Codes localement recouvrables (LRC) à partir de courbes

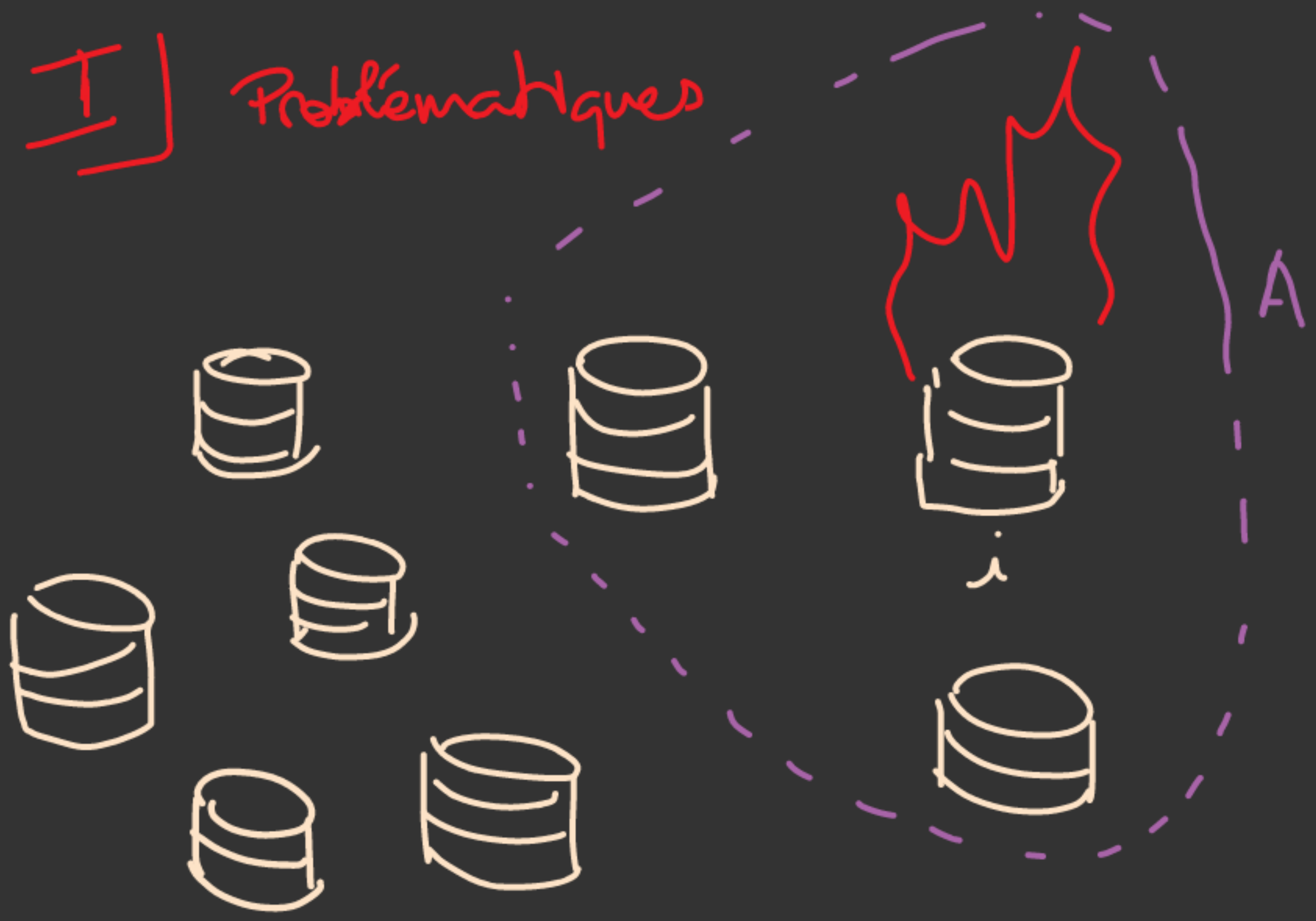
I) Problématiques

II) Codes "à la RS" de Barg & Tamo

III) ——— AG ——— + Vlăduț

IV) Questions.

I] Problématiques



<u>Notation</u>: $C \subseteq \mathbb{F}_q^n$ un code

$A \subset \{1, \dots, n\}$. $C_A = \{(c_i)_{i \in A} \mid c \in C\}$

<u>Déf°</u>: Un code $C \subseteq \mathbb{F}_q^n$ est localement recouvrable (LR) de localité r. si pour tout $i \in \{1..n\}$

$\exists A \subseteq \{1..n\}$, $i \in A$, $|A| \leq r+1$

tq : $\dim C_A = \dim C_{A \setminus \{i\}}$

$$c = (c_1, \dots, \underbrace{\boxed{c_i, c_{i+1}, \dots, c_s}}_{A}, \dots, c_n)$$

Lemme: $C \subseteq \mathbb{F}_q^n$ est r-LR ssi Pour tout $i \in \{1 \dots n\}$, $\exists\, c \in C^{\perp}$

$w(c) \leq r+1$ et $c_i \neq 0$.

