

Fonctions de Möbius - Formule de Rota

Robert Rolland

Révisé 10 Janvier 2006

R. Rolland, C.N.R.S. Institut de Mathématiques de Luminy
Luminy Case 930, F13288 Marseille CEDEX 9
e-mail: rolland@iml.univ-mrs.fr

1 Chaînes dans les ensembles finis ordonnés

Soit \mathbb{L} un ensemble **fini ordonné** par une relation notée \leq .

Definition 1.1 *Pour tout entier $p \geq 0$ et tout couple (x, y) d'éléments de \mathbb{L} tels que $x \leq y$ on appelle chaîne de longueur p joignant x à y toute suite finie (x_0, x_1, \dots, x_p) d'éléments de \mathbb{L} tels que*

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

On note $c_p(x, y)$ le nombre de ces chaînes.

Il est clair que

- $c_0(x, x) = 1$
- $c_0(x, y) = 0$ pour $x < y$
- $c_p(x, x) = 0$ pour $p > 0$
- $c_1(x, y) = 1$ pour $x < y$

Proposition 1.1 *On dispose des relations de récurrence suivantes entre les nombres $c_p(x, y)$:*

$$c_{p+1}(x, y) = \sum_{x \leq z < y} c_p(x, z)$$

$$c_{p+1}(x, y) = \sum_{x < z \leq y} c_p(z, y)$$

Proof. Toute chaîne de longueur $p + 1$ joignant x à y est constituée d'une chaîne de longueur p joignant x à un certain $z < y$ à laquelle on adjoint comme point x_{p+1} le point extrémité y . Ceci nous donne la première relation. La deuxième relation se démontre de manière analogue.

2 Fonction de Möbius

Definition 2.1 *La fonction de Möbius $\mu_{\mathbb{L}}$ de l'ensemble ordonné \mathbb{L} est la fonction définie sur $\mathbb{L} \times \mathbb{L}$ à valeurs dans \mathbb{Z} par*

$$\mu_{\mathbb{L}}(x, y) = \sum_{p \geq 0} (-1)^p c_p(x, y)$$

si $x \leq y$ et par

$$\mu_{\mathbb{L}}(x, y) = 0$$

sinon.

Proposition 2.1 *La fonction $\mu_{\mathbb{L}}$ vérifie*

$$\mu_{\mathbb{L}}(x, x) = 1$$

et si $x < y$

$$\sum_{x \leq z \leq y} \mu_{\mathbb{L}}(x, z) = 0$$

$$\sum_{x \leq z \leq y} \mu_{\mathbb{L}}(z, y) = 0.$$

Proof. La première relation est une conséquence du fait que $\mu_{\mathbb{L}}(x, x) = c_0(x, x)$.

En ce qui concerne la deuxième relation en utilisant la définition de $\mu_{\mathbb{L}}$ et la proposition 1.1 on obtient la suite de calculs

$$\begin{aligned} \sum_{x \leq z \leq y} \mu_{\mathbb{L}}(x, z) &= \sum_{x \leq z \leq y} \sum_{p \geq 0} (-1)^p c_p(x, z) \\ \sum_{x \leq z \leq y} \mu_{\mathbb{L}}(x, z) &= \sum_{p \geq 0} (-1)^p \sum_{x \leq z \leq y} c_p(x, z) \\ \sum_{x \leq z \leq y} \mu_{\mathbb{L}}(x, z) &= \sum_{p \geq 0} (-1)^p (c_{p+1}(x, y) + c_p(x, y)) \end{aligned}$$

donc

$$\sum_{x \leq z \leq y} \mu_{\mathbb{L}}(x, z) = 0.$$

La dernière relation s'obtient de manière analogue.

Remarque 1: Si on considère la relation d'ordre \geq au lieu de \leq sur \mathbb{L} , on obtient une fonction de Möbius $\mu'_{\mathbb{L}}$ qui vérifie

$$\mu'_{\mathbb{L}}(x, y) = \mu_{\mathbb{L}}(y, x).$$

Remarque 2: Toute cette étude reste encore valable sur un ensemble infini pourvu que pour tout couple x, y tel que $x \leq y$ il n'y ait qu'un ensemble fini de z tels que $x \leq z \leq y$. Tout ce qui est fait par la suite reste aussi valable dans ce cas.

