DS 3 de mathématiques

1 Formule d'inversion de Möbius

1.1 Cadre théorique

0. Si $n \in \mathbb{N}$ et si $x = x_0 < x_1 < \cdots < x_n = y$, on a, pour tous $i < j$: $x_i < x_j$ par transitivité. En particulier, si $i \neq j$, alors x_i et x_j sont distincts. Donc, pour un tel n, on a $n \leq |P|$.

   Si on note A l'ensemble des $n \in \mathbb{N}$ tels qu'il existe $(x_0, \ldots, x_n)$ comme dans la définition, on a donc que A est une partie majorée de $\mathbb{N}$. De plus, si $x = y$, on a $0 \in A$ (en considérant $x = x_0 = y$ et si $x < y$, on a $1 \in A$ (en considérant $x = x_0 < x_1 = y$). Dans les deux cas, A est non vide. Donc A admet un plus grand élément et la notion de distance est bien définie.

   Si $x = y$, on ne peut pas prendre de $n \geq 1$ car si $x = x_0 < x_1 < \cdots < x_n = y$, avec $n \geq 1$, l'inégalité $x < y$. Donc, si $x = y$, $d(x, y) = 0$.

   Réciproquement, si $d(x, y) = 0$, il existe x_0 tel que $x = x_0 = y$. Donc $x = y$.

1. Soit $x \in P$. On note $\mathcal{P}(k)$ la propriété suivante :

   Il existe une unique définition de μ sur les couples (x, z) pour lesquels $d(x, z) \leq k$, telle que, pour ces couples :

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

   On le montre par récurrence sur $k \in \mathbb{N}$.

   - Initialisation. Si $k = 0$, le seul z tel que $d(x, z) = 0$ est $z = x$. μ doit alors vérifier $\mu(x, x) = 1$, ce qu'on impose.
   - Hérédité. On suppose $\mathcal{P}(k)$ vraie pour un $k \in \mathbb{N}$ et on montre $\mathcal{P}(k+1)$. Soit $z \in P$ tel que $x \leq z$ et $d(x, z) \leq k + 1$. Si $d(x, z) \leq k$, la définition de $\mu(x, z)$ provient de l'hypothèse de récurrence ; on suppose donc $d(x, z) = k + 1$. La seule contrainte sur la valeur de $\mu(x, z)$ est alors donnée par la relation

$$\sum_{x \leq y \leq z} \mu(x, y) = 0,$$

ce qui revient à demander que $\mu(x,z) = -\sum_{x\leq y<z} \mu(x,y)$. Les y intervenant dans cette somme sont à distance $\leq k$ de x (sinon, on montre que z est à distance $\geq k+2$ de x) ; donc les valeurs $\mu(x,y)$ sont déterminées de façon unique par hypothèse de récurrence. Dès lors, la valeur de $\mu(x,z)$ est aussi déterminée de façon unique.

Par récurrence, on a $\mathcal{P}(k)$, pour tout $k \in \mathbb{N}$. Or, si $(x,z) \in P^{2,\leq}$, on a $d(x,z) \leq |P|$ par exemple. Donc, l'assertion $\mathcal{P}(|P|)$ est équivalence à l'énoncé de la question. Ceci conclut.

2. Soient f et g deux applications de P dans $\mathbb{R}$. On suppose $i)$ et on montre $ii)$. Soit $y \in P$.

$$\begin{aligned}\sum_{x\leq y} g(x)\mu(x,y) &= \sum_{x\leq y} \big(\sum_{u\leq x} f(u)\big)\mu(x,y)\\ &= \sum_{u\leq x\leq y} f(u)\mu(x,y)\\ &= \sum_{u\leq y} f(u) \sum_{u\leq x\leq y} \mu(x,y)\\ &= \sum_{u\leq y} f(u)\delta_{u,y}\\ &= f(y).\end{aligned}$$

On suppose $ii)$ et on montre $i)$. Soit $x \in P$.

$$\begin{aligned}\sum_{x\leq y} f(x) &= \sum_{x\leq y} \big(\sum_{u\leq x} g(u)\mu(u,x)\big)\\ &= \sum_{u\leq x\leq y} g(u)\mu(u,x)\\ &= \sum_{u\leq y} g(u) \sum_{u\leq x\leq y} \mu(u,x)\\ &= \sum_{u\leq y} g(u)\delta_{u,y}\\ &= g(y).\end{aligned}$$

1.2 Principe d'inclusion-exclusion

3. La distance de A à B est le plus grand entier naturel n tel qu'il existe des parties $A_0, \ldots, A_n$ dans E avec $A = A_0 \subsetneq A_1 \subsetneq \cdots \subsetneq A_n = B$. Si on a une telle chaine d'inclusions, on a, par une récurrence finie immédiate, que $|B| \geq |A| + n$.

