Mathématiques discrètes

Pascal SZACHERSKI

8 décembre 2007

Ceci n'est qu'une copie de mes notes que j'ai prises dans le cours. De plus, je n'ai pas fait l'éffort de copier les preuves (vous savez que c'est chiant …). Ce PDF voire son imprimée n'est ni autorisé ni vérifié ; distribution seulement gratuitement ou au prix coûtant.

l'auteur

Table des matières

Chapitre 1

Introduction

1.1 Groupes, sous-groupes, ...

1.1.1 Groupes

Definition [1.1.1] Un groupe $(G, \cdot)$ est un ensemble non vide muni d'une loi de composition de termes $G \times G \to G$, $(x, y) \mapsto x \cdot y$ possedant les propriétés suivants :

(1) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ $\forall x, y, z \in G$ (associativité)

(2) $\exists$ un élélement noté 1 tel que $1 \cdot x = x \cdot 1 = x$ $\forall x \in G$. 1 est appelé élément neutre de G.

(3) $\forall x \in G$ $\exists y \in G$ tel que $x \cdot y = y \cdot x = 1$. Cet élément y est appelé inverse de x est noté x^{-1}.

Un groupe est dit commutatif ou abelien si $xy = yx$ $\forall x, y \in G$. Pour les groupes commutatifs on utilise souvent la notation additive. La loi est notée $+$, l'élément neutre noté 0, l'inverse est appelé opposé et noté $-x$.

Exemple [1.1.2] S_n est le groupe des permutation d'ordre n : c'est l'ensemble des bijections σ de l'ensemble $\{1, \ldots, n\}$. Le produit est la composition des application $(\sigma \circ \tau)(j) = \sigma(\tau(j))$ $\forall j \in \{1, \ldots, n\}$. L'élément unité est défini par $\mathbb{1}(j) = j$ $\forall j \in \{1, \ldots, n\}$. S_n a $n!$ élément.

Les transformations du plan $\mathcal{P}$ donnent des exemples de groupes :

- groupe des isométries : applications φ telles que $\varphi(M)\varphi(N) = MN$ $\forall M, N \in \mathcal{P}$. On vérifie qu'elles sont bijectives et forment un groupe pour la composition des applications.
- groupe des homothéties-translations

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sont des groupes. Si on pose $\mathbb{K}^* := \mathbb{K} \setminus \{0\}$, alors $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ sont des groupes.

Si E est un espace vectoriel, l'ensemble $GL(E)$ des applications linéaires bijectives de E dans lui-même est un groupe pour la composition des application. De même $GL(n, \mathbb{R})$, ensemble des matrices inversible à coéfficients réels, est un groupe pour la multiplication des matrices. Même chose pour $GL(n, \mathbb{C})$, ensemble des matrices inversibles à coéfficients dans $\mathbb{C}$.

1.1.2 Sous-groupes

Definition [1.1.3] Soit $(G, \cdot)$ un groupe. On dit que $H \subseteq G$ est un sous-groupe de G si et seulement si on a

(1) $H \neq \emptyset$

(2) $x \cdot y \in H$ $\forall x, y \in H$ et $(H, \cdot)$ est lui-même un groupe.

On montre que (2) est équivalent à

(2') $xy^{-1} \in H$ $\forall x, y \in H$

Exemple [1.1.4] Le cercle unité $\mathbb{T} := \{z \in \mathbb{C} \mid |z| = 1\}$ est un sous-guope de $(\mathbb{C}^*, \cdot)$.

Definition [1.1.5] On appelle ordre d'un groupe fini le nombre d'éléments de ce groupe.

Théorème [1.1.6] *Soit G un groupe fini et soit H un sous-groupe de G. Alors l'ordre de H divise l'ordre de G.*

Definition [1.1.7] Soit G un groupe fini. On appelle ordre de $x \in G$ le plus petit entier $d \geq 1$ tel que $x^d = 1$.

Proposition [1.1.8] *Les éléments $1, x, \ldots, x^{d-1}$ sont distincts deux à deux et l'ensemble $\{1, x, \ldots, x^{d-1}\}$ est un sous-groupe de G. (On pose par convention $x^0 := 1$.)*

Corollaire [1.1.9] *L'ordre d'un élément divise l'ordre du groupe. Si G est un groupe fini d'ordre p, alors $x^p = 1$ $\forall x \in G$.*

1.1.3 Homomorphismes

Definition [1.1.10] Soient $(G, \cdot)$, $(H, \cdot)$ deux groupes. On dit qu'une application $\varphi : G \to H$ est un homomorphisme de groupes si $\varphi(xy) = \varphi(x)\varphi(y)$ $\forall x, y \in G$.
Dans ce cas on pose $\text{im}\,\varphi = \{\varphi(x) \mid x \in G\}$, $\ker\varphi = \{x \in G \mid \varphi(x) = 1\}$.

Proposition [1.1.11] *Si $\varphi : G \to H$ est un homomorphisme, $\varphi(1_G) = 1_H$, $\text{im}\,\varphi$ est un sous-groupe de H, $\ker\varphi$ est un sous-groupe de G et $\varphi(x^{-1}) = \varphi(x)^{-1}$ $\forall x \in G$.*

Definition [1.1.12] Soit $(G, \cdot)$ un groupe, soit H un sous-groupe de G. On dit que H est un sous-groupe distingué de G si $aha^{-1} \in H$ $\forall h \in H$, $a \in G$.

Remarque [1.1.13] Si G abelien, $aha^{-1} = aa^{-1}h = h$ $\forall h \in H$ et tout sous-groupe est dinstingué.

Exemple [1.1.14] Si $\varphi : G \to H$ est un homomorphisme, $\ker\varphi$ est un sous-groupe distingué de G.

1.1.4 Groupe quotien

Definition [1.1.15] Soit $(G, \cdot)$ un groupe et soit H un sous-groupe distingué de G. Pour $x \in G$ on pose $\Pi(x) := x \cdot H := \{xh \mid h \in H\}$. Par définition l'ensemble quotient G/H est égal à l'ensemble $\{\Pi(x) \mid x \in G\} = \{xH \mid x \in G\}$.

Théorème [1.1.16] *Avec les hypothèses ci-dessus on pose $\Pi(x)\Pi(y) = \Pi(xy)$ pour $x, y \in G$. Alors la loi $\cdot$ est bien définie de $G/H \times G/H \to G/H$, $(G/H, \cdot)$ est un groupe et $\Pi : G \to G/H$ est un homomorphisme de groupes.*

(Dans la preuve, on utilise la propriété suivante : $\{xh \mid h \in H\} = \{hx \mid h \in H\}$ $\forall x \in G$.)

Exemple [1.1.17] $\mathbb{Z}/n\mathbb{Z} : n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Si $x, y \in \mathbb{Z}$ $\exists p, q \in \mathbb{Z}$ tels que $x = np$, $y = nq$ et $x - y = (p - q)n \in n\mathbb{Z}$. On peut former le groupe quotient $(\mathbb{Z}/n\mathbb{Z}, +)$. Les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont les sous-ensembles de $\mathbb{Z}$ de la forme $\Pi(p) = p + n\mathbb{Z} = \{p + qn \mid q \in \mathbb{Z}\}$. On peut faire la division de p par n. $\Rightarrow p = na + b$, $a \in \mathbb{Z}$, $0 \leq b \leq n - 1$. $\Rightarrow p + n\mathbb{Z} = b + \underbrace{na + n\mathbb{Z}}_{=n\mathbb{Z}} = b + n\mathbb{Z}$. $\mathbb{Z}/n\mathbb{Z}$ possède n éléments, $\Pi(0), \ldots, \Pi(n-1)$. $\Pi(i) + \Pi(j) = \Pi(i + j) = r_{i+j}$ où r_{i+j} designe le reste de la division de $i + j$ par n.
En pratique on note $\overline{p}$ au lieu de $\Pi(p)$.
On pose par définition $\overline{p} \cdot \overline{q} = \overline{pq}$. C'est bien défini car si $\overline{p} = \overline{p'}$, $\overline{q} = \overline{q'}$, $\Rightarrow p' = p + nu$, $q' = q + nv$ $(u, v \in \mathbb{Z})$: $p'q' = (p + nu) \cdot (q + nv) = pq + n[uq + vp + nuv]$. $\Longrightarrow \overline{p'q'} = \overline{pq}$.
On note $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, \cdot)$.

Proposition [1.1.18] *(1)* $\bar{i} \in (\mathbb{Z}/n\mathbb{Z})^*$ *si et seulement si* $\text{pgcd}(i, n) = 1$

(2) $(\mathbb{Z}/n\mathbb{Z})^*$ *est un groupe.*
De plus : $(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$ ***si et seulement si*** *n est premier. Autrement dit : $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.*

Théorème [1.1.19] (Théorème de factorisation) *Soient G et H deux groupes et soit $\varphi : G \to H$ un homomorphisme. Alors $\ker\varphi$ est un sous-groupe distingué de G et $\exists!\widetilde{\varphi} : G/\ker\varphi \to H$ telle que $\widetilde{\varphi} \circ \Pi = \varphi$ où $\Pi : G \to G/\ker\varphi$ est l'application définie par la formule $\Pi(g) = g\ker\varphi$.*
De plus $\widetilde{\varphi}$ est un homomorphisme injectif et $\text{im}\,\widetilde{\varphi} = \text{im}\,\varphi$. En particulier : $\widetilde{\varphi}$ est bijective si φ est surjective.

Exemple [1.1.20] (1) $GL(n,\mathbb{R})$ groupe des matrices inversibles $n \times n$ à coéfficients réels.
$\varphi : GL(n,\mathbb{R}) \to \mathbb{R}$, $A \mapsto \det A$.
φ est un homomorphisme de $GL(n,\mathbb{R}) \to \mathbb{R}$. Si $\lambda \in \mathbb{R}$, $\varphi \begin{pmatrix} \lambda & & \\ & 1 & \\ & & \ddots \\ & & & 1 \end{pmatrix} = \det \begin{pmatrix} \lambda & & \\ & 1 & \\ & & \ddots \\ & & & 1 \end{pmatrix} = \lambda$.
Donc φ est surjective.
$\ker \varphi = \{A \in GL(n,\mathbb{R}) \mid \det A = 1\} =: SL(n,\mathbb{R})$. $\exists \widetilde{\varphi} : GL(n,\mathbb{R})/SL(n,\mathbb{R}) \to \mathbb{R}$ homomorphisme bijectif tel que $(\widetilde{\varphi} \circ \Pi)(A) = \det A \ \forall A \in GL(n,\mathbb{R})$. ($\Pi(A) = \{AB \mid \det B = 1\}$.)

(2) $\varphi : \mathbb{R} \to \mathbb{T}$, $x \mapsto \mathbf{e}^{2\mathbf{i}\pi x}$. On a bien $\varphi(x) \in \mathbb{T}$ car $|\varphi(x)| = 1 \ \forall x \in \mathbb{R}$. $\Rightarrow \varphi$ est surjective.
$\ker \varphi = \left\{x \in \mathbb{R} \;\middle|\; \mathbf{e}^{2\mathbf{i}\pi x} = 1\right\} = \mathbb{Z}$. L'application $\widetilde{\varphi}$ telle que $\widetilde{\varphi} \circ \Pi = \varphi$ est un homomorphisme bijectif de $\mathbb{R}/\mathbb{Z}$ sur $\mathbb{T}$.

Proposition [1.1.21] *Les sous-groupes de $\mathbb{Z}$ sont de la forme $H = d\mathbb{Z}$ où $d = 0$ si $H = \{0\}$ et où d est le plus petit élément strictement positif de H si $H \neq \{0\}$.*

Remarque [1.1.22] Si G est un groupe et si $x \in G$, alors $\{x^n \mid n \in \mathbb{Z}\}$ est un sous-groupe de G, appelé le sous-groupe de G engendré par x.

Definition [1.1.23] On dit qu'un groupe est cyclique s'il existe $x \in G$ tel que $G = \{x^n \mid n \in \mathbb{Z}\}$. Dans ce cas on dit que x est un générateur de G.

Théorème [1.1.24] *Soit G un groupe cyclique fini, soit x un générateur de G et soit d l'ordre de G ($d := \mathrm{ord}(G)$). Alors x est d'ordre d ($\mathrm{ord}(x) = d$) et l'application $\overline{p} \mapsto x^p$ est un homomorphisme bijectif de $(\mathbb{Z}/d\mathbb{Z}, +)$ sur G.*

Corollaire [1.1.25] *Si G est cyclique fini de générateur x, alors x^p est un générateur si et seulement si $\mathrm{pgcd}(p,d) = 1$ où $d = \mathrm{ord}\, x$.*

Fonction de comptage $\varphi(n)$ $\varphi(n)$ est le nombre d'entiers k, $1 \leq k \leq n$, tel que $pgcd(k,n) = 1$.
Exercices

(1) Si $n = p^k$, p premier, alors $\varphi(n) = p^k - p^{k-1}$.

(2) Si $n_1, \ldots, n_q$ sont premiers entre eux deux à deux, alors $\varphi(n_1 \cdots n_q) = \varphi(n_1) \cdots \varphi(n_q)$.

