Formule de Poisson discrète

réf : Peyré

<u>Déf</u> : Soit G un groupe abélien et $H \leq G$. On pose

$$H^{\#} = \{ \chi \in \widehat{G} : \chi(h) = 1 \ \forall h \in H \}$$

<u>Lemme</u> : $H^{\#} \simeq \widehat{G/H}$

<u>Thm</u> : [formule de Poisson] G abélien fini, $H \leq G$, $f : G \to \mathbb{C}$. Alors

$$\forall g \in G \quad \sum_{h \in H} f(gh) = \frac{|H|}{|G|} \sum_{\chi \in H^{\#}} \hat{f}(\overline{\chi}) \chi(g)$$

<u>Déf</u> : Sur $\mathbb{F}_2^k$ on pose $d(x,y) = w(x-y)$ où $w(z) = |\{ i \in [\![1;k]\!] : z_i \neq 0 \}|$

Soit H sev de $\mathbb{F}_2^k$. On note $A_H \in \mathbb{Z}[X,Y]$ le polynôme énumérateur de poids de H : $A_H(X,Y) = \sum_{c \in H} X^{k-w(c)} Y^{w(c)} = \sum_{i=0}^{n} A_i X^{k-i} Y^i$

où A_i est le nombre de vecteurs de H de poids i.

<u>Thm</u> [identités de Mac Williams] Soit H un sev de $\mathbb{F}_2^k$. Alors :

$$A_{H^\perp}(X,Y) = \frac{1}{|H|} A_H(X+Y, X-Y).$$

(à admettre)

<u>Dém lemme</u> : On pose $\varphi : \widehat{G/H} \to H^{\#}$, $\chi \mapsto \tilde{\chi}$ où $\tilde{\chi}(g) = \chi(\bar{g}) \ \forall g \in G$.

Mq <u>$\tilde{\chi} \in H^{\#}$</u> : Soit $h \in H$, $\tilde{\chi}(h) = \chi(\bar{h}) = \chi(H) = 1$

Mq <u>φ surjective</u> : Soit $\tilde{\chi} \in H^{\#}$, $H \subset \operatorname{Ker} \tilde{\chi}$. On pose

$\chi(\bar{g}) = \tilde{\chi}(g)$ qui est bien défini car $H \subset \operatorname{Ker} \tilde{\chi}$.

On a $\varphi(\chi) = \tilde{\chi}$ donc φ est surjective.

Mq <u>φ injective</u> : Soit $\chi \in \widehat{G/H}$, $c \in \widehat{G/H}$ tels que $\tilde{\chi} = \tilde{c}$. Donc

$\chi(\bar{g}) = c(\bar{g}) \ \forall g \in G$. Donc $\chi = c$.

φ est un <u>morphisme</u>.

$\hookrightarrow$ on a un isomorphisme.

<u>Dém poisson</u> : On note S un système de représentants de G/H dans G.

On pose $\hat{f} : G/H \to \mathbb{C}$ telle que :

$$\hat{f}(\bar{g}) = \sum_{h\in H} f(gh) \quad \text{pour } g\in G.$$

$\hat{f}$ est bien définie car si $g = g'h'$ avec $g'\in G$, $h'\in H$ on a :

$$\sum_{h\in H} f(gh) = \sum_{h\in H} f(g'h'h) = \sum_{h\in H} f(g'h) \quad \text{car } \begin{array}{l} H \to H \\ h \mapsto h'h \end{array} \text{ est une bijection.}$$

On peut donc la décomposer en série de Fourier :

$$\hat{f}(\bar{g}) = \sum_{\chi\in\widehat{G/H}} \langle \hat{f},\chi\rangle \chi(\bar{g}) \quad \text{pour } g\in S.$$

Calculons les coefficients de Fourier : $\langle \hat{f},\chi\rangle = \sum_{g\in S} \frac{\hat{f}(\bar{g})\overline{\chi(\bar{g})}}{|G/H|} = \frac{|H|}{|G|}\sum_{g\in S}\sum_{h\in H} f(gh)\overline{\chi(\bar{g})}$