Def: $C \subset \mathbb{F}_q^n$ est (ρ, r)-LR si $\forall i \in \{1 .. n\}$

$\exists A \subseteq \{1 .. n\}$, $|A| \leq r+\rho-1$, $A \ni i$

et C_A de $d_{min} \geq \rho$ (⚠ On ne va pas parler de ρ aujourd'hui)

$\rho = 2 \Rightarrow$ r-LR

Un (ρ, r)-LR tolère jusqu'à $\rho - 1$ effacements.

$$c = (c_1, \dots, \overbrace{\boxed{c_i, c_{i+1}, \dots, c_j}}^{C_A}, \dots, c_n)$$

$$\underbrace{X \; \dots \; X}_{\rho-1 \text{ effacements}} \qquad T$$

$$\downarrow$$

$$(c_j, \dots, c_j)$$

$\phi : C_A \longrightarrow C_{A \setminus \{\text{posi° effacées}\}}$

ϕ inj car $\ker \phi \not\ni$ mots de C_A supportés par $\rho - 1$ posi°

Déf° : Soit $C \subseteq \mathbb{F}_q^n$ un code r-LC. On dit qu'il est de disponibilité t si

$\forall i \in \{1,\dots,n\}$, $\exists A_1,\dots,A_t$ tq $\forall j \in \{1..t\}$, $A_j \ni i$, $|A_j| \leq r+1$

et $\dim C_{A_j} = \dim C_{A_j \setminus \{i\}}$

$\forall j,k$, $A_j \cap A_k = \{i\}$.

Exemples

1) Codes de Reed–Solomon

(codes géométriques sur $\mathbb{P}^1$)

$[n \leq q, k, n-k+1]_q$

$r = k$ (mauvais)

$c = (P(\alpha_1), \dots, P(\alpha_n))$

$P \in \mathbb{F}_q[X]_{<k}$

+ Interpolation de Lagrange.

