

Arrangements d'hyperplans et arithmétique

Pauline Bailet

18 février 2013

Table des matières

1	Introduction	1
2	Arrangements d'hyperplans affines et projectifs	3
3	Treillis d'intersection et ses propriétés	5
4	Polynôme caractéristique	7
5	Nombre de régions	11
6	Théorème d'omission-restriction	14
7	Application au calcul du nombre de régions	20
8	Arrangements et corps finis	24
9	Fibre de Milnor d'un arrangement d'hyperplans	33
10	Conclusion	44

1 Introduction

Dans tout le mémoire, on considèrera que $\mathbb{K} = \mathbb{R}, \mathbb{C}$ ou encore \mathbb{F}_q pour $q = p^s$ avec p premier. Les références principales sont le livre de Orlik et Terao [3] et celui de Stanley [4], ainsi que l'exposé Bourbaki de Cartier [1].

Soit $\mathcal{A} \subset \mathbb{K}^n$ une collection finie d'hyperplans, et soit $M(\mathcal{A}) = \mathbb{K}^n \setminus \bigcup_{H \in \mathcal{A}} H$ le complémentaire de cet arrangement.

Si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$, $M(\mathcal{A})$ est muni de la topologie induite par la topologie métrique de l'espace affine \mathbb{K}^n , et on peut se poser des questions sur les propriétés topologiques de cet espace.

Par exemple si $\mathbb{K} = \mathbb{R}$, on s'intéresse au nombre $r(\mathcal{A})$ de composantes connexes de $M(\mathcal{A})$.

Si $\mathbb{K} = \mathbb{F}_q$, on peut se demander combien d'éléments l'ensemble fini $M(\mathcal{A})$ possède-t-il.

On a découvert que beaucoup d'invariants associés à un arrangement \mathcal{A} dépendent uniquement de son treillis d'intersection $L(\mathcal{A})$.

Dans notre mémoire, nous introduisons ce treillis $L(\mathcal{A})$ (voir le chapitre 3), puis le polynôme caractéristique $\chi(\mathcal{A}, t)$ (voir la définition 4.8), et nous démontrons le théorème d'omission-restriction (voir le théorème 6.1) qui nous permet de faire des démonstrations par récurrence sur le nombre d'hyperplans $|\mathcal{A}|$ de l'arrangement \mathcal{A} .

Dans cette démonstration, nous corrigeons une erreur présente dans le livre de Stanley [4] (voir la remarque 6.8).

Une conséquence spectaculaire de ce théorème est la formule de Zaslavsky (voir le théorème 7.1) qui dit que

$$r(\mathcal{A}) = (-1)^n \chi(\mathcal{A}, -1).$$

En utilisant ce résultat, nous donnons une nouvelle preuve d'une formule classique de Roberts obtenue en 1889 (voir le théorème 7.2).

Si les équations des hyperplans d'un arrangement $\mathcal{A} \subset \mathbb{R}^n$ ont des coefficients entiers, alors en utilisant la composition des morphismes suivants

$$\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \hookrightarrow \mathbb{F}_q$$

on obtient un arrangement $\hat{\mathcal{A}}_q \subset \mathbb{F}_q^n$ pour tout $q = p^s$, où p est un nombre premier.

Le résultat principal du chapitre 3 est l'égalité :

$$|M(\hat{\mathcal{A}}_q)| = \chi(\mathcal{A}, q)$$

pour presque tous les nombres premiers p .

Une question ouverte est de savoir si de telles formules existent pour la fibre de Milnor $F(\mathcal{A})$ associée à un arrangement \mathcal{A} (voir le chapitre 9).

On sait qu'une telle égalité ne peut pas avoir lieu pour la plupart des arrangements centraux dans \mathbb{C}^3 , par exemple pour l'arrangement donné par l'équation $xyz(x + y + z) = 0$ (voir l'exemple 9.7).

Dans une telle situation, on aimerait savoir quel est le comportement de la fonction $q \mapsto |F(\hat{\mathcal{A}}_q)|$ et ceci est le but de la dernière partie de notre mémoire.

2 Arrangements d'hyperplans affines et projectifs

Définition 2.1 Soit V un \mathbb{K} - espace vectoriel de dimension n .

1. On dit que $H \subset V$ est un hyperplan si H est un sous espace vectoriel de V de dimension $n - 1$.
2. Un ensemble fini $\mathcal{A} = \{H_i\}_{i \in I}$ d'hyperplans est appelé arrangement d'hyperplans.
3. On dit que $H \subset V$ est un hyperplan affine si il existe $v \in V$ et $H_0 \subset V$ un sous espace vectoriel de dimension $n - 1$ tels que $H = v + H_0$.
4. On dit que $\mathcal{A} = \{H_i\}_{i \in I}$ est un arrangement affine si les H_i sont des hyperplans affines.
5. On dit que l'arrangement affine \mathcal{A} est central si $\bigcap_{i \in I} H_i \neq \emptyset$. Par une translation on supposera alors que $0 \in \bigcap_{i \in I} H_i$.
6. On dit que l'arrangement central \mathcal{A} est essentiel si $\bigcap_{i \in I} H_i = \{0\}$.
7. On dit qu'un arrangement central \mathcal{A} est générique si pour toute famille $\{H_1, \dots, H_p\} \subset \mathcal{A}$ on a :

$$\text{codim}(H_1 \cap \dots \cap H_p) = \min\{p, n\}.$$

En particulier, si $p \geq n$ on a $H_1 \cap \dots \cap H_p = \{0\}$.

Exemple 2.2 1. L'arrangement de Boole : dans \mathbb{K}^n , l'arrangement de Boole est la réunion des hyperplans coordonnés : $x_i = 0$, $1 \leq i \leq n$. C'est un arrangement central de n hyperplans, qui est essentiel.

2. L'arrangement des tresses : dans \mathbb{K}^n , l'arrangement des tresses est la réunion des hyperplans : $H_{i,j} : x_i - x_j = 0$, $1 \leq i < j \leq n$. C'est un arrangement central de $\binom{n}{2}$ hyperplans, qui n'est pas essentiel car

$$\bigcap H_{i,j} = D$$

où D est la droite définie par $x_1 = x_2 = \dots = x_n$.

3. Un exemple d'arrangement générique :

l'arrangement de \mathbb{K}^3 défini par l'équation $xyz(x + y + z) = 0$.

Définition 2.3 (espace projectif)

Soit V un \mathbb{K} - espace vectoriel, alors l'espace projectif $\mathbb{P}(V) = V \setminus \{0\} / \mathbb{K}^*$, est l'ensemble des droites de V passant par l'origine, donc l'ensemble quotient pour la relation d'équivalence sur $V \setminus \{0\}$:

$$u \sim v \Leftrightarrow \exists a \in \mathbb{K}^* \mid u = a.v.$$

On notera $\mathbb{P}(\mathbb{K}^n) = \mathbb{P}_{\mathbb{K}}^{n-1}$.

Soit $H \subset V$ un hyperplan. Alors $H' = H \setminus \{0\} / \mathbb{K}^* \subset \mathbb{P}(V)$ est un hyperplan projectif dans $\mathbb{P}(V)$. La correspondance $H \rightarrow H'$ établit une bijection entre les arrangements centraux dans V et les arrangements projectifs dans $\mathbb{P}(V)$.

Exemple 2.4 On a par exemple :

- $\mathbb{P}_{\mathbb{C}}^0 = \mathbb{C} \setminus \{0\} / \mathbb{C}^* = \{\text{point}\}$.
- $\mathbb{P}_{\mathbb{C}}^1 = \mathbb{C}^2 \setminus \{0\} / \mathbb{C}^* \simeq S^2 = \mathbb{C} \sqcup \{\infty\}$.

Plus généralement, on a le résultat suivant :

Théorème 2.5 L'espace projectif $\mathbb{P}_{\mathbb{K}}^n$ est une compactification de l'espace vectoriel \mathbb{K}^n et $\mathbb{P}_{\mathbb{K}}^n \setminus \mathbb{K}^n = \mathbb{P}_{\mathbb{K}}^{n-1}$.

Il y a une relation étroite entre un arrangement central \mathcal{A} et l'arrangement projectif associé \mathcal{A}' . Par exemple on a le résultat suivant :

Proposition 2.6 Soit \mathcal{A} un arrangement d'hyperplans central non vide dans \mathbb{K}^n . Soit \mathcal{A}' l'arrangement projectif associé dans $\mathbb{P}_{\mathbb{K}}^{n-1}$. On pose

$$M(\mathcal{A}) = \mathbb{K}^n \setminus \bigcup_{H \in \mathcal{A}} H \text{ et } M(\mathcal{A}') = \mathbb{P}_{\mathbb{K}}^{n-1} \setminus \bigcup_{H' \in \mathcal{A}'} H'.$$

Alors il existe une bijection naturelle

$$M(\mathcal{A}) \sim M(\mathcal{A}') \times \mathbb{K}^*.$$

Démonstration :

Soient $H \in \mathcal{A}$ et $l_H(x) = a_1x_1 + a_2x_2 + \dots + a_nx_n$ une équation linéaire telle que $H = \{x \in \mathbb{K}^n \mid l_H(x) = 0\}$.

On définit f et g par :

$f : M(\mathcal{A}) \longrightarrow M(\mathcal{A}') \times \mathbb{K}^*$, $f(x) = ([x], l_H(x))$, et

$g : M(\mathcal{A}') \times \mathbb{K}^* \longrightarrow M(\mathcal{A})$, $g([x], a) = \frac{a}{l_H(x)} x$

où $[x]$ est la classe de x dans $\mathbb{P}_{\mathbb{K}}^{n-1}$.

On a que g est bien définie, car $g(x)$ ne dépend pas du représentant de la classe de x .

En effet, si $[x]'$ est un autre représentant de la classe de x , alors il existe un u dans \mathbb{K}^* , tel que $[x]' = u.[x]$ et on a bien $g([x]', a) = g(u.[x], a) = g([u.x], a) = \frac{a}{l_H(u.x)} u.x = \frac{a}{l_H(x)} x$.

Enfin, on a $g \circ f = Id$ et $f \circ g = Id$ donc $g = f^{-1}$ et on a bien une bijection entre les deux ensembles.

Notations :

Soit \mathcal{A} un arrangement d'hyperplans dans V . On pose

$$L(\mathcal{A}) := \{X = H_1 \cap \dots \cap H_p \mid H_1, \dots, H_p \in \mathcal{A}, X \neq \emptyset\}.$$

Si $X \in L(\mathcal{A})$, alors on définit

$$\mathcal{A}_X = \{H \in \mathcal{A} \mid X \subset H\}, \text{ et } \mathcal{A}^X = \{H \cap X \mid H \in \mathcal{A} \setminus \mathcal{A}_X, H \cap X \neq \emptyset\}.$$

Définition 2.7 (*suppression et restriction*)

Soit \mathcal{A} un arrangement d'hyperplans non vide, $H \in \mathcal{A}$. On pose :

$$\mathcal{A}' = \mathcal{A} \setminus \{H\}, \text{ et } \mathcal{A}'' = \mathcal{A}^H = \{H_1 \cap H \mid H_1 \in \mathcal{A}', H_1 \cap H \neq \emptyset\}.$$

On dit que $(\mathcal{A}, \mathcal{A}', \mathcal{A}'')$ est un triplet distingué d'arrangements.

Les triplets distingués d'arrangements sont particulièrement intéressants car ils vont nous permettre de faire des démonstrations par récurrence sur le cardinal d'un arrangement \mathcal{A} , comme dans le théorème 7.1 ou encore le théorème 8.9.

3 Treillis d'intersection et ses propriétés

On munit $L = L(\mathcal{A})$ d'une relation d'ordre \leq telle que pour tous $X, Y \in L(\mathcal{A})$:

$$X \leq Y \Leftrightarrow X \supseteq Y.$$

On pose aussi :

$$X < Y \Leftrightarrow (X \leq Y \text{ et } X \neq Y).$$

Définition 3.1 Un treillis L est un ensemble ordonné possédant un plus petit élément $\bar{0}$, un plus grand élément $\bar{1}$, et tel que les bornes inférieure $x \wedge y$ et supérieure $x \vee y$ existent pour tous x et y dans L .

On appelle atome un élément minimal de L distinct de $\bar{0}$.

Exemple 3.2 Soit \mathcal{A} un arrangement central dans V , \leq la relation d'ordre définie par :

$$X \leq Y \Leftrightarrow X \supseteq Y$$

alors $L(\mathcal{A})$ est un treillis.

De plus, on a : $\bar{0} = V$ et $\bar{1} = \bigcap_{H \in \mathcal{A}} H = V_{\mathcal{A}}$.

Les atomes sont les hyperplans.

Soient X et Y dans \mathcal{A} , alors $X \vee Y = X \cap Y$ et $X \wedge Y = \bigcap_{H \supset X \cup Y, H \in \mathcal{A}} H$.

Définition 3.3 (treillis d'intersection)

Si \mathcal{A} est un arrangement central, $L(\mathcal{A})$ muni de la relation d'ordre définie comme dans l'exemple 3.2 est appelé treillis d'intersection de l'arrangement \mathcal{A} .

Définition 3.4 (treillis géométrique)

On dit qu'un treillis L est géométrique si

1. $\forall x \in L, \exists a_1, a_2, \dots, a_r$ des atomes tels que $x = a_1 \vee a_2 \vee \dots \vee a_r = ((a_1 \vee a_2) \vee a_3) \vee \dots \vee a_r \dots$). Le r minimal est appelé rang de x , noté $r(x)$, et on définit $r(L) = r(\bar{1})$
2. $x < y \Rightarrow r(x) < r(y)$
3. $r(x \vee y) + r(x \wedge y) \leq r(x) + r(y) \quad \forall x, y \in L$

Proposition 3.5 Soit \mathcal{A} un arrangement d'hyperplans central dans $V = \mathbb{K}^n$, alors $L(\mathcal{A})$ est un treillis géométrique tel que

$$r(X) = \text{codim}(X) = \dim V - \dim X.$$

En particulier,

$$r(L(\mathcal{A})) = r(V_{\mathcal{A}}) = \text{codim}(V_{\mathcal{A}}).$$

Démonstration :

1. Il est clair que $X \in L(\mathcal{A})$ est un atome si et seulement si $X = H \in \mathcal{A}$.
Or, si $X = H_{i_1} \cap \dots \cap H_{i_p}$, où les H_i sont dans \mathcal{A} , alors $X = H_{i_1} \vee \dots \vee H_{i_p}$ et le premier point est vérifié.
De plus, p est minimal si et seulement si $H_{i_1} \not\supseteq H_{i_1} \cap H_{i_2} \not\supseteq \dots \not\supseteq H_{i_1} \cap \dots \cap H_{i_p}$. Or $\text{codim}(H_{i_1}) = 1$ donc $\text{codim}(H_{i_1} \cap H_{i_2}) = 2 \dots \text{codim}(H_{i_1} \cap \dots \cap H_{i_p}) = p$. On a donc bien $r(X) = \text{codim}(X)$.
2. $X < Y \Leftrightarrow Y \subsetneq X$ donc $\dim(X) > \dim(Y) \Rightarrow r(X) < r(Y)$.
3. on démontre ce point à partir de l'inégalité :
 $\dim(X) + \dim(Y) = \dim(X \cap Y) + \dim(X + Y) \leq \dim(X \vee Y) + \dim(X \wedge Y)$.

Définition 3.6 (*semi-treillis*)

Un semi-treillis L est un ensemble partiellement ordonné tel que la borne inférieure $x \wedge y$ existe pour tous x, y dans L .

Exemple 3.7 Si $\mathcal{A} \subset V$ est un arrangement affine, alors $L(\mathcal{A})$ est un semi-treillis ayant pour plus petit élément $\bar{0} = V$.

Lemme 3.8 Un semi-treillis fini qui admet un unique élément maximal est un treillis.

Démonstration :

Soient x et y dans L . Il suffit de prendre $x \vee y = \bigwedge_{x \leq z, y \leq z} z$ qui existe bien car l'ensemble $\{x \leq z, y \leq z\}$ est fini et non vide.

Proposition 3.9 Soit \mathcal{A} un arrangement, alors $L(\mathcal{A})$ est un semi-treillis. En particulier, pour tous X, Y dans $L(\mathcal{A})$, $[X, Y] = \{Z \in L(\mathcal{A}) \mid X \leq Z \leq Y\}$ est un treillis.

En outre, $L(\mathcal{A})$ est un treillis $\Leftrightarrow \mathcal{A}$ est central.

Démonstration :

on a que $L(\mathcal{A})$ est un ensemble partiellement ordonné et si X, Y sont dans $L(\mathcal{A})$, $X \wedge Y = \bigcap_{H \supset X \cup Y, H \in \mathcal{A}} H \neq \emptyset$, car $X \wedge Y \supset X \neq \emptyset$.

Ainsi, $L(\mathcal{A})$ est un semi-treillis. De plus, $[X, Y]$ est un semi-treillis fini admettant pour unique élément maximal Y et c'est donc un treillis d'après le lemme 3.8.

Montrons enfin $L(\mathcal{A})$ est un treillis $\Leftrightarrow \mathcal{A}$ est central.

\Leftarrow : si \mathcal{A} est central, alors $\bigcap_{H \in \mathcal{A}} H$ est non vide, et c'est le plus grand élément de

$L(\mathcal{A})$. Ainsi, $L(\mathcal{A}) = [\bar{0}, \bar{1}]$ est un treillis (avec $\bar{0} = V$; $\bar{1} = \bigcap_{H \in \mathcal{A}} H$).

\Rightarrow : $L(\mathcal{A})$ est un treillis $\Rightarrow \exists X \in L(\mathcal{A})$ un élément maximal

$\Rightarrow H \supset X \forall H \in \mathcal{A} \Rightarrow \bigcap_{H \in \mathcal{A}} H \supset X \Rightarrow \mathcal{A}$ est central.

4 Polynôme caractéristique

Définition 4.1 Soit L un ensemble fini ordonné par une relation \leq . On pose $x < y \Leftrightarrow x \leq y$ et $x \neq y$.

Soient $x, y \in L$, $x \leq y$, et $p \geq 0$. On appelle chaîne de longueur p de x à y toute suite x_0, x_1, \dots, x_p d'éléments de L telle que

$$x = x_0 < x_1 < \dots < x_p = y.$$

On note $C_p(x, y)$ le nombre de chaînes de longueur p de x à y .

Remarque 4.2 $C_0(x, x) = 1$, $C_0(x, y) = 0$ si $x < y$, et $C_p(x, x) = 0$ si $p \geq 1$.

Définition 4.3 Soient $x, y \in L$, $x \leq y$. On définit la fonction de Möbius-Rota de L par la formule :

$$\mu_L(x, y) = \sum_p (-1)^p \cdot C_p(x, y), \quad \mu_L(x, y) = 0 \text{ si } x \not\leq y.$$

Le lemme suivant caractérise totalement la fonction de Möbius-Rota :

Lemme 4.4 Il existe une unique fonction $\mu_L : L \times L \rightarrow \mathbb{Z}$ telle que

$$\mu_L(x, x) = 1 \tag{4.1}$$

et

$$\sum_{x \leq z \leq y} \mu_L(x, z) = 0 = \sum_{x \leq z \leq y} \mu_L(z, y) \text{ si } x < y. \tag{4.2}$$

Notations : Si $\bar{0}$ existe, on note $\mu_L(x) = \mu_L(\bar{0}, x)$.