3 Formule sommatoire de Rota

Soit f une fonction définie sur \mathbb{L} à valeurs dans un groupe abélien G . Posons

$$g(x) = \sum_{y \leq x} f(y).$$

Theorem 3.1 (Inversion de Rota) *Il est possible de retrouver la fonction f connaissant la fonction g grâce à la formule*

$$f(x) = \sum_{y \leq x} \mu_{\mathbb{L}}(y, x) g(y).$$

Proof.

$$\sum_{y \leq x} \mu_{\mathbb{L}}(y, x)g(y) = \sum_{y \leq x} \mu_{\mathbb{L}}(y, x) \sum_{z \leq y} f(z)$$

et par un autre regroupement des termes

$$\sum_{y \leq x} \mu_{\mathbb{L}}(y, x)g(y) = \sum_{z \leq x} f(z) \sum_{z \leq y \leq x} \mu_{\mathbb{L}}(y, x)$$

or le seul cas où la somme $\sum_{z \leq y \leq x} \mu_{\mathbb{L}}(y, x)$ est non nulle est quand $z = x$ auquel cas cette somme vaut 1, donc

$$\sum_{y \leq x} \mu_{\mathbb{L}}(y, x)g(y) = f(x).$$

Remarquons que dans la formule d'inversion de Rota les $\mu_{\mathbb{L}}(y, x)$ sont dans \mathbb{Z} alors que les $g(y)$ sont dans G . La signification des produits $\mu_{\mathbb{L}}(y, x)g(y)$ est claire; c'est la signification classique, à l'aide d'une itération d'additions, de la multiplication d'un élément d'un groupe par un entier.

Remarquons aussi que cette formule d'inversion, en raison de la remarque faite à la fin de la section précédente, peut aussi s'écrire, lorsque la fonction h est définie par

$$h(x) = \sum_{x \leq y} f(y),$$

sous la forme

$$f(x) = \sum_{x \leq y} \mu(x, y)h(y).$$

Si on remplace G par un corps K de caractéristique nulle alors $\mathbb{Z} \subset K$ et dans ce cas on peut énoncer le résultat suivant

Theorem 3.2 *Si pour tout couple (x, y) de points de \mathbb{L} tels que $x \leq y$ il existe un $a(x, y)$ dans K , de telle sorte que pour toute fonction f de \mathbb{L} dans K et tout x de \mathbb{L} on ait*

$$f(x) = \sum_{y \leq x} a(x, y)g(y)$$

où

$$g(y) = \sum_{z \leq y} f(z)$$

alors

$$a(x, y) = \mu_{\mathbb{L}}(x, y)$$

pour tout $x \leq y$.

Proof. Notons s la cardinalité de \mathbb{L} . Indexons les éléments de \mathbb{L} sous la forme $\mathbb{L} = \{l_1, l_2, \dots, l_s\}$ de telle sorte que l_1 soit minimal dans \mathbb{L} et que pour $k > 1$ l_k soit minimal dans $\mathbb{L} \setminus \{l_1, l_2, \dots, l_{k-1}\}$. Soient f_1, f_2, \dots, f_s des fonctions de \mathbb{L} dans K linéairement indépendantes et g_1, g_2, \dots, g_s les fonctions correspondantes. On sait donc que

$$g_j(l_i) = \sum_{l \leq l_i} f_j(l)$$

Si bien que si on note F la matrice dont les coefficients sont les $f_j(l_i)$ et G celle dont les coefficients sont les $g_j(l_i)$ alors $G = BF$ où B est une matrice triangulaire inférieure (à cause de l'indexation des éléments de \mathbb{L}) ayant des 1 sur la diagonale. Donc la matrice B est inversible et comme F aussi par le choix des fonctions f_j , il en découle que G est inversible.

Par hypothèse on sait que $F = AG$ où les coefficients de A sont des zéros ou des $a(x, y)$. Alors $A = FG^{-1}$. On en conclut que A est entièrement déterminée par F et G ce qui montre le résultat.

Pour calculer la fonction de Möbius d'un ensemble concret L on peut donc penser aux diverses démarches suivantes:

- Calculer tous les coefficients $c_p(x, y)$.
- Utiliser la proposition 2.1 pour calculer par récurrence les $\mu_{\mathbb{L}}(x, y)$.
- Utiliser une formule d'inversion connue par d'autres moyens pour en déduire grâce au théorème 3.2 la fonction de Möbius.