Or $\begin{array}{l} S\times H \to G \\ (g,h)\mapsto gh \end{array}$ est une bijection et $\chi\in\widehat{G/H}$ donc $\chi(\overline{gh}) = \chi(\bar{g})$. On a :

$$\langle \hat{f},\chi\rangle = \frac{|H|}{|G|}\sum_{g\in G} f(g)\overline{\tilde{\chi}(g)} = \frac{|H|}{|G|}\hat{f}(\tilde{\chi})$$

On en déduit : $\hat{f}(\bar{g}) = \frac{|H|}{|G|}\sum_{\chi\in\widehat{G/H}} \hat{f}(\tilde{\chi})\chi(\bar{g}) = \sum_{h\in H} f(gh)$

Donc par l'isomorphisme précédent on a la formule de Poisson car

$\chi(\bar{g}) = \tilde{\chi}(g)$ $\forall g\in G$.

<u>Dém identité MacWilliams</u> : Soient $x,y\in\mathbb{C}$. On pose $f\in\mathbb{C}[\mathbb{F}_2^k]$ tq

$f(a) = x^{k-w(a)}y^{w(a)}$ $\forall a\in\mathbb{F}_2^k$. Calculons $\hat{f}(\chi_a)$

$$\hat{f}(\chi_a) = \sum_{t\in\mathbb{F}_2^k} f(t)\chi_a(t) = \sum_{t\in\mathbb{F}_2^k} x^{k-w(t)}y^{w(t)}(-1)^{\langle t,a\rangle}$$

$$= \sum_{t\in\mathbb{F}_2^k}\prod_{i=0}^{k-1} x^{1-t_i}y^{t_i}(-1)^{a_it_i} = \prod_{i=0}^{k-1}\sum_{t_i=0}^{1} x^{1-t_i}y^{t_i}(-1)^{a_it_i}$$

$$\sum_{t_i=0}^{1} x^{1-t_i}y^{t_i}(-1)^{a_it_i} = \begin{cases} x+y & \text{si } a_i=0 \\ x-y & \text{si } a_i=1 \end{cases} \quad \text{Donc}$$

$\hat{f}(\chi_a) = (x+y)^{k-w(a)}(x-y)^{w(a)}$ D'après la formule de Poisson pour $g=1$ et $H=H^\perp$ on a :

$$\sum_{g\in H^\perp} f(g) = \sum_{a\in(H^\perp)^\perp}\hat{f}(\chi_a)\frac{|H^\perp|}{|G|}$$

Or $|H^\perp| = \frac{|G|}{|H|}$ car $H^\perp \simeq H^\#$ et $(H^\perp)^\perp = H$ par inclusion et cardinalité.

C'est vrai pour tout $x, y \in \mathbb{C}$ donc on peut identifier les polynômes de $\mathbb{Z}[X,Y]$. On a donc

$$A_{H^\perp}(X,Y) = \frac{1}{|H|} \quad A_H(X+Y, X-Y).$$

↳ petites explications pour la fin de la dém.

$H^\perp = H^\#$ car $\chi_a \in H^\#$ $\iff \chi_a(h) = 1 \ \forall h \in H$
$\iff (-1)^{\langle a, h\rangle} = 1 \ \forall h \in H$
$\iff \langle a, h\rangle = 0 \ \forall h \in H$
$\iff a \in H^\perp$

$(H^\perp)^\perp = H$? on a $|H^\perp| = |H^\#| = |\widehat{G/H}| = |G/H| = \frac{|G|}{|H|}$.
(abélien)

Donc $|H^{\perp\perp}| = |H|$. De plus $H \subset (H^\perp)^\perp$ car si $h \in H$ et $g \in H^\perp$, alors $\langle g, h\rangle = 0$ ...

Applications : code correcteurs :
- on peut calculer les poids de quelques codes (Hamming, ...)
- on peut obtenir la borne de la programmation linéaire

cf Peyré chapitre 6