Remarque 4.5 La même définition marche aussi si L est un semi-treillis.

Exemple 4.6 (Le treillis des parties d'un ensemble)

Soit S un ensemble fini et $\mathcal{P}(S)$ l'ensemble des parties de S . Soit \leq la relation d'ordre telle que

$$A \leq B \Leftrightarrow A \subseteq B.$$

On montre facilement par récurrence que $\mu(A, B) = (-1)^{|B|-|A|}$.

Proposition 4.7 (Formule d'inversion de Möbius-Rota)

Soient G un groupe abélien, $f : L \rightarrow G$ et g la fonction sommatoire associée :

$$g : L \rightarrow G \\ x \mapsto \sum_{y \leq x} f(y).$$

Alors on a la formule d'inversion suivante :

$$f(x) = \sum_{y \leq x} \mu_L(y, x) \cdot g(y) \quad \forall x \in L.$$

De même, si $g(x) = \sum_{y \geq x} f(y)$, alors on a la formule :

$$f(x) = \sum_{y \geq x} \mu_L(x, y) \cdot g(y) \quad \forall x \in L.$$

Définition 4.8 (*Polynôme caractéristique et polynôme de Poincaré*)

Soit L un treillis géométrique. On définit le polynôme caractéristique combinatoire de L par la formule :

$$p(L, t) = \sum_{x \in L} \mu_L(x) \cdot t^{r(L) - r(x)}.$$

Si $L = L(\mathcal{A})$, on utilise la notation $p(\mathcal{A}, t)$.

On appelle polynôme caractéristique de \mathcal{A} le polynôme :

$$\chi(\mathcal{A}, t) = \sum_{x \in L(\mathcal{A})} \mu_{L(\mathcal{A})}(x) \cdot t^{\dim x}.$$

Enfin, on définit le polynôme de Poincaré de l'arrangement \mathcal{A} par :

$$\pi(\mathcal{A}, t) = \sum_{x \in L(\mathcal{A})} \mu_{L(\mathcal{A})}(x) \cdot (-t)^{r(x)}.$$

Remarque 4.9 On a que :

1. si $e = \dim(V_A)$,

$$\chi(\mathcal{A}, t) = t^e \cdot p(\mathcal{A}, t) \quad \text{et} \quad p(\mathcal{A}, 0) = \mu_L(\bar{1}) = \mu_L(V_A).$$

En particulier, si \mathcal{A} est essentiel, $\chi(\mathcal{A}, t) = p(\mathcal{A}, t)$.

2. les polynômes $\chi(\mathcal{A}, t)$ et $\pi(\mathcal{A}, t)$ peuvent être définis pour un arrangement affine en utilisant les mêmes formules et le semi-treillis $L(\mathcal{A})$.

Exemple 4.10 On peut montrer que :

1. si \mathcal{A} est l'arrangement de Boole dans \mathbb{R}^n ou \mathbb{C}^n , alors

$$\chi(\mathcal{A}, t) = p(\mathcal{A}, t) = (t - 1)^n.$$

2. si \mathcal{A} est l'arrangement des tresses dans \mathbb{R}^n ou \mathbb{C}^n , alors

$$p(\mathcal{A}, t) = (t - 1)(t - 2) \dots (t - n + 1),$$

$$\chi(\mathcal{A}, t) = t(t - 1)(t - 2) \dots (t - n + 1).$$

3. Si $\mathcal{A} = \{H_1, \dots, H_d\}$ est un arrangement générique dans \mathbb{R}^n ou \mathbb{C}^n formé de d hyperplans, alors

$$\chi(\mathcal{A}, t) = \sum_{k=0}^n \binom{d}{k} (-1)^k t^{n-k} + \sum_{k=n+1}^d \binom{d}{k} (-1)^k. \quad (1)$$

Démonstration :

Démontrons 3. en distinguant deux cas :

– si $1 \leq d \leq n$, alors on a un isomorphisme de treillis :

$$\phi : (L(\mathcal{A}), \leq) \longrightarrow (\mathcal{P}(S), \subseteq), \quad S = \{1, \dots, d\}$$

$$\text{tel que } \phi(\cap_{i \in I} H_i) = I, \quad \phi(\mathbb{R}^n) = \emptyset, \quad \phi(H_1 \cap \dots \cap H_d) = S.$$

$$\text{En effet, } \cap_{i \in I} H_i = \cap_{i \in J} H_i \Leftrightarrow I = J, \quad \text{et } \cap_{i \in I} H_i \leq \cap_{i \in J} H_i \Leftrightarrow I \subseteq J.$$

Ainsi, si $X = \cap_{i \in I} H_i$ alors $\mu_{L(\mathcal{A})}(X) = \mu_{\mathcal{P}(S)}(\phi(X)) = (-1)^{|I|} = (-1)^{\text{codim}(X)}$ d'après l'exemple 4.6 et on a :

$$\begin{aligned} \chi(\mathcal{A}, t) &= \sum_{X \in L(\mathcal{A})} \mu_{L(\mathcal{A})}(X) t^{\dim X} = \sum_{k=0}^d \sum_{\substack{X \in L(\mathcal{A}) \\ \dim(X) = n-k}} (-1)^k t^{n-k} = \sum_{k=0}^d \binom{d}{k} (-1)^k t^{n-k} \\ &= t^{n-d} (t-1)^d. \end{aligned}$$

– Si $d > n$, cette fois-ci nous ne pouvons pas trouver un isomorphisme de treillis entre $L(\mathcal{A})$ et $\mathcal{P}(S)$ car l'écriture de $\{0\}$ n'est plus unique.

Cependant $L(\mathcal{A}) = \{0\} \sqcup L(\mathcal{A})_1$, avec $L(\mathcal{A})_1 = \{H_{i_1} \cap \dots \cap H_{i_k} \mid k \leq n-1\}$.

Soit $E = \{B \subseteq S \mid |B| \leq n-1\}$. On a une bijection d'ensemble entre $L(\mathcal{A})_1$ et E .

En effet, à un élément $H_{i_1} \cap \dots \cap H_{i_k}$ de $L(\mathcal{A})_1$ correspond un unique

$B = \{i_1, \dots, i_k\}$ de E . Ainsi,

$$\begin{aligned} \chi(\mathcal{A}, t) &= \sum_{X \in L(\mathcal{A})} \mu_{L(\mathcal{A})}(X) t^{\dim X} = \mu_{L(\mathcal{A})}(\{0\}) + \sum_{X \in L(\mathcal{A})_1} \mu_{L(\mathcal{A})}(X) t^{\dim X} \\ &= \mu_{L(\mathcal{A})}(\{0\}) + \sum_{k=0}^{n-1} \sum_{\substack{X \in L(\mathcal{A})_1 \\ \dim(X) = n-k}} (-1)^k t^{n-k} = \mu_{L(\mathcal{A})}(\{0\}) + \sum_{k=0}^{n-1} \binom{d}{k} (-1)^k t^{n-k}. \end{aligned}$$

Reste à calculer $\mu_{L(\mathcal{A})}(\{0\})$.

On a que $\mu_{L(\mathcal{A})}(\{0\}) = \mu_{L(\mathcal{A})}(\bar{0}, \{0\}) = \mu_{L(\mathcal{A})}(\bar{0}, \bar{1})$.

Or $\sum_{\bar{0} \leq z \leq \bar{1}} \mu_{L(\mathcal{A})}(\bar{0}, z) = 0$ d'après le lemme 4.4.

Ainsi

$$\begin{aligned} \mu_{L(\mathcal{A})}(\bar{0}, \bar{0}) + \binom{d}{1} \mu_{L(\mathcal{A})}(\bar{0}, H_i) + \binom{d}{2} \mu_{L(\mathcal{A})}(\bar{0}, H_i \cap H_j) + \dots + \\ \binom{d}{n-1} \mu_{L(\mathcal{A})}(\bar{0}, H_{i_1} \cap \dots \cap H_{i_{n-1}}) + \mu_{L(\mathcal{A})}(\{0\}) = 0. \end{aligned}$$

D'où

$$\begin{aligned} \mu_{L(\mathcal{A})}(\{0\}) &= -[\mu_{L(\mathcal{A})}(\bar{0}, \bar{0}) + \binom{d}{1} \mu_{L(\mathcal{A})}(\bar{0}, H_i) + \binom{d}{2} \mu_{L(\mathcal{A})}(\bar{0}, H_i \cap H_j) + \\ &\dots + \binom{d}{n-1} \mu_{L(\mathcal{A})}(\bar{0}, H_{i_1} \cap \dots \cap H_{i_{n-1}})] = - \sum_{k=0}^{n-1} \binom{d}{k} (-1)^k = \sum_{k=n}^d \binom{d}{k} (-1)^k. \end{aligned}$$

5 Nombre de régions

Définition 5.1 Soit \mathcal{A} un arrangement d'hyperplans réels, et $M(\mathcal{A}) = \mathbb{R}^n \setminus \bigcup_{H \in \mathcal{A}} H$.

On appelle région de \mathcal{A} toute composante connexe de $M(\mathcal{A})$ et on note $r(\mathcal{A})$ le nombre de régions de \mathcal{A} .

Exemple 5.2 Considérons un arrangement \mathcal{A} composé de n droites quelconques dans le plan \mathbb{R}^2 . La formule de Roberts, que nous ne démontrerons pas ici, assure que dans ce cas

$$r(\mathcal{A}) = n + 1 + \binom{n}{2} - \sum_{i=1}^m \binom{a_i-1}{2} - \sum_{j=1}^p \binom{b_j}{2}.$$

avec m points de multiplicités $a_1 \geq 3, \dots, a_m \geq 3$, et p familles de droites parallèles comportant $b_1 \geq 2, \dots, b_p \geq 2$ éléments.

Définition 5.3 Soit \mathcal{A} un arrangement d'hyperplans réels. Pour chaque $H \in \mathcal{A}$, soient $u_H \in \mathbb{R}^n$ et $a_H \in \mathbb{R}$ tels que :

$$H = \{x \in \mathbb{R}^n \mid \langle x, u_H \rangle + a_H = 0\}.$$

Pour chaque H dans \mathcal{A} , on associe \tilde{H} l'hyperplan défini par :

$$\tilde{H} = \{x \in \mathbb{R}^n \mid \langle x, u_H \rangle = 0\}.$$

Notons maintenant $\tilde{V}_{\mathcal{A}} = \bigcap_{H \in \mathcal{A}} \tilde{H}$. Deux cas se présentent alors :

1. $\tilde{V}_{\mathcal{A}} = \{0\}$: on dit que \mathcal{A} est essentiel, et qu'une composante connexe de $M(\mathcal{A})$ est relativement bornée si elle est bornée.
2. $\tilde{V}_{\mathcal{A}} \neq \{0\}$: on dit qu'une composante connexe C de $M(\mathcal{A})$ est relativement bornée si $C \cap \tilde{V}_{\mathcal{A}}^\perp$ est borné.

On note $b(\mathcal{A})$ le nombre de composantes connexes relativement bornées de $M(\mathcal{A})$.

Exemple 5.4 – Si $\mathcal{A} = \emptyset$, alors $M(\mathcal{A}) = \mathbb{R}^n$ est relativement bornée car $\tilde{V}_{\mathcal{A}}^\perp = \{0\}$.
– Si $\mathcal{A} = \{H\}$, alors $M(\mathcal{A}) = \mathbb{R}^n \setminus H$ a deux composantes connexes mais $b(\mathcal{A}) = 0$.

Nous allons voir maintenant quels sont les liens entre le polynôme caractéristique d'un arrangement \mathcal{A} et les invariants $r(\mathcal{A})$ et $b(\mathcal{A})$. Nous aurons tout d'abord besoin du lemme suivant :

Lemme 5.5 Soit $(\mathcal{A}, \mathcal{A}', \mathcal{A}'')$ un triplet distingué d'arrangements. Alors on a :

1. $r(\mathcal{A}) = r(\mathcal{A}') + r(\mathcal{A}'')$.
2. $b(\mathcal{A}) = \begin{cases} b(\mathcal{A}') + b(\mathcal{A}'') & \text{si } \text{rang}(\mathcal{A}) = \text{rang}(\mathcal{A}') \\ 0 & \text{si } \text{rang}(\mathcal{A}) = \text{rang}(\mathcal{A}') + 1 \end{cases}$
où $\text{rang}(\mathcal{A}) = \text{codim}(\tilde{V}_{\mathcal{A}})$, $\text{rang}(\mathcal{A}') = \text{codim}(\tilde{V}_{\mathcal{A}'})$ et $\text{rang}(\mathcal{A}'') = \text{codim}(\tilde{V}_{\mathcal{A}''})$.

Démonstration :

Préliminaire :

Montrons que $\text{rang}(\mathcal{A}) = \text{rang}(\mathcal{A}'') + 1$.

Si $\mathcal{A} = \{H_0, H_1, \dots, H_p\}$, $\mathcal{A}' = \mathcal{A} \setminus \{H_0\}$, $\mathcal{A}'' = \{H_0 \cap H_1, \dots, H_0 \cap H_p\}$, notons

$N(\mathcal{A}) = \text{vect}\{u_{H_0}, u_{H_1}, \dots, u_{H_p}\} = \tilde{V}_{\mathcal{A}}^\perp$.

Pour chaque $i \in \{1, \dots, p\}$, on note u'_{H_i} la projection du vecteur u_{H_i} sur l'hyperplan H_0 .

On a donc que $\text{vect}\{u_{H_0}, u_{H_i}\} = \text{vect}\{u_{H_0}, u'_{H_i}\}$ et

$N(\mathcal{A}) = \text{vect}\{u_{H_0}, u_{H_1}, \dots, u_{H_p}\} = \text{vect}\{u_{H_0}, u'_{H_1}, \dots, u'_{H_p}\} = u_{H_0}\mathbb{R} \oplus \text{vect}\{u'_{H_1}, \dots, u'_{H_p}\} = u_{H_0}\mathbb{R} \oplus N(\mathcal{A}'')$.

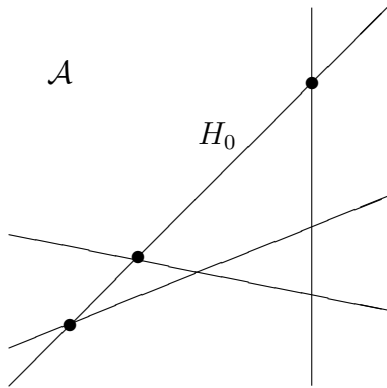
On en déduit que $\text{rang}(\mathcal{A}) = \dim(N(\mathcal{A})) = \dim(N(\mathcal{A}'')) + 1 = \text{rang}(\mathcal{A}'') + 1$.

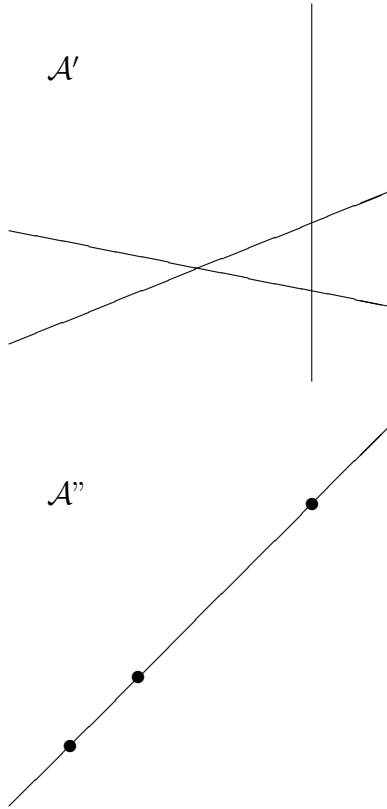
Revenons à notre démonstration.

1. Si $\mathcal{A} = \mathcal{A}' \cup \{H_0\}$, alors $r(\mathcal{A})$ vaut $r(\mathcal{A}')$ auquel on ajoute le nombre de régions de $M(\mathcal{A}')$ coupées en deux par H_0 . Or à chaque composante connexe de $M(\mathcal{A}')$ coupée en deux par H_0 correspond une unique composante connexe de $M(\mathcal{A}'')$.

Réciproquement, à chaque composante connexe $C'' \subset M(\mathcal{A}'')$ correspond une composante connexe de $M(\mathcal{A}')$ qui a été coupée en deux par H_0 .

Il y a donc une bijection entre les régions de \mathcal{A}' coupées en deux par H_0 et les régions de \mathcal{A}'' .





2. (a) Si $\text{rang}(\mathcal{A}) = \text{rang}(\mathcal{A}')$, alors $\dim(\tilde{V}_{\mathcal{A}}^{\perp}) = \dim(\tilde{V}_{\mathcal{A}'}^{\perp})$. De plus $\tilde{V}_{\mathcal{A}} \subset \tilde{V}_{\mathcal{A}'}$, d'où $\tilde{V}_{\mathcal{A}'}^{\perp} \subset \tilde{V}_{\mathcal{A}}^{\perp}$, donc $\tilde{V}_{\mathcal{A}}^{\perp} = \tilde{V}_{\mathcal{A}'}^{\perp}$.
- Si $\tilde{V}_{\mathcal{A}} = \tilde{V}_{\mathcal{A}'} = \tilde{V}_{\mathcal{A}''} = \{0\}$ alors les composantes connexes relativement bornées de $M(\mathcal{A})$ sont les composantes connexes bornées de $M(\mathcal{A})$. Elles contiennent les composantes connexes bornées de $M(\mathcal{A}')$ non intersectées par H_0 auxquelles on ajoute les composantes connexes bornées résultant de l'intersection d'une région C_1 de $M(\mathcal{A}')$ avec H_0 .
Par cette construction, une région bornée de \mathcal{A}' donne naissance à deux régions bornées de \mathcal{A} et une région non bornée de \mathcal{A}' donne naissance à une seule région bornée de \mathcal{A} .
 - Si $\tilde{V}_{\mathcal{A}} = \tilde{V}_{\mathcal{A}'} = \tilde{V}_{\mathcal{A}''} \neq \{0\}$, alors soit $1 \leq m \leq n - 1$ tel que $\dim(\tilde{V}_{\mathcal{A}}) = \dim(\tilde{V}_{\mathcal{A}'}) = \dim(\tilde{V}_{\mathcal{A}''}) = n - m$.
On peut choisir les coordonnées x_1, \dots, x_n sur \mathbb{K}^n tel que :
 $E' = \tilde{V}_{\mathcal{A}} : x_1 = x_2 = \dots = x_m = 0$ et $H_0 : x_1 = 0$.
On pose $E = \tilde{V}_{\mathcal{A}}^{\perp} : x_{m+1} = \dots = x_n = 0$.
Si $H \in \mathcal{A}'$, alors pour ce choix de coordonnées $l_{\tilde{H}}(x)$ s'écrit $l_{\tilde{H}}(x) = \alpha_1 x_1 + \dots + \alpha_m x_m$ (il n'y a pas de composante en

x_{m+1}, \dots, x_n), d'où $l_H(x) = \alpha_1 x_1 + \dots + \alpha_m x_m + \beta$.