4 Exemples

4.1 Intervalles finis d'entiers

Prenons $\mathbb{L} = \{1, 2, \dots, n\}$ muni de l'ordre habituel. La fonction de Möbius dans ce cas est donnée par

$$\mu_{\mathbb{L}}(i, i) = 1$$

$$\mu_{\mathbb{L}}(i, i + 1) = -1$$

et pour $j > i + 1$

$$\mu_{\mathbb{L}}(i, j) = 0.$$

Proof. Nous avons déjà vu que la relation $\mu_{\mathbb{L}}(x, x) = 1$ a lieu dans tous les cas.

Pour la deuxième égalité il suffit de voir que le coefficient $c_r(i, i + 1)$ est nul sauf pour $r = 1$ auquel cas il vaut 1.

Enfin quand $j > i + 1$

$$\mu_{\mathbb{L}}(i, j) = \sum_{p=1}^{j-i} (-1)^p c_p(i, j)$$

et comme $c_p(i, j)$ est égal au coefficient binomial C_{j-i-1}^{p-1} la somme considérée est nulle.

Ainsi si $g(i) = \sum_{j=1}^i f(j)$ alors par la formule d'inversion de Rota on trouve la relation bien claire

$$f(i) = g(i) - g(i - 1).$$

On aurait pu partir de cette relation visiblement vraie et utiliser le théorème 3.2 pour en déduire la fonction de Möbius.

4.2 Diviseurs d'un entier

On se place dans l'ensemble \mathbb{N} des nombres naturels. Soit $n \in \mathbb{N}$ et \mathbb{L} l'ensemble des diviseurs de n ordonné par la relation de divisibilité. La fonction de Möbius dans ce cas est

$$\mu_{\mathbb{L}}(r, s) = \mu(s/r)$$

où μ est la fonction de Möbius classique donnée par

$$\mu(1) = 1$$

si p_1, p_2, \dots, p_k sont des nombres premiers distincts

$$\mu(p_1 \cdot p_2 \cdots p_k) = (-1)^k$$

et dans tous les autres cas

$$\mu(r) = 0.$$

Proof. Remarquons tout d'abord que $\mu_{\mathbb{L}}(r, s) = \mu_{\mathbb{L}}(1, r/s)$. Si on considère la fonction de Möbius arithmétique il est facile de voir que $\sum_{z|y} \mu(z) = 0$ ou encore $\mu(y) = -\sum_{z|y, z \neq y} \mu(z)$. Comme $\mu_{\mathbb{L}}(1, y)$ vérifie la même relation de récurrence et que $\mu_{\mathbb{L}}(1, 1) = \mu(1)$ on conclut que $\mu_{\mathbb{L}}(1, y) = \mu(y)$. D'où le résultat annoncé.

Ici on a pu déterminer la fonction de Möbius sans faire appel au nombre de chaînes.

4.3 Parties d'un ensemble fini

Soit S un ensemble fini et $\mathbb{L} = \mathcal{P}(S)$ l'ensemble des parties de S ordonné par inclusion. La fonction de Möbius dans ce cas est

$$\mu_{\mathbb{L}}(A, B) = (-1)^{\#B - \#A}$$

(où $\#X$ désigne le nombre d'éléments de X) si $A \subset B$ et

$$\mu_{\mathbb{L}}(A, B) = 0$$

sinon.

Proof. La démonstration se fait par récurrence sur $\#(B-A)$. Si $\#(B-A) = 0$ (cas où $A=B$) le résultat est vrai (on obtient bien $\mu_{\mathbb{L}}(A, A) = 1$). Supposons le résultat vrai pour toutes les parties $A \subset B$ telles que $\#(B-A) = k$ et montrons le résultat pour un couple B, A , où $A \subset B$ et $\#(B-A) = k+1$. Alors

$$\sum_{A \subset T \subset B} \mu_{\mathbb{L}}(A, T) = 0$$

et par hypothèse de récurrence

$$\sum_{A \subset T \subsetneq B} (-1)^{\#T - \#A} + \mu_{\mathbb{L}}(A, B) = 0.$$