Réciproquement, on peut construire une telle chaine avec $n = |B| - |A|$, en ajoutant un à un à A les éléments de $B - A$.

Donc, $d(A, B) = |B| - |A|$.

4. Soient A, C dans P telles que $A \subset C$. On calcule $\sum_{A \subset B \subset C} \mu(A, B)$.

$$\begin{aligned}
\sum_{A \subset B \subset C} \mu(A, B) &= \sum_{A \subset B \subset C} (-1)^{|B|-|A|} \\
&= \sum_{k=|A|}^{|C|} \sum_{\substack{A \subset B \subset C \\ |B|=k}} (-1)^{k-|A|} \\
&= \sum_{k=|A|}^{|C|} \binom{|C| - |A|}{k - |A|} (-1)^{k-|A|} \\
&= \sum_{l=0}^{|C|-|A|} \binom{|C| - |A|}{l} (-1)^{l} \\
&= (1-1)^{|C|-|A|} \\
&= \delta_{A,C}.
\end{aligned}$$

5. **Première application.** On suppose les suites u et v comme dans l'énoncé. Soit $n \in \mathbb{N}$. On se place dans $P = \mathcal{P}(E)$, avec $E = [\![1, n]\!]$. On considère f et g définies de P dans $\mathbb{R}$ par

$$\forall I \in P, f(I) = u_{|I|} \text{ et } g(I) = \sum_{J \subset I} f(J).$$

On a donc, $\forall I \in P, g(I) = \sum_{k=0}^{|I|} \binom{|I|}{k} u_k = v_{|I|}$. On applique maintenant la (première) formule d'inclusion-exclusion :

$$\begin{aligned}
u_n &= f([\![1, n]\!]) \\
&= \sum_{I \subset [\![1,n]\!]} v_{|I|} (-1)^{n-|I|} \\
&= \sum_{k=0}^{n} \binom{n}{k} v_k (-1)^{n-k}.
\end{aligned}$$

6. **Deuxième application.**

   (a) Pour $I \in \mathcal{P}(E)$, notons B_I l'ensemble $\left(\bigcap_{i \in I} A_i\right) \bigcap \left(\bigcap_{j \in \overline{I}} \overline{A_j}\right)$. B_I est l'ensemble des éléments qui sont exactement dans les ensembles A_i pour $i \in I$ (et pas dans

les autres). Ainsi, $\bigcup_{I\subset J} B_J$ est une union disjointe et est l'ensemble des éléments qui sont exactement dans A_j, pour $j \in J$, où J est un ensemble contenant I. Cela revient simplement à dire que $\bigcup_{I\subset J} B_J = \bigcap_{i\in I} A_i$. Donc, comme l'union était disjointe, on a par principe d'addition :

$$\forall I \in \mathcal{P}(E), g(I) = |\bigcap_{i\in I} A_i|.$$

(b) On applique la (deuxième) formule d'inclusion-exclusion à $f(\emptyset)$. On a donc :

$$|\bigcap_{i\in I} \overline{A_i}| = f(\emptyset) = \sum_{J\subset[\![1,n]\!]} (-1)^{|J|-0} g(J) = \sum_{J\subset[\![1,n]\!]} (-1)^{|J|} |\bigcap_{j\in J} A_j|.$$