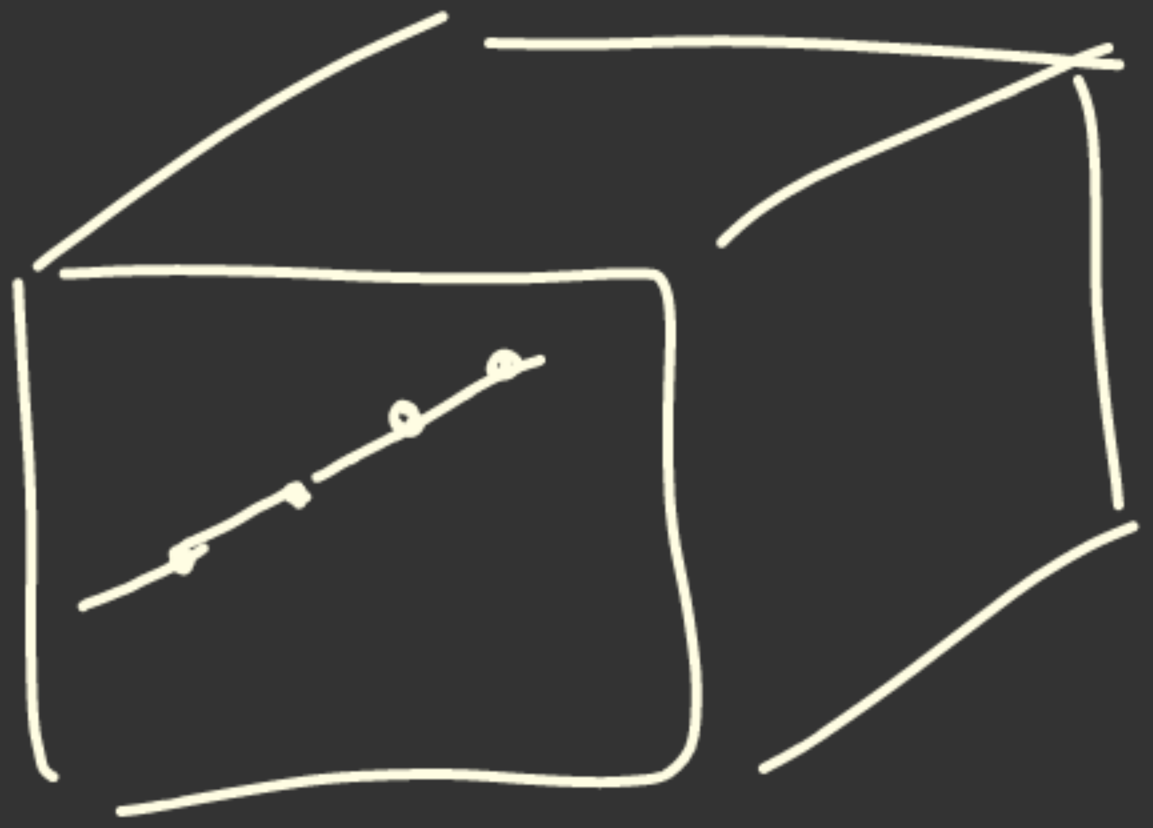
2) Codes de Reed-Muller

$$RM_q(d,m) = \left\{ (f(P_1),\dots,f(P_{q^m})) \;\middle|\; P_i \in \mathbb{F}_q^m,\ f \in \mathbb{F}_q[X_1,\dots,X_m]_{\leq d} \right\}$$

$d<q$

$$\left[q^m, \binom{d+m}{d}, q^m - d q^{m-1}\right]$$

$r = d+1$



Interpolation de Lagrange univariée sur une droite.

II] Construction de Berg & Tamo

Q : Peut-on avoir r "bon" et une "bonne" distance minimale et un bon k ?

Borne de Singleton :

$$d \leq n-k+2-\left\lceil \frac{k}{r} \right\rceil$$

Construction :

Soient $\alpha_1, \dots, \alpha_n \in \mathbb{F}_q$

Supp : $(r+1) \mid n$

$r \mid k$

$$\underbrace{A_1 \sqcup A_2 \sqcup \dots \sqcup A_{\frac{n}{r+1}}}_{\text{partition}} = \{1, \dots, n\}$$

$|A_i| = r+1$

$g \in \mathbb{F}_q[X]$, $d^\circ g = r+1$

g constant sur A_i pour tout i

$$C = \Big\{ \big(f(\alpha_1), \dots, f(\alpha_n)\big)$$

$$f = P(x, g(x))$$

$$d^\circ_x P < r \,, \quad d^\circ_y P < \frac{k}{r} \Big\}$$

$$f = \sum_{i=0}^{r-1} \sum_{j=0}^{\frac{k}{r}-1} a_{ij}\, x^i g(x)^j$$

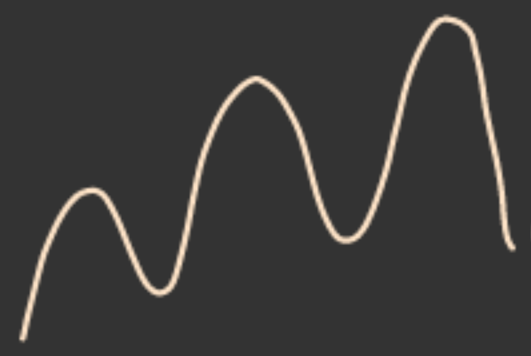
$$d^\circ f \leq (r-1) + \left(\frac{k}{r}-1\right)(r+1)$$

$$\leq \cancel{r} - 1 + k + \frac{k}{r} - \cancel{r} - 1 = k + \frac{k}{r} - 2$$

Interprétations

A)

$$\begin{aligned} i : \mathbb{P}^1 &\longrightarrow \mathbb{P}^1 \times \mathbb{P}^1 \\ t &\longmapsto (t, g(t)) \end{aligned}$$