(3) $n = \sum_{d|n} \varphi(d)$ où la notation $d|n$ signifie que d divise n. (Dans la somme $d > 0$).

Remarque [1.1.26]
- Tout groupe fini d'ordre premier est cyclique, mais la réciproque, $\forall n \geq 1 \ \exists$ un groupe cyclique d'ordre n.
- $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n engendré par $\overline{1}$.
- Si G est d'ordre n premier, tout élément $g \neq 1$ de G est générateur car $\mathrm{ord}(g)|n$. $\Rightarrow \mathrm{ord}(g) = n$ sauf si $\mathrm{ord}(g) = 1$ ce qui donne $g = 1$.

Théorème [1.1.27] *Tout groupe fini commutatif G est produit cartésien de groupes cycliques : $\exists G_1, \ldots, G_k$ cycliques tels que $G \cong G_1 \times \ldots \times G_k$ où $(x_1, \ldots, x_k) \cdot (y_1, \ldots, y_k) = (x_1 y_1, \ldots, x_k, y_k)$ ce qui définit une structure de groupe sur $G_1 \times \ldots \times G_k$.*

Théorème [1.1.28] (Théorème chinois) Forme abstraite *Si $a_1, \ldots, a_k$ sonst premiers entre eux deux à deux, le groupe $\mathbb{Z}/a_1 \cdots a_k\mathbb{Z}$ est isomorphe au produit $\mathbb{Z}/a_1 \times \ldots \times \mathbb{Z}/a_k$.*

Forme contrète *Si $a_1, \ldots, a_k$ sont premiers entre eux deux à deux, alors pour toute famille $b_1, \ldots, b_k$ d'entiers relatifs $\exists x \in \mathbb{Z}$ vérifiant $x \equiv b_1 \mod a_1, \ldots, x \equiv b_k \mod a_k$.*
De plus, si x_0 est solution, l'ensemble des solutions est égal à $x_0 + a_1 \cdots a_k\mathbb{Z}$.

1.1.5 Groupe dual

Definition [1.1.29] Soit G un groupe abelien fini. Un caractère de G est un homomorphisme $\chi : G \to \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ muni de la multiplication. L'ensemble des caractères de G est noté $\hat{G}$.

Proposition [1.1.30] *(1) $|\chi(x)| = 1 \ \forall x \in G$, $\chi \in \hat{G}$.*

(2) On pose $(\chi_1\chi_2)(x) = \chi_1(x)\chi_2(x) \ \forall \chi_1, \chi_2 \in \hat{G}$, $x \in G$. Alors $(\hat{G}, \cdot)$ est un groupe.

Proposition [1.1.31] *Si G est fini cyclique de générateur x_0 et d'ordre d, alors $\chi(x_0)$ est une racine $d^{ème}$ de l'unité $\forall \chi \in \hat{G}$. De plus si on note $U_d := \left\{ z \in \mathbb{C} \;\middle|\; z^d = 1 \right\}$ l'ensemble des racines $d^{ème}$ de l'unité, alors l'application $\chi \to \chi(x_0)$ est un isomorphisme de $\hat{G}$ sur U_d. En particulier $\hat{G}$ a d éléments.*

Proposition [1.1.32] *Si $G = G_1 \times \ldots \times G_k$ alors $\hat{G} \cong \hat{G_1} \times \ldots \times \hat{G_k}$. Plus précisément si on pose*

$$[\chi_1, \ldots, \chi_k](x_1, \ldots, x_k) = \chi_1(x_1) \cdots \chi_k(x_k)$$

pour $(\chi_1, \ldots, \chi_k) \in \hat{G_1} \times \ldots \times \hat{G_k}$, $(x_1, \ldots, x_k) \in G_1 \times \ldots \times G_k$ alors l'application $(\chi_1, \ldots, \chi_k) \to [\chi_1, \ldots, \chi_k]$ est un isomorphisme de $\hat{G_1} \times \ldots \times \hat{G_k}$ sur $\widehat{(G_1 \times \ldots \times G_k)}$.

Corollaire [1.1.33] *Si G est un groupe commutatif fini, alors* $\operatorname{ord} \hat{G} = \operatorname{ord} G$.

Exemple [1.1.34] (Dual de $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$) $G = \{(\overline{0},\overline{0}), (\overline{1},\overline{0}), (\overline{0},\overline{1}), (\overline{1},\overline{1}), (\overline{0},\overline{2}), (\overline{1},\overline{2})\}$. $\Rightarrow \operatorname{ord} G = 6$. $\Rightarrow$ On a six caractères sur le groupe produit. On peut identifier les caractères de $\mathbb{Z}/2\mathbb{Z}$ à $U_2 = \{-1, 1\}$ et ceux de $\mathbb{Z}/3\mathbb{Z}$ à $U_3 = \{1, \underbrace{\mathbf{e}^{2\mathbf{i}\pi/3}}_{=:j}, \underbrace{\mathbf{e}^{4\mathbf{i}\pi/3}}_{=j^2}\}$.

$\chi_{a,b}(\overline{u},\overline{v}) = (-1)^{au} j^{bv} = (-1)^{au}\, \mathbf{e}^{2\mathbf{i}bv\pi/3}$, $a \in \{0,1\}, b \in \{0,1,2\}$.

Théorème [1.1.35] *Si G est un groupe, on définit pour $x \in G$: $\theta_x : \hat{G} \to \mathbb{C}^*, \chi \mapsto \chi(x)$ de sorte que $\theta : x \mapsto \theta_x$ est un homomorphisme de groupes de G dans $\hat{\hat{G}}$.*

Alors θ est une bijection de G sur $\hat{\hat{G}}$, appelé ***isomorphisme canonique****.*

Remarque [1.1.36] Si G est fini abelien et si $x, y \in G$, $x \neq y$, $\exists \chi \in \hat{G}$ telle que $\chi(x) \neq \chi(y)$.

Chapitre 2

Vers les transformées de Fourier...

2.1 transformée de Fourier

Soit G un groupe fini, $\mathbb{C}[G]$ l'espace vectoriel de toutes les fonctions de G dans $\mathbb{C}$.
Première base de $\mathbb{C}[G]$: l'ensemble $\{\delta_x \mid x \in G\}$ où $\delta_x(y) = \begin{cases} 0 \text{ si } x \neq y \\ 1 \text{ si } x = y \end{cases}$.
δ_x est bien une application de G dans $\mathbb{C}$.
δ_x est une base de $\mathbb{C}[G]$: $\forall f \in \mathbb{C}[G]$ s'écrit de manière unique $f = \sum_{x \in G} \alpha(x)\delta_x$. Si $f = \sum_{x \in G} \alpha(x)\delta_x$ alors pour $y \in G$ on a $f(y) = \sum_{x \in G} \alpha(x)\delta_x(y) = \alpha(y)$. $\Rightarrow \alpha(y) = f(y)\ \forall y \in G$ et $\alpha(x) = f(x)$.

Réciproquement on a bien $f = \sum_{x \in G} f(x)\delta_x\ \forall f \in \mathbb{C}[G]$. En effet

$\left(\sum_{x \in G} f(x)\delta_x\right)(y) = \sum_{x \in G} f(x)\delta_x(y) = f(y)\ \forall y \in G. \Rightarrow \sum_{x \in G} f(x)\delta_x = f.$

D'autre part, la famille $\{\chi \mid \chi \in \hat{G}\}$ est également une base de $\mathbb{C}[G]$.
On introduit un produit hermitien sur $\mathbb{C}[G]$. On pose

$$\langle f, g \rangle := \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g}(x).$$

On pose $\|g\| = \sqrt{\langle f, f \rangle} = \sqrt{\frac{1}{|G|} \sum_{x \in G} |f(x)|^2}$. $\Rightarrow \|f\| > 0\ \forall f \neq 0$, $\|f + g\| \leq \|f\| + \|g\|$, $\|\lambda f\| = |\lambda|\,\|f\|$ $\forall f, g \in \mathbb{C}[G]$, $\lambda \in \mathbb{C}$.

Proposition [2.1.1] *Si $\chi \in \hat{G}$, $\|x\| = 1$. Si $\chi_1, \chi_2 \in \hat{G}$, $\chi_1 \neq \chi_2 \Rightarrow \langle \chi_1, \chi_2 \rangle = 0$.*
En particulier, $\{\chi \mid \chi \in \hat{G}\}$ forme une base de $\mathbb{C}[G]$ pour ce produit hermitien et $\forall f \in \mathbb{C}[G]$ s'écrit

$$\begin{aligned} f &= \sum_{\chi \in \hat{G}} \langle f, \chi \rangle \chi \\ &= \sum_{\chi \in \hat{G}} c_f(\chi)\chi \end{aligned}$$

avec $c_f(\chi) = \langle f, \chi \rangle = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{\chi}(x)$.

Definition [2.1.2] $f \in \mathbb{C}[G]$. $\hat{f} \in \mathbb{C}[\hat{G}]$ est définie par

$$\hat{f}(\chi) = \sum_{x \in G} f(x)\chi(x).$$

On a établie les relations d'orthogonalité

$$\begin{aligned} \sum_{x \in G} \chi_1(x)\overline{\chi_2}(x) &= |G| \cdot \delta_{\chi_1\chi_2} \qquad \chi_1, \chi_2 \in \hat{G} \\ \sum_{\chi \in \hat{G}} \chi(x_1)\chi(x_2) &= \delta_{x_1,x_2} \cdot \left|\hat{G}\right| = \delta_{x_1,x_2} \cdot |G| \end{aligned}$$

Les autres relations se démontrent en remarquant que si $x_1, x_2 \in G$, $\varphi_{x_1} : \chi \mapsto \chi(x_1)$, $\varphi_{x_2} : \chi \mapsto \chi(x_2)$ appartiennent à $\hat{\hat{G}}$.

On obtient $f = \sum_{x\in G} f(x)\delta_x = \sum_{\chi\in\hat{G}} c_f(\chi)\chi$ avec $c_f = \langle f, \chi\rangle = \frac{1}{|G|}\sum_{x\in G} f(x)\overline{\chi}(x)$.

La deuxième formule montre en calculant

$$\left\langle f - \sum_{\chi\in\hat{G}} c_f(\chi)\chi,\ \theta \right\rangle = \langle f, \theta\rangle - \sum_{\chi\in\hat{G}} \langle f, \chi\rangle \langle \chi, \theta\rangle .$$

Or, $\langle \chi, \theta\rangle = 0$ si $\theta \neq \chi$, $\langle \chi, \theta\rangle = 1$ si $\chi = \theta$. Alors on obtient

$$\left\langle f - \sum_{\chi\in\hat{G}} \langle f, \chi\rangle \chi,\ \theta \right\rangle = \langle f, \theta\rangle - \langle f, \theta\rangle = 0 \quad \forall\theta \in \hat{G}$$

$\Longrightarrow f - \sum_{\chi\in\hat{G}} \langle f, \chi\rangle \chi = 0$ car $\hat{G}$ forme une base orthonormale de $\mathbb{C}[G]$.

$\langle u, \theta\rangle = 0\ \forall\theta \in \hat{G}. \Rightarrow \langle u, g\rangle = 0\ \forall g \in \mathbb{C}[G]. \Rightarrow \langle u, u\rangle = \frac{1}{|G|}\sum_{x\in G} |u(x)|^2 = 0\ \forall x \in G. \Rightarrow u = 0.$ (L'élément orthogonal à tous les caractères n'est que l'élément nul.)

Soit $f \in \mathbb{C}[G]$. On a défini $\mathcal{F}(f) = \hat{f} \in \mathbb{C}[G]$ par la formule

$$\hat{f}(\chi) = \sum_{x\in G} f(x)\chi(x)$$

Exemple [2.1.3] $a \in G$. On va calculer $\hat{\delta}_a$.

$$\begin{aligned}\hat{\delta}_a(\chi) &= \sum_{x\in G} \delta_a(x)\chi(x)\\ &= \chi(a)\end{aligned}$$

$\hat{\delta}_a$ est l'élément $\widetilde{a} : \chi \to \chi(a)$ de $\hat{\hat{G}}$ canoniquement associé à a. $\Rightarrow \hat{\delta}_a$ est le caractère de $\hat{G}$ canoniquement associé à a.

L'ensemble $\{\widetilde{a} \mid a \in G\}$ est une base orthonormale de $\mathbb{C}[\hat{G}]$. Donc la transformée de Fourier $\mathcal{F} : f \to \hat{f}$ transforme la BON $\{\delta_a \mid a \in G\}$ de $\mathbb{C}[G]$ en la BON $\{\widetilde{a} \mid a \in G\}$ de $\mathbb{C}[\hat{G}]$; donc $\mathcal{F}$ conserve la norme et le produit scalaire et $\mathcal{F}$ est un isomorphisme car $\dim \mathbb{C}[\hat{G}] = \dim \mathbb{C}[G] = \left|\hat{G}\right| = |G|$.