1.3 Inversion de Möbius dans $\mathbb{N}^*$

7. Soit $n > 1$. On note $p_1, \ldots, p_r$ les nombres premiers divisant n et $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ la décomposition en facteurs premiers, avec donc $\alpha_i \geq 1$, pour tout i. Les diviseurs d de n sont de la forme $d = \prod_{i=1}^{r} p_i^{\beta_i}$ où $\beta_i \leq \alpha_i$, pour tout i. Ceux pour lesquels au moins un β_i est ≥ 2 sont tels que $\tilde{\mu}(d) = 0$. Donc les seuls diviseurs comptant dans la somme sont ceux de la forme $\prod_{k\in K} p_k$ où $K \subset [\![1, r]\!]$. Ainsi,

$$\begin{aligned}
\sum_{\substack{d|n \\ d>0}} \tilde{\mu}(d) &= \sum_{K\subset[\![1,r]\!]} \tilde{\mu}(\prod_{k\in K} p_k) \\
&= \sum_{k=0}^{r} \sum_{|K|=k} (-1)^k \\
&= \sum_{k=0}^{r} \binom{r}{k} (-1)^k \\
&= (1-1)^r \\
&= 0
\end{aligned}$$

car $r \geq 1$ (car $n \geq 2$).

8. **Une application.**

(a) Soit $d \in [\![1, N]\!]$. L'union $B_d = \bigcup_{d|n} H_n^N$ est disjointe car le pgcd d'un couple (u, v)

ne peut pas prendre deux valeurs différentes. Donc,

$$|B_d| = \sum_{\substack{1\leq n\leq N \\ d|n}} |H_n^N|.$$

Un couple $(u,v) \in [\![1,N]\!]^2$ est dans B_d ssi $u \wedge v = n$, où $d \mid n$, c'est-à-dire ssi $d \mid u \wedge v$. Ceci est équivalent à $d \mid u$ et $d \mid v$. On compte donc les couples d'entiers $(u,v) \in [\![1,N]\!]$, tous deux divisibles par d. On a $\lfloor \frac{N}{d} \rfloor$ multiples de d entre 1 et N. Donc, $|B_d| = \lfloor \frac{N}{d} \rfloor^2$, ce qui montre le résultat.

(b) Par la (deuxième) formule d'inversion de Möbius, on déduit de la question précédente que

$$|H_1^N| = \sum_{1|n} \lfloor \frac{N}{n} \rfloor^2 \mu(1,n) = \sum_{n=1}^{N} \tilde{\mu}(n) \lfloor \frac{N}{n} \rfloor^2.$$

2 Théorème d'Erdős-Ginzburg-Ziv

2.1 Généralités et structure de la démonstration

1. Soient x_1, x_2 et x_3 trois entiers naturels. Par principe des tiroirs (version bébé), deux au moins ont même parité. Leur somme est divisible par 2.

2. Soient x_1, x_2, x_3, x_4, x_5 des entiers naturels. On note r_i le reste de x_i dans la division euclidienne par 3. On a l'un des cas suivants :

   - Trois r_i (au moins) sont égaux. Alors, la somme des x_i est divisible par 3.
   - Les trois restes possibles 0, 1 et 2 apparaissent. Alors, la somme des trois nombres ayant ces restes est divisible par 3.

3. Considérons les entiers $x_1 = \cdots = x_{n-1} = 0$ et $x_n = x_{n+1} = \cdots = x_{2n-2} = 1$. Alors une somme de n de ces entiers est strictement positive (car il n'y a que $n-1$ valeurs 0), mais strictement inférieure à n (car il n'y a que $n-1$ valeurs 1). Dès lors, aucune de ces sommes n'est divisible par n.

4. Soient $n, m \geq 2$ tels que $\mathcal{P}(n)$ et $\mathcal{P}(m)$ sont vraies. On considère $x_1, \ldots, x_{2nm-1}$ des entiers. Comme $\mathcal{P}(n)$ est vraie, on peut en choisir n dont la somme est divisible par n. Notons y_1 cette somme et $x_{i_1}, \ldots, x_{i_n}$ les entiers pris. On enlève ces entiers et on en prend n autres dont la somme est divisible par n ; on note y_2 cette somme et $x_{i_{n+1}}, \ldots, x_{i_{2n}}$ ces entiers. On continue ce procédé jusqu'à ce que le nombre d'entiers restants soit strictement inférieur à $2n-1$. Comme $2nm-1 = n(2m-1)+n-1$, on peut faire $2m-1$ étapes (à la dernière étape, on a bien $n+(n-1) = 2n-1$ éléments parmi lesquels choisir).