$C_g = \mathbb{P}^1$

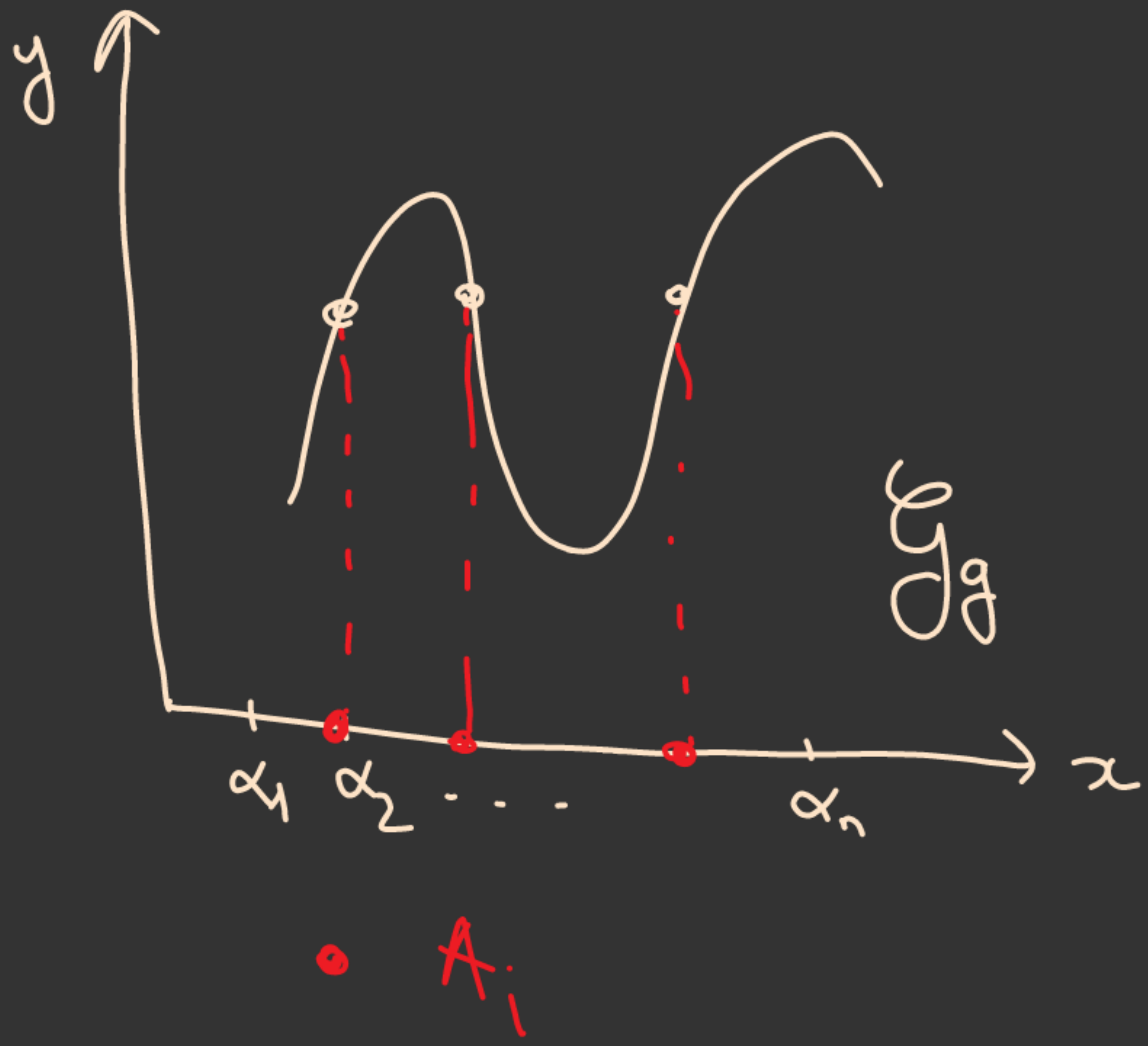
On évalue sur C_g les fonctions $H^0\left(\mathbb{P}^1 \times \mathbb{P}^1, \mathcal{O}\left(r-1, \frac{k}{r}-1\right)\right) =$

$$\left\{ P(x,y) \;\middle|\; d^\circ_x P \leq r-1 \,, \; d^\circ_y P \leq \frac{k}{r} - 1 \right\}$$

B)

$$\begin{array}{cc} \mathbb{P}^1 & t \\ \downarrow & \downarrow \\ \mathbb{P}^1 & g(t) \end{array}$$

On évalue les $\sum a_{ij}\, x^i g(x)^j$



Localité : r

$$c = (f(\alpha_1), \dots, f(\alpha_n))$$

$$c_{A_i} = (f(\alpha_{i_1}), \dots, f(\alpha_{i_{r+1}}))$$

$$f = \sum_{i=0}^{r-1} \sum_{j=0}^{\frac{k}{r}-1} a_{ij} \, x^i g(x)^j$$

$\forall x \in A_i \quad g(x) = c \leftarrow$ indep de x

$f_{|A} = \sum_i \sum_j a_{ij} \, c^j \, x^i \leftarrow$ poly de degré $\leqslant r-1$

Dimension : On évalue :

$$\sum_{i=0}^{r-1} \sum_{j=0}^{k/r-1} a_{ij}\, x^i g(x)^j$$

On rappelle $d^\circ g = r+1$

Une base est donnée par $\langle x^i g(x)^j \rangle$

$$\dim = r \cdot \left(\frac{k}{r}\right) = k$$

Distance minimale

Le code est $\subseteq$ dans un RS donné par l'évaluaᵒ de polynômes de degré

$$\leq k + \frac{k}{r} - 2$$

$$d \geq n - k - \frac{k}{r} + 2$$

Singleton

- C'est pas un code $\otimes$

parce que on évalue

$$H^0\left(\mathbb{P}^1\times\mathbb{P}^1, \mathcal{O}\left(r-1, \frac{k}{r}-1\right)\right)$$

$$\|$$

$$H^0(\mathbb{P}^1,\mathcal{O}(r-1))\otimes H^0\left(\mathbb{P}^1,\mathcal{O}\left(\frac{k}{r}-1\right)\right)$$

