Corrigé ENS oraux 2023

V.Vong

Treillis distributifs

Réponse 1. On peut prendre par exemple $(\{0,1,2\}, \max, \min)$.

Réponse 2.
- Réfléxivité : montrons que $a \wedge a = a$. On a par absorption $a \wedge a = a \wedge (a \vee (a \wedge a))$ et on retrouve avec la deuxième loi d'absorption $a \wedge a = a$.
- Anti-symétrie : on a $a \wedge b = a$ et $b \wedge a = b$ Par commutativité de $\wedge$, on en déduit $a = b$.
- Transitivité : on a $a \wedge b = a$ et $b \wedge c = b$. Donc $a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$.

Il est clair que $(a \wedge b)$ et $(a \vee b)$ sont respectivement des minorants et majorants de $\{a, b\}$. Montrons que ce sont respectivement la borne inférieure et supérieure. Soit un x vérifiant $a \wedge x = a$ et $b \wedge x = b$. On a $x \wedge (a \vee b) = (x \wedge a) \vee (x \wedge b) = a \vee b$. Donc $a \wedge b \leq x$. Si $x \wedge a = x, x \wedge b = x$, on a $x \wedge a \wedge b = x$ par associatvité. Ce qui conclut.

Réponse 3. Considérons $\{\emptyset, \{0\}, \{1\}\}$ muni de l'ordre d'inclusion. (Est-ce que l'on cherche un ensemble partiellement ordonné qui ne se plonge pas dans un treillis distributif ?)

Réponse 4. On numérote les éléments de S comme suit $s_1, \cdots s_n$. Considérons le plongement $\varphi(P) = (1_{\{s_1\}}(P), \cdots 1_{\{s_n\}}(P))$. Celui est bien un morphisme injectif de treillis. La dimension de $(\mathcal{P}(S), \cup, \cap)$ est bien finie et est inférieure à n à priori. On pourrait même remarquer qu'elle est en fait égale à n : en effet, le singleton est incomparable avec toute partie non vide de $\{s_1, \cdots, s_{n-1}\}$ ce qui impose l'ajout d'une nouvelle composante pour prendre en compte ce dernier élément.

Réponse 5. Dans un treillis distributif fini, si b n'est pas irréductible, il existe p irréductible et a vérifiant $b = p \vee a$ avec $p \neq b, a \neq b$. Si ce n'est pas le cas, on construit une suite par récurrence comme ceci :

$$b = u_0 \vee v_0$$

avec $u_0 \neq b, v_0 \neq b$, les deux n'étant pas irréductibles. De même, u_0 se décompose en deux composant u_1, v_1. u_1 et v_1 n'étant pas irréductibles. Ainsi, on a construit une suite (u_n) strictement décroissante. Comme le treillis est fini, la suite finit par stationner, ce qui est absurde. Donc il existe p irréductible vérifiant $b = p \vee a$. De plus p est clairement incomparable à a. Donc p est un irréductible inférieur à b n'apparaissant pas dans les irréductibles de a. Ainsi, a est un élément dont l'ensemble des irréductibles est strictement inclus dans $\{a_1, \cdots, a_k\}$. En effectuant une récurrence sur le nombre d'irréductibles, on en déduit que $b = a_1 \vee \cdots a_k$.

Réponse 6. On considère le plongment $a \mapsto \{p \text{ irreductible}, p \leq a\}$. Ainsi, si E est fini, avec deux plongements successifs, on en déduit que E est de dimension au plus $|E|$.

Réponse 7. Si on a $a_1 \vee a_2 < b$, on a trouvé un élément tel que $a_1 < a_1 \vee a_2, a_2 < a_1 \vee a_2$ car a_1, a_2 sont distincts et donc a_1 et a_2 ne sont pas couverts par b.

Réponse 8. Pour tout élément $x \in couv(b)$, on note $\phi(x)$ le plus petit indice de i tel que $b_i > x_i$. Il existe bien car $b > x$. Justifions que ϕ est injective sur $couv(b)$. Soit x, y deux éléments de $couv(b)$. si $\phi(x) = \phi(y)$, on a necessairement $(x \vee y)_{\phi(x)} < b_{\phi(x)}$. Donc $x \vee y \neq b$. Ainsi, $x = y$. Donc ϕ est injective, ce qui conclut.

Réponse 9. Soit E un treillis distributif fini. Considérons un plongement de E dans $\mathbb{Z}^d$. D'après la question 8, on en déduit que $\max_{a \in E} couv(a) \leq d$. Ceci est valide pour tout plongement. Ainsi, en minimisant, on en déduit que $dim(E) \geq \max_{a \in E} couv(a)$.