A ce stade, on a donc $2m-1$ paquets de n nombres dont les sommes, notées $y_1, \ldots, y_{2m-1}$ sont toutes divisibles par n. On note $u_i = y_i/n$. En appliquant $\mathcal{P}(m)$ aux u_i, on peut en sélectionner m dont la somme est divisible par m. La somme des y_i correspondants est donc divisible par nm. Comme chaque y_i est une somme de n nombres x_j, on a finalement une somme de nm nombres x_j divisible par nm.

5. Supposons que $\mathcal{P}(p)$ est établi pour tout nombre premier p. Par le résultat précédent, on a $\mathcal{P}(n)$ pour tout n qui est produit de deux nombres premiers (non nécessairement distincts). Puis, on a $\mathcal{P}(n)$ pour tout nombre produit de trois nombres premiers, etc. Par une récurrence immédiate, $\mathcal{P}(n)$ est alors vrai, pour tout nombre n, produit d'un nombre fini de nombres premiers. Or, par le théorème fondamental de l'arithmétique, tout $n \geq 2$ est produit de nombres premiers. Ce qui conclut.

2.2 Démonstration de $\mathcal{P}(p)$, p premier

6. On fait une interversion de somme.

$$\begin{aligned} S &= \sum_{|I|=p} S_I^{p-1} \\ &= \sum_{|I|=p} \sum_{\substack{0\leq\alpha_1,\ldots,\alpha_p\leq p-1 \\ \alpha_1+\cdots+\alpha_p=p-1}} \binom{p-1}{\alpha_1,\ldots,\alpha_p} \prod_{i_j\in I} x_{i_j}^{\alpha_j} \\ &= \sum_{\substack{0\leq\alpha_1,\ldots,\alpha_p\leq p-1 \\ \alpha_1+\cdots+\alpha_p=p-1}} \binom{p-1}{\alpha_1,\ldots,\alpha_p} \sum_{|I|=p} \prod_{i_j\in I} x_{i_j}^{\alpha_j} \end{aligned}$$

Considérons des indices $\alpha_1, \ldots, \alpha_p \in [\![1, p-1]\!]$ tels que $\alpha_1 + \cdots + \alpha_p = p-1$. Notons K l'ensemble des indices des α_k différents de 0. On a $|K| = k$, pour un entier $k \in [\![1, p-1]\!]$ (l'un au moins est nul mais tous ne le sont pas). Tous les I de cardinal p contenant K vont donner les mêmes $\prod_{i_j\in I} x_{i_j}^{\alpha_j}$. Il y a $\binom{2p-1-k}{p-k}$ telles parties I contenant K (il faut choisir $p-k$ indices parmi les $2p-1-k$ indices restants dans le complémentaire de K). Ainsi, on a :

$$S = \sum_{\substack{0\leq\alpha_1,\ldots,\alpha_p\leq p-1 \\ \alpha_1+\cdots+\alpha_p=p-1}} \binom{p-1}{\alpha_1,\ldots,\alpha_p} \binom{2p-1-|K(\alpha_1,\ldots,\alpha_p)|}{p-|K(\alpha_1,\ldots,\alpha_n)} \prod_{i\in K(\alpha_1,\ldots,\alpha_p)} x_i^{\alpha_i}.$$

D'après la question précédente, chacun des coefficients binomiaux de la forme $\binom{2p-1-k}{p-k}$ est divisible par p. Donc, S, combinaison linéaire ces coefficients est aussi divisible par p.

7. Si $\mathcal{P}(p)$ est faux, aucune somme S_I n'est divisible par p. Comme p est premier, on a $S_I \wedge p = 1$ pour tout I. Donc, par le petit théorème de Fermat, on a $S_I^{p-1} \equiv 1\,[p]$, pour tout I. En sommant, il vient :

$$S \equiv \sum_{[I|=p} 1 \equiv \binom{2p-1}{p}\,[p].$$

Or, $\binom{2p-1}{p} = \dfrac{(2p-1)\cdots\times p}{p!} = \dfrac{(2p-1)(2p-2)\ldots(p+1)}{(p-1)!}$. Comme p est premier avec tous les facteurs du numérateur, il ne divise pas le numérateur. En particulier, p ne divise pas $\binom{2p-1}{p}$. D'où la contradiction.