On a donc une bijection entre l'arrangement \mathcal{A} de \mathbb{R}^n et l'arrangement $\mathcal{B} = \{H \cap E \mid H \in \mathcal{A}\}$ de E :

on a que $\mathbb{R}^n = E \times E'$, donc $\forall H \in \mathcal{A}$, $H = (H \cap E) \times (H \cap E')$
 $= (H \cap E) \times E'$ pour ce choix de coordonnées.

Ainsi le nombre de composantes connexes relativement bornées de $M(\mathcal{A})$ correspond au nombre de composantes connexes bornées de $M(\mathcal{B})$ dans E , ce qui nous ramène au cas précédent.

(b) Si $\text{rang}(\mathcal{A}) = \text{rang}(\mathcal{A}') + 1$, alors $\dim(\tilde{V}_{\mathcal{A}'}) = \dim(\tilde{V}_{\mathcal{A}}) + 1$.

– commençons par étudier le cas particulier où $\tilde{V}_{\mathcal{A}} = \{0\}$.

Dans ce cas, $\dim(\tilde{V}_{\mathcal{A}'}) = 1$ et $\tilde{V}_{\mathcal{A}'}$ est une droite.

On peut choisir les coordonnées x_1, \dots, x_n sur \mathbb{K}^n tel que :

$\tilde{V}_{\mathcal{A}'} : x_2 = \dots = x_n = 0$.

Alors l'hyperplan H_0 est défini par une équation linéaire de la forme $l_{H_0}(x) = a_1 x_1 + \dots + a_n x_n + \beta$ avec $a_1 \neq 0$.

On peut supposer $a_1 > 0$.

Soient maintenant C une composante connexe de $M(\mathcal{A})$ et $p \in C$, alors $l_{H_0}(p) \neq 0$.

Supposons par exemple $l_{H_0}(p) > 0$. Alors la demi-droite

$$\{p + te_1; t \geq 0\}, \quad e_1 = (1, 0, \dots, 0)$$

est contenue dans C qui n'est donc pas bornée.

– Si $\tilde{V}_{\mathcal{A}} \neq \{0\}$, on a évidemment toujours $\dim(\tilde{V}_{\mathcal{A}'}) = \dim(\tilde{V}_{\mathcal{A}}) + 1$.

Soit alors $1 \leq m \leq n - 1$ tel que $\dim(\tilde{V}_{\mathcal{A}}) = n - m$, $\dim(\tilde{V}_{\mathcal{A}'}) = n - m + 1$.

On peut choisir les coordonnées sur \mathbb{K}^n tel que :

$\tilde{V}_{\mathcal{A}} : x_1 = \dots = x_m = 0$ et $\tilde{V}_{\mathcal{A}'} : x_2 = \dots = x_m = 0$.

On a donc :

$\tilde{V}_{\mathcal{A}}^\perp : x_{m+1} = \dots = x_n = 0$ et $\tilde{V}_{\mathcal{A}'}^\perp : x_1 = 0, x_{m+1} = 0, \dots = x_n = 0$.

Pour ce choix, les hyperplans de \mathcal{A}' sont définis par une équation linéaire de la forme $\alpha_2 x_2 + \dots + \alpha_m x_m + \beta = 0$, et H_0 par une équation linéaire de la forme $a_1 x_1 + a_2 x_2 + \dots + a_m x_m + \beta_0 = 0$ avec $a_1 \neq 0$.

On a que $\tilde{V}_{\mathcal{A}}^\perp = \tilde{V}_{\mathcal{A}'}^\perp \times \mathbb{K}e_1$, donc si C est une composante connexe de $M(\mathcal{A})$, alors $C \cap \tilde{V}_{\mathcal{A}}^\perp = C \cap \tilde{V}_{\mathcal{A}'}^\perp \times \mathbb{K}e_1$ est un cylindre. Ce cylindre est coupé en deux par H_0 car $a_1 \neq 0$, et donc les composantes connexes de $M(\mathcal{A})$ intersectées avec $\tilde{V}_{\mathcal{A}}^\perp$ sont des demis-cylindres qui ne sont pas bornés.

6 Théorème d'omission-restriction

Le but de cette partie est de démontrer le théorème suivant :

Théorème 6.1 (*théorème d'omission-restriction*)

Si $(\mathcal{A}, \mathcal{A}', \mathcal{A}'')$ est un triplet distingué d'arrangements, alors

$$\chi(\mathcal{A}, t) = \chi(\mathcal{A}', t) - \chi(\mathcal{A}'', t).$$

Mais avant nous avons besoin d'introduire de nouvelles notions.

Nous allons maintenant nous intéresser à l'algèbre de Möbius associée à un treillis L , notée $A(L)$.

$$A(L) = \left\{ \sum \alpha_x \cdot x \mid \alpha_x \in \mathbb{R}, x \in L \right\}.$$

Pour tous x, y dans L on définit : $x \cdot y = x \vee y$.

L'algèbre de Möbius est isomorphe en tant que \mathbb{R} -algèbre à $\mathbb{R}^{|L|}$ (voir le théorème 6.2). Pour chaque x dans L on pose $\sigma_x = \sum_{y \geq x} \mu_L(x, y) \cdot y \in A(L)$.

La formule d'inversion de Möbius de la proposition 4.7 donne :

$x = \sum_{y \geq x} \sigma_y$ ce qui montre bien que $\{\sigma_x\}_{x \in L}$ est une base de $A(L)$ en tant que

\mathbb{R} -espace vectoriel.

Théorème 6.2 Soit L un treillis fini. Soient x, y dans L .

Alors $\sigma_x \cdot \sigma_y = \delta_{xy} \cdot \sigma_x$ et de plus on a un isomorphisme de \mathbb{R} -algèbres :

$$A(L) = \bigoplus_{x \in L} \mathbb{R} \cdot \sigma_x.$$

Démonstration :

On introduit une autre \mathbb{R} -algèbre $A'(L)$ ayant pour base $\{\sigma_x'\}_{x \in L}$ et telle que $\sigma_x' \cdot \sigma_y' = \delta_{xy} \cdot \sigma_x'$.

Ici, $\{\sigma_x'\}_{x \in L}$ est une collection des symboles, en bijection avec la collection $\{\sigma_x\}_{x \in L}$ que l'on avait déjà.

L'application $\phi : A(L) \rightarrow A'(L)$ induite par $\sigma_x \mapsto \sigma_x'$ est un isomorphisme d'espace vectoriel.

D'autre part, soit $x \in L$, on a $x' = \phi(x) = \sum_{y \geq x} \sigma_y' \in A(L)$, et

$$x' \cdot y' = \left(\sum_{s \geq x} \sigma_s' \right) \cdot \left(\sum_{t \geq y} \sigma_t' \right) = \sum_{u \geq x \vee y} \sigma_u' = (x \vee y)'$$

On a donc un isomorphisme de \mathbb{R} -algèbres $\phi : A(L) \rightarrow A'(L)$.

Ainsi $\phi(\sigma_x \cdot \sigma_y) = \phi(\sigma_x \vee \sigma_y) = (\sigma_x \vee \sigma_y)' = \sigma_x' \cdot \sigma_y' = \delta_{xy} \cdot \sigma_x' = \phi(\delta_{xy} \cdot \sigma_x)$, et comme ϕ est injective, on en déduit que $\sigma_x \cdot \sigma_y = \delta_{xy} \cdot \sigma_x$.

De plus, les σ_x étant orthogonaux on a la somme directe :

$$A(L) = \bigoplus_{x \in L} \mathbb{R} \cdot \sigma_x.$$

Venons en maintenant au **théorème de la section** :

Théorème 6.3 (théorème de la section)

Soit L un treillis fini de cardinal n . Soit X dans L tel que $\bar{0} \notin X$ et tel que :

si $y \in L$ et $y \neq \bar{0}$, alors il existe un $x \in X$ tel que $x \leq y$.

Soit N_k le nombre de sous ensembles $\{x_1, \dots, x_k\}$ à k éléments de X tels que $x_1 \vee x_2 \vee \dots \vee x_k = \bar{1}$. Alors

$$\mu_L(\bar{0}, \bar{1}) = N_0 - N_1 + N_2 - \dots + (-1)^n N_n$$

Démonstration :

Pour tout x dans L , on a que $\bar{0} - x = 1 \cdot \bar{0} - 1 \cdot x \in A(L)$ et

$$\bar{0} - x = \sum_{t \geq \bar{0}} \sigma_t - \sum_{s \geq x} \sigma_s = \sum_{t \not\geq x} \sigma_t$$

et comme les σ_t sont orthogonaux,

$$\prod_{x \in X} (\bar{0} - x) = \sum_y \sigma_y, \text{ où } y \not\geq x \ \forall x \in X$$

$$\prod_{x \in X} (\bar{0} - x) = \sigma_{\bar{0}} = \sum_{y \geq \bar{0}} \mu_L(\bar{0}, y) \cdot y.$$

Maintenant, si $X = \{x_1, x_2, \dots, x_n\}$, alors en développant $\prod_{i=1}^n (\bar{0} - x_i)$ on trouve que $\mu(\bar{0}, \bar{1})$, le coefficient de $\bar{1}$ vaut bien $N_0 - N_1 + N_2 - \dots + (-1)^n N_n$.

Exemple 6.4 Soit \mathcal{B} le treillis des parties de l'ensemble $S = \{1, \dots, n\}$. Ce treillis est isomorphe au treillis d'intersection $L(\mathcal{A})$ où \mathcal{A} est l'arrangement de Boole constitué des hyperplans coordonnés

$H_i : x_i = 0, 1 \leq i \leq n$.

On a que $\bar{1} = \{0\} = H_1 \vee H_2 \vee \dots \vee H_n$ et $N_0 = \dots = N_{n-1} = 0, N_n = 1$.

Ainsi, en appliquant le théorème de la section 6.3 avec $L = L(\mathcal{A})$ et $X = \{H_1, \dots, H_n\}$ on trouve : $\mu_{L(\mathcal{A})}(\bar{0}, \bar{1}) = (-1)^n$ d'où $\mu_{\mathcal{B}}(\emptyset, S) = (-1)^{|S|}$.

Définition 6.5 Soit \mathcal{A} un arrangement affine de \mathbb{K}^n . On dit que $\mathcal{B} \subset \mathcal{A}$ est un arrangement central si $\bigcap_{H \in \mathcal{B}} H \neq \emptyset$.

Théorème 6.6 (théorème de Whitney)

Soit \mathcal{A} un arrangement affine de \mathbb{K}^n .

$$\chi(\mathcal{A}, t) = \sum_{\substack{\mathcal{B} \subset \mathcal{A} \\ \mathcal{B} \text{ central}}} (-1)^{|\mathcal{B}|} \cdot t^{n-\text{rang}(\mathcal{B})}.$$

Démonstration :

Soit $Z \in L(\mathcal{A})$. On considère $\mathcal{A}_Z = \{X \in L(\mathcal{A}) \mid X \leq Z\}$ qui est un treillis d'après le lemme 3.8 car c'est un semi-treillis fini qui possède un unique élément maximal Z . On peut donc utiliser le théorème 6.3 de la section avec

$$L = \mathcal{A}_Z, \quad X = X_Z = \{H \in \mathcal{A} \mid H \leq Z\}.$$

En effet, $\bar{0} = V \notin X_Z$.

Soit $Y \in \mathcal{A}_Z$, $Y \neq \bar{0}$, et soient $H_{i_1}, H_{i_2}, \dots, H_{i_p} \in \mathcal{A}$ tels que

$Y = H_{i_1} \cap H_{i_2} \cap \dots \cap H_{i_p}$. On a que $Z \subset H_k \forall k \in \{i_1, \dots, i_p\}$, donc les hyperplans $H_{i_1}, H_{i_2}, \dots, H_{i_p}$ appartiennent à X_Z et $H_k \leq Y \forall k \in \{i_1, \dots, i_p\}$.

D'après le théorème 6.3 on a que $\mu(\bar{0}, \bar{1}) = \mu(\bar{0}, Z) = \mu(Z) = \sum_k (-1)^k N_k(Z)$

où $N_k(Z)$ est le nombre de sous ensembles $\{H_{i_1}, H_{i_2}, \dots, H_{i_k}\}$ de X_k à k éléments tels que $H_{i_1} \cap \dots \cap H_{i_k} = Z \neq \emptyset$.

Un tel sous ensemble \mathcal{B} est un arrangement central qui vérifie $\text{rang}(\mathcal{B}) = n - \dim(Z)$. On peut donc écrire :

$$\mu(Z) \cdot t^{\dim Z} = \sum_{\substack{\mathcal{B} \subset X_Z \\ Z = \bigcap_{H \in \mathcal{B}} H}} (-1)^{|\mathcal{B}|} \cdot t^{n-\text{rang}(\mathcal{B})}$$

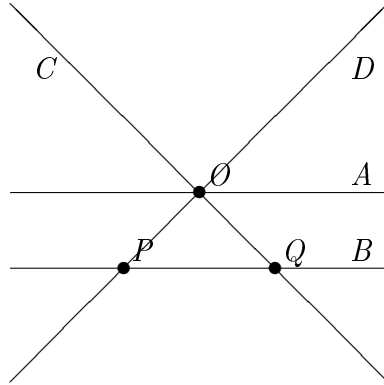
et

$$\chi(\mathcal{A}, t) = \sum_{Z \in L(\mathcal{A})} \mu(Z) \cdot t^{\dim Z} = \sum_{Z \in L(\mathcal{A})} \sum_{\substack{\mathcal{B} \subset X_Z \\ Z = \bigcap_{H \in \mathcal{B}} H}} (-1)^{|\mathcal{B}|} \cdot t^{n-\text{rang}(\mathcal{B})}$$

Or en parcourant tous les $Z \in L(\mathcal{A})$ on trouve tous les arrangements centraux de \mathcal{A} et inversement : à chaque arrangement central \mathcal{B}_0 de \mathcal{A} correspond un Z_0 de $L(\mathcal{A})$ tel que $Z_0 = \bigcap_{H \in \mathcal{B}_0} H \neq \emptyset$. Ainsi :

$$\sum_{Z \in L(\mathcal{A})} \sum_{\substack{\mathcal{B} \subset X_Z \\ Z = \bigcap_{H \in \mathcal{B}} H}} (-1)^{|\mathcal{B}|} \cdot t^{n-\text{rang}(\mathcal{B})} = \sum_{\substack{\mathcal{B} \subset \mathcal{A} \\ \mathcal{B} \text{ central}}} (-1)^{|\mathcal{B}|} \cdot t^{n-\text{rang}(\mathcal{B})}.$$

Exemple 6.7 Donnons maintenant un exemple de calcul du polynôme caractéristique d'un arrangement $\mathcal{A} \in \mathbb{R}^2$:



Les arrangements centraux de \mathcal{A} sont :

- \emptyset de cardinal 0 et de rang 0
- $\{A\}$, $\{B\}$, $\{C\}$ et $\{D\}$ de cardinal 1 et de rang 1
- $\{A, C\}$, $\{A, D\}$, $\{B, C\}$, $\{B, D\}$, et $\{D, C\}$ de cardinal 2 et de rang 2
- $\{A, C, D\}$ de cardinal 3 et de rang 2.

Ainsi $\chi(\mathcal{A}, t) = t^2 - 4t + 4$.

Nous avons maintenant toutes les cartes en main pour pouvoir démontrer le théorème d'omission-restriction.

Démonstration du théorème d'omission-restriction :

Soient $(\mathcal{A}, \mathcal{A}', \mathcal{A}'')$ un triplet distingué d'arrangements dans \mathbb{K}^n et $H_0 \in \mathcal{A}$ tel que $\mathcal{A}' = \mathcal{A} \setminus \{H_0\}$, $\mathcal{A}'' = \{H \cap H_0 \mid H \in \mathcal{A}'\}$. D'après le théorème 6.6 de Whitney on a que

$$\chi(\mathcal{A}, t) = \sum_{\substack{\mathcal{B} \subset \mathcal{A} \\ \mathcal{B} \text{ central}}} (-1)^{|\mathcal{B}|} \cdot t^{n-\text{rang}(\mathcal{B})}$$

$$\chi(\mathcal{A}, t) = \sum_{\substack{\mathcal{B} \subset \mathcal{A} \\ \mathcal{B} \text{ central} \\ H_0 \notin \mathcal{B}}} (-1)^{|\mathcal{B}|} \cdot t^{n-\text{rang}(\mathcal{B})} + \sum_{\substack{\mathcal{B} \subset \mathcal{A} \\ \mathcal{B} \text{ central} \\ H_0 \in \mathcal{B}}} (-1)^{|\mathcal{B}|} \cdot t^{n-\text{rang}(\mathcal{B})}$$

d'où :

$$\chi(\mathcal{A}, t) = \sum_{\substack{\mathcal{B}' \subset \mathcal{A}' \\ \mathcal{B}' \text{ central}}} (-1)^{|\mathcal{B}'|} \cdot t^{n-\text{rang}(\mathcal{B}')} + \sum_{\substack{\mathcal{B} \subset \mathcal{A} \\ \mathcal{B} \text{ central} \\ H_0 \in \mathcal{B}}} (-1)^{|\mathcal{B}|} \cdot t^{n-\text{rang}(\mathcal{B})}$$

$$\chi(\mathcal{A}, t) = \chi(\mathcal{A}', t) + \sum_{\substack{\mathcal{B} \subset \mathcal{A} \\ \mathcal{B} \text{ central} \\ H_0 \in \mathcal{B}}} (-1)^{|\mathcal{B}|} \cdot t^{n-\text{rang}(\mathcal{B})}$$

ainsi pour démontrer l'égalité demandée, il faut montrer que la dernière somme vaut $-\chi(\mathcal{A}^n, t)$.

Or, à chaque arrangement central $\{H_0, H_1, \dots, H_k\}$ de \mathcal{A} correspond en prenant la trace sur H_0 un arrangement central de \mathcal{A}^n : $\{H_0 \cap H_1, \dots, H_0 \cap H_k\}$.

Nous pouvons donc écrire :

$$\begin{aligned} \sum_{\substack{\mathcal{B} \subset \mathcal{A} \\ \mathcal{B} \text{ central} \\ H_0 \in \mathcal{B}}} (-1)^{|\mathcal{B}|} \cdot t^{n-\text{rang}(\mathcal{B})} &= \sum_{\substack{\mathcal{B}_1 \subset \mathcal{A}^n \\ \mathcal{B}_1 \text{ central}}} \sum_{\substack{\mathcal{B} \subset \mathcal{A} \\ \mathcal{B} \text{ central}, H_0 \in \mathcal{B} \\ \text{la trace de } \mathcal{B} \text{ sur } H_0 \text{ est } \mathcal{B}_1}} (-1)^{|\mathcal{B}|} \cdot t^{n-\text{rang}(\mathcal{B})} \\ \sum_{\substack{\mathcal{B} \subset \mathcal{A} \\ \mathcal{B} \text{ central} \\ H_0 \in \mathcal{B}}} (-1)^{|\mathcal{B}|} \cdot t^{n-\text{rang}(\mathcal{B})} &= \sum_{\substack{\mathcal{B}_1 \subset \mathcal{A}^n \\ \mathcal{B}_1 \text{ central}}} t^{n-\text{rang}(\mathcal{B}_1)} \cdot \sum_{\substack{\mathcal{B} \subset \mathcal{A} \\ \mathcal{B} \text{ central}, H_0 \in \mathcal{B} \\ \text{la trace de } \mathcal{B} \text{ sur } H_0 \text{ est } \mathcal{B}_1}} (-1)^{|\mathcal{B}|} \end{aligned}$$

Il suffit donc de montrer que

$$\sum_{\substack{\mathcal{B} \subset \mathcal{A} \\ \mathcal{B} \text{ central}, H_0 \in \mathcal{B} \\ \text{la trace de } \mathcal{B} \text{ sur } H_0 \text{ est } \mathcal{B}_1}} (-1)^{|\mathcal{B}|} = -(-1)^{|\mathcal{B}_1|}.$$

Soit $\mathcal{B}_1 = \{H_1'', H_2'', \dots, H_p''\}$ un arrangement central de \mathcal{A}^n de cardinal p .

