Nous avons terminé le premier chapitre de ce rendu par la présentation de diverses familles -ou classes- de polynôme de permutation. Une fois la "forme" d'un polynôme établit, moulte résultats nous permette de dire si le polynôme est ou non de permutations ; et ce avec efficacité.
Nous allons ici revenir un tantinet en arrière et présenter un critère qui ne sera pas des plus convenant dans la pratique ; mais qui a le mérite de s'appuyer sur une belle théorie, celle des caractères sur un corps fini.

Définition 1. Soit G un groupe abélien fini d'ordre n. On appelle caractère additif de G tout homomorphisme χ de G dans le groupe W_n des racines n-ièmes de l'unité.

Nous admettrons ici la

Proposition 1. *L'ensemble $\hat{G}$ des caractères additifs sur un groupe G forme un groupe multiplicatif.*

Par conséquent, nous avons aussi la

Proposition 2 (admise)**.** *$\forall \chi \in \hat{G}$, $\chi^{-1} = \overline{\chi}$, où $\overline{\chi(x)}$ est définit comme le conjugué complexe de $\chi(x)$ dans W_n.*

Notation 1. On notera $\chi_0 := 1_{\hat{G}}$ le caractère trivial, définit comme $\forall g \in G, \chi_0(g) = 1$.

Avant d'exhiber le lien entre polynômes de permutations et caractère additif, nous allons donner un résultat élémentaire.

Théorème 1. *Soit G un groupe abélien fini d'ordre n, alors*

i) Pour $g \in G$ fixé,

$$\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} n & \textit{si } g = 1_G \\ 0 & \textit{sinon.} \end{cases}$$

et de manière similaire

ii) Pour $\chi \in \hat{G}$ fixé,

$$\sum_{g \in G} \chi(g) = \begin{cases} n & \textit{si } \chi = 1_{\hat{G}} \\ 0 & \textit{sinon.} \end{cases}$$

Démonstration. Utile ? □

Ce résultat nous sera utile pour démontrer notre critère, mais avant concentrons nous sur le cas où G est le groupe additif de $\mathbb{F}_q$, que nous noterons ici de manière abusive $\mathbb{F}_q^+$. Nous allons donner aux caractères additifs une forme plus familière.

On rappelle la

Définition 2. On note $\mathbb{F}_p$ le sous-corps premier de $\mathbb{F}_q$. L'application trace est définit comme

$$Tr : \left| \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_p \\ \alpha & \longmapsto & \displaystyle\sum_{i=0}^{n-1} \alpha^{q^i} \end{array} \right.$$

Proposition 3. *Soit la fonction χ_α définit par*

$$\chi_\alpha : \left| \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & W_n \\ c & \longmapsto & e^{\frac{2\pi.i.Tr(\alpha.c)}{p}} \end{array} \right.$$

, alors χ_α est un caractère additif de $\mathbb{F}_q$.

Démonstration. $\chi_\alpha(c_1+c_2) = e^{\frac{2\pi.i.Tr(\alpha.(c_1+c_2))}{p}} = e^{\frac{2\pi.i.[Tr(\alpha.(c_1))+Tr(\alpha.(c_2))]}{p}} = \chi_\alpha(c_1)\chi_\alpha(c_2)$. Les autres propriétés de morphisme sont toutes aussi claires. □

Remarque 1. Précisons que $e^{\frac{2\pi.i.Tr(\alpha.c)}{p}}$ a bien un sens, car la trace est par définition à valeur dans $\mathbb{F}_p$ et que $\mathbb{F}_p \simeq \mathbb{Z}\backslash p\mathbb{Z}$.

Définition 3. En particulier, remarquons que $\chi_1(c) = e^{\frac{2\pi.i.Tr(c)}{p}}$. Ce caractère sera appellé caractère additif canonique.

Proposition 4 (Admise)**.** *L'application*

$$\phi : \left| \begin{array}{ccc} \mathbb{F}_q^+ & \longrightarrow & \hat{\mathbb{F}_q^+} \\ \alpha & \longmapsto & \chi_\alpha \end{array} \right.$$

est un isomorphisme de groupes.