Ainsi, $\mathcal{P}(p)$ est vraie pour tout nombre premier p. Donc $\mathcal{P}(n)$ est vraie pour tout entier $b \geq 2$, d'après la question 5.

3 Théorème de l'amitié

3.1 Tous les $d(x)$ sont égaux.

0. cf. fichier amitie.pdf

1. Supposons l'existence d'un 4-cycle $(x_0, x_1, x_2, x_3, x_4)$ dans E (avec donc $x_0 = x_4$). Par définition, x_1 et x_3 sont donc adjacents à x_0 et x_2. Or x_1 et x_3 sont supposés distincts. Ceci contredit l'hypothèse $|N(x_1) \neq N(x_3)| = 1$.

2. Voir le fichier joint pour le graphique.

   - x et y sont distincts par hypothèse.
   - z est distinct de x et y car sinon x et y seraient adjacents.
   - u est distinct de x et z car il leur est adjacent ; il est distinct de y car sinon x serait adjacent à y.
   - De même, v est distinct de x, y et z.
   - u et v sont distincts car sinon, $u = v$ serait adjacent à x et y (mais $x \vee y = z \neq u$).
   - Un u_i est distinct de x et de u car il leur est adjacent ; il est distinct de z par hypothèse ; u_i est différent de y car il est adjacent à x ; u_i est différent de v car sinon $(x, u_i = v, y, z, x)$ est un 4-cycle.
   - Un v_i est distinct de u_i et de y car il leur est adjacent ; il est distinct de u car sinon on a un 4-cycle $(x, u = v_i, y, z, x)$; il est distinct de v car sinon on a un 4-cycle $(z, u, u_i, v_i = v, z)$; il est distinct de z car sinon on a un 4-cycle $(x, u_i, v_i = z, u, x)$; il est distinct de v car sinon on a un 4-cycle $(x, u_i, v_i = v, z, x)$; il est distinct de u_j (avec $j \neq i$) car sinon on a un 4-cycle $(x, u_j = v_i, u_i, u, x)$

- Enfin, si $i \neq j$, v_i et v_j sont distincts. Sinon, on a un 4-cycle $(x, u_i, v_i = v_j, u_j, x)$.

3. Avec les notations précédentes, on a $d(x) = s + 2$. Or, on a construit $s + 2$ éléments adjacents à y : z, v et les v_i et on a montré qu'ils étaient deux à deux distincts. On en déduit que $d(y) \geq d(x)$.

   Par symétrie des rôles joués par x et y, on a aussi $d(x) \geq d(y)$. Donc $d(x) = d(y)$ si x et y ne sont pas adjacents.

4. Supposons par l'absurde qu'il existe deux éléments $x, y \in E$ tels que $d(x) \neq d(y)$. D'après ce qui précède, $d(x)$ et $d(y)$ doivent être adjacents. Notons $z = x \vee y$. On doit avoir $d(z) \neq d(x)$ ou $d(z) \neq d(y)$. Disons $d(z) \neq d(x)$. Comme $(E, \mathcal{R})$ ne vérifie par la propriété (B), il existe un $u \in E - \{x, y, z\}$, non adjacent à x. Par la question précédente, on a $d(u) = d(x)$. Donc $d(u) \neq d(y)$ et $d(u) \neq d(z)$. Toujours par la question précédente, u et y sont adjacents ; de même u et z sont adjacents. On a alors un 4-cycle (x, z, u, y, x), ce qui est absurde.

5. Fixons x un élément de E. Notons $N(x) = \{x_1, \ldots, x_m\}$. Comme $x_i \vee x$ est adjacent à x, c'est l'un des x_j. Quitte à renuméroter, on peut supposer que x_1 et x_2 sont adjacents, x_3 et x_4,..., jusqu'à x_{m-1} et x_m (en particulier m est pair) et qu'il n'y a pas d'autres couples x_i, x_j de points adjacents.