Proposition [2.1.4] (Plancherel-Parseval)

$$\begin{aligned}\sum_{x\in G} f(x)\overline{g}(x) &= \frac{1}{|G|}\sum_{\chi\in\hat{G}} \hat{f}(\chi)\overline{\hat{g}(x)},\\ \sum_{x\in G} |f(x)|^2 &= \frac{1}{|G|}\sum_{\chi\in\hat{G}} \left|\hat{f}(x)\right|^2 \qquad \forall f, g \in \mathbb{C}[G].\end{aligned}$$

Proposition [2.1.5] (Formule d'inversion)

$$f = \sum_{\chi\in\hat{G}} c_f(\chi)\chi = \frac{1}{|G|}\sum_{\chi\in\hat{G}} \hat{f}(\chi)\chi^{-1}$$

avec $c_f(\chi) = \langle f, \chi\rangle = \frac{1}{|G|}\sum_{x\in G} f(x)\overline{\chi}(x)$.

Nous rappelons que G est toujours un groupe abélien fini.

Definition [2.1.6] $\forall f, g \in \mathbb{C}[G], \forall x \in G$ on pose

$$f * g(x) = \sum_{y\in G} f(y)g(y^{-1}x).$$

L'opération $*$ est appelée convolution.

Théorème [2.1.7] *$(\mathbb{C}[G], *)$ est une algèbre et la transformée de Fourier*

$$\widehat{(f * g)} = \hat{f} \cdot \hat{g} \quad \forall f, g \in \mathbb{C}[G].$$

Exemple [2.1.8] On donne f et v et on veut resoudre $f * u = v. \iff \hat{f} \cdot \hat{u} = \hat{v}$ ce qui n'est plus qu'un problème de division.

Pour χ fixé :

$$\hat{f}(\chi)\hat{u}(\chi) = \hat{v}(\chi) \quad \iff \quad \begin{cases} \hat{u}(\chi) = \frac{\hat{v}(\chi)}{\hat{f}(\chi)} & \text{si } \hat{f}(\chi) \neq 0 \\ \hat{u}(\chi) \text{ quelconque} & \text{si } \hat{f}(\chi) = \hat{v}(\chi) = 0 \\ \text{impossible} & \text{si } \hat{f}(\chi) = 0, \hat{v}(\chi) \neq 0 \end{cases}.$$

On obtient un ensemble de solutions qui peut être vide pour $\hat{u}$. On revient aux solutions de u par Fourier inverse.

2.2 Formule de Poisson

Definition [2.2.1] G groupe abélien fini, H sous-groupe de G. L'othogonal de H, noté $H^\perp$, est défini par la formule

$$H^\perp := \left\{ \chi \in \hat{G} \mid \chi(x) = 1 \quad \forall x \in H \right\}.$$

Proposition [2.2.2] *$H^\perp$ est un sous-groupe de $\hat{G}$ et $H^\perp$ est isomorph à $\widehat{(G/H)}$. En particulier : $\left|H^\perp\right| = |G/H| = \frac{|G|}{|H|}$.*

Théorème [2.2.3] *Soit G abélien fini, $f \in \mathbb{C}[G]$, H sous-groupe de G. On a*

$$\sum_{x \in H} f(x) = \frac{1}{|H^\perp|} \sum_{\chi \in H^\perp} \hat{f}(\chi). \qquad \text{(formule de Poisson)}$$

Chapitre 3

Transformée de Walsh

3.1 Définition et propriétés

$$
\begin{aligned}
W_1 &= [1] \\
W_2 &= \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \\
W_4 &= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \\
W_8 &= \begin{bmatrix} W_4 & W_4 \\ W_4 & -W_4 \end{bmatrix} \\
&\vdots \\
W_{2^n} &= \begin{bmatrix} W_{2^{n-1}} & W_{2^{n-1}} \\ W_{2^{n-1}} & -W_{2^{n-1}} \end{bmatrix}
\end{aligned}
$$

On prend $f \in \mathbb{C}^{2^n}$, $f = (f[0], f[1], \ldots, f[2^n - 1])$. $\mathcal{W}_{2^n}(f)$ est définie par

$$
\begin{bmatrix} \mathcal{W}_{2^n} f[0] \\ \vdots \\ \mathcal{W}_{2^n} f[2^n - 1] \end{bmatrix} = W_{2^n} \begin{bmatrix} f[0] \\ \vdots \\ f[2^n - 1] \end{bmatrix}
$$

Soit $f \in \mathbb{C}^{2^n}$. On pose $f_0[i] = f[i]$ pour $0 \leq i \leq 2^{n-1} - 1$, $f_1[i] = f[i - 2^{n-1}]$ pour $2^{n-1} \leq i \leq 2^n - 1$ et on obtient

$$
\begin{aligned}
\mathcal{W}_{2^n}(f)^{\mathrm{T}} &= \begin{bmatrix} W_{2^{n-1}} & W_{2^{n-1}} \\ W_{2^{n-1}} & -W_{2^{n-1}} \end{bmatrix} \begin{bmatrix} f[0]^{\mathrm{T}} \\ \vdots \\ f[2^n - 1]^{\mathrm{T}} \end{bmatrix} \\
&= \begin{bmatrix} \mathcal{W}_{2^{n-1}}(f_0)^{\mathrm{T}} + \mathcal{W}_{2^{n-1}}(f_1)^{\mathrm{T}} \\ \mathcal{W}_{2^{n-1}}(f_0)^{\mathrm{T}} - \mathcal{W}_{2^{n-1}}(f_1)^{\mathrm{T}} \end{bmatrix}
\end{aligned}
$$

ce qui nous raccourcit le temps de calcul.

Propriétés [3.1.1]
- $W_1^2 = [1] = 1I_1$
- $W_2^2 = \begin{bmatrix} W_1 & W_1 \\ W_1 & -W_1 \end{bmatrix} \begin{bmatrix} W_1 & W_1 \\ W_1 & -W_1 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = 2I_2$
- $W_4^2 = \begin{bmatrix} 4I_2 & 0 \\ 0 & 4I_2 \end{bmatrix} = 4I_4$

– *On montre facilement que*

$$W_{2^n}^2 = 2^n I_{2^n}$$

Donc la transformée de Walsh est à un facteur près son inverse :

$$W_{2^n}{}^{-1} = \frac{1}{2^n} W_{2^n}$$

Changements de signes sur les lignes

Le vecteur C_{2^n} qui a le même nombre de lignes que W_{2^n} note le nombre de changements de signes de la $k^{\text{ème}}$ ligne de W_{2^n} dans sa $k^{\text{ème}}$ ligne.

– $C_1 = [0]$
– $C_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
– $C_4 = \begin{bmatrix} 0 \\ 3 \\ 1 \\ 2 \end{bmatrix}$
– $C_8 = \begin{bmatrix} 0 \\ 7 \\ 3 \\ 4 \\ 1 \\ 6 \\ 2 \\ 5 \end{bmatrix}$

Théorème [3.1.2] *Les nombres $n(L_i)$ de changements de signe des lignes de la matrix W_{2^n} sont tous distincts et prennent les valeur $\{0, 1, \ldots, 2^n - 1\}$.*

Problème technique : Le clacul de W_{2^n} nécessite beaucoup d'opérations :

$$\begin{pmatrix} \mathcal{W}_{2^n}(f)[0] \\ \vdots \\ \mathcal{W}_{2^n}(f)[2^n-1] \end{pmatrix} = W_{2^n} \begin{pmatrix} f[0] \\ \vdots \\ f[2^n-1] \end{pmatrix}$$

On a 2^n coefficients à calculer et pour chaque coefficient 2^n opérations â faire. $\Rightarrow 2^{2^n}$ opérations ! Pour W_{1024} on a ainsi plus d'un million d'opérations !

3.2 transformée de Walsh rapide

Exemple [3.2.1] transformée de Walsh de $A := [1,2,3,4]$, $B := [8,7,6,5]$, $C := [AB] = [1,2,3,4,8,7,6,5]$.

$$U := \begin{bmatrix} W(A)[0] \\ W(A)[1] \\ W(A)[2] \\ W(A)[3] \end{bmatrix} = W_4 A^{\mathrm{T}} = \begin{bmatrix} 10 \\ -2 \\ -4 \\ 0 \end{bmatrix}$$

$$V := \begin{bmatrix} W(B)[0] \\ W(B)[1] \\ W(B)[2] \\ W(A)[3] \end{bmatrix} = W_4 B^{\mathrm{T}} = \begin{bmatrix} 26 \\ 2 \\ 4 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} W(C)[0] \\ W(C)[1] \\ \vdots \\ W(C)[6] \\ W(C)[7] \end{bmatrix} = \begin{bmatrix} W_4 & W_4 \\ W_4 & -W_4 \end{bmatrix} \begin{bmatrix} A^{\mathrm{T}} B^{\mathrm{T}} \end{bmatrix}$$

$$= \begin{bmatrix} U+V \\ U-V \end{bmatrix}$$

$$= \begin{bmatrix} 36 \\ 0 \\ 0 \\ 0 \\ -16 \\ -4 \\ -8 \\ 0 \end{bmatrix}$$

Voyant cela, on peut se demander pourquoi on n'a pas appliqué cette "règle" dès le début pour A et B : (exemple pour A)

Posons $D := [1,2]$ et $E := [3,4]$ $W(D) = W_2 D^{\mathrm{T}} = \left[\begin{smallmatrix} 3 \\ -1 \end{smallmatrix}\right]$, $W(E) = W_2 E^{\mathrm{T}} = \left[\begin{smallmatrix} 7 \\ -1 \end{smallmatrix}\right]$.

$$W(A) = \begin{bmatrix} W_2 & W_2 \\ W_2 & -W_2 \end{bmatrix} \begin{bmatrix} D^{\mathrm{T}} \\ E^{\mathrm{T}} \end{bmatrix} = \begin{bmatrix} W(D) + W(E) \\ W(D) - W(E) \end{bmatrix} = \begin{bmatrix} 10 \\ -2 \\ -4 \\ 0 \end{bmatrix}.$$

Exemple [3.2.2] (Algorithme de Walsh rapide sur l'exemple)

k	0	1	2	3	4	5	6	7
$f[k]$	1	2	3	4	8	7	6	5
$(1)_{Wf}$	$3 = 1+2$	$-1 = 1-2$	$7 = 3+4$	$-1 = 3-4$	$15 = 8+7$	$1 = 8-7$	$11 = 6+5$	$1 = 6-5$
$(2)_{Wf}$	$10 = 3+7$	$-2 = -1+-1$	$-4 = 3-7$	$0 = -1--1$	$26 = 15+11$	$2 = 1+1$	$4 = 15-11$	$0 = 1-1$
$(3)_{Wf} = Wf$	$36 = 10+26$	$0 = -2+2$	$0 = -4+4$	$0 = 0+0$	$-16 = 10-26$	$-4 = -2--2$	$-8 = -4-4$	$0 = 0-0$

A la $k^{\text{ème}}$ étape on obtient 2^{n-k} blocs à 2^k éléments. Pour passer à la $(k+1)^{\text{ème}}$ étape on les regroupe deux à deux et on obtiendra 2^{n-k-1} lignes à 2^{k+1} éléments selon le principe

u	v
$u+v$	$u-v$

.

Au lieu d'avoir 2^{2^n} d'opérations, on en a $n \cdot 2^n$, donc pour W_{1024} 10240 opérations ...

3.3 Principe de la compression du signal 1-D

signal $f = (f[0], \ldots, f[2^n - 1])$.

(1) On calcule la transformée de Walsh.

(2) On supprime les coefficients associés à des lignes avec beaucoup de changements de signe.

(3) On calcule la transformée de Walsh inverse du résultat obtenu.

Exemple [3.3.1] Compression à 50 % du signal ci-dessus. On va jeter les lignes d'indice 1, 3, 5, 7 (sachant qu'on commence à indicer avec 0).

Wf	36	∅	0	∅	-16	~~-4~~	-8	∅
$W_{50\%}f$	36	0	0	0	-16	0	-8	0
$(1)_{W_{50\%}f}$	36	36	0	0	-16	-16	-8	-8
$(2)_{W_{50\%}f}$	36	36	36	36	-24	-24	-8	-8
$(3)_{W_{50\%}f} = 2^3 \cdot f_{50\%}$	12	12	28	28	60	60	44	44
$f_{50\%}$	1.5	1.5	3.5	3.5	7.5	7.5	5.5	5.5
f	1	2	3	4	8	7	6	5

$\Longrightarrow \|f - f_{50\%}\|_2 = \sqrt{2}$.

*I*mage : Tableau de pixels.

$$A = (a_{ij})_{0 \le i,j \le 2^n - 1}$$

Pour $0 \le i, j \le 1024$ on a plus d'un million de pixels.

$$\mathcal{W}_{2^n}(A) = W_{2^n} A W_{2^n}$$

Ca revient à faire une transformée de Walsh vectorielle sur les lignes puis sur les colonnes. On obtient

$$B = (b_{ij})_{0 \le i,j \le 2^n - 1}.$$

Pour classer les couples (i, j) on ordonne selon $n(L_i) + n(L_j)$ et en cas d'égalité selon $n(L_i)$. On comprime comme précédemment.

3.4 Lien entre transformée de Walsh et transformée de Fourier

Bijection entre $\{0,\dots,2^k-1\}$ et $\{0,1\}^k$.
On écrit un entier n avec $0 \leq n \leq 2^k-1$ en base 2.
$\Rightarrow n = n_k n_{k-1}\cdots n_1 = \sum_{i=1}^{k} n_i 2^{i-1}$ avec $n_i \in \{0,1\}\ \forall i$.