Réponse 10. Le point important est de vérifier que $Id(S)$ est non vide et est stable pour les deux opérations. Les différentes propriétés résultent alors du fait que l'on a un sous-treillis distributif de $P(S)$.
- L'ensemble vide est clairement un idéal.
- Justifions de la stabilité par intersection. Soit I et J deux idéaux. Montrons que $I \cap J$ est bien un idéal. Soit $x \in I \cap J$. Soit $y \leq x$. Comme I, J sont des idéaux, on a $y \in I, y \in J$, ce qui conclut.
- Montrons que si I et J sont des idéaux, alors $I \cup J$ est bien un idéal. Soit $x \in I \cup J$. Soit $y \leq x$. Si $x \in I$, alors $y \in I$ et si $x \in J$, alors $y \in J$. Dans tous les cas $y \in I \cup J$, ce qui conclut.

Réponse 11. Étant donné un idéal I, on peut remarquer qu'il est généré par l'antichaîne formé par les éléments maximaux de I. Remarquons qu'également que l'on a $J \prec I$ si et seulement s'il existe m maximal dans I tel que $J = I \backslash \{m\}$. De plus, à partir de tout antichaîne on construit l'idéal généré par cette antichaîne. Ainsi, $max_{I \in Id(S)} couv(I)$ est égal à la taille de la plus grande antichaîne dans S.

On applique le théorème de Dilworth. Ainsi, on obtient une partition de S en k chaînes $C_1, \cdots C_k$, avec k la taille de la plus grande antichaîne de S. On note $c_1, \cdots c_k$ les cardinaux des C_i. On numérote par ordre croissant les éléments de $C_i : a_{1,i} < a_{2,i} < \cdots a_{c_i,i}$.

On construit une application allant des antichaînes de S à $\mathbb{N}^k$ comme suit :

pour une antichaîne donnée $s_1, \cdots s_j$ on attribue le k uplet $(\alpha_1, \cdots, \alpha_k)$ où pour tout $l \in \{1, \cdots k\}$ $\alpha_l = 0$ si aucun élément de l'antichaîne n'appartient à C_l et α_l est le numéro de l'élément de $\{s_1, \cdots, s_j\}$ présent dans l'antichaine C_l sinon.

Remarquons du fait que les C_i sont des chaînes deux éléments de l'antichaine ne peuvent pas appartenir à la même antichaine.

On vient de construire un plongement. Ainsi, la dimension est au plus k. Ainsi, il y a égalité.

Énumération de fonctions booléennes

Réponse 1. On génère les 2^n éléments de $(\mathbb{Z}/2\mathbb{Z})^n$, ce qui se fait en $O(2^n)$. Puis on effectue le calcul pour chaque pour chaque $n-$uplet. Or pour chaque $n-$uplet x, le calcul des $f_k(x)$ se fait en n^3. Ainsi, la complexité est bien en $O(n^3 2^n)$.

Réponse 2.

1. — Pour $n = 2$: 00,10,11,01.
   — Pour $n = 3$: 000,100,110,010,011,111,101,001.
2. On procède par récurrence. Il est clair que le cardinal double à chaque étape et que la longueur des élements est égal à n pour l'étape n. Reste à vérifier que chaque élément apparaît au plus une fois. Suposons que c'est le cas au rang n. Pour le rang $n+1$, les 2^n premiers sont différents des 2^n derniers sur la dernière composante. Puis par récurrence, un élément de rang i est différent de ce qui ont la même dernière composante que lui. Ce qui permet de conclure.
3. On procède par récurrence sur n. La formule est valide pour $n = 1$. Supposons le résultat acquis pour n. Vérifions la propriété pour $n+1$. Pour le passage à $n+1$, pour $t < 2^n$ ceci résulte directement de l'hypothèse de récurrence et du fait que l'on ne fait que rajouter un 0 à gauche pour chaque séquence de $\mathbf{Gray}(n)$. Reste à traiter pour $t \geq 2^n$.

   Par construction, $\mathbf{Gray}(n+1, 2^n) = \mathbf{Gray}(n, 2^n - 1)1$ mais

   $$\mathbf{Gray}(n+1, 2^n - 1) = \mathbf{Gray}(n, 2^n - 1)0$$

   et $\nu(2^n) = n$. On a bien $\mathbf{Gray}(n+1, 2^n-1) + e_n = \mathbf{Gray}(n+1, 2^n)$. Pour $t > 2^n$, par définition $\mathbf{Gray}(n+1, t) = \mathbf{Gray}(n, 2^{n+1} - 1 - t)1 = (\mathbf{Gray}(n, 2^{n+1} - t) + e_{\nu(2^{n+1}-t)})1 = \mathbf{Gray}(n, 2^{n+1} - t)1 + e_{\nu(2^{n+1}-t)} = \mathbf{Gray}(n+1, t-1) + e_{\nu(2^{n+1}-t)}$.

Réponse 3.