Or il y a autant de parties entre A et B ayant un nombre pair d'éléments que de parties ayant un nombre impair d'éléments par suite

$$\sum_{A \subset T \subset B} (-1)^{\#T - \#A} = 0$$

donc

$$\mu_{\mathbb{L}}(A, B) = (-1)^{\#B - \#A}.$$

4.4 Transformation de Reed et Müller

Soit $\mathbb{L} = \{0, 1\}^m$. Si $u = (u_1, u_2, \dots, u_m) \in \mathbb{L}$ notons

$$\text{supp}(u) = \{i \mid u_i \neq 0\}.$$

Sur \mathbb{L} on considère la relation d'ordre

$$(u \leq v) \iff (\text{supp}(u) \subset \text{supp}(v)).$$

Dans ce cas la fonction de Möbius est

$$\mu_{\mathbb{L}}(u, v) = (-1)^{\#\text{supp}(u) - \#\text{supp}(v)}.$$

Proof. On se ramène clairement à l'exemple précédent des parties d'un ensemble fini.

Remarquons qu'on sait que si f est une fonction booléenne de m variables booléennes et si on pose

$$g(u) = \sum_{v \leq u} f(v)$$

alors

$$f(u) = \sum_{v \leq u} g(v).$$

On est ici dans un cas où une formule d'inversion (transformation de Reed Müller) ne nous permet pas de retrouver la fonction de Mobius (bien sûr à partir de la fonction de Mobius on retrouve cette formule puisque dans $\{0, 1\}$ $1 = -1$).

4.5 Formule d'inclusion exclusion

Soit E un ensemble fini non vide, P_1, P_2, \dots, P_n , des sous ensembles de E . Notons S l'ensemble $\{1, \dots, n\}$ et $\mathcal{P}(S)$ l'ensemble de ses parties, ordonné par inclusion. Définissons les fonctions f et g de $\mathcal{P}(S)$ dans \mathbb{Z} par

$$f(I) = \# \left(\bigcap_{i \in I} P_i \bigcap_{i \notin I} \overline{P_i} \right)$$

$$g(I) = \# \left(\bigcap_{i \in I} P_i \right).$$

Rappelons que si $I = \emptyset$ alors $\bigcap_{i \in I} P_i = E$.
On vérifie que

$$g(I) = \sum_{I \subset J} f(J),$$

et donc par inversion

$$f(I) = \sum_{I \subset J} (-1)^{\#J - \#I} g(J).$$

En particulier si $I = \emptyset$ alors

$$\# \left(\bigcap_{1 \leq i \leq n} \overline{P}_i \right) = \sum_{k \geq 0} (-1)^k \sum_{\#J=k} g(J),$$

ou encore par passage au complémentaire

$$\# \left(\bigcup_{1 \leq i \leq n} P_i \right) = \#E - \sum_{k \geq 0} (-1)^k \sum_{\#J=k} g(J) = \sum_{k \geq 1} (-1)^{k+1} \sum_{\#J=k} g(J).$$

4.6 Familles d'hyperplans

Soit \mathcal{A} un arrangement d'hyperplans (nombre fini d'hyperplans d'un espace vectoriel de dimension finie V). Soit $\mathbb{L} = L(\mathcal{A})$ l'ensemble des intersections d'éléments de \mathcal{A} . Sur \mathbb{L} on met la relation d'ordre $(X \leq Y) \iff (Y \subset X)$. La fonction de Möbius obtenue est appelée fonction de Möbius de l'arrangement. Cette fonction dépend de l'arrangement. Dans certains cas particulier on sait calculer cette fonction.

Remarquons que V qui peut être considéré comme l'intersection de zéro éléments de \mathcal{A} est dans \mathbb{L} , et avec la relation d'ordre considérée, V est le plus petit élément de \mathbb{L} . On définit alors

$$\mu(X) = \mu(V, X).$$

Dans le cas où $V = \mathbb{F}_q^n$ on obtient la formule

$$\# \left(\bigcup_{H \in \mathcal{A}} H \right) = q^n - \sum_{X \in \mathbb{L}} \mu(X) q^{\dim(X)}.$$

Pour démontrer cette formule il suffit de montrer que

$$\# \left(\bigcap_{H \in \mathcal{A}} \overline{H} \right) = \sum_{X \in \mathbb{L}} \mu(X) q^{\dim(X)}.$$