En base 10, $a = a_k a_{k-1}\dots a_1 = \sum_{i=1}^{k} a_i 10^{i-1}$, $0 \leq a_i \leq 9\ \forall i$.

Les deux ensembles $\{0,\dots,2^k-1\}$ et $\{0,1\}^k$ ont le même nombre d'éléments. Pour montrer qu'on a une bijection il suffit de montrer que tout élément entier $n \in \{0,\dots,2^k-1\}$ s'écrit

$$n = \sum_{i=1}^{k} \alpha_i 2^{i-1}$$

avec $\alpha_i \in \{0,1\}\ \forall i$.

Cela montre que $\theta : \{0,1\}^k \to \{0,\dots,2^k-1\}$, $(\alpha_1,\dots,\alpha_k) \mapsto \sum_{i=1}^{k} \alpha_i 2^{i-1}$ est surjective, donc aussi injective et par conséquent bijective.

Preuve (par recurrence) $\underline{k=1}$ Dans ce cas, on a une application $\{0,1\} \to \{0,1\}$, $\theta(\alpha_1) = \alpha_1 \cdot 2^{1-1} = \alpha_1$.
$\underline{k \to k+1}$ On suppose maintenant que c'est vrai pour k.

$\theta(\alpha_1,\dots,\alpha_k,\alpha_{k+1}) = \sum_{i=1}^{k+1} \alpha_i 2^{i-1}$, $\theta : \{0,1\}^{k+1} \to \{0,\dots,2^{k+1}-1\}$.

Soit $p \in \{0,\dots,2^{k+1}-1\}$. On a $p = 2^k \cdot q + r$ avec $0 \leq r \leq 2^k-1$. Alors $2^{k+1} \geq p \geq 2^k q$.

$\Rightarrow q \leq \frac{2^{k+1}}{2^k} - \frac{1}{2^k} = 2 - \frac{1}{2^k} < 2$. Donc, $q \in \{0,1\}$.

Par hypotèse de recurrence, $\exists \alpha_1,\dots,\alpha_k$ tels que $r = \sum_{i=1}^{k} \alpha_i 2^{i-1}$.

$\Rightarrow p = \sum_{i=1}^{k} \alpha_1 2^{i-1} + q2^k = \sum_{i=1}^{k+1} \alpha_i 2^{i-1}$ avec $\alpha_{k+1} = q$.

$\Rightarrow$ La propriété est vraie pour $k+1$. $\Rightarrow$ vraie $\forall k \in \mathbb{N}$. ■

Dans la preuve, on obtient comme cadeau un algorithme !

On rappelle que $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{\overline{0},\overline{1}\}$ est un corps avec les tables d'addition et de multiplication suivantes :

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

$\mathbb{F}_2^k$ est un espace vectoriel sur $\mathbb{F}_2$ de dimension k qui admet pour base $\{e_i\}_{1\leq i\leq k}$ avec $e_i = (\delta_{ji})_{1\leq j\leq k}$.
F_2^k a 2^k éléments.
On a un isomorphisme entre $\mathbb{F}_2^k$ et $\{0,1\}^k$: tout élément x de $\mathbb{F}_2^k$ s'écrit de manière unique sous la forme $x = (\overline{x}_1,\dots,\overline{x}_k)$ avec $\overline{x}_i \in \{\overline{0},\overline{1}\}\ \forall i$.
On a une bijection Δ de $\mathbb{F}_2^k$ sur $\{0,\dots,2^k-1\}$ avec

$$\Delta(\overline{x}_1,\dots,\overline{x}_k) = \sum_{i=1}^{k} x_i 2^{i-1},$$

$x_i \in \{0,1\}\ \forall i$.
On peut numéroter de 0 à 2^k-1 les éléments de $\mathbb{F}_2^k$. Pour $u = (u_1,\dots,u_k)$, $v = (v_1,\dots,v_k) \in \mathbb{F}_2^k$ on pose (de manière analogue du cas $\mathbb{R}^n$)

$$\langle u, v\rangle = \sum_{i=1}^{k} u_i v_i.$$

Attention : $\langle u, v\rangle \in \mathbb{F}_2$!!

Pour $u, v \in \mathbb{F}_2^k$ on pose $\chi_v(u) = (-1)^{\langle u,v\rangle}$ avec la convention $(-1)^{\overline{0}} = 1$, $(-1)^{\overline{1}} = -1$. (On vérifie directement la symétrie de χ : $\chi_v(u) = \chi_u(v)$.)

De plus, on voit

$$\begin{aligned}\chi_v(u_1 + u_2) &= (-1)^{\langle u_1+u_2,v\rangle} \\ &= (-1)^{\langle u_1,v\rangle+\langle u_2,v\rangle} \\ &= (-1)^{\langle u_1,v\rangle} \cdot (-1)^{\langle u_2,v\rangle} \\ &= \chi_v(u_1) \cdot \chi_v(u_2)\end{aligned}$$

Resumé

(1) On sait numéroter les éléments de $\mathbb{F}_2^k$ de 0 à $2^k - 1$:

$$N(\overline{x}_1, \ldots, \overline{x}_k) = \sum_{i=1}^{k} x_i 2^{i-1},$$

$x_i \in \mathbb{F}_2$ $\forall i$.

(2) L'application $v \mapsto \chi_v : u \mapsto (-1)^{\langle u,v\rangle}$ est une bijection de $\mathbb{F}_2^k$ sur $\hat{\mathbb{F}_2^k}$.

On note U_p le $p^{\text{ème}}$ élément de F_2^k, $0 \leq p \leq 2^k - 1$. On pose $\widetilde{W}_{p,q} = \chi_{U_p}(U_q) = \chi_{U_q}(U_p)$. Alors :

$$\widetilde{W}_{2^k} = \left(\widetilde{W}_{p,q}\right)_{0\leq p,q\leq 2^k-1}.$$

Exemple (pour $k = 1$) $U_0 = \overline{0}$, $U_1 = \overline{1}$.

$$\widetilde{W}_{0,0} = (-1)^{\langle\overline{0},\overline{0}\rangle} = 1 \qquad \widetilde{W}_{0,1} = (-1)^{\langle\overline{0},\overline{1}\rangle} = 1$$
$$\widetilde{W}_{1,0} = (-1)^{\langle\overline{1},\overline{0}\rangle} = 1 \qquad \widetilde{W}_{1,1} = (-1)^{\langle\overline{1},\overline{1}\rangle} = -1$$

Donc,

$$\widetilde{W}_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = W_2,$$

W_2 étant la matrice de Walsh. On montre par recurrence que $\widetilde{W}_{2^k} = W_{2^k}$ $\forall k$.

Chapitre 4

Fonctions booléennes

4.1 Définitions et propriétés

Definition [4.1.1] Une fonction booléenne est une application $\mathbb{F}_2^k \to \mathbb{F}_2$. L'ensemble des fonctions booléennes est noté $\mathcal{B}_k$. On munit $\mathcal{B}_k$ des opérations usuelles : pour $f, g \in \mathcal{B}_k$:

(1) $(f+g)(x) = f(x) + g(x) \quad \forall x \in \mathbb{F}_2^k$.

(2) $(fg)(x) = f(x)\, g(x) \quad \forall x \in \mathbb{F}_2^k$.

(3) $(\lambda f)(x) = \lambda f(x) \quad x \in \mathbb{F}_2, \forall \lambda \in \mathbb{F}_2$.

On obtient une algèbre sur $\mathbb{F}_2$.

Proposition [4.1.2] *On a les résulats suivants :*

$$\begin{aligned} \operatorname{card}(\mathcal{B}_k) &= 2^{2^k} \\ \dim(\mathcal{B}_k) &= 2^k \end{aligned}$$

La famille $(\delta_a)_{a \in \mathbb{F}_2^k}$ *est une base de* $\mathcal{B}_k$ *avec* $\delta_a(x) = \begin{cases} 0 & a \neq x \\ 1 & a = x \end{cases}$.

Exemple [4.1.3] $k = 1$ **:** On a quatre fonctions booléennes :

x	$\overline{0}$	$\overline{1}$
$f_1(x)$	$\overline{0}$	$\overline{0}$
$f_2(x)$	$\overline{0}$	$\overline{1}$
$f_3(x)$	$\overline{1}$	$\overline{0}$
$f_4(x)$	$\overline{1}$	$\overline{1}$

$k = 2$ **:** On a seize fonctions booléennes.

x	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$f_1(x)$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$f_2(x)$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{1}$
$f_3(x)$	$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{0}$
$f_4(x)$	$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{1}$
$f_5(x)$	$\overline{0}$	$\overline{1}$	$\overline{0}$	$\overline{0}$
$f_6(x)$	$\overline{0}$	$\overline{1}$	$\overline{0}$	$\overline{1}$
$f_7(x)$	$\overline{0}$	$\overline{1}$	$\overline{1}$	$\overline{0}$
$f_8(x)$	$\overline{0}$	$\overline{1}$	$\overline{1}$	$\overline{1}$
$f_9(x)$	$\overline{1}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$f_{10}(x)$	$\overline{1}$	$\overline{0}$	$\overline{0}$	$\overline{1}$
$f_{11}(x)$	$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{0}$
$f_{12}(x)$	$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{1}$
$f_{13}(x)$	$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{0}$
$f_{14}(x)$	$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{1}$
$f_{15}(x)$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{0}$
$f_{16}(x)$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$

Definition [4.1.4] Pour $1 \leq i \leq k$ on note

$$\begin{aligned} X_i : \mathbb{F}_2^k &\to F_2 \\ (\alpha_1, \ldots, \alpha_k) &\mapsto \alpha_1. \end{aligned}$$

Un **monôme** est une application de la forme $X_{i_1} \cdots X_{i_p}$ avec $1 \leq i_m \leq k \; \forall m \leq p$.

Si $u \in F_2$, alors $u^2 = u$. Donc $X_i^2 = X_i \; \forall i$. Si $f \in \mathcal{B}_k$, on a $f^2(x) = f(x)^2 = f(x) \; \forall x \in \mathbb{F}_2^k$. $\Rightarrow f^2 = f$ et $(f+f)(x) = f(x) + f(x) = \overline{0} \; \forall x \in \mathbb{F}_2^k$.

$\Rightarrow X_i^p = X_i \; \forall i, p$.

Les monômes sont des monômes de degré 1 par rapport à chacune des variables.

Tout monôme est de la forme $\prod_{i \in S} X_i$ avec $S \subseteq \{1, \ldots, k\}$ avec la convention $\prod_{i \in \emptyset} X_i = 1$.

Le nombre de monômes est égal au nombre de sous-ensembles de $\{1, \ldots, k\}$, soit 2^k. Rappelons que $\dim \mathcal{B}_k = 2^k$.

$$\left(\prod_{i \in S} X_i \right) (\alpha_1, \ldots, \alpha_k) = \prod_{i \in S} \alpha_i$$

(par convention égal à 1 si $S = \emptyset$).

Proposition [4.1.5] $\delta_a = \prod_{i=1}^{k} \left(X_i + a_i + \overline{1} \right)$ *pour* $a = (a_1, \ldots, a_k) \in \mathbb{F}_2^k$.

Cela fait que toute fonction booléenne est un polynôme de degré ≤ 1 par rapport à chacune des variables.

Exemple [4.1.6]

x	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
f_7	$\overline{0}$	$\overline{1}$	$\overline{1}$	$\overline{0}$

$$\begin{aligned} f_7 &= \overline{0} \cdot \delta_{(0,0)} + \overline{1} \cdot \delta_{(0,1)} + \overline{1} \cdot \delta_{(1,0)} + \overline{0} \cdot \delta_{(1,1)} \\ &= \delta_{(0,1)} + \delta_{(1,0)}. \end{aligned}$$

Soit $a := (0,1)$, $b := (1,0)$.

$$\begin{aligned}\delta_a &= \prod_{i=1}^{2}(X_i + a_i + \overline{1}) \\ &= (X_1 + \overline{0} + \overline{1}) \cdot (X_2 + \overline{1} + \overline{1}) \\ &= (X_1 + 1) \cdot X_2 \\ &= X_1X_2 + X_2.\end{aligned}$$

$$\begin{aligned}\delta_b &= \prod_{i=1}^{2}(X_i + b_i + 1) \\ &= (X_1 + \overline{1} + \overline{1}) \cdot (X_2 + \overline{0} + \overline{1}) \\ &= X_1 \cdot (X_2 + 1) \\ &= X_1X_2 + X_1.\end{aligned}$$

On a donc,

$$\begin{aligned}f_7 &= \delta_a + \delta_b \\ &= X_1X_2 + X_1 + X_1X_2 + X_2 \\ &= X_1 + X_2.\end{aligned}$$

Definition [4.1.7] Une fonction affine est une fonction booléenne qui s'écrit comme somme d'une constante et d'une famille (éventuellement vide) de monômes de degré 1.
On note Aff_k (ou Aff) l'ensemble des fonctions affines.

Propriétés [4.1.8] *On a que* $\mathrm{card}(\mathrm{Aff}_k) = 2^{k+1}$.