   Considérons un $u \in E - \{x, x_1, x_2, \ldots, x_m\}$. Nécessairement $u \vee x$ est l'un des x_i. De plus, chaque x_i a m points adjacents : x, un x_j et $m - 2$ autres points (et il n'y a pas de recoupement). Il y a donc $m(m-2)$ points de $E - \{x, x_1, x_2, \ldots, x_m\}$. D'où $N = 1 + m + m(m-2) = m(m-1) + 1$.

3.2 Conclusion arithmético-combinatoire

6. Considérons deux boucles $(x_0, \ldots, x_p)$ et $(y_0, \ldots, y_p)$. On dira qu'elles sont équivalentes s'il existe $k \in [\![0, p-1]\!]$ tel que, en considérant les indices modulo p, on a $x_0 = y_k$, $x_1 = y_{k+1}$,...,$x_{p-1} = y_{k+p-1}$. *Les boucles considérées passent donc pas les mêmes sommets, dans le même ordre, mais en changeant le point initial.* On vérifie aisément que c'est une relation d'équivalence.

   Notons $B_0 = (x_0, \ldots, x_p)$ une boucle et $B_i = (x_i, x_{i+1}, \ldots, x_i)$ la boucle équivalente à B_0 et commençant en x_i (pour $i \in [\![0, p-1]\!]$). La classe d'équivalence de B_0 est $\{B_0, \ldots, B_{p-1}\}$. De plus, si deux boucles B_i et B_j sont égales, avec $i \neq j$, on a avec $k = j - i$, que $x_l = x_{l+k}$ pour tout $l \in [\![0, p-1]\!]$ (modulo p sur les indices). Par une récurrence immédiate, $x_l = x_{l+nk}$, pour tout entier n. Pour tout $i \in [\![0, p-1]\!]$, l'équation $i \equiv l + nk\,[p]$ a une solution (prendre pour n un inverse de k modulo p, multiplié par $i - l$).

   Ainsi, tous les sommets de la boucle seraient égaux. Ce qui est absurde puisqu'un sommet n'est pas adjacent à lui-même.

   Donc, toutes les classes d'équivalence ont cardinal p. Donc $|\mathcal{B}_p| \equiv 0\,[p]$.

7. Par définition, $K_1 + K_2 = K$. De plus, pour définir un élément de $\mathcal{C}_{p-2}$, on a N choix pour le sommet initial, m choix pour le point suivant (qui doit lui être adjacent), m choix pour le point suivant, etc. D'où $K = Nm^{p-2}$ (il y a $p-2$ choix à faire après le sommet initial).

8. Les boucles $(x_0, \ldots, x_p)$ de $\mathcal{B}_p$ sont de deux types :

   - celles pour lesquelles $x_0 = x_{p-2}$. Définir une telle boucle revient à choisir la boucle $(x_0, \ldots, x_{p-2})$ de $\mathcal{B}_{p-2}$, puis le choix de x_{p-1}. Il y a respectivement K_1 et m choix possibles donc il y a mK_1 telles boucles.
   - celles pour lesquelles $x_0 \neq x_{p-2}$. Il y a autant de telles boucles que de chemins $(x_0, \ldots, x_{p-2})$ tels que $x_0 \neq x_{p-2}$) ; en effet, une fois x_0 et x_{p-2}, il y a une seule façon de choisir x_{p-1}, en prenant $x_{p-1} = x_{p-2} \vee x_0$. Par définition de K_2, il y a donc K_2 telles boucles.

   Par addition, on a donc $|\mathcal{B}_p| = mK_1 + K_2$.

9. On écrit $|\mathcal{B}_p| = mK_1 + K_2 = (m-1)K_1 + K = (m-1)K_1 + Nm^{p-2}$. Comme $p \mid m-1$, $m - 1 \equiv 0\,[p]$ et $m^{p-2} \equiv 1\,[p]$. Donc, $|\mathcal{B}_p| \equiv N \equiv m(m-1) + 1 \equiv 1\,[p]$.

   C'est en contradiction avec le résultat de la question 6. Donc, l'hypothèse selon laquelle $(E, \mathcal{R})$ ne vérifie pas la propriété (B) est absurde : il existe donc $x \in E$ tel que $d(x) = N - 1$.