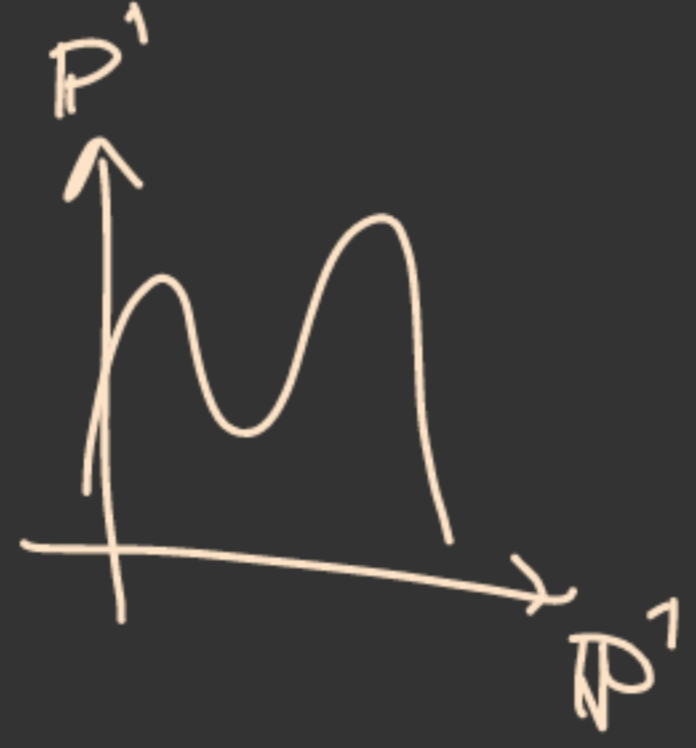
Mais l'ens d'évaluaᵒ (les points du graphe de G n'ont pas de structure produit.

C'est un poinçonné du code produit.

- C'est pas un RS

C'est un code sur $\mathcal{G}_g \simeq \mathbb{P}^1$

mais $i: \mathbb{P}^1 \longrightarrow \mathbb{P}^1\times\mathbb{P}^1$



$$i^* H^0\left(\mathbb{P}^1\times\mathbb{P}^1, \mathcal{O}\left(r-1, \frac{k}{r}-1\right)\right)$$