1. On fixe $x = (x_1, \cdots, x_n)$. On a :

   $$f(x+e_p) = f(0) + \sum_{i \neq p, j \neq p} a_{ij} x_i x_j + \sum_{i \neq p} a_{ip} x_i (x_p+1) + \sum_{j \neq p} a_{pj} (x_p+1) x_j + a_{pp} (x_p+1)^2$$

   En développant et en regroupant, on trouve :

   $$f(x + e_p) = f(x) + \sum_{i \neq p} (a_{ip} + a_{pi}) x_i + a_{pp}$$

   Donc :

   $$f(x + e_p) + f(x) = \sum_{i \neq p} (a_{ip} + a_{pi}) x_i + a_{pp}$$

   il en résulte que $x \mapsto f(x + e_p) + f(x)$ est bien affine.
2. On garde en mémoire tous les coefficients a_{ij}. D'après la formule précédente, si on connaît $f(x)$, on trouve en $O(n)$ opérations $f(x + e_p)$. En parcourant les 2^n possibilités suivant l'ordre du code de Gray, deux éléments successifs différant uniquement d'un seul bit, tous les $f(x)$ se calculent alors en $O(n2^n)$. Il en vient directement les zeros de f.

Réponse 4. On a $t = k2^\nu$ avec k impair. Donc $s = (k+2)2^\nu$. Ainsi, on obtient par récurrence direct :

$$\mathbf{Gray}(n, s-1) = \mathbf{Gray}(n, t) + \sum_{i=t+1}^{s-1} e_{\nu(i)}$$

En effectuant un comptage, on remarque que l'on a :

$$\mathbf{Gray}(n, s-1) = \mathbf{Gray}(n, t) + e_{\nu(t+2^\nu)} + \sum_{j=0}^{\nu-1} 2^{\nu-j} e_j$$

Les calculs étant en caractéristique 2, on en déduit que

$$\mathbf{Gray}(n, s-1) = \mathbf{Gray}(n, t) + e_{\nu(t+2^\nu)}$$

Or $s = t + 2^{\nu+1}$. Dond $t + 2^\nu = s - 2^\nu$. Ainsi :

$$\mathbf{Gray}(n, s-1) = \mathbf{Gray}(n, t) + e_{\nu'(s)}$$

Réponse 5. On peut maintenant exploiter cette relation de récurrence (en gardant les notations précédentes) :

$$f(\mathbf{Gray}(n, s)) = f(\mathbf{Gray}(n, s-1)) + \frac{\partial f}{\partial \nu(t)}(\mathbf{Gray}(n, t)) + \overline{\frac{\partial f}{\partial \nu(t)}}(e_{\nu'(s)} + e_{\nu(s)})$$

$\overline{\frac{\partial f}{\partial \nu(t)}}$ correspond à la partie linéaire de l'application affine $\frac{\partial f}{\partial \nu(t)}$.

On procède alors par propgrammation dynamique en gardant en mémoire $(f(x), \frac{\partial f}{\nu(x)}(x))$. La récurrence permet de passer au terme suivant en temps constant.

Ainsi, la complexité est bien en $O(2^n)$.

Réponse 6. Partie 5 de l'article : Fast exhaustive Search For Polynomial Systems in $\mathbb{F}_2$.

Auteurs : Charles Bouillaguet, Hsieh-Chung Chen, Chen-Mou Cheng, Tung Chou, Ruben Niederhagen, Adi Shamir, and Bo-Yin Yang

Lien vers l'article :

https ://www-almasty.lip6.fr/ bouillaguet/static/publis/CHES10.pdf

Graphes, rayons et applications

Réponse 1. Si G admet un rayon $s_0 \cdots, s_n, \cdots$, on a alors une injection naturelle de $\mathbb{N}$ vers l'ensemble des sommets du graphe. Ainsi, G est infini.

Réponse 2.
1. On considère un graphe où les sommets sont des entiers naturels supérieurs à 1, et un entier i est relié au sommets suivants : $2i, 2i+1$ que l'on étend par symétrie (cela signifie que pour $i > 1$, i est relié à $\lfloor \frac{i}{2} \rfloor$).
2. Au graphe précédent, on rajoute les arêtes suivante : pour $i = 2^p$ une puissance de 2, on le connecte également à tous les entiers compris $2^p + 1, \cdots 2^{p+1} - 1$.

Réponse 3.
— Si on enlève le caractère connecté, en considérant le graphe où les sommets sont des entiers et tous les sommets sont isolés, on n'a alors pas de rayon.
— Si on enlève le caractère infini, d'après Q1, il n'y a pas de rayon.
— Si on enlève le caractère localement fini, il suffit de considérer le graphe où 1 est le sommet relié à tous les autres. Tout chemin de longueur supérieur à 3 passent nécessairement par 1. Ainsi, il n'y a pas de chemin simple de longueur supérieur à 4.