Soit $\mathcal{B}_{max} = \{H_0, H_1, \dots, H_{i_1}, H_{i_1+1}, \dots, H_{i_1+i_2}, \dots, H_{i_1+\dots+i_{p-1}}, \dots, H_{i_1+\dots+i_p}\}$ tel que :

- $H_1'' = H_0 \cap H_1 = \dots = H_0 \cap H_{i_1}$ et
 $H_0 \cap H_i \neq H_1'' \quad \forall i \neq 1, \dots, i_1$.
- $H_2'' = H_0 \cap H_{i_1+1} = \dots = H_0 \cap H_{i_1+i_2}$ et
 $H_0 \cap H_i \neq H_2'' \quad \forall i \neq i_1 + 1, \dots, i_1 + i_2$.
- ...

- $H_p'' = H_0 \cap H_{i_1+\dots+i_{p-1}+1} = \dots = H_0 \cap H_{i_1+\dots+i_p}$ et
 $H_0 \cap H_i \neq H_p'' \quad \forall i \neq i_1 + \dots + i_{p-1} + 1, \dots, i_1 + \dots + i_p$.

\mathcal{B}_{max} est central, il possède $1 + i_1 + \dots + i_p$ éléments.

Soit maintenant un arrangement central \mathcal{B} de \mathcal{A} contenant H_0 et tel que sa trace sur H_0 est \mathcal{B}_1 . Pour construire un tel arrangement il suffit de choisir

j_1 hyperplans parmi $\{H_1, \dots, H_{i_1}\} \rightarrow j_1 \in \{1, \dots, i_1\}$

j_2 hyperplans parmi $\{H_{i_1+1}, \dots, H_{i_1+i_2}\} \rightarrow j_2 \in \{1, \dots, i_2\}$

...

j_p hyperplans parmi $\{H_{i_1+\dots+i_{p-1}+1}, \dots, H_{i_1+\dots+i_p}\} \rightarrow j_p \in \{1, \dots, i_p\}$

Ainsi :

$$\text{card}(\mathcal{B}) = p + 1 \rightarrow \binom{i_1}{1} \dots \binom{i_p}{1} \text{ possibilités}$$

$$\text{card}(\mathcal{B}) = p + 2 \rightarrow \sum_{\substack{a_1 + \dots + a_p = p+1 \\ a_i \geq 1}} \binom{i_1}{a_1} \dots \binom{i_p}{a_p} \text{ possibilités}$$

...

$$\text{card}(\mathcal{B}) = p + k \rightarrow \sum_{\substack{a_1 + \dots + a_p = p+k-1 \\ a_i \geq 1}} \binom{i_1}{a_1} \dots \binom{i_p}{a_p} \text{ possibilités}$$

...

$\text{card}(\mathcal{B}) = 1 + i_1 + \dots + i_p \rightarrow$ une seule possibilité, c'est \mathcal{B}_{max} .

D'où :

$$\sum_{\substack{\mathcal{B} \subset \mathcal{A} \\ \mathcal{B} \text{ central}, H_0 \in \mathcal{B} \\ \text{la trace de } \mathcal{B} \text{ sur } H_0 \text{ est } \mathcal{B}_1}} (-1)^{|\mathcal{B}|} = \sum_{k=1}^{1+i_1+\dots+i_p-p} (-1)^{p+k} \cdot \sum_{\substack{a_1+\dots+a_p=p+k-1 \\ a_i \geq 1}} \binom{i_1}{a_1} \dots \binom{i_p}{a_p}$$

$$\sum_{\substack{\mathcal{B} \subset \mathcal{A} \\ \mathcal{B} \text{ central}, H_0 \in \mathcal{B} \\ \text{la trace de } \mathcal{B} \text{ sur } H_0 \text{ est } \mathcal{B}_1}} (-1)^{|\mathcal{B}|} = \sum_{k=1}^{1+i_1+\dots+i_p-p} \sum_{\substack{a_1+\dots+a_p=p+k-1 \\ a_i \geq 1}} (-1)^{a_1+\dots+a_p+1} \cdot \binom{i_1}{a_1} \dots \binom{i_p}{a_p}$$

$$\sum_{\substack{\mathcal{B} \subset \mathcal{A} \\ \mathcal{B} \text{ central}, H_0 \in \mathcal{B} \\ \text{la trace de } \mathcal{B} \text{ sur } H_0 \text{ est } \mathcal{B}_1}} (-1)^{|\mathcal{B}|} = - \left(\sum_{1 \leq a_1 \leq i_1} (-1)^{a_1} \cdot \binom{i_1}{a_1} \right) \dots \left(\sum_{1 \leq a_p \leq i_p} (-1)^{a_p} \cdot \binom{i_p}{a_p} \right)$$

$$\sum_{\substack{\mathcal{B} \subset \mathcal{A} \\ \mathcal{B} \text{ central}, H_0 \in \mathcal{B} \\ \text{la trace de } \mathcal{B} \text{ sur } H_0 \text{ est } \mathcal{B}_1}} (-1)^{|\mathcal{B}|} = -(-1)^p \quad \text{car} \quad \sum_{0 \leq j \leq m} (-1)^j \cdot \binom{m}{j} = 0 \quad \forall m \in \mathbb{N}^* .$$

Finalement on a bien :

$$\sum_{\substack{\mathcal{B} \subset \mathcal{A} \\ \mathcal{B} \text{ central}, H_0 \in \mathcal{B} \\ \text{la trace de } \mathcal{B} \text{ sur } H_0 \text{ est } \mathcal{B}_1}} (-1)^{|\mathcal{B}|} = -(-1)^{|\mathcal{B}_1|}$$

ce qui termine la démonstration du théorème.

Remarque 6.8 Dans le livre de Stanley [4] qui nous sert de référence principale, cette preuve n'est pas correcte car l'application qui à un arrangement central \mathcal{B} de \mathcal{A} contenant H_0 associe la trace de \mathcal{B} sur H_0 n'est en réalité pas une bijection entre $\{\mathcal{B} \subset \mathcal{A} \mid \mathcal{B} \text{ central}, H_0 \in \mathcal{B}\}$ et $\{\mathcal{B}_1 \subset \mathcal{A} \mid \mathcal{B}_1 \text{ central}\}$.

7 Application au calcul du nombre de régions

Nous allons voir qu'il est possible de calculer les invariants $r(\mathcal{A})$ et $b(\mathcal{A})$ à partir du polynôme caractéristique d'un arrangement \mathcal{A} de \mathbb{R}^n . C'est le théorème de Thomas Zaslavsky, dont la preuve repose essentiellement sur le théorème d'omission-

restriction.

Théorème 7.1 (théorème de Zaslavsky, 1975)

Soit \mathcal{A} un arrangement dans \mathbb{R}^n , alors

1. $r(\mathcal{A}) = \pi(\mathcal{A}, 1) = (-1)^n \chi(\mathcal{A}, -1)$
2. $b(\mathcal{A}) = |\pi(\mathcal{A}, -1)| = (-1)^{\text{rang}(\mathcal{A})} \chi(\mathcal{A}, 1)$

Démonstration :

1. Posons $\rho(\mathcal{A}) = (-1)^n \chi(\mathcal{A}, -1)$, $\beta(\mathcal{A}) = (-1)^{\text{rang}(\mathcal{A})} \chi(\mathcal{A}, 1)$.

On a que $\rho(\mathcal{A}) = \rho(\mathcal{A}') + \rho(\mathcal{A}'')$ (*)

Pour voir cela, on utilise le théorème d'omission-restriction 6.1 qui dit que $\chi(\mathcal{A}, -1) = \chi(\mathcal{A}', -1) - \chi(\mathcal{A}'', -1)$ puis on multiplie les membres de cette égalité par $(-1)^n$.

On conclut en utilisant : $\rho(\mathcal{A}'') = (-1)^{n-1} \chi(\mathcal{A}'', -1)$.

Comme $|\mathcal{A}'| < |\mathcal{A}|$ et $|\mathcal{A}''| < |\mathcal{A}|$, on peut faire une démonstration par récurrence sur $|\mathcal{A}|$.

– Si $|\mathcal{A}| = 0$, alors $\mathcal{A} = \emptyset$ et $L(\mathcal{A}) = \mathbb{R}^n$. Ainsi $\chi(\mathcal{A}, t) = \mu_{L(\mathcal{A})}(\mathbb{R}^n) t^n = t^n$, $\rho(\mathcal{A}) = 1$. Or, $M(\mathcal{A}) = \mathbb{R}^n$ est connexe et on a bien $r(\mathcal{A}) = 1$.

– Supposons qu'il existe $N \in \mathbb{N}$ tel que 1. est vérifié pour tout arrangement \mathcal{A} tel que $|\mathcal{A}| \leq N$. Montrons alors 1. pour un arrangement \mathcal{A} de cardinal $N + 1$:

Comme $|\mathcal{A}'| \leq N$ et $|\mathcal{A}''| \leq N$ on peut utiliser l'hypothèse de récurrence sur \mathcal{A}' et \mathcal{A}'' ($\rho(\mathcal{A}') = r(\mathcal{A}')$, $\rho(\mathcal{A}'') = r(\mathcal{A}'')$). Avec la relation (*) on trouve directement le résultat cherché car $r(\mathcal{A}) = r(\mathcal{A}') + r(\mathcal{A}'')$ d'après le lemme 5.5.

2. Posons $\beta(\mathcal{A}) = (-1)^{\text{rang}(\mathcal{A})} \chi(\mathcal{A}, 1)$.

Rappelons que $\text{rang}(\mathcal{A}) = \text{rang}(\mathcal{A}'') + 1$.

Comme $|\mathcal{A}'| < |\mathcal{A}|$ et $|\mathcal{A}''| < |\mathcal{A}|$, montrons par récurrence sur $|\mathcal{A}|$ que $\beta(\mathcal{A}) = b(\mathcal{A})$ (**):

– si $|\mathcal{A}| = 0$, $\mathcal{A} = \emptyset$, $\tilde{V}_{\mathcal{A}} = \mathbb{R}^n$, $\tilde{V}_{\mathcal{A}}^{\perp} = \{0\}$, $\text{rang}(\mathcal{A}) = 0$ et $L(\mathcal{A}) = \mathbb{R}^n$.

Ainsi $\beta(\mathcal{A}) = 1$, ce qui est correct, car \mathbb{R}^n est la seule région de \mathcal{A} et elle est relativement bornée car $\mathbb{R}^n \cap \{0\} = \{0\}$ est borné.

– Supposons qu'il existe un $N \in \mathbb{N}$ tel que (**) est vérifié pour tout arrangement de cardinal inférieur ou égal à N .

Soit \mathcal{A} un arrangement de cardinal $N + 1$.

(a) si $\text{rang}(\mathcal{A}) = \text{rang}(\mathcal{A}')$, on a que

$\beta(\mathcal{A}) = (-1)^{\text{rang}(\mathcal{A})} \chi(\mathcal{A}, 1) = (-1)^{\text{rang}(\mathcal{A})} \chi(\mathcal{A}', 1) - (-1)^{\text{rang}(\mathcal{A})} \chi(\mathcal{A}'', 1)$ d'après le théorème d'omission-restriction.

Or $\text{rang}(\mathcal{A}) = \text{rang}(\mathcal{A}') = \text{rang}(\mathcal{A}'') + 1$,
donc $\beta(\mathcal{A}) = \beta(\mathcal{A}') + \beta(\mathcal{A}'') = b(\mathcal{A}') + b(\mathcal{A}'')$ par hypothèse de récurrence.

Enfin, $\beta(\mathcal{A}) = b(\mathcal{A})$ d'après le lemme 5.5.

- (b) si $\text{rang}(\mathcal{A}) = \text{rang}(\mathcal{A}') + 1$, on sait d'après le lemme 5.5 que $b(\mathcal{A}) = 0$. On a toujours $\chi(\mathcal{A}, 1) = \chi(\mathcal{A}', 1) - \chi(\mathcal{A}'', 1)$, donc $\beta(\mathcal{A}) = (-1)^{\text{rang}(\mathcal{A})} \chi(\mathcal{A}, 1) = (-1)^{\text{rang}(\mathcal{A}'+1)} \chi(\mathcal{A}', 1) - (-1)^{\text{rang}(\mathcal{A}''+1)} \chi(\mathcal{A}'', 1)$, d'où :

$$\beta(\mathcal{A}) = -\beta(\mathcal{A}') + \beta(\mathcal{A}'').$$

Il suffit donc de montrer que $\beta(\mathcal{A}') = \beta(\mathcal{A}'') \Leftrightarrow \chi(\mathcal{A}', 1) = \chi(\mathcal{A}'', 1)$ car ici $\text{rang}(\mathcal{A}') = \text{rang}(\mathcal{A}'')$.

Or on a un isomorphisme de treillis ϕ entre $L(\mathcal{A}')$ et $L(\mathcal{A}'')$ tel que :

$$\phi(X) = H_0 \cap X \quad \forall X \in L(\mathcal{A}')$$

En effet, l'écriture d'un élément $H_0 \cap X$ de $L(\mathcal{A}'')$ est unique puisque $\text{rang}(\mathcal{A}') = \text{rang}(\mathcal{A}'') \Rightarrow |\mathcal{A}'| = |\mathcal{A}''| \Rightarrow |L(\mathcal{A}')| = |L(\mathcal{A}'')|$. Ces deux treillis étant isomorphes, ils ont la même fonction caractéristique ce qui permet de conclure.

Théorème 7.2 (*formule de Roberts, 1889*)

Soit $\mathcal{A} = \{d_1, d_2, \dots, d_n\}$ un arrangement de n droites dans \mathbb{R}^2 possédant p familles de droites parallèles de b_1, \dots, b_p éléments et m points x_1, \dots, x_m de multiplicité $a_1 \geq 3, \dots, a_m \geq 3$. On a que :

$$\begin{aligned} - r(\mathcal{A}) &= 1 + n + \binom{n}{2} - \sum_{j=1}^p \binom{b_j}{2} - \sum_{i=1}^m \binom{a_i-1}{2}. \\ - b(\mathcal{A}) &= 1 - n + \binom{n}{2} - \sum_{j=1}^p \binom{b_j}{2} - \sum_{i=1}^m \binom{a_i-1}{2}. \end{aligned}$$

Démonstration :

Les éléments de $L(\mathcal{A})$ sont :

- \mathbb{R}^2 de rang 0, avec $\mu_{L(\mathcal{A})}(\mathbb{R}^2) = 1$.
- les droites d_1, \dots, d_n de rang 1, avec $\mu_{L(\mathcal{A})}(d_i) = -1 \forall i$.
- les points d'intersection p_j de multiplicité 2, de rang 2, avec $\mu_{L(\mathcal{A})}(p_j) = 1 \forall j$.

En effet, $\mu_{L(\mathcal{A})}(p_j) = C_0(\bar{0}, p_j) - C_1(\bar{0}, p_j) + C_2(\bar{0}, p_j)$.

Or $C_2(\bar{0}, p_j) = 2$ car si d_{i_1}, d_{i_2} sont les deux droites qui passent par p_j , alors on a bien deux chaînes de longueur 2 : $\bar{0} = \mathbb{R}^2 < d_{i_1} < p_j$ et $\mathbb{R}^2 < d_{i_2} < p_j$.

Ainsi, $\mu_{L(\mathcal{A})}(p_j) = 0 - 1 + 2 = 1 \forall j$.

– les points d'intersection x_l de multiplicité $a_l \geq 3$, de rang 2,

avec $\mu_{L(\mathcal{A})}(x_l) = a_l - 1 \forall l$.

En effet, $\mu_{L(\mathcal{A})}(x_l) = C_0(\bar{0}, x_l) - C_1(\bar{0}, x_l) + C_2(\bar{0}, x_l)$.

Or $C_2(\bar{0}, x_l) = a_l$ car si $d_{i_1}, \dots, d_{i_{a_l}}$ sont les a_l droites qui passent par x_l , alors on a exactement a_l chaînes de longueur 2 :

$$\mathbb{R}^2 < d_{i_1} < x_l, \dots, \mathbb{R}^2 < d_{i_{a_l}} < x_l.$$

Ainsi, $\mu_{L(\mathcal{A})}(x_l) = 0 - 1 + a_l = a_l - 1 \forall l$.

Or, on va montrer qu'il y a $\binom{n}{2} - \sum_{j=1}^p \binom{b_j}{2} - \sum_{i=1}^m \binom{a_i}{2} + m$ points d'intersection.

On montre ce résultat en utilisant le fait que si on a déjà k droites d_1, \dots, d_k , alors l'ajout d'une $k + 1$ -ième droite d_{k+1} va créer :

$$k - |\{ \text{droites parallèles à } d_{k+1} \}| - \sum_{y \in d_{k+1}} m_k(y)$$

points d'intersection supplémentaires, où $m_k(y)$ est la multiplicité de y dans $\mathcal{A}_k = \{d_1, \dots, d_k\}$.

Ainsi, si à chaque étape on place une droite supplémentaire, et si N_k est le nombre de points d'intersection obtenus à l'étape k , alors on a :

$$N_{k+1} = N_k + k - |\{ \text{droites parallèles à } d_{k+1} \}| - \sum_{y \in d_{k+1}} m_k(y).$$

A la dernière étape on trouve :

$$N_n = N_{n-1} + n - 1 - |\{ \text{droites parallèles } d_n \}| - \sum_{y \in d_n} m_{n-1}(y).$$

Il suffit ensuite de sommer tous les termes et de séparer les termes positifs des termes négatifs.

Les termes positifs sont : $1 + 2 + 3 + \dots + n - 1 = \frac{n(n-1)}{2} = \binom{n}{2}$.

Les termes négatifs sont :

– $1 + 2 + \dots + b_1 - 1 = \binom{b_1}{2}$, correspondant à la famille de b_1 droites parallèles.

⋮

– $1 + 2 + \dots + b_p - 1 = \binom{b_p}{2}$, correspondant à la famille de b_p droites parallèles.

– $2 + \dots + a_1 - 1 = \binom{a_1}{2} - 1$, correspondant au point x_1 qui apparaît d'abord comme un point double, puis comme un point de multiplicité 3, ..., finalement comme un point de multiplicité $a_1 - 1$.

⋮

– $2 + \dots + a_m - 1 = \binom{a_m}{2} - 1$, correspondant au point x_m qui apparaît d'abord comme un point double, puis comme un point de multiplicité 3, ..., finalement comme un point de multiplicité $a_m - 1$.