$$\subsetneq$$

$$H^0\left(\mathbb{P}^1, i^*\mathcal{O}\left(r-1, \frac{k}{r}-1\right)\right)$$

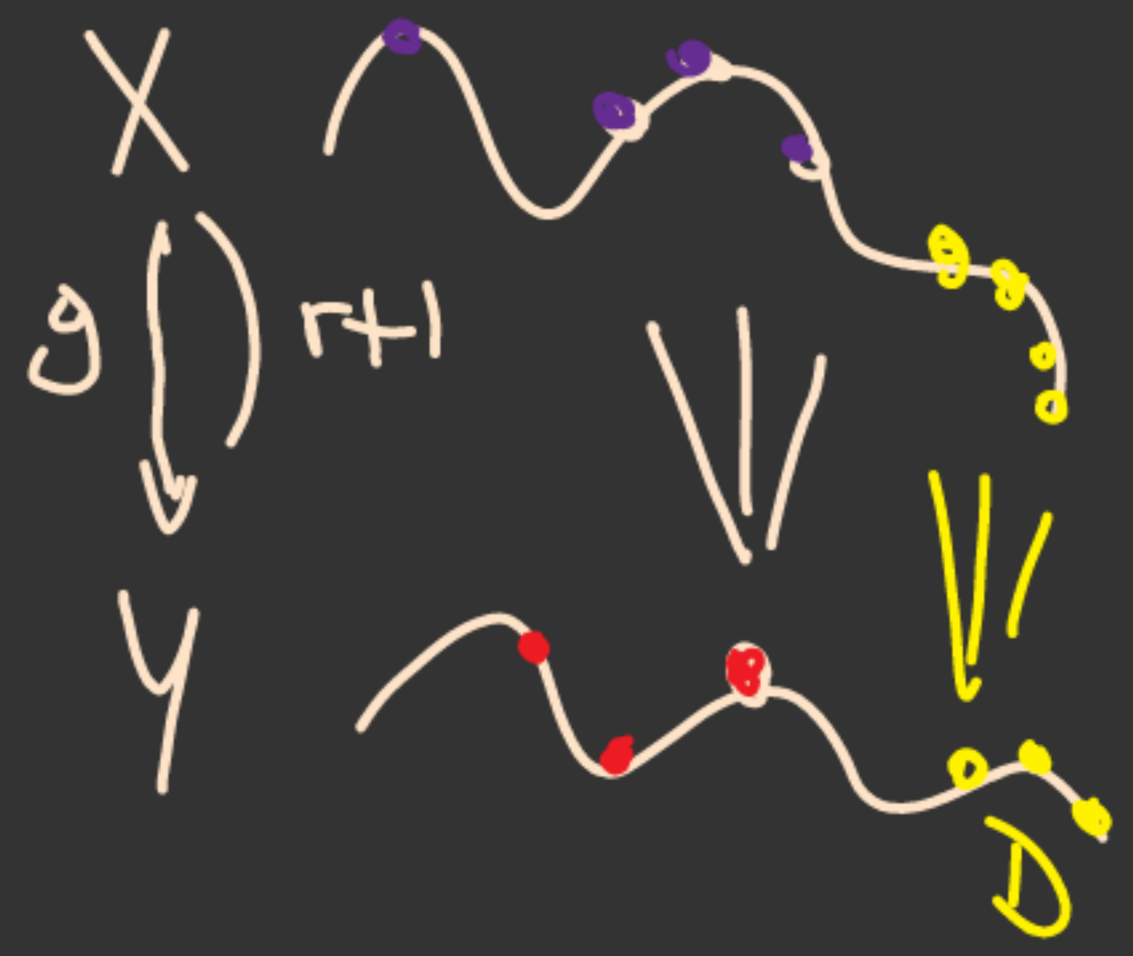
C'est un sous code d'un RS

III) Barg, Tamo & Vlăduţ

On a vu:

<u>Défaut</u>: $n \le \#\mathbb{P}^1(\mathbb{F}_q) \le q+1$

→ On peut considérer la situation:



- X, Y courbes proj lisses...
- $Q_1,\dots,Q_s \in Y(\mathbb{F}_q)$ tot dec sous g
- $P_1,\dots,P_n$ leurs images réciproques (partition naturelle)
- $D \in \mathrm{Div}_{\mathbb{F}_q}(Y)$ à support disjoint de $Q_1,\dots,Q_s$ et
- $x \in k(X)$ tq $k(X)=k(Y)(x)$ entière sur $k[Y \setminus \mathrm{Supp}\, D]$

i.e il y a une rela°:

$$x^{r+1}+b_r x^r+\dots+b_0=0$$

$\forall i$ $b_i \in L(n_i D)$ pour $n_i \geq 0$

$$\begin{tikzcd} X \arrow[r, "x"] \arrow[d, "g"'] & \mathbb{P}^1 \arrow[d] \\ Y \arrow[r, hook] & Y \times \mathbb{P}^1 \end{tikzcd}$$

$$X \longrightarrow Y \times \mathbb{P}^1$$
$$P \longmapsto (g(P), x(P))$$

Cette application est injective

Car x "sépare" les pts d'une fibre :

Soient $P, Q \in X(\bar{\mathbb{F}}_q)$, $g(P) = g(Q)$, $P \neq Q$

si $x(P) = x(Q)$

Alors pour tout $f \in k(X)$

on aurait $f(P) = f(Q)$ car

$k(X) = k(Y)(x)$ donc :

$$f = \frac{\sum a_i x^i}{\sum b_j x^j}, \quad a_i, b_j \in k(Y)$$

$\forall i, \forall j$ $\quad a_i(P) = a_i(Q)$
$\quad b_j(P) = b_j(Q)$

Le Code :