Exemple [4.1.9] $k = 1$ **:** $\mathcal{B}_1$ a quatre éléments, Aff_1 en a quatre. $\Rightarrow$ Toute fonction de $\mathcal{B}_1$ est affine.

$$\mathcal{B}_1 = \{0, 1, X_1, 1 + X_1\}.$$

$k = 2$ **:** $\mathcal{B}_2$ a 16 éléments, Aff_2 en a huit.

$k = 3$ **:** $\mathcal{B}_3$ a 256 éléments, Aff_3 en a 16.

$k = 4$ **:** $\mathcal{B}_4$ a 65 536 éléments, Aff_4 en a 32.

Definition [4.1.10] Si $f, g \in \mathcal{B}_k$, on pose

$$\mathrm{dist}(f,g) := \mathrm{card}\left\{ x \in \mathbb{F}_2^k \;\middle|\; f(x) \neq g(x) \right\},$$

la distance de Hammings.
Si $f \in \mathcal{B}_k$ on pose

$$\mathrm{dist}(f, \mathrm{Aff}_k) = \inf\{\mathrm{dist}(f,g) \mid g \in \mathrm{Aff}_k\}.$$

On numérote les éléments de $\mathbb{F}_2^k$ de 0 à $2^k - 1$. Pour $f \in \mathcal{B}_k$, $0 \leq j \leq 2^k - 1$, on pose

$$f^*(j) := (-1)^{f(a_j)}$$

où a_j est le $j^{\text{ème}}$ élément de F_2^k.

Exemple [4.1.11] Si $j = \alpha_k\alpha_{k-1}\cdots\alpha_1 = \sum_{i=1}^{k} \alpha_i 2^{i-1}$, $a_j = (\alpha_1, \ldots, \alpha_k)$.

j	0	1	2	3
a_j	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$f_7(a_j)$	$\overline{0}$	$\overline{1}$	$\overline{1}$	$\overline{0}$
$f_7^*(j)$	1	-1	-1	1

Théorème [4.1.12] *Pour $y = (y_1, \dots, y_k) \in \mathbb{F}_2^k$, $x = (x_1, \dots, x_k) \in \mathbb{F}_2^k$, on pose*

$$\Phi_y(x) := \sum_{j=1}^{k} x_j y_j = \langle x, y \rangle ,$$

soit $\Phi_y = \sum_{j=1}^{k} X_j y_j \in \mathrm{Aff}_k$.

Soit $f \in \mathcal{B}_k$.

(1) $\mathrm{dist}(f, \Phi_y) = 2^{k-1} - \frac{1}{2} W(f^*)[y]$

(2) $\mathrm{dist}(f, \mathrm{Aff}_k) = 2^{k-1} - \frac{1}{2} \max \left\{ |W(f^*)[y]| \;\middle|\; y \in \mathbb{F}_2^k \right\}$.

(3) $\mathrm{dist}(f, \mathrm{Aff}_k) \leq 2^{k-1} - 2^{\frac{k}{2}-1}$

(4) On a $\mathrm{dist}(f, \mathrm{Aff}_k) = 2^{k-1} - 2^{\frac{k}{2}-1}$ *si k est pair* ***et si*** $|W(f^*)[y]| = 2^{\frac{k}{2}}\ \forall y$ *; on dit alors que f est une fonction courbe.*

Par exemple, $\sum_{j=0}^{\frac{k}{2}-1} X_{2j+1} X_{2j+2}$ est une fonction courbe.

Au niveau des notations, on a identifié $a_j \in \mathbb{F}_2^k$ à $j \in \{0, \dots, 2^k - 1\}$.

Exemple [4.1.13] $k = 1$ **:** $\mathrm{dist}(f, \mathrm{Aff}_1) \leq 2^0 - 2^{-\frac{1}{2}} < 1 \quad \forall f.\ \mathrm{dist}(f, \mathrm{Aff}_k) = 0. \Rightarrow$ Toute fonction est affine.

$k = 2$ **:** $\mathrm{dist}(f, \mathrm{Aff}_2) \leq 2^1 - 2^0 = 1$ et $\mathrm{dist}(f, Aff_2) = 1$ si $f = X_1 X_2$.

$k = 3$ **:** $\mathrm{dist}(f, \mathrm{Aff}_3) \leq 2^2 - 2^{\frac{1}{2}} = 4 - \sqrt{2}. \Rightarrow \mathrm{dist}(f, \mathrm{Aff}_3) \leq 2$.

$k = 4$ **:** $\mathrm{dist}(f, \mathrm{Aff}_4) \leq 2^3 - 2^1 = 6$, atteint pour $f = X_1 X_2 + X_3 X_4$.

Pour $k = 2$, $f = X_1 X_2$, on écrit f^*.

j	0	1	2	3
a_j	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$f(a_j)$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{1}$
$f_7^*(j)$	1	1	1	-1
$(1)_{Wf^*}$	2	0	0	2
Wf^*	2	2	2	-2

$\mathrm{dist}(f, \mathrm{Aff}_2) = 2 - \frac{1}{2} \max \left\{ |Wf^*(y)| \;\middle|\; y \in F_2^2 \right\} = 2 - 1 = 1$.

On veut maintenant calculer les valeurs propres de la matrice de Walsh.

$$W_{2^k}^2 = 2^k I_{2^k} \qquad \Longrightarrow \qquad \left(W_{2^k} - 2^{\frac{k}{2}} I_{2^k} \right) \left(W_{2^k} + 2^{\frac{k}{2}} \right) = 0.$$

On sait que W_{2^k} est diagonialisable sur $\mathbb{R}$ car elle est symétrique réelle. Si λ est valeur propre, on pose Λ le vecteur propre associé.

On a $W_{2^k}^2 \Lambda = W_{2^k}(W_{2^k}\Lambda) = W_{2^k} \lambda \Lambda = \lambda^2 \Lambda$. On en déduit que $\lambda^2 \Lambda = 2^k \Lambda$, alors $\lambda^2 = 2^k$. On a alors que

$$\lambda = \pm 2^{\frac{k}{2}}.$$

Le vecteur propre se fabrique par recurrence pour k pair :

(i) $\Lambda_{2^0} = [1]$.

(ii) $\Lambda_{2^{2p+2}} = [\Lambda_{2^{2p}}, \Lambda_{2^{2p}}, \Lambda_{2^{2p}}, -\Lambda_{2^{2p}}]$.

Chapitre 5

FFT (Fast Fourier Transform)

5.1 Définitions

Soit $f = [f[0], \ldots, f[N-1]]$, $N \geq 1$, et $\omega_N := \mathbf{e}^{\frac{2\mathbf{i}\pi}{N}}$.
On pose

$$\begin{aligned} \mathrm{DFT}_N(f)[k] &:= \sum_{n=0}^{N-1} f[n]\omega_N^{-nk} \\ &= \sum_{n=0}^{N-1} f[n]\,\mathbf{e}^{\frac{2\mathbf{i}\pi nk}{N}} \end{aligned}$$

Au point de vue matriciel, on a

$$\begin{bmatrix} \mathrm{DFT}_N(f)[0] \\ \vdots \\ \mathrm{DFT}_N(f)[N-1] \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \omega_N^{-1} & \omega_N^{-2} & \ldots & \omega_N^{-(N-1)} \\ 1 & \omega_N^{-2} & \omega_N^{-4} & \ldots & \omega_N^{-2(N-1)} \\ & & \vdots & & \\ 1 & \omega_N^{-(N-1)} & \omega_N^{-2(N-1)} & \ldots & \omega_N^{-(N-1)(N-1)} \end{bmatrix} \begin{bmatrix} f[0] \\ \vdots \\ f[N-1] \end{bmatrix}$$

$$= F_N \begin{bmatrix} f[0] \\ \vdots \\ f[N-1] \end{bmatrix}$$

où F_N est la matrice de Fourier $F_N = \left(\omega_N^{-(i-1)(j-1)}\right)_{1 \leq i,j \leq N}$ qui est symétrique.

Exemple [5.1.1] On va écrire quelques matrices de Fourier

(a) $\omega_2 = \mathbf{e}^{\mathbf{i}\pi} = (-1)$.

$$F_2 = \begin{bmatrix} 1 & 1 \\ 1 & \omega_2^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

qui coïncide avec la matrice de Walsh W_2.

(b) $\omega_3 = \mathbf{e}^{\frac{2\mathbf{i}\pi}{3}} = j$.

$$F_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & j^2 & j \\ 1 & j & j^2 \end{bmatrix}$$

car $j^3 = 1 \Longleftrightarrow j^2 = j^{-1}$.

(c) $\omega_4 = \mathbf{e}^{\frac{\mathbf{i}\pi}{2}} = \mathbf{i}$. $\Rightarrow \omega_4^{-1} = -\mathbf{i}$.

$$F_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -\mathbf{i} & -1 & \mathbf{i} \\ 1 & -1 & 1 & -1 \\ 1 & \mathbf{i} & -1 & -\mathbf{i} \end{bmatrix}$$

On se place maintenant dans $\mathbb{Z}/N\mathbb{Z}$ et on définit $\Delta : \widehat{(\mathbb{Z}/N\mathbb{Z})} \to U_N$, $\chi \mapsto \chi(\overline{1})^{-1}$, avec $U_N = \left\{ \mathbf{e}^{2\mathbf{i}\pi k/N} \;\middle|\; 0 \leq k \leq N-1 \right\}$, et $\Theta : U_N \to \{0, 1, \ldots, N-1\}$, $\mathbf{e}^{2\mathbf{i}\pi k/N} \mapsto k$.

La fonction composée $\Theta \circ \Delta : \widehat{(\mathbb{Z}/N\mathbb{Z})} \to \{0, 1, \ldots, N-1\}$ est bijective. On note $\chi_k \in \widehat{(\mathbb{Z}/N\mathbb{Z})}$ le caractèe de $\mathbb{Z}/N\mathbb{Z}$ tel que $(\Theta \circ \Delta)(\chi_k) = k$.
$\Rightarrow \chi_k(\overline{1})^{-1} = \mathbf{e}^{2k\mathbf{i}\pi/N}$.
$\Rightarrow \chi_k(\overline{1}) = \mathbf{e}^{-2k\mathbf{i}\pi/N} = \omega_N^{-k}$.
$\Rightarrow \chi_k(\overline{n}) = \chi_k(\overline{1})^n = \omega_N^{-nk}$.
Soit $f = \left(f[\overline{0}], f[\overline{1}], \ldots, f[\overline{N-1}]\right) \in \mathbb{C}[\mathbb{Z}/N\mathbb{Z}]$.

$$\begin{aligned}
\mathcal{F}(f)(\chi_k) = \hat{f}(\chi_k) &= \sum_{u \in \mathbb{Z}/N\mathbb{Z}} f(\overline{u})\chi_k(\overline{u}) \\
&= \sum_{n=0}^{N-1} f[\overline{n}]\omega_N^{-kn} \\
&= \mathrm{DFT}_N(\tilde{f})[k] \qquad \text{avec } \tilde{f}[n] = f[\overline{n}].
\end{aligned}$$

Propriétés [5.1.2] $F_N\overline{F_N} = NI_N$ *et* $F_N^{-1} = \frac{1}{N}\overline{F_N}$.

Théorème [5.1.3] (Plancherel-Parseval)

$$\begin{aligned}
\sum_{n=0}^{N-1} \tilde{f}[n]\overline{\tilde{g}[n]} &= \sum_{n=0}^{N-1} f[\overline{n}]\overline{g[\overline{n}]} \\
&= \frac{1}{N}\sum_{k=0}^{N-1} \hat{f}(\chi_k)\overline{\hat{g}(\chi_k)} \\
&= \frac{1}{N}\sum_{k=0}^{N-1} \mathrm{DFT}_N(\tilde{f})[k] \cdot \overline{\mathrm{DFT}_N(\tilde{g})[k]}
\end{aligned}$$

$$\sum_{n=0}^{N-1} \left|\tilde{f}(n)^2\right| = \frac{1}{N}\sum_{k=0}^{N-1} \left|\mathrm{DFT}_N(\tilde{f})[k]\right|^2$$

En pratique, on écrit $\mathrm{DFT}_N(f) = \hat{f}$.

5.2 Deux algorithmes rapides

(a) Décimation temporelle
(b) Décimation fréquentielle

Soit N une puissance de 2.

5.2.1 Procédure de "renversement de bits"

$Rev : a_{p-1} \cdots a_1 a0 \mapsto a_0 a_1 \cdots a_{p-1}$, $\{0, 1, \ldots, 2^p - 1\} \to \{0, 1, \ldots, 2^p - 1\}$.