Donc le nombre de points d'intersection est :

$$N_n = \binom{n}{2} - \sum_{j=1}^p \binom{b_j}{2} - \sum_{i=1}^m \left(\binom{a_i}{2} - 1 \right) = \binom{n}{2} - \sum_{j=1}^p \binom{b_j}{2} - \sum_{i=1}^m \binom{a_i}{2} + m,$$

et le nombre de points doubles est :

$$N_n - m = \binom{n}{2} - \sum_{j=1}^p \binom{b_j}{2} - \sum_{i=1}^m \binom{a_i}{2}.$$

Ainsi, on obtient :

$$\begin{aligned} \pi(\mathcal{A}, t) &= \mu_{L(\mathcal{A})}(\mathbb{R}^2) + \sum_{i=1}^n \mu_{L(\mathcal{A})}(d_i)(-t) + \sum_j \mu_{L(\mathcal{A})}(p_j)(-t)^2 + \sum_{l=1}^m \mu_{L(\mathcal{A})}(x_l)(-t)^2 \\ &= 1 + nt + (N_n - m)(-t)^2 + \sum_{l=1}^m (a_l - 1)(-t)^2 \\ &= 1 + nt + \left(\binom{n}{2} - \sum_{j=1}^p \binom{b_j}{2} - \sum_{i=1}^m \binom{a_i - 1}{2} \right) t^2. \end{aligned}$$

Enfin, en utilisant le théorème 7.1 on trouve :

$$\begin{aligned} - r(\mathcal{A}) &= \pi(\mathcal{A}, 1) = 1 + n + \binom{n}{2} - \sum_{j=1}^p \binom{b_j}{2} - \sum_{i=1}^m \binom{a_i - 1}{2}. \\ - b(\mathcal{A}) &= |\pi(\mathcal{A}, -1)| = 1 - n + \binom{n}{2} - \sum_{j=1}^p \binom{b_j}{2} - \sum_{i=1}^m \binom{a_i - 1}{2}. \end{aligned}$$

8 Arrangements et corps finis

8.1 Arrangements d'hyperplans dans \mathbb{F}_q^n

Soit p un nombre premier, $q = p^s$ où $s \in \mathbb{N}^*$.

Rappelons que $\mathbb{F}_q = \{x \in \overline{\mathbb{F}_p} \mid x^q - x = 0\}$ est l'unique corps à q éléments.

Exemple 8.2 On a par exemple :

$$\begin{aligned} - \mathbb{F}_p &= \mathbb{Z}/p\mathbb{Z} = \{1, \dots, p-1\}. \\ - \mathbb{F}_4 &= \mathbb{F}_2[x]/(x^2 + x + 1). \end{aligned}$$

Théorème 8.3 Soit k un corps fini, alors le groupe multiplicatif (k^*, \cdot) est cyclique.

Pour démontrer ce théorème nous avons besoin du lemme suivant :

Lemme 8.4 Soit G un groupe multiplicatif fini d'ordre m , tel que pour tout diviseur d de m dans \mathbb{N}^* , le nombre d'éléments x de G vérifiant $x^d - 1 = 0$ est au plus égale à d ; alors G est cyclique.

Démonstration :

Soit $d \in \mathbb{N}^*$, tel que $d|n$. Notons $\lambda(d)$ le nombre d'éléments de G d'ordre d .

On a que $\lambda(d) \geq 0$ et $m = \sum_{\substack{d|m \\ 1 \leq d \leq m}} \lambda(d)$, l'ordre d'un élément de G divisant nécessairement m .

Montrons que :

$$(1 \leq d \leq m, d|m, \text{ et } \lambda(d) \neq 0) \implies \lambda(d) = \varphi(d)$$

où φ est la fonction d'Euler.

Si $d|m$, $1 \leq d \leq m$, et $\lambda(d) \neq 0$, alors il existe au moins un élément y de G d'ordre d .

$\langle y \rangle$, le sous groupe de G engendré par y , est cyclique et d'ordre d .

Or tout $x \in \langle y \rangle$ vérifie $x^d - 1 = 0$, mais par hypothèse, il y a au plus d éléments dans G qui vérifient cette équation.

Ainsi, les seuls éléments de G vérifiant $x^d - 1 = 0$ sont les éléments de $\langle y \rangle$, et donc les éléments d'ordre d de G sont les éléments d'ordre d de $\langle y \rangle$ et il y en a $\varphi(d)$ par définition de la fonction d'Euler.

On a donc bien $\lambda(d) = \varphi(d)$.

Montrons maintenant que $\lambda(m) \neq 0$, ce qui équivaut à dire que G est cyclique.

Rappelons que $m = \sum_{\substack{d|m \\ 1 \leq d \leq m}} \varphi(d)$, et que $\varphi(d) > 0 \forall d|m, 1 \leq d \leq m$.

On a que

$$\lambda(m) = m - \sum_{\substack{d|m \\ 1 \leq d \leq m-1}} \lambda(d) \geq m - \sum_{\substack{d|m \\ 1 \leq d \leq m-1}} \varphi(d) = \varphi(m) > 0.$$

Démontrons maintenant le théorème 8.3 :

Soit k un corps fini de cardinal N , alors k^* a pour cardinal $N - 1$.

Pour tout diviseur d de $N - 1$ dans \mathbb{N}^* , le polynôme $X^d - 1$ a au plus d racines dans k , et plus précisément dans k^* car 0 n'est pas l'une de ces racines.

On en déduit que le groupe fini k^* satisfait les hypothèses du lemme 8.4, donc que k^* est cyclique.

En particulier, on a que (\mathbb{F}_q^*, \cdot) est cyclique d'ordre $q - 1$.

Remarque 8.5 Il y a exactement $\frac{q-1}{2}$ carrés dans \mathbb{F}_q^* .

Démonstration :

Soit $(\mathbb{F}_q^*)^2 = \{x^2 \mid x \in \mathbb{F}_q^*\}$.

L'application $\phi : \mathbb{F}_q^* \mapsto (\mathbb{F}_q^*)^2$ telle que $\phi(x) = x^2$ est un morphisme de groupe surjectif, de noyau $\{1, -1\}$.

Ainsi, $|(\mathbb{F}_q^*)^2| = \frac{|\mathbb{F}_q^*|}{2} = \frac{q-1}{2}$.

Définition 8.6 *On dit qu'un arrangement \mathcal{A} est défini sur \mathbb{Q} si tout hyperplan H de \mathcal{A} est défini sur \mathbb{Q} , donc admet une équation*

$$H : a_1x_1 + \dots + a_nx_n = b, \quad \text{où } a_i, b \in \mathbb{Q}.$$

Soit \mathcal{A} un arrangement d'hyperplans dans \mathbb{R}^n défini sur \mathbb{Q} . Chaque hyperplan H de \mathcal{A} est défini par une équation linéaire $l_H(x)$:

$$H = \{x \in \mathbb{R}^n \mid a_1^Hx_1 + \dots + a_n^Hx_n = b_H\}, \text{ avec } a_i^H, b_H \in \mathbb{Q}.$$

On peut supposer que les a_j^H et les b_H sont dans \mathbb{Z} .

On peut, pour tout nombre premier p , considérer l'arrangement $\hat{\mathcal{A}}_q$ de \mathbb{F}_q^n dont les hyperplans \hat{H} sont définis par :

$$\hat{H} = \{x \in \mathbb{F}_q^n \mid \hat{a}_1^Hx_1 + \dots + \hat{a}_n^Hx_n = \hat{b}_H\}, \text{ où } \hat{a}_j^H \text{ est la classe de } a_j^H \text{ dans } \mathbb{F}_q,$$

et \hat{b}_H est la classe de b_H dans \mathbb{F}_q selon le schéma suivant où \mathbb{F}_q est une extension du corps \mathbb{F}_p :

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{F}_p \hookrightarrow \mathbb{F}_q \\ & & x \mapsto \hat{x} \end{array}$$

Le but de cette partie est de calculer $|M(\hat{\mathcal{A}}_q)|$, avec $M(\hat{\mathcal{A}}_q) = \mathbb{F}_q^n \setminus \cup_{\hat{H} \in \hat{\mathcal{A}}_q} \hat{H}$.

Définition 8.7 *Soit \mathcal{A} un arrangement défini sur \mathbb{Z} .*

On dit que \mathcal{A} a une bonne réduction modulo p si il existe un isomorphisme naturel de semi-treillis :

$$L(\mathcal{A}) \cong L(\hat{\mathcal{A}}_q).$$

Lemme 8.8 *Soit \mathcal{A} un arrangement défini sur \mathbb{Z} , alors \mathcal{A} admet une bonne réduction modulo p pour tous les nombres premiers p , sauf peut-être pour un nombre fini de nombres premiers.*

Démonstration :

On a que :

$$L(\mathcal{A}) \cong L(\hat{\mathcal{A}}_q) \Leftrightarrow \begin{cases} H_{i_1} \cap \dots \cap H_{i_l} \in L(\mathcal{A}) \Leftrightarrow \hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_l} \in L(\hat{\mathcal{A}}_q). \\ \dim(H_{i_1} \cap \dots \cap H_{i_l}) = \dim(\hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_l}) \quad \forall H_{i_1} \cap \dots \cap H_{i_l} \in L(\mathcal{A}). \end{cases}$$

Soient $v_{i_j} \in \mathbb{Z}^n$, $a_{i_j} \in \mathbb{Z}$ tels que $H_{i_j} = \{x \in \mathbb{Z}^n \mid v_{i_j1}x_1 + \dots + v_{i_jn}x_n = a_{i_j}\}$.
A chaque élément $H_{i_1} \cap \dots \cap H_{i_l}$ de $L(\mathcal{A})$, on associe la matrice $R_{\{i_1, \dots, i_j\}}$:

$$\begin{pmatrix} v_{i_11} & \cdots & v_{i_1n} & a_{i_1} \\ \vdots & & \vdots & \vdots \\ v_{i_l1} & \cdots & v_{i_ln} & a_{i_l} \end{pmatrix}$$

et la matrice $C_{\{i_1, \dots, i_j\}}$:

$$\begin{pmatrix} v_{i_11} & \cdots & v_{i_1n} \\ \vdots & & \vdots \\ v_{i_l1} & \cdots & v_{i_ln} \end{pmatrix}$$

A chaque élément $\hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_l}$ de $L(\hat{\mathcal{A}}_q)$, on associe la matrice $\hat{R}_{\{i_1, \dots, i_j\}}$:

$$\begin{pmatrix} \hat{v}_{i_11} & \cdots & \hat{v}_{i_1n} & \hat{a}_{i_1} \\ \vdots & & \vdots & \vdots \\ \hat{v}_{i_l1} & \cdots & \hat{v}_{i_ln} & \hat{a}_{i_l} \end{pmatrix}$$

et la matrice $\hat{C}_{\{i_1, \dots, i_j\}}$:

$$\begin{pmatrix} \hat{v}_{i_11} & \cdots & \hat{v}_{i_1n} \\ \vdots & & \vdots \\ \hat{v}_{i_l1} & \cdots & \hat{v}_{i_ln} \end{pmatrix}$$

D'après le théorème de Cramer on a que :

$$\text{rang}(R_{\{i_1, \dots, i_j\}}) = \text{rang}(C_{\{i_1, \dots, i_j\}}) \Leftrightarrow H_{i_1} \cap \dots \cap H_{i_l} \neq \emptyset \Leftrightarrow H_{i_1} \cap \dots \cap H_{i_l} \in L(\mathcal{A})$$

et de même,

$$\text{rang}(\hat{R}_{\{i_1, \dots, i_j\}}) = \text{rang}(\hat{C}_{\{i_1, \dots, i_j\}}) \Leftrightarrow \hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_l} \neq \emptyset \Leftrightarrow \hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_l} \in L(\hat{\mathcal{A}}_q)$$

Ainsi lorsque $H_{i_1} \cap \dots \cap H_{i_l} \in L(\mathcal{A})$ et $\hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_l} \in L(\hat{\mathcal{A}}_q)$, on a :

$$\dim(H_{i_1} \cap \dots \cap H_{i_l}) = n - \text{rang}(C_{\{i_1, \dots, i_j\}})$$

et aussi

$$\dim(\hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_l}) = n - \text{rang}(\hat{C}_{\{i_1, \dots, i_j\}}).$$

Posons maintenant :

$$E = \{p \text{ premiers} \mid L(\mathcal{A}) \not\cong L(\hat{\mathcal{A}}_q)\}.$$

$$E_1 = \{p \text{ premiers} \mid \exists \{i_1, \dots, i_l\} \text{ avec } H_{i_1} \cap \dots \cap H_{i_l} \in L(\mathcal{A}) \text{ et } \hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_l} \notin L(\hat{\mathcal{A}}_q)\}.$$

$$E_2 = \{p \text{ premiers} \mid \exists \{i_1, \dots, i_l\} \text{ avec } H_{i_1} \cap \dots \cap H_{i_l} \notin L(\mathcal{A}) \text{ et } \hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_l} \in L(\hat{\mathcal{A}}_q)\}.$$

$$E_3 = \{p \text{ premiers} \mid \exists \{i_1, \dots, i_l\} \text{ avec } H_{i_1} \cap \dots \cap H_{i_l} \in L(\mathcal{A}), \hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_l} \in L(\hat{\mathcal{A}}_q), \text{ et } \text{rang}(C_{\{i_1, \dots, i_l\}}) \neq \text{rang}(\hat{C}_{\{i_1, \dots, i_l\}})\}.$$

On a que $E = E_1 \cup E_2 \cup E_3$.

Montrons que $|E| < \infty$:

– $|E_1| < \infty$:

Pour chaque $\{i_1, \dots, i_l\}$ tel que $H_{i_1} \cap \dots \cap H_{i_l} \in L(\mathcal{A})$, on se demande combien de p premiers sont tels que $\hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_l} \notin L(\hat{\mathcal{A}}_q)$.

Or $\hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_l} \notin L(\hat{\mathcal{A}}_q) \Leftrightarrow \text{rang}(\hat{R}_{\{i_1, \dots, i_l\}}) \neq \text{rang}(\hat{C}_{\{i_1, \dots, i_l\}})$.

Posons $S_{\{i_1, \dots, i_l\}} = \{D \text{ matrices carrées extraites de } \hat{R}_{\{i_1, \dots, i_l\}} \text{ de taille } \text{rang}(\hat{C}_{\{i_1, \dots, i_l\}})\}$.

Ainsi, $\text{rang}(\hat{R}_{\{i_1, \dots, i_l\}}) \neq \text{rang}(\hat{C}_{\{i_1, \dots, i_l\}}) \Leftrightarrow \det(D) = 0 \forall D \in S_{\{i_1, \dots, i_l\}}$

$\Leftrightarrow p \mid \det(D) \forall D \in S_{\{i_1, \dots, i_l\}}$.

Seul un nombre fini de p premiers, s'il y en a, peut réaliser cette hypothèse (car p est majoré par $\max \{\det(D) \mid D \in S_{\{i_1, \dots, i_l\}}\}$), donc $|E_1| < \infty$.

– $|E_2| < \infty$:

Pour chaque $\{i_1, \dots, i_l\}$ tel que $H_{i_1} \cap \dots \cap H_{i_l} = \emptyset$, on se demande combien de p premiers sont tels que $\hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_l} \in L(\hat{\mathcal{A}}_q)$.

Or $\hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_l} \in L(\hat{\mathcal{A}}_q) \Leftrightarrow \text{rang}(\hat{R}_{\{i_1, \dots, i_l\}}) = \text{rang}(\hat{C}_{\{i_1, \dots, i_l\}})$.

Posons $S_{\{i_1, \dots, i_l\}} = \{D \text{ matrices carrées extraites de } \hat{R}_{\{i_1, \dots, i_l\}} \text{ de taille } \text{rang}(\hat{C}_{\{i_1, \dots, i_l\}})\}$.

$T_{\{i_1, \dots, i_l\}} = \{Q \text{ matrices carrées extraites de } \hat{R}_{\{i_1, \dots, i_l\}} \text{ de taille } > \text{rang}(\hat{C}_{\{i_1, \dots, i_l\}})\}$.

Ainsi,

$\text{rang}(\hat{R}_{\{i_1, \dots, i_l\}}) = \text{rang}(\hat{C}_{\{i_1, \dots, i_l\}}) \Leftrightarrow (\exists D \in S \mid \det(D) \neq 0, \det(Q) = 0 \forall Q \in T_{\{i_1, \dots, i_l\}})$

$\Leftrightarrow (\exists D \in S \mid p \nmid \det(D), p \mid \det(Q) \forall Q \in T_{\{i_1, \dots, i_l\}})$.

Seul un nombre fini de p premiers, s'il y en a, peut réaliser cette hypothèse (car p est majoré par $\max \{\det(Q) \mid Q \in T_{\{i_1, \dots, i_l\}}\}$), donc $|E_2| < \infty$.

– $|E_3| < \infty$:

Pour chaque $\{i_1, \dots, i_l\}$ tel que $H_{i_1} \cap \dots \cap H_{i_l} \in L(\mathcal{A})$, on se demande combien de p premiers sont tels que $\hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_l} \in L(\hat{\mathcal{A}}_q)$, et $\text{rang}(C_{\{i_1, \dots, i_l\}}) \neq \text{rang}(\hat{C}_{\{i_1, \dots, i_l\}})$.

$$\text{Or, } \begin{cases} \hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_l} \in L(\hat{\mathcal{A}}_q) \\ \text{rang}(C_{\{i_1, \dots, i_l\}}) \neq \text{rang}(\hat{C}_{\{i_1, \dots, i_l\}}) \end{cases} \Leftrightarrow \begin{cases} \text{rang}(\hat{R}_{\{i_1, \dots, i_l\}}) = \text{rang}(\hat{C}_{\{i_1, \dots, i_l\}}) \\ \text{rang}(C_{\{i_1, \dots, i_l\}}) \neq \text{rang}(\hat{C}_{\{i_1, \dots, i_l\}}) \end{cases}$$

Le même type d'argument que dans le point précédent permet de montrer que la première équation, $\text{rang}(\hat{R}_{\{i_1, \dots, i_l\}}) = \text{rang}(\hat{C}_{\{i_1, \dots, i_l\}})$, n'est réalisée, si c'est possible que pour un nombre fini de nombres premiers p .

Posons $S_{\{i_1, \dots, i_l\}} = \{D \text{ matrices carrées extraites de } \hat{C}_{\{i_1, \dots, i_l\}} \text{ de taille } \text{rang}(C_{\{i_1, \dots, i_l\}})\}$.

On a alors :

$$\begin{aligned} \text{rang}(C_{\{i_1, \dots, i_l\}}) \neq \text{rang}(\hat{C}_{\{i_1, \dots, i_l\}}) &\Leftrightarrow \det(D) = 0 \quad \forall D \in S_{\{i_1, \dots, i_l\}} \\ &\Leftrightarrow p | \det(D) \quad \forall D \in S_{\{i_1, \dots, i_l\}}. \end{aligned}$$

Seul un nombre fini de p premiers, s'il y en a, peuvent réaliser cette hypothèse, donc seul un nombre fini de p premiers, s'il y en a, peuvent réaliser les deux hypothèses à la fois, donc $|E_3| < \infty$.

Conclusion : $|E| = |E_1 \cup E_2 \cup E_3| \leq |E_1| + |E_2| + |E_3| < \infty$.