Ceci se fait comme pour la formule d'inclusion exclusion. Soit $X \in \mathbb{L}$, et $\mathcal{B}(X)$ le sous ensemble de \mathcal{A} constitué des hyperplans qui contiennent X . Définissons :

$$X' = X \bigcap_{H \notin \mathcal{B}(X)} \overline{H},$$

puis :

$$f(X) = \#X'$$

et

$$g(X) = \#X.$$

Alors on vérifie que :

$$g(X) = \sum_{X \leq Y} f(Y)$$

et donc

$$f(X) = \sum_{X \leq Y} \mu(X, Y) g(Y).$$

Si on prend $X = V$ on trouve la formule annoncée.

Preuve du fait que :

$$X = \bigcup_{X \leq Y} Y'$$

où la réunion est disjointe.

Si $Y_1 \subseteq X$ et $Y_2 \subseteq X$ sont deux éléments de \mathbb{L} tels que $Y_1 \neq Y_2$, alors on peut se ramener au cas où il existe un hyperplan H de $\mathcal{B}(Y_1)$ qui n'est pas dans $\mathcal{B}(Y_2)$. De ce fait, $Y_2' \subseteq \overline{H}$ tandis que $Y_1' \subseteq Y_1 \subseteq H$. On en conclut que Y_1' et Y_2' sont disjoints.

Soit $x \in X$. Notons $\mathcal{B}(x)$ l'ensemble des hyperplans de \mathcal{A} qui contiennent le point x . Posons :

$$Y = \bigcap_{H \in \mathcal{B}(x)} H.$$

Alors $Y \in \mathbb{L}$ et $Y \subseteq X$. Il est clair que si $H \notin \mathcal{B}(Y)$ alors $H \notin \mathcal{B}(x)$, donc $x \notin H$ et par suite $x \in \overline{H}$. On en conclut que $x \in Y'$. Ceci achève la preuve.

4.7 Nombre de polynômes irréductibles sur un corps fini

Nous allons compter le nombre N_k de polynômes irréductibles et normalisés (dont le coefficient du terme de plus haut degré est 1) de degré k sur le corps fini \mathbb{F}_q à q éléments. Le calcul utilise la fonction de Möbius μ sur les entiers (fonction liée à la relation de divisibilité sur \mathbb{N}).

Considérons le corps fini \mathbb{F}_{q^k} , extension de degré k de \mathbb{F}_q . On sait qu'on a la factorisation suivante sur \mathbb{F}_q :

$$X^{q^k} - X = \prod Q(X)$$

où les polynômes $Q(X)$ sont tous les polynômes irréductibles normalisés de degré $\leq k$ sur \mathbb{F}_q . Ces polynômes ont des degrés l qui divisent k , ils se décomposent entièrement sur \mathbb{F}_{q^k} où ils ont chacun l racines distinctes, et distinctes des racines des autres. Globalement ces racines sont exactement les q^k éléments de \mathbb{F}_{q^k} . En conséquence :

$$\sum_{l|k} lN_l = q^k.$$

Si on pose :

$$g(k) = q^k$$

et

$$f(k) = kN_k,$$

on voit que :

$$g(k) = \sum_{l|k} f(l).$$

Donc par inversion de Möbius on obtient :

$$f(k) = \sum_{l|k} \mu(k/l)g(l),$$

soit aussi en posant $u = k/l$:

$$f(k) = \sum_{u|k} \mu(u)g(k/u).$$

Donc on obtient :

$$N_k = \frac{1}{k} \sum_{u|k} \mu(u) q^{k/u}.$$

5 Aspect fonctionnel

Soit \mathbb{L} un ensemble **fini ordonné** par une relation notée \leq . Notons $\mathbb{A}(\mathbb{L})$ l'espace des fonctions f de $\mathbb{L} \times \mathbb{L}$ dans \mathbb{R} telles que $f(x, y) = 0$ si $x \not\leq y$. Définissons en outre la multiplication dans $\mathbb{A}(\mathbb{L})$ par

$$f \star g(x, y) = \sum_{x \leq z \leq y} f(x, z)g(z, y).$$

On obtient ainsi une algèbre dont l'unité est

$$\delta(x, y) = \begin{cases} 1 & \text{si } x = y, \\ 0 & \text{sinon.} \end{cases}$$

