^{j \wedge m}}$ $\forall\, z \in K$
- Un seul point fixe $F(z) = (az + b)^{p^j}$ et $Tr_{F_{p^{m \wedge j}}}(b) \neq 0$
- Pas de points fixes $F\,(z) = \left(\frac{1}{cz+d}\right)^{p^j}$, $P(X) = cX^{p^{m-j+1}} + dX - 1$ n'a pas de racine sur K

- ***Proposition*:** soit $A_k(\alpha, y)$ un code alternant cyclique induit par $F \in P\Gamma L(2, K)$ telle que $L = \{\alpha_0, \dots, \alpha_n\}$ est l'orbite de α_0 par F. Soit s un entier positif premier avec n. Soit $\sigma \in S_n \; tq \; \sigma_s^{-1}(i) = si \; mod \; n$ alors l'image de $A_k(\alpha, y)$ par σ_s est le code alternant cyclique $A_k(\sigma_s(\alpha), \sigma_s(y))$ induit par F^s.
- ***Proposition*:** Soit $F \in P\Gamma L(2, K)$ et F de la forme $F(z) = az^{p^j} + b$

$A_k(\alpha, y)$ un code alternant cyclique induit par F si et seulement s'ill existe un scalaire $\lambda \in K^*$ tel que $y = (1, \lambda, \lambda^{p^j+1}, \dots, \lambda^{\sum_{i=0}^{n-2} p^{ij}})$ et $\lambda^{\sum_{i=0}^{n-1} p^{ij}} = 1$

- $Preuve$: on remarque que $\theta_1(f, \alpha_i) = 1$ alors $y_{i+1} = (\lambda' y_i)^{p^j}$ et $y_{n+1} = y_1$
- En posant $y_1 = 1$ alors $y = (1, \lambda'^{p^j}, \lambda'^{p^{2j}+p\hat{}j}, \dots, \lambda'^{\sum_{i=0}^{n} p^{ij}})$ comme $y_{n+1} = y_1$ alors $\lambda'^{\sum_{i=0}^{n} p^{ij}}$=1. Posons $\lambda = \lambda'^{p^j}$ alors $y = (1, \lambda, \lambda^{p^j+1}, \dots, \lambda^{\sum_{i=0}^{n-2} p^{ij}})$ et $\lambda^{\sum_{i=0}^{n-1} p^{ij}} = 1$

- Exemples:
- Posons $K = F_{64}$ α primitif tel que $\alpha^6 = \alpha + 1$

Posons $f(z) = z^2$ alors l'orbite de α est $\boldsymbol{\alpha} = (\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32})$ et d'après le théorème précédent alors $y = (1, \lambda, \lambda^3, \lambda^7, \lambda^{15}, \lambda^{31})$ et $\lambda^{1055} = 1$

$$\boldsymbol{\alpha} = (\alpha, \alpha^2, \alpha^4, \alpha^3 + \alpha^2, \alpha^4 + \alpha + 1, \alpha^3 + 1)$$

Construire la matrice jusqu'à la dimension du code.