Théorème 8.9 *Soit \mathcal{A} un arrangement défini sur \mathbb{Q} qui admet une bonne réduction modulo p .*

Soit $q = p^s$, $s \in \mathbb{N}^$, alors :*

$$|M(\hat{\mathcal{A}}_q)| = \chi(\mathcal{A}, q). \quad (1)$$

Démonstration :

Préliminaire : montrons que si \mathcal{A} admet une bonne réduction modulo p , il en est de même pour $\mathcal{A}' = \mathcal{A} \setminus \{H_0\}$ et \mathcal{A}'' .

– Si \mathcal{A} admet une bonne réduction modulo p , il en est de même pour \mathcal{A}' .

En effet, tout élément $H_{i_1} \cap \dots \cap H_{i_k}$ de $L(\mathcal{A}')$ peut être vu comme un élément de $L(\mathcal{A})$, donc $\dim(\hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_k}) = \dim(H_{i_1} \cap \dots \cap H_{i_k})$ et on a bien $L(\mathcal{A}') \simeq L(\hat{\mathcal{A}}'_q)$.

– Si \mathcal{A} admet une bonne réduction modulo p , il en est de même pour \mathcal{A}'' .

Soit $v_0 = (v_{01} \dots v_{0n}) \in \mathbb{Q}^n$ le vecteur tel que H_0 est défini par l'équation $v_{01}x_1 + \dots + v_{0n}x_n = 0$.

Pour chaque hyperplan $H_{i_l} \in \mathcal{A}'$, soit $v_{i_l} = (v_{i_l1} \dots v_{i_ln}) \in \mathbb{Q}^n$ le vecteur tel que H_{i_l} est défini par l'équation $v_{i_l1}x_1 + \dots + v_{i_ln}x_n = 0$.

Soit $(H_0 \cap H_{i_1}) \cap \dots \cap (H_0 \cap H_{i_k}) \in L(\mathcal{A}'')$.

Montrons que

$$\dim_{\mathbb{R}^{n-1}}((H_0 \cap H_{i_1}) \cap \dots \cap (H_0 \cap H_{i_k})) = \dim_{\mathbb{F}_q^{n-1}}((\hat{H}_0 \cap \hat{H}_{i_1}) \cap \dots \cap (\hat{H}_0 \cap \hat{H}_{i_k})) :$$

Si $\text{rang} \begin{pmatrix} v_0 \\ v_{i_1} \\ \vdots \\ v_{i_k} \end{pmatrix} = R + 1$, soient alors $H_{j_1}, \dots, H_{j_R} \subset \{H_{i_1}, \dots, H_{i_k}\}$ tels que

$$\text{rang} \begin{pmatrix} v_0 \\ v_{i_1} \\ \vdots \\ v_{i_k} \end{pmatrix} = \text{rang} \begin{pmatrix} v_0 \\ v_{j_1} \\ \vdots \\ v_{j_R} \end{pmatrix}.$$

On a alors $\text{rang} \begin{pmatrix} v_{i_1} \\ \vdots \\ v_{i_k} \end{pmatrix} = R$.

Ainsi, $\text{codim}_{\mathbb{R}^{n-1}}((H_0 \cap H_{i_1}) \cap \dots \cap (H_0 \cap H_{i_k})) = 1 + \text{codim}_{\mathbb{R}^n}(H_{i_1} \cap \dots \cap H_{i_k})$.

De la même façon, on peut montrer que

$$\text{codim}_{\mathbb{F}_q^{n-1}}((\hat{H}_0 \cap \hat{H}_{i_1}) \cap \dots \cap (\hat{H}_0 \cap \hat{H}_{i_k})) = 1 + \text{codim}_{\mathbb{F}_q^n}(\hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_k}).$$

Or $\text{codim}_{\mathbb{R}^n}(H_{i_1} \cap \dots \cap H_{i_k}) = \text{codim}_{\mathbb{F}_q^n}(\hat{H}_{i_1} \cap \dots \cap \hat{H}_{i_k})$ car \mathcal{A} admet une bonne réduction modulo p , donc

$$\text{codim}_{\mathbb{R}^{n-1}}((H_0 \cap H_{i_1}) \cap \dots \cap (H_0 \cap H_{i_k})) = \text{codim}_{\mathbb{F}_q^{n-1}}((\hat{H}_0 \cap \hat{H}_{i_1}) \cap \dots \cap (\hat{H}_0 \cap \hat{H}_{i_k})).$$

Revenons maintenant à notre démonstration :

On sait que $|\mathcal{A}'| < |\mathcal{A}|$ et que $|\mathcal{A}''| < |\mathcal{A}|$. On peut donc effectuer une démonstration par récurrence sur $|\mathcal{A}|$:

- si $|\mathcal{A}| = 0$, alors $\mathcal{A} = \emptyset$ et $L(\mathcal{A}) = \{\mathbb{R}^n\}$. On a que $M(\hat{\mathcal{A}}_q) = \mathbb{F}_q^n$.
Enfin, $\chi(\mathcal{A}, t) = t^n$ et on a bien $|M(\hat{\mathcal{A}}_q)| = q^n$.
- Supposons qu'il existe un $N \in \mathbb{N}$ tel que (1) est vérifié pour tout arrangement de cardinal inférieur ou égal à N .

Soit $\mathcal{A} = \{H_0, H_1, \dots, H_N\}$ un arrangement de cardinal $N + 1$.

On a que $M(\hat{\mathcal{A}}_q) = \{x \in \mathbb{F}_q^n \mid x \notin \hat{H}_1, \dots, x \notin \hat{H}_N\}$

$$= \{x \in \mathbb{F}_q^n \cap \hat{H}_0 \mid x \notin \hat{H}_1, \dots, x \notin \hat{H}_N\} \sqcup \{x \in \mathbb{F}_q^n \setminus \hat{H}_0 \mid x \notin \hat{H}_1, \dots, x \notin \hat{H}_N\}$$

$$= M(\hat{\mathcal{A}}''_q) \sqcup M(\hat{\mathcal{A}}_q).$$

$|M(\hat{\mathcal{A}}_q)| = |M(\hat{\mathcal{A}}'_q)| - |M(\hat{\mathcal{A}}''_q)| = \chi(\mathcal{A}', q) - \chi(\mathcal{A}'', q)$ par hypothèse de récurrence sur \mathcal{A}' et \mathcal{A}'' qui admettent une bonne réduction modulo p .

Enfin, $\chi(\mathcal{A}', q) - \chi(\mathcal{A}'', q) = \chi(\mathcal{A}, q)$ d'après le théorème 6.1 d'omission-restriction.

Exemple 8.10 Dans \mathbb{C}^2 , on considère l'arrangement \mathcal{A} donné par l'équation $Q(x, y) = (x + iy)(x - iy) = 0$ qui n'est pas défini sur \mathbb{Q} .

Ainsi, $\mathcal{A} = \{H_1, H_2\}$ avec $H_1 = \{(x, y) \in \mathbb{C}^2 \mid x + iy = 0\}$,
 $H_2 = \{(x, y) \in \mathbb{C}^2 \mid x - iy = 0\}$.

Soit maintenant p un nombre premier, $q = p^s$ avec $s \in \mathbb{N}^*$.

Comme $Q(x, y) = x^2 + y^2 \in \mathbb{Z}[x, y]$, on peut considérer l'ensemble
 $M(\mathcal{A}, q) = \{(x, y) \in \mathbb{F}_q^2 \mid Q(x, y) \neq 0\} = \mathbb{F}_q^2 \setminus \{(x, y) \in \mathbb{F}_q^2 \mid x^2 + y^2 = 0\}$.

Calculons $|M(\mathcal{A}, q)|$:

Pour cela, posons $E = \{(x, y) \in \mathbb{F}_q^2 \mid x^2 + y^2 = 0\}$.

On a que $|M(\mathcal{A}, q)| = q^2 - |E|$.

Soit $(x, y) \in \mathbb{F}_q^2$, on a que :

$(x, y) \in E \Leftrightarrow (x, y) = (0, 0)$ ou $(x, y) \in \mathbb{F}_q^{*2}, (xy^{-1})^2 + 1 = 0$.

Nous sommes donc amenés à nous demander quant est-ce que -1 est un carré dans F_q^* , or :

-1 est un carré dans $F_q^* \Leftrightarrow \exists \alpha \in F_q^* \mid \alpha^2 = -1$

$\Leftrightarrow \text{car}(F_q) = 2$ ou $\exists \alpha \in F_q^* \mid \text{ord}(\alpha) = 4$

$\Leftrightarrow p = 2$ ou $4 \mid q - 1$.

En effet, si $\text{car}(F_q) = 2$, alors $-x = x \ \forall x \in F_q$ et $-1 = (-1)^2$.

Si non, $\exists \alpha \in F_q^* \mid \text{ord}(\alpha) = 4 \Leftrightarrow 4 \mid q - 1$, car si $\text{ord}(\alpha) = 4$, alors bien sur $4 \mid q - 1 = |F_q^*|$.

Inversement, si $4 \mid q - 1$, alors comme F_q^* est cyclique d'après le théorème 8.3, on peut prendre $\alpha = a^{\frac{q-1}{4}}$, où a est un générateur de F_q^* .

On a donc :

-1 est un carré dans $F_q^* \Leftrightarrow p = 2$ ou $q \equiv 1 \pmod{4}$.

Ainsi, $E = \begin{cases} \{(0, 0)\} \cup \{(-y, y), y \in F_q^*\} & \text{si } p = 2 \\ \{(0, 0)\} & \text{si } p \neq 2, q \equiv 3 \pmod{4} \\ \{(0, 0)\} \cup \{(\alpha y, y), y \in F_q^*\} & \text{si } p \neq 2, q \equiv 1 \pmod{4} \end{cases}$

donc $|E| = \begin{cases} q & \text{si } p = 2 \\ 1 & \text{si } p \neq 2, q \equiv 3 \pmod{4} \\ q & \text{si } p \neq 2, q \equiv 1 \pmod{4} \end{cases}$

enfin, $|M(\mathcal{A}, q)| = \begin{cases} q^2 - q & \text{si } p = 2 \\ q^2 - 1 & \text{si } p \neq 2, q \equiv 3 \pmod{4} \\ q^2 - q & \text{si } p \neq 2, q \equiv 1 \pmod{4} \end{cases}$

Cet exemple montre que l'hypothèse \mathcal{A} est défini sur \mathbb{Q} est indispensable pour appliquer le théorème 8.9. Ainsi ici $\chi(\mathcal{A}, t) = t^2 - 2t + 1$, et $\chi(\mathcal{A}, q) \neq |M(\mathcal{A}, q)| \ \forall q$.

8.11 Arrangements projectifs

Soit $Q \in \mathbb{Z}[x_1, \dots, x_n]$ un polynôme homogène. On pose :
 $M(Q, q) := \{(x_1, \dots, x_n) \in \mathbb{F}_q^n \mid Q(x_1, \dots, x_n) \neq 0\}$,

$M'(Q, q) := \{(x_1 : \dots : x_n) \in \mathbb{P}(\mathbb{F}_q^n) \mid Q(x_1, \dots, x_n) \neq 0\}$.

Alors le théorème 8.9 nous donne le résultat suivant :

Proposition 8.12 *On a que :*

$$|M(Q, q)| = (q - 1) \cdot |M'(Q, q)|.$$

En particulier, si $Q(x) = 0$ est l'équation de définition d'un arrangement central dans \mathbb{C}^n défini sur \mathbb{Z} et ayant une bonne réduction modulo p , alors :

$$|M'(Q, q)| = \frac{\chi(\mathcal{A}, q)}{q-1}.$$

Exemple 8.13 *Appliquons ce théorème aux arrangements suivants :*

1. l'arrangement de Boole dans \mathbb{C}^n :

$Q(x_1, \dots, x_n) = x_1 x_2 \dots x_n \in \mathbb{Z}[x_1, \dots, x_n]$ est un polynôme homogène qui définit l'arrangement de Boole \mathcal{A} .

L'arrangement de Boole a une bonne réduction modulo p pour tout p premier.

En effet, les matrices définissant les éléments de $L(\mathcal{A})$ ont des lignes contenant des 0 et un seul 1. Les mineurs de ces matrices valent donc 0, 1 ou -1, et leur rang reste le même que ce soit dans \mathbb{Z} ou dans \mathbb{F}_q . Ainsi,

$$\begin{aligned} |\{(x_1, \dots, x_n) \in \mathbb{F}_q^n \mid x_1 x_2 \dots x_n \neq 0\}| &= \chi(\mathcal{A}, q) = (q - 1)^n, \\ |\{(x_1 : \dots : x_n) \in \mathbb{P}(\mathbb{F}_q^n) \mid x_1 x_2 \dots x_n \neq 0\}| &= \frac{\chi(\mathcal{A}, q)}{q-1} = (q - 1)^{n-1}. \end{aligned}$$

2. l'arrangement des tresses dans \mathbb{C}^n :

$Q(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j) \in \mathbb{Z}[x_1, \dots, x_n]$ est un polynôme homogène qui définit l'arrangement des tresses \mathcal{A} .

L'arrangement des tresses a une bonne réduction modulo p pour tout p premier.

En effet, les matrices définissant les éléments de $L(\mathcal{A})$ ont des lignes contenant des 0, un seul 1, et un seul -1. Les mineurs de ces matrices valent donc 0, 1 ou -1, et leur rang reste le même que ce soit dans \mathbb{Z} ou dans \mathbb{F}_q . Ainsi,

$$\begin{aligned} |\{(x_1, \dots, x_n) \in \mathbb{F}_q^n \mid \prod_{1 \leq i < j \leq n} (x_i - x_j) \neq 0\}| &= \chi(\mathcal{A}, q) \\ &= q(q - 1)(q - 2) \dots (q - n + 1), \\ |\{(x_1 : \dots : x_n) \in \mathbb{P}(\mathbb{F}_q^n) \mid \prod_{1 \leq i < j \leq n} (x_i - x_j) \neq 0\}| &= \frac{\chi(\mathcal{A}, q)}{q-1} \\ &= q(q - 2) \dots (q - n + 1). \end{aligned}$$

3. l'arrangement générique dans \mathbb{C}^n :

Soit \mathcal{A} un arrangement générique dans \mathbb{C}^n défini par un polynôme Q .

On sait, d'après l'exemple 4.10 que $\chi(\mathcal{A}, t) = \sum_{k=0}^n \binom{d}{k} (-1)^k t^{n-k} + \sum_{k=n+1}^d \binom{d}{k} (-1)^k$.

Une division euclidienne donne :

$$\chi(\mathcal{A}, t) = (t-1) \cdot \sum_{k=1}^n \left[\sum_{j=0}^{k-1} \binom{d}{j} (-1)^j \right] t^{n-k}.$$

En utilisant l'égalité

$$\binom{d}{j} = \binom{d-1}{j} + \binom{d-1}{j-1}$$

on trouve que la somme $\sum_{j=0}^{k-1} \binom{d}{j} (-1)^j$ est une somme télescopique valant $(-1)^{k-1} \binom{d-1}{k-1}$. On a donc :

$$\chi(\mathcal{A}, t) = (t-1) \cdot \sum_{k=1}^n (-1)^{k-1} \binom{d-1}{k-1} t^{n-k}.$$

Ainsi, si \mathcal{A} admet une bonne réduction modulo p on a :

$$\begin{aligned} |M(Q, q)| &= \chi(\mathcal{A}, q) = \sum_{k=0}^n \binom{d}{k} (-1)^k q^{n-k} + \sum_{k=n+1}^d \binom{d}{k} (-1)^k. \\ |M'(Q, q)| &= \frac{\chi(\mathcal{A}, q)}{q-1} = \sum_{k=1}^n (-1)^{k-1} \binom{d-1}{k-1} q^{n-k} \\ &= q^{n-1} - \binom{d-1}{1} q^{n-2} + \binom{d-1}{2} q^{n-3} - \dots + (-1)^{n-2} \binom{d-1}{n-2} q + (-1)^{n-1} \binom{d-1}{n-1}. \end{aligned}$$

9 Fibre de Milnor d'un arrangement d'hyperplans

Définition 9.1 Soit $Q \in \mathbb{Z}[x_1, \dots, x_n]$ un polynôme homogène définissant un arrangement d'hyperplans \mathcal{A} dans \mathbb{K}^n .

On appelle fibre de Milnor de \mathcal{A} sur \mathbb{K} l'ensemble

$$F(\mathbb{K}) = \{x \in \mathbb{K}^n \mid Q(x) = 1\}.$$

Définition 9.2 – On dit qu'un arrangement $\mathcal{A} \subset \mathbb{K}^n$ défini par un polynôme $Q(x_1, \dots, x_n) \in \mathbb{K}[x_1, \dots, x_n]$ est irréductible si Q ne peut pas s'écrire sous la forme $Q_1(x_{i_1}, \dots, x_{i_k}) \cdot Q_2(x_{j_1}, \dots, x_{j_l})$ avec $x_{i_s} \neq x_{j_t} \forall i_s, j_t$.

- Si $Q(x_1, \dots, x_n) = \prod_i Q_i(x_{i_1}, \dots, x_{i_{n_i}})$, avec $x_{i_s} \neq x_{i_t} \forall i_s, i_t$ est la décomposition du polynôme Q en produit de polynômes à variables indépendantes, alors la décomposition en facteurs irréductibles de l'arrangement \mathcal{A} est :

$$\mathcal{A} = \otimes_i \mathcal{A}_i \text{ où } \mathcal{A}_i \text{ est défini par } Q_i \forall i.$$

Exemple 9.3 Soit \mathcal{A} l'arrangement de \mathbb{R}^3 défini par le polynôme $Q(x, y, z) = xyz(x - 3z)$. Alors $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2$, où \mathcal{A}_1 est l'arrangement irréductible défini par $Q_1(x, y, z) = y$, \mathcal{A}_2 l'arrangement irréductible défini par $Q_2(x, y, z) = xz(x - 3z)$.

Dans cette dernière partie de notre mémoire, nous allons calculer $|F(\mathbb{F}_q)|$ pour des exemples d'arrangements particuliers, puis nous comparerons les résultats obtenus avec le théorème suivant de Mr Dimca :

Théorème 9.4 Soit $\mathcal{A} \subset \mathbb{R}^n$ un arrangement central défini sur \mathbb{Q} par le polynôme $Q(x_1, \dots, x_n)$.

Soit $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2 \times \dots \times \mathcal{A}_k$ la décomposition en produit de facteurs irréductibles de \mathcal{A} .

Notons $d_i = |\mathcal{A}_i| \forall i$.

On a que :

si $\text{pgcd}(d_1, d_2, \dots, d_k) = 1$, alors pour $q = p^s$ tel que l'arrangement \mathcal{A} a une bonne réduction modulo p , $|F(\mathbb{F}_q)| = \frac{\chi(\mathcal{A}, q)}{q-1} = |M'(Q, q)|$.

Remarque 9.5 Dire que $\text{pgcd}(d_1, d_2, \dots, d_k) = 1$ équivaut à dire que la monodromie est triviale sur la cohomologie de la fibre de Milnor complexe $F(\mathbb{C})$.

L'équivalence entre ces deux hypothèses est démontrée dans l'article d'A. Dimca [2] mais nous ne nous y attarderons pas dans notre mémoire. Nous cherchons ici juste à savoir si il existe, dans certains cas, des formules pour calculer $|F(\mathbb{F}_q)|$.