Exemple [5.2.1] $p = 3$.

k	0	1	2	3	4	5	6	7
	000	001	010	011	100	101	110	111
	000	100	010	110	001	101	011	111
$Rev(k)$	0	4	2	6	1	5	3	7
$f(k)$	1	2	3	4	5	6	7	8
$Rev(f)(k)$	1	5	3	7	2	6	4	8

5.2.2 Décimation temporelle

$f = [0, 2, -1, 0]$. (La fonction du cours était plus grande, mais ayant compris cet exemple, on peut calculer la FFT de n'importe quelle fonction.)

k	0	1	2	3
$(k)_{\text{bin}}$	00	01	10	11
$Rev((k)_{\text{bin}})$	00	10	01	11
$Rev(k)$	0	2	1	3
$f(k)$	0	2	-1	0
$f(Rev(k))$	0	-1	2	0
$\omega_2^{-1} = (-1)$ $(1)_{\hat{f}}$	-1	1	2	2
$\omega_4^{-1} = (-i)$ $(2)_{\hat{f}}$	1	$1+2(-\mathbf{i})$	-3	$1-2(-\mathbf{i})$

Alors, $\hat{f} = [1, 1-2\mathbf{i}, -3, 1+2\mathbf{i}]$.

5.2.3 Décimation fréquentielle

k	0	1	2	3
$(k)_{\text{bin}}$	00	01	10	11
$Rev((k)_{\text{bin}})$	00	10	01	11
$Rev(k)$	0	2	1	3
$f(k)$	0	2	-1	0
$\omega_4^{-1} = -\mathbf{i}$ $(1)_{\hat{f}}$	-1	2	$(-\mathbf{i})^0 \cdot 1$	$(-\mathbf{i})^1 \cdot 2$
	-1	2	1	$-2\mathbf{i}$
$\omega_2^{-1} = -1$ $(2)_{\hat{f}}$	1	-3	$1-2\mathbf{i}$	$1+2\mathbf{i}$
$\hat{f}(k) = Rev(\ (2)_{\hat{f}}\ )$	1	$1-2\mathbf{i}$	-3	$1+2\mathbf{i}$

Alors, les deux algorithmes menent au même résultat : $\hat{f} = [1, 1-2\mathbf{i}, -3, 1+2\mathbf{i}]$.

Chapitre 6

FFT sur des anneaux, polycopie de M. Esterle

Suite au blocage contre le loi Pécresse du novembre/décembre 2007, le cours du 30/11 n'a pas eu lieu. Pour compenser cela, M. Esterle nous a aimablement envoyé une polycopie (erronnée ...) que voici sur les pages suivantes.

« **Introduction** : On va présenter une application de la FFT au calcul d'un produit de polynômes, puis au calcul d'un produit d'entiers. On abordera ensuite la transformée de Fourier discrète sur $\mathbb{C}^{\mathbb{N}}$ dans un anneau possédant une racine primitive $N^{\text{ème}}$ de l'unité, ainsi que l'algorithme de Schonhäge et Strassen qui fonctionne dans des anneaux commutatifs où $2 := 1 + 1$ est inversible. On se propose enfin de présenter les identités de Mac Williams, qui jouent un rôle important en théorie des codes.»

Chapitre 2

Applications de la FFT au calcul de produits de polynômes ou d'entiers

On va utiliser la FFT pour calculer le produit des deux polynômes $p = 1-x+x^2$ et $q = 1+x^4+x^5$. On peut effectuer les calculs dans $\mathbb{Z}/8\mathbb{Z}$, puisque le degré du produit est égal à 7. On calcule les transformées de Fourier de p et q par décimation fréquentielle, ce qui donne lieu à un renversement de bits à la fin. On obtient la transformée de Fourier du produit pq (qui au niveau des coefficients des polynômes se traduit par un produit de convolution) en faisant le produit au sens usuel des transformées de Fourier de p et q, et on applique ensuite la transformation de Fourier inverse par décimation temporelle. Dans ce cas à chaque étape on effectue un calcul analogue à celui d'une FFT en remplaçant ω_n^{-1} par ω_n, et on divise le résultat obtenu par 8.

k	0	1	2	3	4	5	6	7
$p(k)$	1	-1	1	0	0	0	0	0
$\omega_8^{-1} = e^{-i\frac{\pi}{4}}$	1	-1	1	0	1	$e^{-i\frac{\pi}{4}}$	-i	0
$\omega_4^{-1} = -i$	2	-1	0	$(-i)(-1) = i$	$1-i$	$-e^{-i\frac{\pi}{4}}$	$1+i$	$e^{i\frac{\pi}{4}}$
$\omega_2^{-1} = -1$	1	3	i	$-i$	$(\sqrt{2}-1)e^{-i\frac{\pi}{4}}$	$(\sqrt{2}+1)e^{-i\frac{\pi}{4}}$	$(\sqrt{2}+1)e^{i\frac{\pi}{4}}$	$(\sqrt{2}-1)e^{i\frac{\pi}{4}}$
$F_8(p)(k)$ (Revbits)	1	$(\sqrt{2}-1)e^{-i\frac{\pi}{4}}$	i	$(\sqrt{2}+1)e^{i\frac{\pi}{4}}$	3	$(\sqrt{2}+1)e^{-i\frac{\pi}{4}}$	$-i$	$(\sqrt{2}-1)e^{i\frac{\pi}{4}}$
$q(k)$	1	0	0	0	1	1	0	0
$\omega_8^{-1} = e^{-i\frac{\pi}{4}}$	2	1	0	0	0	$-e^{-i\frac{\pi}{4}}$	0	0
$\omega_4^{-1} = -i$	2	1	2	$-i$	0	$-e^{-i\frac{\pi}{4}}$	0	$e^{-i\frac{\pi}{4}}$
$\omega_2^{-1} = -1$	3	1	$2-i$	$2+i$	$-e^{-i\frac{\pi}{4}}$	$e^{-i\frac{\pi}{4}}$	$e^{i\frac{\pi}{4}}$	$-e^{i\frac{\pi}{4}}$
$F_8(q)(k)$ (Revbits)	3	$-e^{-i\frac{\pi}{4}}$	$2-i$	$e^{i\frac{\pi}{4}}$	1	$e^{-i\frac{\pi}{4}}$	$2+i$	$-e^{i\frac{\pi}{4}}$
$F_8(p*q)(k)$	3	$(\sqrt{2}-1)i$	$1+2i$	$(\sqrt{2}+1)i$	3	$-(\sqrt{2}+1)i$	$1-2i$	$-(\sqrt{2}-1)i$
$\mathrm{Rv}(F_8(p*q))(k)$	3	3	$1+2i$	$1-2i$	$(\sqrt{2}-1)i$	$-(\sqrt{2}+1)i$	$(\sqrt{2}+1)i$	$-(\sqrt{2}-1)i$
$\omega_2 = -1$	6	0	2	$4i$	$-2i$	$2\sqrt{2}i$	$2i$	$2\sqrt{2}i$
$\omega_4 = i$	8	-4	4	4	0	$-4e^{-i\frac{\pi}{4}}$	$-4i$	$4e^{i\frac{\pi}{4}}$
$\omega_8 = e^{i\frac{\pi}{4}}$	8	-8	8	0	8	0	0	8
$(p*q)(k)$ (diviser par 8)	1	-1	1	0	1	0	0	1

On obtient donc

$$pq = 1 - x + x^2 + x^4 + x^7.$$

Ceci est évidemment confiré par un calcul direct : on a $(1-x+x^2)(1+x^4+x^5) = 1 - x + x^2 + x^4 - x^5 + x^6 + x^5 - x^6 + x^7 = 1 - x + x^2 + x^4 + x^7$.

Notons que l'on peut appliquer ceci au calcul du produit

$$91 \times 110001 = p(10)q(10) = pq(10) = 10^7 + 10^4 + 10^2 + 1 - 10 = 10010101 - 10 = 10010091.$$

L'utilisation de la FFT n'est bien sûr intéressante en pratique que pour des polynômes de degré très élevé et des nombres très grands.

Chapitre 3

DFT sur un anneau

Au chapitre précédent, on a pu accélérer la multiplication des polynômes à coefficients complexes grâce à la FFT. En fait la seule propriété de $\mathbb{C}$ que nous utilisons est que $\mathbb{C}$ contient les racines N-ièmes de l'unité. Afin d'obtenir un algorithme rapide de multiplication des polynômes dont les coefficients appartiennent à un anneau A quelconque, par exemple un corps fini, ou bien $\mathbb{Z}$, nous allons généraliser la DFT. C'est facile si l'anneau A contient des racines N-ièmes de 1 pour tout N ; sinon, nous verrons comment Schönhage et Strassen contournent le problème, au prix d'un $\log\log(N)$ supplémentaire. Cela conduit aussi à un algorithme rapide pour la multiplication des entiers.

3.1 L'anneau A contient une racine primitive N-ième de l'unité

Définition 3.1.1 *Soit A un anneau commutatif (et unitaire). On dit que $w_N \in A$ est une racine primitive N-ième de l'unité, si les conditions suivantes sont vérifiées :*

1. $w_N^N = 1$
2. *Pour tout $l < N$, l divisant N, N/l premier, $w_N^l - 1$ n'est pas un diviseur de zéro de A.*

exemple : $A = \mathbb{C}$, $A = \mathbb{F}_q$ et N divise $q - 1$.

Proposition 3.1.2 *Si w_N est une racine primitive N-ième de l'unité dans A, alors $w^l - 1$ n'est pas un diviseur de zéro dans A, pour tout $0 < l < N$. De plus, on a :*

$$\sum_{j=0}^{N-1} w_N^{lj} = 0. \tag{3.1}$$

Preuve : Remarquons d'abord que, si $w^a - 1$ n'est pas un divideur de zéro, alors $w^b - 1$ non plus dès que b divise a. En effet, cela découle de l'identité :

$$(w^a - 1) = (w^b - 1)(w^{b(a/b-1)} + w^{b(a/b-2)} + \ldots + w^b + 1). \tag{3.2}$$

Donc, la condition 2. implique que $w_N^l - 1$ n'est pas diviseur de 0 quel que soit l divisant N, $l < N$. Soit maintenant un entier $l < N$ ne divisant pas nécessairement N. Soit d le pgcd de l et N, et une relation de Bezout $d = lu + Nv$. On a $w_N^d = w_N^{lu}$. Comme d divise N, on sait que $w_N^d - 1$ n'est pas diviseur de zéro ; donc $w_N^{lu} - 1$ n'est pas diviseur de zéro ; mais l divise lu donc $w_N^l - 1$ n'est pas diviseur de zéro.

On a

$$(w_N^l - 1)(\sum_{j=0}^{N-1} w_N^{lj}) = w_N^{lN} - 1 = 0. \tag{3.3}$$

On conclut en utilisant le fait que $w_N^l - 1$ n'est pas diviseur de zéro.

On est en mesure de définir l'application DFT_N sur A, exactement comme sur $\mathbb{C}$.

Définition 3.1.3 *Supposons que l'anneau A contienne une racine primitive N-ième de l'unité w_N. L'application $DFT_N : A^N \to A^N$ est définie par :*

$$DFT_N(f) = \hat{f} := (\hat{f}[k])_{0 \leq k \leq N-1}$$

où :

$$\widehat{f}[k] = \sum_{n=0}^{N-1} f[n] w_N^{-nk}. \tag{3.4}$$

Si $a \in A$ est inversible, posons

$$V_a = [a^{-(i-1)(j-1)}]_{\substack{0 \leq i \leq N-1 \\ 0 \leq j \leq N-1}}.$$

Théorème 3.1.4 *Sous les mêmes hypothèses, l'application DFT_N est A-linéaire, et sa matrice dans la base canonique de A^N est V_{w_N} et vérifie : $V_{w_N} V_{w_N^{-1}} = NI_N$.*

Le produit de convolution, défini sur A^N par :

$$(f * g)[k] = \sum_{\substack{0 \leq i,j \leq N-1 \\ i+j=k \ (modN)}} f[i]g[j]$$

vérifie :

$$DFT_N(f * g) = DFT_N(f) DFT_N(g).$$

Preuve : Il suffit de reprendre les arguments invoqués sur $\mathbb{C}$. La démonstration de l'identité matricielle $V_{w_N} V_{w_N^{-1}} = NI_N$ utilise les identités de la Proposition 3.1.2 :

$$(V_{w_N} V_{w_N^{-1}})[i,j] = \sum_{k=1}^{N} V_{w_N}[i,k] V_{w_N^{-1}}[k,j] = \sum_{k=1}^{N} w_N^{-(i-1)(k-1)} w_N^{(k-1)(j-1)}$$

$$= \sum_{k=1}^{N} w_N^{(j-i)(k-1)} = \{ N \text{ si } j - i = 0(modN) 0 \text{ si } j - i \neq 0(modN)$$

Calculons $DFT_N(f * g)$.