Theorem 5.1 *Un élément f de l'algèbre $\mathbb{A}(\mathbb{L})$ a un inverse si et seulement si $f(x, x) \neq 0$.*

La condition est nécessaire car dans ce cas

$$\sum_{x \leq z \leq y} f(x, z)g(z, y) = \delta(x, y),$$

ce qui donne pour $x = y$, $f(x, x)g(x, x) = 1$. Réciproquement, l'égalité précédente définit $g(x, y)$ lorsque $\sharp[x, y] = 1$. Par récurrence en supposant $g(x, y)$ défini lorsque $\sharp[x, y] = k$, montrons qu'on peut définir $g(x, y)$ lorsque $\sharp[x, y] = k + 1$. Pour cela puisque $x \neq y$ il suffit de voir qu'en prenant

$$f(x, x)g(x, y) = - \sum_{x < z \leq y} f(x, z)g(z, y)$$

on obtient ce qu'il faut (on obtient un inverse à gauche, mais comme pour tout h on a $\delta \star h = h \star \delta = h$, c'est aussi un inverse à droite).

Definition 5.1 *La fonction ζ définie par*

$$\zeta(x, y) = \begin{cases} 1 & \text{si } x \leq y, \\ 0 & \text{sinon.} \end{cases}$$

est la fonction zeta.

Theorem 5.2 *La fonction zeta a un inverse qui est la fonction de Möbius.*

Pour le montrer il suffit d'effectuer la convolution $\mu \star \zeta$ ou la convolution $\zeta \star \mu$. Dans les deux cas on trouve facilement δ .

Ce dernier résultat permet en fait de rétablir la formule d'inversion de Rota. Pour ce faire il faut tout d'abord remarquer que puisqu'on suppose \mathbb{L} fini, on peut toujours lui rajouter un élément noté 0 plus petit que tous les autres. Dans ces conditions si on définit

$$G = F \star \zeta$$

on a alors

$$F = G \star \mu.$$

En posant $g(x) = G(0, x)$ et $f(x) = F(0, x)$ et en plus en posant $F(0, 0) = 0$ (ce qui implique $G(0, 0) = 0$) on obtient d'une part

$$g(x) = G(0, x) = F \star \zeta(0, x) = \sum_{0 \leq z \leq x} F(0, z) \zeta(z, x),$$

$$g(x) = \sum_{z \leq x} f(z),$$

d'autre part

$$f(x) = F(0, x) = G \star \mu(0, x) = \sum_{z \leq x} \mu(z, x) f(z).$$

6 Produit d'ensembles ordonnés

Soient $\mathbb{L}_1, \dots, \mathbb{L}_n$ des ensembles ordonnés finis. On considère l'ensemble $\mathbb{L} = \prod_{i=1}^n \mathbb{L}_i$ ordonné par l'ordre produit ($x \leq y$ si et seulement si $x_i \leq y_i$ pour tout i).

Theorem 6.1 *La fonction de Möbius du produit \mathbb{L} est le produit des fonctions de Möbius des \mathbb{L}_i .*

Ceci se voit facilement en utilisant la fonction zeta qui vérifie clairement

$$\zeta(x, y) = \prod_{i=1}^m \zeta_i(x_i, y_i)$$

en conséquence de quoi la fonction

$$\prod_{i=1}^m \mu_i(x_i, y_i)$$

est l'inverse pour la convolution de la fonction zeta. C'est donc la fonction de Möbius.

Exemple: Définissons pour tout nombre premier p l'ensemble

$$E_p = \{1, p, p^2, \dots, p^k, \dots\}$$

que nous munissons de l'ordre naturel. Ainsi la fonction de Möbius de E_p est

$$\mu_p(p^i, p^j) = \begin{cases} 1 & \text{si } i = j, \\ -1 & \text{si } j = i + 1, \\ 0 & \text{dans les autres cas.} \end{cases}$$

Le produit des ensembles ordonnés E_p (limité aux suites formées de 1 à partir d'un certain rang) n'est rien d'autre que \mathbb{N} ordonné par la divisibilité. On obtient ainsi la fonction de Möbius classique comme produit des fonctions de Möbius des E_p .