Exemple 9.6 Si \mathcal{A} est l'arrangement de Boole, $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2 \times \dots \times \mathcal{A}_n$ avec $\mathcal{A}_i = \{ \{x_i = 0\} \}$ vérifie les hypothèses du théorème 9.4, et on a bien :

$$\begin{aligned} |F(\mathbb{F}_q)| &= |\{(x_1, \dots, x_n) \in \mathbb{F}_q^n \mid x_1 \dots x_n = 1\}| \\ &= |\{((x_2 \dots x_n)^{-1}, x_2, \dots, x_n) \in \mathbb{F}_q^{*n}\}| = (q-1)^{n-1} = \frac{\chi(\mathcal{A}, q)}{q-1} \end{aligned}$$

d'après l'exemple 9.8.

Exemple 9.7 Voici un exemple de calcul d'une fibre de Milnor :

Le nombre de solutions N_q de l'équation (E) : $xyz(x + y + z) = 1$ dans \mathbb{F}_q^3 est :

$$N_q = \begin{cases} q^2 - 3q + 3 & \text{si } p = 2 \\ q^2 - 4q + 3 & \text{si } q \equiv 3 \pmod{4} \end{cases}$$

Démonstration :

Dans \mathbb{R}^3 , considérons l'arrangement $\mathcal{A} = \{H_1, H_2, H_3, H_4\}$, où $H_1 : x = 0$, $H_2 : y = 0$, $H_3 : z = 0$ et $H_4 : x + y + z = 0$.

On a que \mathcal{A} est irréductible, de cardinal 4, et on ne peut donc pas calculer N_q en utilisant le théorème 9.4.

Preliminaire :

Montrons que le nombre R_q de solutions de l'équation $(E_0) : xyz(x + y + z) = 0$ dans \mathbb{F}_q^3 est :

$$4q^2 - 6q + 3.$$

On a que $H_i \cap H_j \cap H_k = \{0\} \forall 1 \leq i < j < k \leq 4$, donc

$L(\mathcal{A}) = \{ \mathbb{R}^3, H_1, H_2, H_3, H_4, H_1 \cap H_2, H_1 \cap H_3, H_1 \cap H_4, H_2 \cap H_3, H_2 \cap H_4, H_3 \cap H_4, \{0\} \}$.

On voit clairement que \mathcal{A} admet une bonne réduction modulo p pour tout p premier, car $\dim(H_i) = \dim(\hat{H}_i) \forall i$, $\dim(H_i \cap H_j) = \dim(\hat{H}_i \cap \hat{H}_j) \forall i, j$.

En effet, les matrices qui définissent les éléments de $L(\mathcal{A})$ ont des mineurs qui valent 1 ou -1. Ces matrices ont donc le même rang dans \mathbb{R} ou dans \mathbb{F}_q .

\mathcal{A} est un arrangement générique, son polynôme caractéristique est :

$$\chi(\mathcal{A}, t) = t^3 - 4t^2 + 6t - 3.$$

D'après le théorème 8.9, $|\{ (x, y, z) \in \mathbb{F}_q^3 \mid xyz(x+y+z) \neq 0 \}| = |M(\hat{\mathcal{A}}_q)| = \chi(\mathcal{A}, q) = q^3 - 4q^2 + 6q - 3$, et comme $|\mathbb{F}_q^3| = q^3$ on a que :

$$R_q = |\mathbb{F}_q^3| - |M(\hat{\mathcal{A}}_q)| = 4q^2 - 6q + 3.$$

Revenons maintenant à notre démonstration.

Remarquons tout d'abord que les solutions de (E) sont dans \mathbb{F}_q^{*3} . En effet, les $3q^2 - 3q + 1$ éléments de $\mathbb{F}_q^3 \setminus \mathbb{F}_q^{*3}$ (ceux qui ont au moins un zéro comme coordonnée) vérifient (E_0) .

Commençons par traiter le cas où $p = 2$, $q = 2^m$, $m \in \mathbb{N}^*$.

Pour tout $b \in \mathbb{F}_{2^m}^*$, soit γ_b le nombre de solutions dans $\mathbb{F}_{2^m}^{*3}$ de l'équation $(E_b) : xyz(x+y+z) = b$. Montrons que γ_b ne dépend pas de b . Autrement dit, montrons que le nombre de solutions dans $\mathbb{F}_{2^m}^{*3}$ de l'équation E_b est le même quelque soit $b \in \mathbb{F}_{2^m}^*$.

Grâce au théorème 8.3, on sait que $\mathbb{F}_{2^m}^*$ est cyclique d'ordre $2^m - 1$. Soit ξ un de ses générateurs.

Soit $(x, y, z) \in \mathbb{F}_{2^m}^{*3}$ une solution de l'équation (E) .

Soit $a \in \mathbb{N}^*$.

Comme $\mathbb{F}_{2^m}^* = \langle \xi \rangle$, il existe $(x', y', z') \in \mathbb{F}_{2^m}^{*3}$ tel que $x = x'\xi^a$, $y = y'\xi^a$, et $z = z'\xi^a$. En remplaçant dans l'équation (E) on trouve :

$$xyz(x+y+z) = 1 \Rightarrow x'y'z'(x'+y'+z') = \xi^{-4a}.$$

Or, $4 \wedge 2^m - 1 = 1$ donc ξ^4 est un générateur de $\mathbb{F}_{2^m}^*$.

Ainsi, si $b \in \mathbb{F}_{2^m}^*$, on peut trouver a tel que $\xi^{-4a} = b$ et on a :

$(x, y, z) \in \mathbb{F}_{2^m}^{*3}$ est solution de l'équation $(E) \Rightarrow (x', y', z') \in \mathbb{F}_{2^m}^{*3}$ est solution de l'équation (E_b) , où $x' = \xi^{-a}x$, $y' = \xi^{-a}y$, $z' = \xi^{-a}z$.

Réciproquement,

$(x, y, z) \in \mathbb{F}_{2^m}^{*3}$ est solution de l'équation $(E_b) \Rightarrow \xi^{4a}xyz(x+y+z) = 1 \Rightarrow (\xi^a x, \xi^a y, \xi^a z) \in \mathbb{F}_{2^m}^{*3}$ est solution de l'équation (E) .

Or il y a $R_{2^m} - |\mathbb{F}_{2^m}^3 \setminus \mathbb{F}_{2^m}^*{}^3| = 2^{2m} - 3 \cdot 2^m + 2$ éléments dans $\mathbb{F}_{2^m}^*{}^3$ qui vérifient (E_0) .

Les autres, qui sont au nombre de

$(2^m - 1)^3 - (2^{2m} - 3 \cdot 2^m + 2) = 2^{3m} - 4 \cdot 2^{2m} + 6 \cdot 2^m - 3$ vérifient une des équations (E_b) , $b \in \mathbb{F}_{2^m}^*$.

Ainsi,

$$N_{2^m} = \frac{2^{3m} - 4 \cdot 2^{2m} + 6 \cdot 2^m - 3}{2^m - 1} = 2^{2m} - 3 \cdot 2^m + 3.$$

Traitons maintenant le cas où $q \equiv 3 \pmod{4}$.

Soit M_q le nombre de solutions de l'équation (E') : $xyz(x + y + z) = t^4$ dans \mathbb{F}_q^4 .

Dans $\mathbb{P}(\mathbb{F}_q^4)$, soit $H := \{t = 0\}$ l'hyperplan projectif correspondant aux points à l'infini.

On a alors la bijection suivante :

$$\mathbb{F}_q^3 \longrightarrow \mathbb{P}(\mathbb{F}_q^4) \setminus H$$

$$(x, y, z) \mapsto (x : y : z : 1).$$

Soit $Q(x, y, z, t) = xyz(x + y + z) - t^4$ l'homogénéisé de $xyz(x + y + z) - 1$. On a alors :

$$\begin{aligned} M(Q, q) &= \{(x, y, z, t) \in \mathbb{F}_q^4 \mid xyz(x + y + z) - t^4 \neq 0\}, \\ M'(Q, q) &= \{(x : y : z : t) \in \mathbb{P}(\mathbb{F}_q^4) \mid xyz(x + y + z) - t^4 \neq 0\} \\ &= \{(x : y : z : 1) \in \mathbb{P}(\mathbb{F}_q^4) \mid xyz(x + y + z) - 1 \neq 0\} \cup \\ &\quad \{(x : y : z : 0) \in \mathbb{P}(\mathbb{F}_q^4) \mid xyz(x + y + z) \neq 0\}, \text{ d'où :} \\ |M(Q, q)| &= q^4 - M_q, \\ |M'(Q, q)| &= |\{(x, y, z) \in \mathbb{F}_q^3 \mid xyz(x + y + z) - 1 \neq 0\}| + \\ &\quad |\{(x : y : z : 0) \in \mathbb{P}(\mathbb{F}_q^4) \mid xyz(x + y + z) \neq 0\}| \\ &= q^3 - N_q + |\{(x : y : z : 0) \in \mathbb{P}(\mathbb{F}_q^4) \mid xyz(x + y + z) \neq 0\}|. \end{aligned}$$

D'après la proposition 8.12 on a également :

$$|M'(Q, q)| = \frac{|M(Q, q)|}{q-1} = \frac{q^4 - M_q}{q-1}.$$

Si $R(x, y, z) = xyz(x + y + z)$, d'après la proposition 8.12 on peut écrire :

$$|M'(R, q)| = \frac{|M(R, q)|}{q-1} = \frac{q^3 - R_q}{q-1} = q^2 - 3q + 3.$$

Or $|M'(R, q)| = |\{(x : y : z) \in \mathbb{P}(\mathbb{F}_q^3) \mid xyz(x + y + z) \neq 0\}|$
 $= |\{(x : y : z : 0) \in \mathbb{P}(\mathbb{F}_q^4) \mid xyz(x + y + z) \neq 0\}| = |M'(Q, q)| - q^3 + N_q.$

On trouve donc la formule :

$$\frac{q^3 - R_q}{q-1} = \frac{q^4 - M_q}{q-1} - q^3 + N_q.$$

Ou encore :

$$N_q = q^3 + q^2 - 3q + 3 - \frac{q^4 + M_q}{q-1} \quad (3)$$

Il nous reste donc à calculer M_q . Montrons que M_q est aussi le nombre de solutions de l'équation (E'') : $xyz(x+y+z) = t^2$:

- $(x, y, z, t) \in \mathbb{F}_q^{*4}$ est solution de (E'') $\Leftrightarrow \alpha = xyz(x+y+z)$ est un carré dans \mathbb{F}_q^* .

Or, α est un carré dans \mathbb{F}_q^* $\Leftrightarrow \exists \beta \in \mathbb{F}_q^* \mid \alpha = \beta^2, \alpha = (-\beta)^2$ ($\beta \neq -\beta$ car q est impair). Ainsi, les solutions de (E'') dans \mathbb{F}_q^{*4} sont :

$$\{(x, y, z, \beta), (x, y, z, -\beta) \mid xyz(x+y+z) = \alpha, \alpha = \beta^2\}_{\alpha \text{ carré dans } \mathbb{F}_q^*}.$$

- (x, y, z, t) est solution de (E') $\Leftrightarrow xyz(x+y+z) = t^4$.

Soient $\alpha, \beta \in \mathbb{F}_q^*$ tels que $\alpha = \beta^4$.

Alors α s'écrit $\alpha = \alpha_1^2$, avec $\alpha_1 = \beta^2$ ou $\alpha_1 = (-\beta)^2$ (le cas $\alpha_1 = -\beta^2$ est impossible car -1 n'est pas un carré dans \mathbb{F}_q^*). Ainsi, les solutions de (E') dans \mathbb{F}_q^{*4} sont :

$$\{(x, y, z, \beta), (x, y, z, -\beta) \mid xyz(x+y+z) = \alpha_1^2, \alpha_1 = \beta^2\}_{\alpha_1 \text{ carré dans } \mathbb{F}_q^*}.$$

Or $\{\alpha_1^2 \mid \alpha_1 \text{ carré dans } \mathbb{F}_q^*\} \subset \{\alpha \mid \alpha \text{ carré dans } \mathbb{F}_q^*\}$, donc le nombre de solutions de (E') est inférieur au nombre de solutions de (E'') .

De plus, $xyz(x+y+z) = t^4 \Rightarrow xyz(x+y+z) = T^2$, avec $T = t^2$, donc le nombre de solutions de (E'') est inférieur à celui de (E') et finalement ces deux nombres sont égaux.

Trouvons donc le nombre M_q de solutions de l'équation (E'') : $xyz(x+y+z) = t^2$.

Soit $V := \{(x, y, z, t) \in \mathbb{F}_q^4 \mid xyz(x+y+z) = t^2\}$.

Soit $F := \{(x, y, z, t) \in \mathbb{F}_q^4 \mid t \neq 0\}$. On a une bijection :

$$\pi : F \longrightarrow F$$

$$(x, y, z, t) \mapsto (xt, y, z, t)$$

d'inverse

$$\pi^{-1} : F \longrightarrow F$$

$$(x, y, z, t) \mapsto \left(\frac{x}{t}, y, z, t\right).$$

On a que $V = F \cap V \sqcup \{(x, y, z, 0) \in \mathbb{F}_q^4 \mid xyz(x+y+z) = 0\}$.

Donc $M_q = |F \cap V| + |\{(x, y, z) \in \mathbb{F}_q^3 \mid xyz(x+y+z) = 0\}| = |F \cap V| + R_q = |\pi^{-1}(F \cap V)| + R_q$ car π est une bijection.

On a que $(x, y, z, t) \in F \cap V \Leftrightarrow \pi^{-1}(x, y, z, t)$ est solution de l'équation $xyz(xt + y + z) = t$ dans F .

Calculons donc le nombre de solutions de l'équation $(\tilde{E}) : xyz(xt + y + z) = t$ dans F :

$(x, y, z, t) \in F$ est solution de $(\tilde{E}) \Leftrightarrow t(x^2yz - 1) + xyz(y + z) = 0, t \neq 0$
 $\Leftrightarrow (1) : x^2yz - 1 = 0, xyz(y + z) = 0, t \neq 0$

ou

(2) : $x^2yz - 1 \neq 0, xyz(y + z) = -t(x^2yz - 1), t \neq 0$.

On est donc amené à calculer $|A|$ et $|B|$ où

$A := \{(x, y, z, t) \in F \mid (x, y, z, t) \text{ est solution de (1)}\}$, et

$B := \{(x, y, z, t) \in F \mid (x, y, z, t) \text{ est solution de (2)}\}$.

On aura $|F \cap V| = |A| + |B|$.

1. $(x, y, z, t) \in A \Rightarrow z = -y, x^2yz = 1 \Rightarrow -1 = (\frac{1}{xy})^2$.

Or, $q \equiv 3 \pmod{4}$ donc -1 n'est pas un carré et c'est impossible.

Ainsi, $|A| = 0$.

2. Montrons tout d'abord que

$|B| = |\{(x, y, z) \in \mathbb{F}_q^3 \mid x^2yz - 1 \neq 0, xyz(y + z) \neq 0\}| :$

Si $(x, y, z, t) \in B$, alors $(x, y, z) \in \mathbb{F}_q^3$ est tel que $x^2yz - 1 \neq 0, xyz(y + z) \neq 0$.

Ainsi, $|B| \leq |\{(x, y, z) \in \mathbb{F}_q^3 \mid x^2yz - 1 \neq 0, xyz(y + z) \neq 0\}|$.

Si $(x, y, z) \in \mathbb{F}_q^3$ est tel que $x^2yz - 1 \neq 0, xyz(y + z) \neq 0$,

alors $(x, y, z, t) \in B$ avec $t = -\frac{xyz(y+z)}{x^2yz-1}$.

Ainsi, $|B| \geq |\{(x, y, z) \in \mathbb{F}_q^3 \mid x^2yz - 1 \neq 0, xyz(y + z) \neq 0\}|$.

Finalement, on a bien

$$|B| = |\{(x, y, z) \in \mathbb{F}_q^3 \mid x^2yz - 1 \neq 0, xyz(y + z) \neq 0\}|.$$

Or, $|\{(x, y, z) \in \mathbb{F}_q^3 \mid x^2yz - 1 \neq 0, xyz(y + z) \neq 0\}|$

$$= q^3 - |\{(x, y, z) \in \mathbb{F}_q^3 \mid x^2yz - 1 = 0 \text{ ou } xyz(y + z) = 0\}|.$$

Calculons donc $|C|$ et $|D|$ où

$$C := \{(x, y, z) \in \mathbb{F}_q^3 \mid x^2yz - 1 = 0\},$$

$$D := \{(x, y, z) \in \mathbb{F}_q^3 \mid xyz(y + z) = 0\}.$$

- $(x, y, z) \in C \Leftrightarrow (x, y, z) \in \mathbb{F}_q^{*3}, x^2 = \frac{1}{yz}$.

Dans \mathbb{F}_q^* , il y a $\frac{q-1}{2}$ carrés d'après la remarque 8.5.

Soit α un de ces carrés, alors il existe $b \in \mathbb{F}_q^*$ tel que $\alpha = b^2$, $\alpha = (-b)^2$.

Soit maintenant $y \in \mathbb{F}_q^*$ quelconque.

$$\alpha = \frac{1}{yz} \Leftrightarrow z = y^{-1}\alpha^{-1}.$$

Les solutions de E_1 sont donc $\{(b, y, y^{-1}\alpha^{-1}), (-b, y, y^{-1}\alpha^{-1}) \mid y \in \mathbb{F}_q^*, \alpha = b^2\}_{\alpha \text{ carré dans } \mathbb{F}_q^*}$.

Ainsi,

$$|C| = 2(q-1) \cdot \frac{q-1}{2} = (q-1)^2.$$

- Les éléments de D sont les triplets qui possèdent au moins un zéro comme coordonnée (il y en a $3q^2 - 3q + 1$), et les triplets de $\mathbb{F}_q^*{}^3$ de la forme $(x, y, -y)$ (il y en a $(q-1)^2$).

Ainsi,

$$|D| = 4q^2 - 5q + 2.$$

On a que C et D sont disjoints comme on l'a vu dans 1. donc

$$|\{(x, y, z) \in \mathbb{F}_q^3 \mid x^2yz - 1 = 0 \text{ ou } xyz(y+z) = 0\}| = |C| + |D|.$$

$$\text{Ainsi, } |B| = |\{(x, y, z) \in \mathbb{F}_q^3 \mid x^2yz - 1 \neq 0, xyz(y+z) \neq 0\}| = q^3 - |C| - |D| = q^3 - 5q^2 + 7q - 3.$$

On a donc que $|F \cap V| = |A| + |B| = q^3 - 5q^2 + 7q - 3$. Finalement,

$$M_q = |F \cap V| + R_q = q^3 - q^2 + q.$$

En utilisant ensuite (2) on trouve :

$$N_q = q^2 - 4q + 3.$$

Il est naturel de se demander si il existe de telles formules pour calculer $N_q = |F(\mathbb{F}_q)|$ lorsque $q \equiv 1 \pmod{4}$.

Le programme suivant nous permet de calculer $|F(\mathbb{F}_q)|$ en utilisant Singular lorsque $s = 1$.