$$DFT_N(f*g)[k] = \sum_{n=0}^{N-1}(f*g)[n]w_N^{-nk} = \sum_{n=0}^{N-1}\Big(\sum_{\substack{0\le i,j\le N-1\\ i+j=n(mod N)}} f[i]g[j]w_N^{-nk}\Big)$$

$$= \sum_{0\le i,j\le N-1} f[i]g[j]w_N^{-(i+j)k}$$

$$= \Big(\sum_{0\le i\le N-1} f[i]w_N^{-ik}\Big)\Big(\sum_{0\le j\le N-1} g[j]w_N^{-jk}\Big)$$

$$= DFT_N(f)[k]DFT_N(g)[k].$$

L'algorithme FFT fonctionne sur A exactement comme sur $\mathbb{C}$. Il permet de calculer $DFT_N(f)$ en $O(N\log(N))$ opérations élémentaires de A. En particulier, on peut l'utiliser pour calculer le produit de deux polynômes de $A[X]$ dont la somme des degrés est au plus égale à N (plus exactement on récupère NPQ ; il faut pouvoir diviser par N dans A). En effet, on a toujours :

$$PQ = P*Q \quad (mod(x^N-1)).$$

Dans $\mathbb{Z}/p\mathbb{Z}$, les seuls éléments dont une puissance est égale à 1 sont les inversibles, c'est à dire les éléments de la forme $\overline{a}$ avec $1\le a\le p-1$, avec $\text{pgcd}(a,p)=1$, et dans ce cas on a $\overline{a}^d = 1$, d désignant le nombre d' éléments inversibles de $\mathbb{Z}/p\mathbb{Z}$. Par exemple dans $\mathbb{Z}/8\mathbb{Z}$ les inversibles distincts de 1, à savoir $\overline{3}, \overline{5}$ et $\overline{7}$, sont tous des racines carrées de l'unité, mais aucune n'est primitive puisque $\overline{3}-\overline{1}$, $\overline{5}-\overline{1}$ et $\overline{7}-\overline{1}$ sont des diviseurs de zéro. Donc $\mathbb{Z}/8\mathbb{Z}$ ne possède de racine primitive N^e de l'unité pour aucun entier $N\ge 1$. Dans $\mathbb{Z}/9\mathbb{Z}$ on a $\overline{2}^6 = \overline{1}$, $\overline{2}^x \ne \overline{1}$ pour $1\le x\le 5$, mais $\overline{2}^2 - \overline{1} = \overline{3}$ est un diviseur de zéro, et $\overline{2}$ est une racine 6^e de l'unité dans $\mathbb{Z}/9\mathbb{Z}$ qui n'est pas primitive. On vérifie de même que $\overline{5}$ est une racine 6^e de l'unité qui n'est pas primitive, que $\overline{4}$ et $\overline{7}$ sont des racines cubiques de l'unité qui ne sont pas primitives, et que par contre $\overline{8}$ est une racine carrée primitive de l'unité dans $\mathbb{Z}/9\mathbb{Z}$.

3.2 L'anneau A est quelconque

On ne suppose plus désormais que A contient des racines primitives de l'unité, mais seulement que 2 est inversible dans A (même cette hypothèse peut être relaxée..). Un algorithme, dû à Schönhage et Strassen (1971), permet de multiplier deux polynômes P et Q de $A[x]$ dont la somme des degrés est au plus égale à N en $O(N\log(N)\log\log(N))$ opérations ; l'idée est de rajouter à A les racines N-ièmes manquantes, par passage au quotient ; si on procède naivement, on perd en complexité. L'idée est de rajouter *les racines $\sqrt{N}$-ièmes de l'unité* à A, comme on va le voir.

On suppose que N est une puissance de 2 et on pose $N = 2^k$. Si k est pair, on pose $m = t = 2^{k/2}$; si k est impair, on pose $m = 2^{(k-1)/2}$ et $t = 2^{(k+1)/2} = m+1$).

On définit des polynômes $P_0,\dots,P_{t-1}$ et $Q_0,\dots,Q_{t-1}$ de degrés inférieur à m tels que

$$P = \sum_{j<t} P_j(x)x^{mj},\ Q = \sum_{j<t} Q_j(x)x^{mj}.$$

On pose maintenant :

$$\tilde{P} = \sum_{j<t} P_j(x) y^j,\ \tilde{Q} = \sum_{j<t} Q_j(x) y^j$$

de sorte que $P(x) = \tilde{P}(x, x^m)$, $Q(x) = \tilde{Q}(x, x^m)$. Nous allons calculer le produit $\tilde{P}\tilde{Q}$. Les coefficients de $\tilde{P}\tilde{Q}$ sont des polynômes en x, de degré inférieur à $2m$, de sorte qu'il suffit de connaitre leur image dans

$$D := A[x]/(x^{2m} + 1)A[x].$$

Le degré en y de $\tilde{P}\tilde{Q}$ est $\deg_y(\tilde{P}\tilde{Q}) < 2t \leq 4m$. D'autre part, D contient une racine primitive $4m$-ième de l'unité. En effet, soit $\pi : A[x] \to D$ la surjection canonique, et posons $w := \pi(x)$. On a $w^{2m} = -1$ et $w^{4m} = 1$. De plus, $w^{2m} - 1 = -2$ n'est pas un diviseur de zéro de D puisqu'on suppose 2 inversible dans A, et comme $4m$ est une puissance de 2 le seul diviseur p de $4m$ tel que $4m/p$ soit premier est égal à $2m$. On se retrouve donc dans la situation du paragraphe précédent, et on peut appliquer l'algorithme FFT pour calculer $\tilde{P}\tilde{Q}$ en $O(m \log(m))$ opérations dans D. Parmi ces opérations, les additions et multiplications par des puissances de x ne coutent que du $O(m)$, tandis que les "vraies" multiplications sont analogues à la multiplication de polynômes de $A[x]$ de degré inférieur à $2m$. Pour ces dernières, on peut appliquer récursivement la FFT à l'ordre $2m \simeq \sqrt{N}$; il faut aussi estimer leur nombre. Une analyse plus fine conduit à une complexité totale en $O(N \log N \log\log N)$.

On va maintenant illuster ceci par un exemple, en calculant dans $\mathbb{Z}/9\mathbb{Z}$ le produit des polynômes $p = \overline{1} + \overline{2}x + x^3$ et $q = \overline{1} - \overline{5}x^2 + x^4$. Ici on peut prendre $N = 8 = 2^3$, $m = 2^{\frac{3-1}{2}} = 2$, $t = m + 1 = 3$, $D = (\mathbb{Z}/9\mathbb{Z})[x]/(x^4 + 1)(\mathbb{Z}/9\mathbb{Z})[x]$. On pose $y = x^m = x^2$, ce qui donne

$$\tilde{p}(x, y) = \overline{1} + \overline{2}x + xy,\ \tilde{q}(x, y) = \overline{1} - \overline{5} + y^2.$$

Pour alléger les notations on note $\pi : (\mathbb{Z}/9\mathbb{Z})[x]/ \to D$ la surjection canonique, et on note $\tilde{p} = [1 + 2w, w, 0, 0]$ et $\tilde{q} = [1, -5, 1, 0]$ les éléments de $D[y]$ associés à $\tilde{p}$ et $\tilde{q}$, avec $w = \pi(x)$. On calcule les transformées de Fourier discrètes de $\tilde{p}$ et $\tilde{q}$ en FFT décimation temporelle, avec renversement de bits au début, on effectue leur produit pour obtenir la transformée de Fourier discrète de $\tilde{p}\tilde{q}$, et on revient à $\tilde{p}\tilde{q}$ par FFT inverse décimation fréquentielle, avec renversement de bits à la fin.

n	0	1	2	3
$\tilde{p}(n)$	$\overline{1}+\overline{2}w$	w	$\overline{0}$	$\overline{0}$
Revbits	$\overline{1}+\overline{2}w$	$\overline{0}$	w	$\overline{0}$
$\omega_2^{-1}=-\overline{1}$	$\overline{1}+\overline{2}w$	$\overline{1}+\overline{2}w$	w	w
$\omega_4^{-1}=w^{-1}$ $F_4(\tilde{p})(n)$	$\overline{1}+\overline{3}w$	$\overline{1}+\overline{2}w+w^{-1}w=$ $\overline{2}+\overline{2}w$	$\overline{1}+w$	$\overline{1}+\overline{2}w-w^{-1}w=$ $\overline{2}w$
$\tilde{q}(n)$	$\overline{1}$	$-\overline{5}$	$\overline{1}$	$\overline{0}$
Revbits	$\overline{1}$	$\overline{1}$	$-\overline{5}$	$\overline{0}$
$\omega_2^{-1}=-\overline{1}$	$\overline{2}$	$\overline{0}$	$-\overline{5}$	$-\overline{5}$
$\omega_4^{-1}=w^{-1}$ $F_4(\tilde{q})(n)$	$-\overline{3}$	$-\overline{5}w^{-1}$	$\overline{7}$	$\overline{5}w^{-1}$
$F_4(\tilde{p})(n)F_4(\tilde{q})(n)$	$-\overline{3}$	$-\overline{1}-w^{-1}$	$\overline{7}+\overline{7}w$	$\overline{1}$
$\omega_4=w$	$\overline{4}+\overline{7}w$	$-w^{-1}=$ w	$-\overline{1}+\overline{2}w$	$-\overline{1}-\overline{2}w$
$\omega_2=-\overline{1}$	$\overline{4}-w$	$\overline{4}-\overline{3}w$	$-\overline{2}$	$\overline{4}w$
$\times\overline{7}=\overline{4}^{-1}$	$\overline{1}+\overline{2}w$	$\overline{1}+\overline{6}w$	$-\overline{5}$	w
(Revbits) $(\tilde{p}*\tilde{q})(n)$	$\overline{1}+\overline{2}w$	$-\overline{5}$	$\overline{1}+\overline{6}w$	w

On obtient donc

$$\pi(\tilde{p}\tilde{q})=(\overline{1}+\overline{2}\pi x)-\overline{5}y+(\overline{1}+\overline{6}\pi(x))y^2+\pi(x)y^3$$

$$\tilde{p}\tilde{q}=(\overline{1}+\overline{2}x)-\overline{5}y+(\overline{1}+\overline{6}x)y^2+xy^3$$

$$pq=\overline{1}+\overline{2}x-\overline{5}x^2+x^4+\overline{6}x^5+x^7.$$

On retrouve bien sûr ce résultat par vérification directe

$$(\overline{1}+\overline{2}x+x^3)(\overline{1}-\overline{5}x^2+x^4)=\overline{1}+\overline{2}x+x^3-\overline{5}x^2-\overline{10}x^3-\overline{5}x^5+x^4+\overline{2}x^5+x^7$$

$$=\overline{1}+\overline{2}x+x^3-\overline{5}x^2+x^4-\overline{3}x^5+x^7$$

$$=\overline{1}+\overline{2}x+x^3-\overline{5}x^2+x^4+\overline{6}x^5+x^7.$$

Chapitre 4

Les identités de Mac Williams

On considère de nouveau le groupe $\mathbb{F}_2^k = (\mathbb{Z}/2\mathbb{Z})^k$, considéré maintenant comme espace vectoriel de dimension k sur le corps $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Comme les seuls éléments de $\mathbb{F}_2$ sont $\overline{0}$ et $\overline{1}$, il est clair que tout sous-groupe de $\mathbb{F}_2^k$, et plus généralement toute partie non vide de $\mathbb{F}_2^k$ stable par addition, est un sous-espace vectoriel de $\mathbb{F}_2^k$. Rappelons que l'application bilinéaire $(x, y) \rightarrow < x, y >$ est définie pour $x = (x_1, ..., x_k) \in \mathbb{F}_{2^k}$ et $y = (y_1, ..., y_k) \in \mathbb{F}_{2^k}$ par la formule

$$< x, y >= \sum_{i=1}^{k} x_i y_i. \tag{4.1}$$

Rappelons aussi que si on pose, pour $a \in \mathbb{F}_2^k, x \in \mathbb{F}_2^k$,

$$\chi_a(x) = (-1)^{<a,x>}, \tag{4.2}$$

avec la convention $(-1)^{\overline{0}} = 1$, $(-1)^{\overline{1}} = -1$, alors l'application $a \rightarrow \chi_a$ est un isomorphisme de groupes de $\mathbb{F}_2^k$ sur le groupe dual $\hat{\mathbb{F}}_2^k$.

Soit H un sous-espace vectoriel de $\mathbb{F}_2^k$. On pose

$$H^{\perp} = \{y \in \mathbb{F}_2^k \mid < x, y >= \overline{0}\ \forall x \in H\},\ H^{\perp,*} = \{\chi \in \hat{H} \mid \chi(x) = 1 \quad \forall x \in H\}.$$

Il résulte immédiatement des définitions ci-dessus qu'aucune confusion n'est à craindre entre ces notions.

Proposition 4.0.1 *Soit H un sous-espace vectoriel de $\mathbb{F}_2^k$, et soit $a \in \mathbb{F}_2^k$. Alors $a \in H^{\perp}$ si et seulement si $\chi_a \in H^{\perp,*}$.*

On peut alors appliquer dans ce contexte la formule de Poisson.

Proposition 4.0.2 *Soit H un sous-espace vectoriel de $\mathbb{F}_2^k$, et soit $f : \mathbb{F}_2^k \rightarrow \mathbb{C}$. On a*
(i) $\sum_{u \in H} f[u] = \frac{|H|}{2^k} \sum_{v \in H^{\perp}} \hat{f}(\chi_v) = \frac{|H|}{2^k} \sum_{v \in H^{\perp}} \mathcal{W}_{2^k}(f)[v]$,
(ii) $\sum_{u \in H^{\perp}} f[u] = \frac{1}{|H|} \sum_{v \in H} \hat{f}(\chi_v) = \frac{1}{|H|} \sum_{v \in H} \mathcal{W}_{2^k}(f)[v]$.