Réponse 4. On considère comme sommet l'ensemble des entiers supérieurs à 1. Pour les arêtes, on créé un cycle sur les ensembles de la forme $\{2^p, 2^p + 1 \cdots 2^p - 1\}$ pour tout $p \geq 1$.

Réponse 5. Si on note $w_1, \cdots, w_p$ les sommets adjacaents à v, le graphe G_v admet au plus p composantes connexes, qui sont tous localement fini, connecté. Si aucun d'entre eux n'était infini, en rajoutant v et les arêtes $\{v, w_i\}$, on aurait que G n'est pas infini, ce qui contredit les hypothèses.

Donc au moins une des composantes connexes vérifie K.

Réponse 6. On construit une suite (s_n) qui correspond à un rayon de la manière suivante. On fixe s_0 un sommet quelconque. Pour constuire s_{n+1} à partir de s_n, on choisit s_{n+1} un sommet dans une composante connexe de G_{s_n} vérifiant la propriété K (possible d'après la question 5).

Par construction, les s_i sont distincts deux à deux et on a un chemin simple.

Réponse 7. Si G est k coloriable, il est clair qu'avec restriction, tous ses sous-graphes finis sont k coloriables.

Démontrons la réciproque.

Notons $C_n = \{f : \{0, \cdots, n-1\} \to \{0, \cdots k-1\} | f\text{coloration de } G_n\}$, G_n étant le sous-graphe restreint aux sommets de $\{0, \cdots, n-1\}$. Si toute partie finie de G est k coloriable, pour tout $n \in \mathbb{N}$, C_n est non vide. On considère le graphe où les sommets sont les éléments des C_n et on a une arête entre $f \in C_n$ et $g \in C_{n+1}$ si g est un prolongement de f. On pourra remarquer que ce graphe est alors infini, connexe, localement fini, dénombrable. Il admet donc un rayon. Ce rayon définit alors naturellement une k coloration de G.

Réponse 8. Ceci est une variante du théorème de l'éventail de Brouwer qui s'énonce ainsi :

Soit Σ un alphabet fini, soit B une partie de $\Sigma^\star$ telle que pour tout mot w infini sur Σ, il existe un préfixe p non vide de w qui appartient à B. Alors il existe une partie finie $A \subset B$ telle que tout mot infini admet un préfixe dans A.

Démontrons ce théorème par l'absurde. On fixe B une partie de $\Sigma^\star$ telle que pour tout mot w infini sur Σ, il existe un préfixe de w qui appartient à B. On suppose de plus que pour tout partie finie A de B, il existe des mots infini qui n'ont pas de préfixe dans A.

Considérons l'arbre T où les noeuds sont les éléments de $\Sigma^\star \backslash B$, et on a une arête entre v, w si $w = va$ ou $v = wa$ où a est une lettre de Σ. Justifions que ceci est bien un arbre infini. Remarquons que pour tout sous-ensemble de B de mots de longueur au plus $n \geq 1$, il existe au moins un mot de longueur n qui n'a pas de préfixe dans B. Ainsi, l'ensemble des sommets est bien infini. Tout sommet est clairement relié au mot vide et donc le graphe est bien connexe. De plus, l'alphabet étant fini, il y a bien le caractère localement fini. Il existe alors un rayon dans ce graphe. À partir de ce rayon, on obtient un mot infini, dont aucun préfixe n'appartient à B, ce qui est une contradiction et on en déduit le théorème.

On propose une démonstration qui n'utilise pas le lemme de Konig (je n'ai pas trouvé un argument type arbre infini).

On fixe u un mot infini, on fixe L une partie de $\Sigma^\star$. On note $u[k:]$ le mot obtenu en enlevant les k première lettres de u (l'indexation commence 0).

On considère la proposition suivante :

$$P(L) : \exists N \in \mathbb{N}(\forall k \geq N(\exists (p, u') \in L \times \Sigma^\infty, u[k:] = pu')) \tag{1}$$

Cette proposition est vérifiée ou non par le langage $L' = L \backslash \{\varepsilon\}$.

— Cas 1 : L' vérifie la propriété P. Dans ce cas, on fixe d'abord $N_0 \in \mathbb{N}$, telle que l'on ait :

$$\forall k \geq N_0(\exists (p, u') \in L' \times \Sigma^\infty, u[k:] = pu').$$

on construit un découpage en considérant à chaque étape le plus court préfixe de $u[k:]$ qui est un élément de L'.

— Cas 2 : L' ne vérifie pas la propriété P. Cela signifie qu'il existe une suite strictement croissante d'entiers $(k_n)_{n\in\mathbb{N}}$ telle que pour tout $n \in \mathbb{N}$, le mot $u[k_n :]$ n'a pas de préfixe dans L'. Ainsi, on obtient directement une par cette suite un découpage où aucun facteur n'appartient à L, ce qui conclut.