Ce programme étant très simple, les calculs se font très rapidement même pour des grandes valeurs de p .

```

> proc nbresol1(int p)
{
LIB "general.lib";
bigint f,x,y,z;
bigint ns=0;
for (x=0;x<=p-1;x=x+1)
{
for (y=0;y<=p-1;y=y+1)
{
for (z=0;z<=p-1;z=z+1)
{

```



```

f= x*y*z*(x+y+z);
if (f mod p == 1) { ns=ns+1;}
}
}
}
write("", "nombre de solutions : "+string(ns));
}

```

Le programme suivant nous permet de calculer $|F(\mathbb{F}_q)|$ lorsque $s \geq 2$. Il fonctionne bien mais les calculs prennent énormément de temps lorsque p et s sont trop grand.

```

> proc nbresol(int p, int s)
{
LIB "general.lib";
ring R=(p ^ s,a),xx,dp;
int q=p^s;
int i,j,k;
number x,y,z;
bigint ns=0;
for (i=0;i<=q-1;i++)
{
if(i==q-1) {x=0;} else {x=a^i;}
for (j=0;j<=q-1;j++)
{
if(j==q-1) {y=0;} else {y=a^j;}
for (k=0;k<=q-1;k++)
{
if(k==q-1) {z=0;} else {z=a^k;}
if ( x*y*z*(x+y+z) == 1 )
{ ns=ns+1;}
}
}
}
}
write("", "nombre de solutions : "+string(ns));
}

```

Nous voulons donc savoir, si dans le cas où $q \equiv 1 \pmod{4}$, il existe p_0, a, b, c tels que N_q s'écrit sous la forme

$$N_q = a.q^2 + b.q + c \quad \text{lorsque } p \geq p_0. \quad (1)$$

Commençons par étudier le cas où $s = 1$, $p \equiv 1 \pmod{4}$.
 Si une telle formule existe, alors si $l_p = \frac{N_p}{p^2}$, $\lim_{p \rightarrow \infty} l_p = a$.
 A l'aide du programme nbresol1 on trouve pour les 18 premiers nombres premiers congrus à 1 modulo 4 :

$$\begin{aligned}
 N_5 &= 24, & l_5 &= 0,96 \\
 N_{13} &= 136, & l_{13} &\approx 0,80 \\
 N_{17} &= 228, & l_{17} &\approx 0,79 \\
 N_{29} &= 744, & l_{29} &\approx 0,88 \\
 N_{37} &= 1368, & l_{37} &\approx 0,99 \\
 N_{41} &= 1620, & l_{41} &\approx 0,96 \\
 N_{53} &= 2616, & l_{53} &\approx 0,93 \\
 N_{61} &= 3624, & l_{61} &\approx 0,97 \\
 N_{73} &= 5076, & l_{73} &\approx 0,95 \\
 N_{89} &= 7668, & l_{89} &\approx 0,97 \\
 N_{97} &= 9348, & l_{97} &\approx 0,99 \\
 N_{101} &= 10200, & l_{101} &\approx 0,99 \\
 N_{109} &= 11848, & l_{109} &\approx 0,99 \\
 N_{113} &= 12516, & l_{113} &\approx 0,98 \\
 N_{137} &= 18708, & l_{137} &\approx 0,99 \\
 N_{149} &= 22008, & l_{149} &\approx 0,99 \\
 N_{157} &= 24168, & l_{157} &\approx 0,98 \\
 N_{173} &= 29256, & l_{173} &\approx 0,98
 \end{aligned}$$

Tout en oscillant, l_p semble bien tendre vers $a = 1$ lorsque p tend vers $+\infty$.
 Etudions donc maintenant le comportement de $r_p = \frac{N_p - p^2}{p}$, car si une telle formule existe, alors $\lim_{p \rightarrow \infty} r_p = b$.

$$\begin{aligned}
 r_5 &= -0,2 \\
 r_{13} &\approx -2,54 \\
 r_{17} &\approx -3,59 \\
 r_{29} &\approx -3,34 \\
 r_{37} &\approx -0,03 \\
 r_{41} &\approx -1,49 \\
 r_{53} &\approx -3,64 \\
 r_{61} &\approx -1,59 \\
 r_{73} &\approx -3,47 \\
 r_{89} &\approx -2,84 \\
 r_{97} &\approx -0,63 \\
 r_{101} &\approx -0,01
 \end{aligned}$$

$$\begin{aligned}
r_{109} &\approx -0,3 \\
r_{113} &\approx -2,24 \\
r_{137} &\approx -0,45 \\
r_{149} &\approx -1,2 \\
r_{157} &\approx -3,06 \\
r_{173} &\approx -3,89
\end{aligned}$$

On remarque que r_p semble appartenir à l'intervalle $[-4, 0]$. Cet intervalle est beaucoup trop grand pour pouvoir estimer b et c .

Exemple 9.8 *Voici maintenant un autre exemple de calcul de fibre de Milnor.*

Soit N_q le nombre de solutions de l'équation

$$(E) : Q(x, y, z) = xyz(x + y + z)(x + 2y + 3z) = 1 \text{ dans } \mathbb{F}_q^3.$$

Ne pouvant pas appliquer le théorème 9.4, nous utilisons cette fois-ci encore Singular pour trouver N_q et en déduire si il existe des formules comme dans l'exemple 9.7 :

Remarquons tout d'abord que l'arrangement \mathcal{A} défini par le polynôme $Q(x, y, z)$ est générique et admet une bonne réduction modulo p pour tout p premier distinct de 2, 3. Commençons donc nos calculs à partir de $p = 5$ et restreignons nous pour commencer au cas où $s = 1$.

On trouve :

$$\begin{aligned}
N_5 &= 11, \quad l_5 = 0,44 \\
N_7 &= 27, \quad l_7 \approx 0,55 \\
N_{11} &= 65, \quad l_{11} \approx 0,54 \\
N_{13} &= 123, \quad l_{13} \approx 0,73 \\
N_{17} &= 227, \quad l_{17} \approx 0,79 \\
N_{19} &= 291, \quad l_{19} \approx 0,81 \\
N_{23} &= 443, \quad l_{23} \approx 0,84 \\
N_{29} &= 731, \quad l_{29} \approx 0,87 \\
N_{31} &= 920, \quad l_{31} \approx 0,96 \\
N_{37} &= 1227, \quad l_{37} \approx 0,90 \\
N_{41} &= 1640, \quad l_{41} \approx 0,98 \\
N_{43} &= 1683, \quad l_{43} \approx 0,91 \\
N_{47} &= 2027, \quad l_{47} \approx 0,92 \\
N_{53} &= 2603, \quad l_{53} \approx 0,93 \\
N_{59} &= 3251, \quad l_{59} \approx 0,93 \\
N_{61} &= 3310, \quad l_{61} \approx 0,89 \\
N_{67} &= 4227, \quad l_{67} \approx 0,94
\end{aligned}$$

$$N_{71} = 4570, \quad l_{71} \approx 0,91$$

Tout en oscillant, l_p semble tendre vers $a = 1$ lorsque p tend vers $+\infty$.
 Etudions donc maintenant le comportement de $r_p = \frac{N_p - p^2}{p}$.

$$\begin{aligned} r_5 &= -2,8 \\ r_7 &\approx -3,14 \\ r_{11} &\approx -5,09 \\ r_{13} &\approx -3,54 \\ r_{17} &\approx -3,65 \\ r_{19} &\approx -3,68 \\ r_{23} &\approx -3,74 \\ r_{29} &\approx -3,79 \\ r_{31} &\approx -1,32 \\ r_{37} &\approx -3,84 \\ r_{41} &= -1 \\ r_{43} &\approx -3,86 \\ r_{47} &\approx -3,87 \\ r_{53} &\approx -3,87 \\ r_{59} &\approx -3,89 \\ r_{61} &\approx -6,74 \\ r_{67} &\approx -3,91 \\ r_{71} &\approx -6,63 \end{aligned}$$

On remarque que :

- $r_p \in [-4, -2, 8]$ si $p = 5, 7, 13, 17, 19, 23, 29, 37, 43, 47, 53, 59, 67$.
- Il y a des sauts en $p = 11, 31, 41, 61, 71$.

A ce stade, on ne peut encore rien dire sur les valeurs de b et c .

10 Conclusion

La théorie générale nous dit en fait qu'il n'existe pas de polynôme en q de degré 2 permettant de calculer le nombre d'éléments de la fibre de Milnor d'un arrangement de \mathbb{C}^3 sur \mathbb{F}_q qui ne vérifie pas les hypothèses du théorème 9.4. En effet, nous avons pu constater que les coefficients b et c ne sont pas constants mais semblent varier selon les valeurs de q .

Cependant, il est possible d'aller un peu plus loin et d'étudier le comportement de la fonction $q \mapsto |F(\mathbb{F}_q)|$ dans le cas d'un arrangement générique.

En effet, si \mathcal{A} est un arrangement générique dans \mathbb{C}^3 défini par un polynôme

$Q(x, y, z) \in \mathbb{Z}[x, y, z]$ homogène et ayant une bonne réduction modulo p , si on note $|\mathcal{A}| = d$ alors on a d'après l'exemple 9.8 :

$$|M'(Q, q)| = q^2 - (d-1)q + \binom{d-1}{2}.$$

Or, il existe une formule, qui est la formule de trace de Grothendieck, dont je n'ai pas eu le temps d'étudier la démonstration dans ce mémoire, qui assure que pour un tel arrangement générique \mathcal{A} on a la formule suivante :

$$|F(\mathbb{F}_q)| = |M'(Q, q)| + \epsilon(q).q, \text{ avec } \epsilon(q) \in \mathbb{Q}, |\epsilon(q)| \leq (d-1)\binom{d-1}{2}.$$

On peut donc en fait écrire $|F(\mathbb{F}_q)|$ sous la forme :

$$|F(\mathbb{F}_q)| = q^2 + b(q).q + c(q), \text{ où } b(q) \text{ et } c(q) \text{ sont bornés indépendamment de } q \\ \text{(i.e. } \exists C_1(d), C_2(d) \mid |b(q)| \leq C_1(d), |c(q)| \leq C_2(d)).$$

Ainsi, calculer la limite des r_q lorsque q est grand, revenait en fait à donner une estimation sur des intervalles de la forme $I_d = [\alpha_d, \beta_d]$ tels que $b(q) \in I_d$. Revenons donc sur les deux exemples précédents.

1. Dans l'exemple 9.7, on est en présence d'un arrangement générique composé de quatre hyperplans. D'après la formule de trace, on a que $|F(\mathbb{F}_q)| = q^2 - 3q + 3 + \epsilon(q).q$.

Ainsi, on a trouvé que $\epsilon(2) = 0$, $\epsilon(q) = -1 \forall q \equiv 3 \pmod{4}$, et que dans le cas où $p \equiv 1 \pmod{4}$, $b(p)$ semble appartenir à l'intervalle $I_4 = [-4, 0]$.

On pourrait également tenter de comprendre le comportement de $\epsilon(p) = \frac{N_p - p^2 + 3p - 3}{p}$ lorsque $p \equiv 1 \pmod{4}$ en testant quelques valeurs :

$$\begin{aligned} \epsilon(5) &= 2, 2 \\ \epsilon(13) &\approx 0, 23 \\ \epsilon(17) &\approx -0, 76 \\ \epsilon(29) &\approx -0, 45 \\ \epsilon(37) &\approx 2, 89 \\ \epsilon(41) &\approx 1, 45 \\ \epsilon(53) &\approx -0, 70 \\ \epsilon(61) &\approx 1, 36 \\ \epsilon(73) &\approx -0, 51 \\ \epsilon(89) &\approx 0, 12 \\ \epsilon(97) &\approx 2, 34 \\ \epsilon(101) &\approx 2, 96 \end{aligned}$$

$$\begin{aligned}
\epsilon(109) &\approx 2,67 \\
\epsilon(113) &\approx 0,73 \\
\epsilon(137) &\approx 2,53 \\
\epsilon(149) &\approx 1,68 \\
\epsilon(157) &\approx -0,08 \\
\epsilon(173) &\approx -0,9
\end{aligned}$$

2. Dans l'exemple 9.8, on est en présence d'un arrangement générique composé de cinq hyperplans.

D'après la formule de trace, on a que $|F(\mathbb{F}_q)| = q^2 - 4q + 6 + \epsilon(q)q$.

$$\text{Calculons donc } \epsilon(p) = \frac{N_p - (p^2 - 4p + 6)}{p} = \frac{N_p - p^2 - 6}{p} + 4 :$$

$$\begin{aligned}
\epsilon(5) &= 0 \\
\epsilon(7) &= 0 \\
\epsilon(11) &= -1,636363\dots \\
\epsilon(13) &= 0 \\
\epsilon(17) &= 0 \\
\epsilon(19) &= 0 \\
\epsilon(23) &= 0 \\
\epsilon(29) &= 0 \\
\epsilon(31) &\approx 2,483871 \\
\epsilon(37) &= 0 \\
\epsilon(41) &\approx 2,853659 \\
\epsilon(43) &= 0 \\
\epsilon(47) &= 0 \\
\epsilon(53) &= 0 \\
\epsilon(59) &= 0 \\
\epsilon(61) &\approx -2,8361 \\
\epsilon(67) &= 0 \\
\epsilon(71) &\approx -2,71831
\end{aligned}$$

Les résultats nous incitent à établir la proposition suivante :

Proposition 10.1 *Soit $p \geq 5$ un nombre premier, $q = p^s$, $s \in \mathbb{N}^*$
Si $q \not\equiv 1 \pmod{10}$, alors $N_q = q^2 - 4q + 6 = |M'(Q, q)|$.*

Démonstration :

Soit \mathcal{A} l'arrangement générique défini par le polynôme

$$Q(x, y, z) = xyz(x + y + z)(x + 2y + 3z).$$

On a que le nombre R_q de solutions de l'équation $Q(x, y, z) = 0$ dans \mathbb{F}_q^3 est :

$$R_q = q^3 - |M(\hat{\mathcal{A}}_q)| = q^3 - \chi(\mathcal{A}, q) = q^3 - (q^3 - 5q^2 + 10q - 6) = 5q^2 - 10q + 6.$$

Pour tout $b \in \mathbb{F}_q^*$, soit γ_b le nombre de solutions dans \mathbb{F}_q^{*3} de l'équation $(E_b) : xyz(x + y + z)(x + 2y + 3z) = b$. Remarquons tout d'abord que les solutions de (E_b) sont dans \mathbb{F}_q^{*3} car les $3q^2 - 3q + 1$ éléments de $\mathbb{F}_q^3 \setminus \mathbb{F}_q^{*3}$ vérifient $Q(x, y, z) = 0$.

Montrons que γ_b ne dépend pas de b . Autrement dit, montrons que le nombre de solutions dans \mathbb{F}_q^{*3} de l'équation E_b est le même quelque soit $b \in \mathbb{F}_q^*$.

Grâce au théorème 8.3, on sait que \mathbb{F}_q^* est cyclique d'ordre $q - 1$. Soit ξ un de ses générateurs.

Soit $(x, y, z) \in \mathbb{F}_q^{*3}$ une solution de l'équation (E) .

Soit $a \in \mathbb{N}^*$.

Comme $\mathbb{F}_q^* = \langle \xi \rangle$, il existe $(x', y', z') \in \mathbb{F}_q^{*3}$ tel que $x = x'\xi^a$, $y = y'\xi^a$, et $z = z'\xi^a$. En remplaçant dans l'équation (E) on trouve :

$$xyz(x + y + z)(x + 2y + 3z) = 1 \Rightarrow x'y'z'(x' + y' + z')(x' + 2y' + 3z') = \xi^{-5a}.$$

Or, 5 est premier donc $5 \wedge q - 1 = 1 \Leftrightarrow 5 \nmid q - 1$.

De plus $p \neq 2$ donc $q = p^s$ est impair et $2 \mid q - 1$.

Donc on a que $5 \wedge q - 1 = 1 \Leftrightarrow 10 \nmid q - 1 \Leftrightarrow q \not\equiv 1 \pmod{10}$.

Ainsi, lorsque $q \not\equiv 1 \pmod{10}$, ξ^5 est un générateur de \mathbb{F}_q^* et si $b \in \mathbb{F}_q^*$, on peut trouver a tel que $\xi^{-5a} = b$. On a donc :

$(x, y, z) \in \mathbb{F}_q^{*3}$ est solution de l'équation $(E) \Rightarrow (x', y', z') \in \mathbb{F}_q^{*3}$ est solution de l'équation (E_b) , où $x' = \xi^{-a}x$, $y' = \xi^{-a}y$, $z' = \xi^{-a}z$.

Réciproquement,

$(x, y, z) \in \mathbb{F}_q^{*3}$ est solution de l'équation $(E_b) \Rightarrow \xi^{5a}xyz(x + y + z)(x + 2y + 3z) = 1$

$\Rightarrow (\xi^a x, \xi^a y, \xi^a z) \in \mathbb{F}_q^{*3}$ est solution de l'équation (E) .

Or il y a $|\mathbb{F}_q^3| - R_q = q^3 - 5q^2 + 10q - 6$ éléments dans \mathbb{F}_q^3 qui vérifient (E_b) pour un certain $b \in \mathbb{F}_q^*$.

Ainsi,

$$N_q = \frac{q^3 - 5q^2 + 10q - 6}{q - 1} = q^3 - 4q + 6.$$

Il faudrait à présent tenter de comprendre qu'est-ce qui se passe lorsque $p \equiv 1 \pmod{10}$ en observant les valeurs de $\epsilon(p)$.

$$\begin{aligned}
\epsilon(11) &\approx -1,64 \\
\epsilon(31) &\approx 2,48 \\
\epsilon(41) &\approx 2,85 \\
\epsilon(61) &\approx -2,84 \\
\epsilon(71) &\approx -6,72 \\
\epsilon(101) &\approx -3,40 \\
\epsilon(131) &\approx -4,53 \\
\epsilon(151) &\approx 0,11 \\
\epsilon(181) &\approx 3,13 \\
\epsilon(191) &\approx 2,92
\end{aligned}$$

Enfin, on pourrait élargir tous nos tests aux cas où $s > 1$, ce que nous n'avons pas fait ici car le programme met énormément de temps à calculer le nombre de solutions pour de grandes valeurs de q . Il y a donc énormément de travail à fournir encore pour ce sujet, et beaucoup de questions ne sont pas résolues de nos jours, notamment quant au comportement de la fonction $\epsilon(q)$ qui reste encore très mystérieux.

Références

- [1] P. Cartier : Les arrangements d'hyperplans : un chapitre de géométrie combinatoire, Séminaire Bourbaki vol. 1980/81 Exposés 561-578, Lecture Notes in Mathematics, 1981, Volume 901/1981, p. 1-22.
- [2] A. Dimca : Tate properties, polynomial-count varieties, and monodromy of hyperplane arrangements, arXiv : 1012.1437.
- [3] P. Orlik et H. Terao : Arrangements of Hyperplanes, Springer-Verlag, Berlin Heidelberg New York, 1992.
- [4] R. P. Stanley : An Introduction to Hyperplane Arrangements, Park City Mathematics Series, volume 14 : Geometric Combinatorics (2004).
- [5] S. Roberts : On figures formed by the intercepts of a system of straight lines in a plane, and on analogous relation in space of three dimensions, Proc. London Math. Soc. 19 (1889), 405-422.