Preuve : Comme $H^\perp$ est isomorphe au groupe quotient $\mathbb{F}_2^k/H$, on a $|H||H^\perp| = |\mathbb{F}_2^k| = 2^k$, et la première formule résulte immédiatement de la formule de Poisson compte tenu de la proposition précédente et de l'interprétation de la transformée de Walsh comme transformée de Fourier sur $\mathbb{F}_2^k$. La seconde formule résulte alors de la première puisque $(H^\perp)^\perp = H$. ♣

Pour $x \in \mathbb{F}_2^k$, on définit le poids $w(x)$ de x par la formule

$$w(x) = \text{card}\left(\{i \in \{1, ..., k\} \mid x_i \neq \overline{0}\}\right).$$

On introduit alors la définition suivante

Définition 4.0.3 *Soit H un sous-espace vectoriel de $\mathbb{F}_2^k$. On définit le* **polynôme énumérateur de poids** *de H par la formule*

$$A_H(X, Y) = \sum_{a \in H} X^{k-w(a)} Y^{w(a)} = \sum_{i=0}^{k} b_H(i) X^{k-i} Y^i,$$

où $b_H(i)$ est le cardinal de l'ensemble des éléments de H dont le poids est égal à i.

On obtient l'importante formule suivante, appelée *identité de Mac Williams.*

Théorème 4.0.4 *Soit H un sous-espace vectoriel de $\mathbb{F}_2^k$. On a*

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

Preuve :

On va illustrer ce résultat par un exemple, où H est le sous-espace vectoriel de $\mathbb{F}_2^3$ engendré par $(\overline{1}, \overline{1}, \overline{0})$ et $(\overline{0}, \overline{1}, \overline{1})$. On a $\dim(H) = 2$, donc H possède 4 éléments qui sont $(\overline{0}, \overline{0}, \overline{0})$, $(\overline{1}, \overline{1}, \overline{0})$, $(\overline{0}, \overline{1}, \overline{1})$, et $(\overline{1}, \overline{0}, \overline{1}) = (\overline{1}, \overline{1}, \overline{0}) + (\overline{0}, \overline{1}, \overline{1})$. On a $b_H(0) = 1, b_H(1) = b_H(3) = 0, b_H(2) = 3$, et on obtient

$$A_H(X, Y) = X^3 + 3XY^2.$$

Soit $u = (x, y, z) \in \mathbb{F}_2^3$. Alors $u \in H^\perp$ si et seulement si on a $x+y = y+z = \overline{0}$, ce qui donne $x = z$, $y = -x = x$, et finalement $x = y = z$. Donc $H^\perp$ possède deux éléments, à savoir $(\overline{0}, \overline{0}, \overline{0})$ et $(\overline{1}, \overline{1}, \overline{1})$. On a donc $b_{H^\perp}(0) = b_{H^\perp}(3) = 1$, et $b_{H^\perp}(1) = b_{H^\perp}(2) = 0$. On obtient

$$A_{H^\perp}(X, Y) = X^3 + Y^3.$$

Dans ce cas

$$\frac{1}{|H|} A_H(X + Y, X - Y) = \frac{1}{4}\left((X + Y)^3 + 3(X + Y)(X - Y)^2\right)$$

$$= \frac{1}{4}(X^3 + 3X^2Y + 3XY^2 + Y^3 + 3X^3 - 6X^2Y + 3XY^2 + 3X^2Y - 6XY^2 + 3Y^3)$$

$$= \frac{1}{4}(4X^3 + 4Y^3) = X^3 + Y^3$$

$$= w_{H^\perp}(X, Y).$$

De même

$$\frac{1}{|H^{\perp}|}A_{H^{\perp}}(X+Y)(X-Y) = \frac{1}{2}\left((X+Y)^3+(X-Y)^3\right) = \frac{1}{2}\left(2X^3+6XY^2\right) = X^3+3XY^2$$

$$= A_{H^{\perp}}(X,Y) = A_{(H^{\perp})^{\perp}}(X,Y),$$

et on voit que l'identité de Mac Williams est bien vérifiée par H et $H^{\perp}$.

Chapitre 7

Dernier cours, précisions

7.1 Codes

$\mathbb{F}_2^k = (\mathbb{Z}/2\mathbb{Z})^k$ est un espace vectoriel sur $\mathbb{F}_2^k$ de dimension k. Tout sous-groupe de F_2^k est un sous-espace vectoriel : Si H est un sous-groupe et si $x, y \in H, \alpha, \beta \in \mathbb{F}_2$, alors

$$\alpha x + \beta y = \begin{cases} 0+0 \in H \\ x+0 \in H \\ 0+y \in H \\ x+y \in H \end{cases}.$$

Si H est de dimension p, alors $|H| = 2^p$ car $H \cong \mathbb{F}_2^p$.
Par analogie avec $\mathbb{R}^k$, on pose pour $x = (x_1, \ldots, x_k), y = (y_1, \ldots, y_k) \in \mathbb{F}_2^k$

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

C'est une forme bilinéaire, symétrique, non-dégénérée à valeurs dans $\mathbb{F}_2$.
On a : $\dim H + \dim H^\perp = k = \dim \mathbb{F}_2^k$, mais on peut avoir $H \cap H^\perp \neq \{0\}$.

non-dégénéré : $\langle x, y \rangle = 0 \ \forall y \in \mathbb{F}_2^k \Leftrightarrow x = 0$.

Lien avec $\widehat{\mathbb{F}_2^k}$, l'ensemble des caractères de $\mathbb{F}_2^k$

L'application $y \mapsto \chi_y$ est une bijection de $\mathbb{F}_2^k$ sur $\widehat{\mathbb{F}_2^k}$ avec $\chi_y(x) = (-1)^{\langle x,y \rangle}$. On pose

$$H^{(\perp)} := \left\{ \chi \in \widehat{\mathbb{F}_2^k} \;\middle|\; \chi(x) = 1 \ \forall x \in H \right\}.$$

Sans surprise, $H^{(\perp)} = \{ \chi_y \mid y \in H^\perp \}$. On a également les formules de Poisson (voir pages précédentes).

7.2 Polynôme énumerateur

On pose $w(x) = \text{card}(\{ i \in \{1, \ldots, k\} \mid x_i \neq \overline{0} \})$ pour $x = (x_1, \ldots, x_k) \in \mathbb{F}_2^k$. $w(x)$ est la distance de Hammings au vecteur nul $(0, \ldots, 0)$.

Exemple $w\left((\overline{1}, \overline{1}, \overline{0}, \overline{1}, \overline{0}\right) = 3$.

Polynôme énumerateur de $H \subseteq \mathbb{F}_2^k$

Le polynôme énumerateur se calcule comme suit :

$$\begin{aligned} A_H(X, Y) &:= \sum_{x \in H} X^{k-w(x)} Y^{w(x)} \\ &= \sum_{i=0}^{k} b_H(i) X^{k-i} Y^i \end{aligned}$$

avec $b_H(i) = \text{card}\left(\left\{x \in \mathbb{F}_2^k \;\middle|\; w(x) = i\right\}\right)$.

Identité de MacWilliams

A l'aide du polynôme énumerateur de H, on peut calculer celui de $H^\perp$:

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

Exemple F_2^6. $H = \left\{x \in F_2^6 \;\middle|\; x_1 + x_2 = x_4 + x_6 = \overline{0}\right\}$. On trouve que

$$\begin{aligned} H = \{&(0,0,0,0,0,0),\ (1,1,0,0,0,0),\\ &(0,0,0,1,0,1),\ (1,1,0,1,0,1),\\ &(0,0,1,0,0,0),\ (1,1,1,0,0,0),\\ &(0,0,1,1,0,1),\ (1,1,1,1,0,1),\\ &(0,0,0,0,1,0),\ (1,1,0,0,1,0),\\ &(0,0,0,1,1,1),\ (1,1,0,1,1,1),\\ &(0,0,1,0,0,1),\ (1,1,1,0,1,0),\\ &(0,0,1,1,1,1),\ (1,1,1,1,1,1)\} \end{aligned}$$

dont on trouve une base

$$\mathcal{B}_H = \{(1,1,0,0,0,0),(0,0,0,1,0,1),(0,0,1,0,0,0),(0,0,0,0,1,0)\} = \{e_1, e_2, e_3, e_4\}.$$

On va réécire H :

$$\begin{aligned} H &= \left\{x = (x_1, -x_1, x_3, x_4, x_5, -x_4 \;\middle|\; (x_1, x_3, x_4, x_5) \in \mathbb{F}_2^4\right\} \\ &= \left\{x = (x_1, x_1, x_3, x_4, x_5, x_4) \;\middle|\; (x_1, x_3, x_4, x_5) \in \mathbb{F}_2^4\right\} \\ &= \{x_1 e_1 + x_3 e_3 + x_4 e_2 + x_5 e_4\}. \end{aligned}$$

$\Longrightarrow$ famille $(e_i)_{i=1,2,3,4}$ est génératrice et on a bien une base de H et $\dim H = 4$. $\Rightarrow \dim H^\perp = 2$.
Par définition de H, $e_1, e_2 \in H^\perp$ (car $x_1 + x_2 = 0 \Leftrightarrow \langle x, e_1\rangle = 0$ et $x_4 + x_6 = 0 \Leftrightarrow \langle x, e_2\rangle = 0$.). $\Rightarrow$ $\mathcal{B}_{H^\perp} = \{e_1, e_2\}$ base de $H^\perp \subseteq H$. Donc : $H \cap H^\perp = H^\perp$.

$$\begin{aligned} H^\perp = \{&(0,0,0,0,0,0), && w = 0\\ &(1,1,0,0,0,0), && w = 2\\ &(0,0,0,1,0,1), && w = 2\\ &(1,1,0,1,0,1)\} && w = 4 \end{aligned}$$

On trouve que

$$A_{H^\perp}(X,Y) = X^6 + 2X^4Y^2 + X^2Y^4.$$

Ayant $(H^\perp)^\perp = H$, on vérifie l'identité de MacWilliams.

7.3 Exemple sur les racines primitives

On regarde les racines de l'unité de $\mathbb{Z}/6\mathbb{Z}$. Il suffit de regarder les éléments inversibles et différents de $\overline{0}$ et $\overline{1}$. Or, $\overline{2}$, $\overline{3}$ et $\overline{4}$ étant des diviseurs de zéro, il ne reste plus que $\overline{5}$ à vérifier. On trouve vite que $\overline{5}^2 = \overline{-1}^2 = \overline{1}$, mais $\overline{5}^1 - 1 = \overline{4}$ étant un diviseur de zéro, $\overline{5}$ n'est pas racine primitive. Donc, $\mathbb{Z}/6\mathbb{Z}$ n'admet pas de racines primitives.

7.4 Schönhage-Strassen

Arnold Schönhage et Volker Strassen sont des mathématiciens allemands, ayant travaillé ensemble pendant un certain temps, surtout sur les algorithmes. Pour l'algorithme de Schönhage-Strassen, ils ont eu les idées suivantes :

(1) Diminuer les calculs en posant $x^m =: y$.

$$\begin{aligned} p &= a_0 + a_1 x^1 + \ldots + a_p x^p \\ &= p_0(x) + p_1(x)x^m + \ldots + p_k(x)x^{mk}, \qquad \deg p_i(x) \leq m-1 \ \forall i. \end{aligned}$$

On pose $\widetilde{p} = p_0(x) + p_1(x)y + \ldots, + p_k(x)y^k \in (A[x])[y] = B[y]$ en posant $B := A[x]$. $\Longrightarrow p(x) = \widetilde{p}(x^m)$.
Pour calculer pq, on calcule $\widetilde{p}\widetilde{q}$ dans $B[y]$ et on revient en remplaçant y par x^m pour obtenir pq.

(2) Utiliser la FFT dans $B^\alpha = (A[x])^\alpha$, $\alpha = 2^\beta$ une puissance de 2. On va en générale rajouter des zéros pour que $\deg \widetilde{p} + \deg \widetilde{q} \leq 2^\beta - 1$.

(3) On a besoin d'une racine $(2^\beta)^{\text{ème}}$ primitive de l'unité qui – en général – n'existe pas dans A, ni dans $A[x] = B$. On fait une «extention algébrique».

Exemple : $\mathbb{C} = \mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$. x^2+1 n'a pas de solution réelle. On en rajoute une : $\mathbf{i} = \pi(x)$ où $\pi : \mathbb{R}[x] \to \mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ est l'application canonique. $\Rightarrow \mathbf{i}^2 = [\pi(x)]^2 = \pi(x^2) = -\pi(1)$ car $\pi(x^2+1) = 0$. $\mathbf{i}$ est racine $4^{\text{ème}}$ primitive de l'unité.

(4) Pour faire la FFT, on se place dans $B[x]/(x^{2^\gamma}+1)B[x]$. On pose $w := \pi(x)$, $\pi : B[x] \to B[x]/(x^{2^\gamma}+1)B[x]$. $\Rightarrow w^{2^\gamma} = -1 \Rightarrow w^{2^{\gamma+1}} = 1$ est une racine $(2^{\gamma+1})^{\text{ème}}$ de l'unité qui sera primitive si 2 est inversible dans A.

Puis, on fait les calculs ... ;-).