Corollaire 1. *On en déduit donc qu'il n'existe qu'un nombre fini de caractères additifs de $\mathbb{F}_q^+$, et que ces derniers sont exactement les χ_α. Ceci étant admis, remarquons que $\chi_\alpha(c) = e^{\frac{2\pi.i.Tr(\alpha.c)}{p}} = e^{\frac{2\pi.i.Tr(1.(\alpha.c))}{p}} = \chi_1(\alpha.c)$. Tout caractère additif peut ainsi être exprimé en fonction de χ_1, d'où l'appellation canonique.*

Proposition 5. *Soient α, c et $d \in \mathbb{F}_q$, alors*

$$\sum_{\alpha\in\mathbb{F}_q} \chi_\alpha(c).\overline{\chi_\alpha(d)} = \begin{cases} 0 & si\ c \neq d \\ q & sinon. \end{cases}$$

Démonstration. De simples calculs suffisent, de par(t ?) le corollaire 1 :

$$\sum_{\alpha\in\mathbb{F}_q} \chi_\alpha(c).\overline{\chi_\alpha(d)}$$

$$= \sum_{\alpha\in\mathbb{F}_q} e^{2i\pi Tr(\alpha.c)/p}.\overline{e^{2i\pi Tr(\alpha.d)/p}}$$
$$= \sum_{\alpha\in\mathbb{F}_q} e^{2i\pi Tr(\alpha.c)/p}.e^{-2i\pi Tr(\alpha.d)/p}$$
$$= \sum_{\alpha\in\mathbb{F}_q} e^{2i\pi Tr(\alpha.(c-d))/p}$$

Ceci est immédiatement égal à q si $c = d$, $\mathbb{F}_q$ étant le corps à q éléments. Si $c \neq d$, remarquons que

$$\phi : \left| \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ \alpha & \longmapsto & \alpha(c-d) \end{array} \right.$$

constitue un isomorphisme (car $c \neq d$), de sorte que pour α parcourant $\mathbb{F}_q$, on a que $\alpha(c-d)$ parcours également $\mathbb{F}_q$. On obtient dès lors que

$$\sum_{\alpha \in \mathbb{F}_q} \chi_\alpha(c).\overline{\chi_\alpha(d)}$$

$$= \sum_{\alpha \in \mathbb{F}_q} e^{2i\pi Tr(\alpha)/p}$$
$$= \sum_{\alpha \in \mathbb{F}_q} \chi_1(\alpha)$$
$$= 0$$

car $\chi_1(\alpha) \neq 1_{\hat{\mathbb{F}_q}^+}$ □

Remarque 2. Il est également possible de conclure directement via le théorème 1, en notant que si $c = d$, $\chi_\alpha(c).\overline{\chi_\alpha(d)} = \chi_\alpha(c).\chi_\alpha^{-1}(c) = 1_{\hat{\mathbb{F}_q}^+}$...

Une dernière proposition est requise avant d'énoncer notre critère. Elle sera considérée comme admise, sa démonstration dépassant le cadre de ce projet et nécessitant surement un projet à elle seule.

Proposition 6. *Soient $P \in \mathbb{F}_q[X]$ et $\alpha \in \mathbb{F}_q$, alors le nombre N de solution de $P(x) = \alpha$ est*

$$N = \frac{1}{q} \sum_{c \in \mathbb{F}_q} \sum_{\chi \in \hat{Fq}^+} \chi(P(c)).\overline{\chi(\alpha)}$$

Donnons nous quelques exemples simples, mettons pour $q = 3$ et $q = 4$:

Exemple 1. i) Soit $P(X) := X^3$; on a bien une unique solution à l'équation $x^3 = 2$, qui est $x = 2$. Vérifions cela à l'aide de la proposition précédente :
$N = \dfrac{1}{3} \displaystyle\sum_{c \in F3} \sum_{\chi \in (\hat{F3})^+} \chi(c^3)\overline{\chi(2)}$
$= \dfrac{1}{3} \displaystyle\sum_{\chi \in (\hat{F3})^+} \overline{\chi(2)}(\chi(0) + \chi(1) + \chi(2))$
$= \dfrac{1}{3} \Big[\overline{\chi_1(2)}(\chi_1(0) + \chi_1(1) + \chi_1(2)) + \overline{\chi_2(2)}(\chi_2(0) + \chi_2(1) + \chi_2(2)) + \overline{\chi_3(2)}(\chi_3(0) + \chi_3(1) +$
$= \dfrac{1}{3} \Big[\overline{\chi_1(2)}(\chi_1(0) + \chi_1(1) + \chi_1(2)) + \overline{\chi_1(4)}(\chi_1(0) + \chi_1(2) + \chi_1(4)) + \overline{\chi_1(6)}(\chi_1(0) + \chi_1(3) +$
or dans F3 6=0 et 4=1, d'ou
$\dfrac{1}{3} \Big[\overline{\chi_1(2)}(\chi_1(0) + \chi_1(1) + \chi_1(2)) + \overline{\chi_1(1)}(\chi_1(0) + \chi_1(2) + \chi_1(1)) + \overline{\chi_1(6)}(\chi_1(0) + \chi_1(0) + \chi_1($