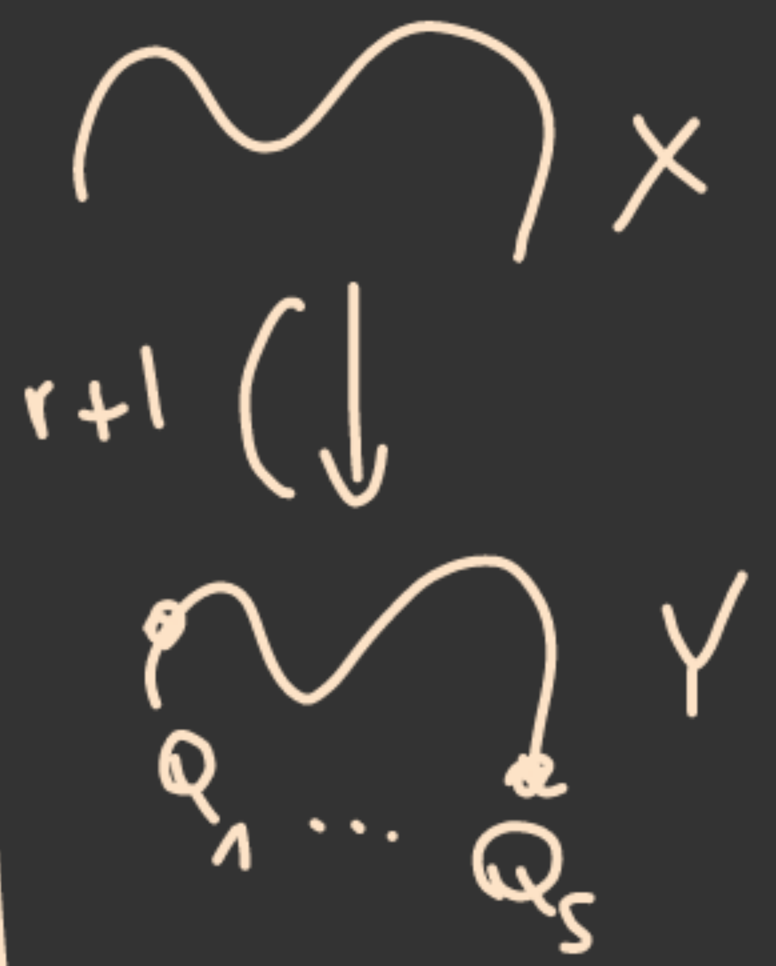
$$C := \Big\{ \big(f(P_1),\dots,f(P_n)\big) \;\Big|\; f \in g^*L(D) \oplus g^*L(D)x \oplus \dots \oplus g^*L(D)x^{r-1} \Big\}$$

Rq : g^* ?

$$\begin{tikzcd} X \arrow[d, "g"'] \arrow[dd, bend left=60] \\ Y \arrow[d, "f \in \mathcal{L}(D)"'] \\ \mathbb{P}^1 \end{tikzcd}$$

$g^*f := f \circ g$

Paramètres :



$\mathrm{loc} = r$

$n = (r+1)s$

$k \geq r(\deg D + 1 - g_Y)$

$d \geq n - (r+1)\deg D - (r-1)\deg(x)$

où $\deg x := \deg(X \xrightarrow{x} \mathbb{P}^1)$

: Remplacer x par $\varphi : X \to Z$? (e.h.)

d_{min} vient de ce qu'on est dans $L(g^*D + (r-1)(x)_\infty)$

Quelle distance à "Singleton".

$$k \geqslant r(\deg D + 1 - g_Y)$$

$$d \geqslant n - (r+1)\deg D - (r-1)\deg(x)$$

$$n - d - k - \frac{k}{r} = (g_Y - 1)(r+1) + (r-1)\deg(x)$$

La disponibilité? $t = 1$

pour faire $t = 2$:

$$X_1 \times_Y X_2 = X$$

$$\begin{tikzcd} & X_1 \times_Y X_2 \arrow[dl] \arrow[dr] & \\ X_1 \arrow[dr, "f"'] & & X_2 \arrow[dl, "g"] \\ & Y & \end{tikzcd}$$

$$X_1 \times_Y X_2 := \{ (P,Q) \in X_1 \times X_2 \text{ tq } f(P) = g(Q) \}$$

x_1 un él^t primitif de $k(X)/k(X_1)$

x_2 ——————— $k(X)/k(X_2)$

$D \in \mathrm{Div}(Y)$

evaluent des

$$x_1^i x_2^j f \mid f \in L(D)$$

Avec des tours de Garcia-Sticht pour les paraux (c.f article)

<u>Idée 1</u> :

$$\begin{tikzcd} \vdots \arrow[d] \\ X_1 \arrow[d] \\ X_0 \end{tikzcd} \qquad \begin{tikzcd} X_{i+1} \arrow[d, "q"] \\ X_i \end{tikzcd} \rightsquigarrow \text{code } (q-1)\text{-LR}$$

<u>Idée 2</u>

$$\begin{tikzcd}
 & & & \cdots \arrow[dl] \\
 & & Y_2 \arrow[dl] \arrow[dd, "3"] & \\
 & Y_1 \arrow[dl] \arrow[dd, "3"] & & \cdots \arrow[dl] \\
 \mathbb{P}^1 \arrow[dd, "3"] & & X_2 \arrow[dl] & \\
 & X_1 \arrow[dl] & & \\
 \mathbb{P}^1 = X_0 & & &
\end{tikzcd} \qquad \begin{array}{c} z \\ \downarrow \\ z^3 \end{array}$$

$\Longrightarrow$ famille de 3-LR avec

$n \to \infty$

$R, \delta > 0$

IV] Questions.