Or, $\chi_1(0) = e^{2\pi.i.Tr(0)/3} = 1$, $\chi_1(1) = e^{2\pi.i.Tr(1)/3} = e^{2\pi.i/3}$ et $\chi_2(1) = e^{2\pi.i.Tr(2)/3} = e^{2\pi.i.2/3}$ donc $\chi_1(0) + \chi_1(1) + \chi_1(2) = 0$.
On obtient finalement que
$N = 1/3(\overline{\chi_1(0)}(\chi_1(0) + \chi_1(0) + \chi_1(0))) = 3/3 = 1$ On retrouve bien notre nombre de solution

ii) On peut faire de même pour le cas F4 et $P := X^2$ Je l'ai fais sur papier, flemme pour le moment

Nous pouvons enfin énoncer notre critère :

Théorème 2 (Critère)**.** *Soit P un polynôme à coefficients dans $\mathbb{F}_q$, alors P est de permutation si et seulement si $\sum_{\alpha \in \mathbb{F}_q} \chi(P(\alpha)) = 0$ pour tout caractère additif non-trivial.*

Démonstration. i) De gauche à droite : Supposons que P soit de permutation ; il réalise donc une bijection et il s'ensuit que l'équation $P(x) = \alpha$ admet une unique solution. Soit $\chi \neq \chi_0$, donc $\exists \alpha \in \mathbb{F}_q$ tel que $\chi(\alpha) \neq 1$. On peut même supposer α non nul. Comme P est une bijection ; si c parcourt $\mathbb{F}_q$, alors $P(c)$ aussi, de sorte que l'on a $\sum_{c \in \mathbb{F}_q} \chi(P(c)) = \sum_{c \in \mathbb{F}_q} \chi(c)$.
Remarquons de plus que

$$\chi(\alpha) \sum_{c \in \mathbb{F}_q} \chi(c) = \sum_{c \in \mathbb{F}_q} \chi(c)\chi(\alpha) \sum_{c \in \mathbb{F}_q} \chi(c.\alpha) = \sum_{c \in \mathbb{F}_q} \chi(c)$$

car χ est un morphisme et que $\phi : c \longmapsto \alpha.c$ est une bijection pour α non nul.
On obtient dès lors que

$$\chi(\alpha) \sum_{c \in \mathbb{F}_q} \chi(c) - \sum_{c \in \mathbb{F}_q} \chi(c) = 0$$

i.e.

$$\sum_{c \in \mathbb{F}_q} \chi(c)(\chi(\alpha) - 1) = 0$$

Or, comme χ est supposé non trivial, $\chi(\alpha) \neq 1$ et donc $\sum_{c \in \mathbb{F}_q} \chi(c) = 0$ pour tout caractère χ non trivial.

ii) De droite à gauche : Supposons que $\sum_{\alpha \in \mathbb{F}_q} \chi(P(\alpha)) = 0$ pour tout caractère additif non-trivial, i.e.

$$\sum_{\chi \in \hat{Fq}^+ / \chi_0} \sum_{c \in \mathbb{F}_q} \chi(P(c)).\overline{\chi(\alpha)} = 0$$

De la proposition précédente, nous avons que

$$N = \frac{1}{q} \sum_{c \in \mathbb{F}_q} \sum_{\chi \in \hat{Fq}^+} \chi(P(c)).\overline{\chi(\alpha)}$$

$$
\begin{aligned}
&= \frac{1}{q} \sum_{\chi \in \hat{Fq}^+} \sum_{c \in \mathbb{F}_q} \chi(P(c)).\overline{\chi(\alpha)} \\
&= \frac{1}{q} \left[\sum_{c \in \mathbb{F}_q} \chi_0(P(c)).\overline{\chi_0(\alpha)} + \sum_{\chi \in \hat{Fq}^+/\chi_0} \sum_{c \in \mathbb{F}_q} \chi(P(c)).\overline{\chi(\alpha)} \right] \\
&= \frac{1}{q} \left[\sum_{c \in \mathbb{F}_q} \chi_1(0).\overline{\chi_1(0)} + \sum_{\chi \in \hat{Fq}^+/\chi_0} \sum_{c \in \mathbb{F}_q} \chi(P(c)).\overline{\chi(\alpha)} \right] \\
&= \frac{1}{q} \left[q + \sum_{\chi \in \hat{Fq}^+/\chi_0} \sum_{c \in \mathbb{F}_q} \chi(P(c)).\overline{\chi(\alpha)} \right] \text{ (par la proposition 5)} \\
&= \frac{1}{q} \left[q + \sum_{\chi \in \hat{Fq}^+/\chi_0} \overline{\chi(\alpha)} \sum_{c \in \mathbb{F}_q} \chi(P(c)) \right] \\
&= 1 + 0 \text{ (par hypothèse)}
\end{aligned}
$$

Il n'existe alors qu'une seule solution à l'équation pour tout $\alpha \in \mathbb{F}_q$. Il s'ensuit que P réalise une bijection et est donc de permutation.

$\square$

1 Références

http://www.numdam.org/article/CIF_1971__4__A5_0.pdf

https://theses.univ-oran1.dz/document/TH4747.pdf