1) Peut-on abstraire la construction ?

$$\begin{tikzcd} X \arrow[r, "\pi"] \arrow[d, "r+1"'] & \mathbb{P}^1 \\ Y & \end{tikzcd}$$

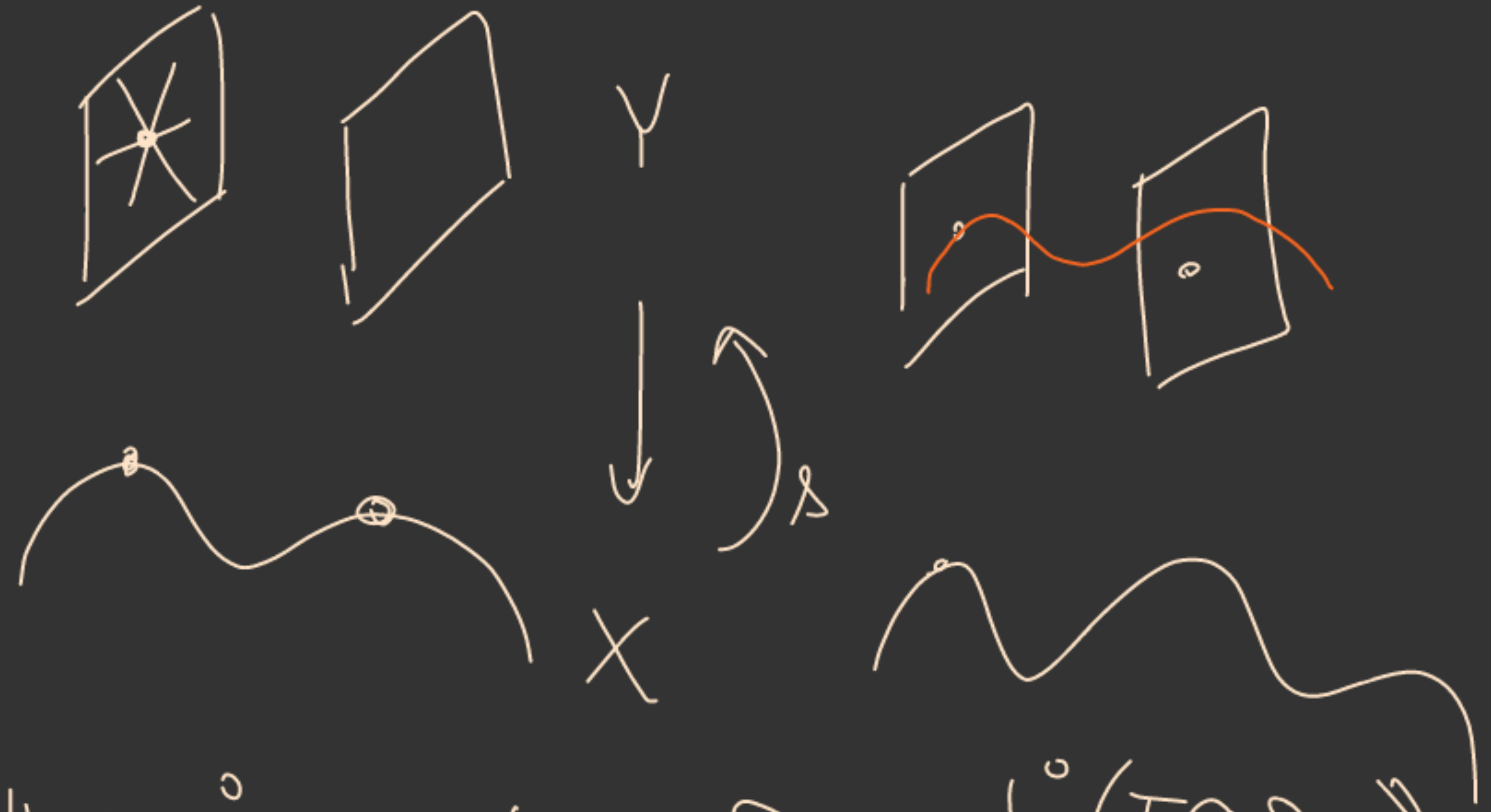
← Un code RS

Y ← Un code AG ici

Y a-t-il un "produit fibré" de codes qui permet d'imiter ça ?

2) Dimension supérieure.

→ Permettrait d'améliorer la disponibilité.



$\#$ sec° passant par $P \simeq q^{h^0(F \otimes \mathcal{O}(-P))}$

$H^0(F \otimes \mathcal{O}(-P-Q))$ sépare les points.