Cours TalENS 2023-2024

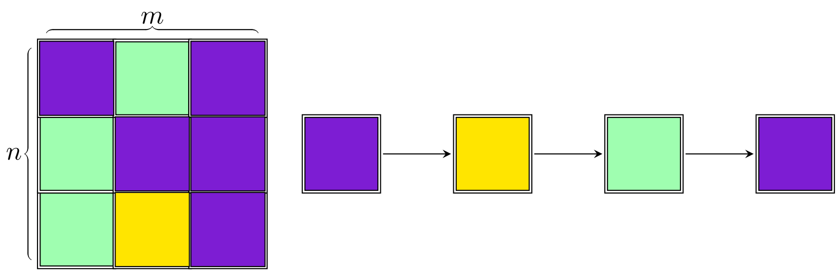
Rrrr, Shadoks et Craies

Matthieu Boyer

22 février 2024

1 Modélisation

On part par exemple d'une situation semblable à celle-ci dessous :

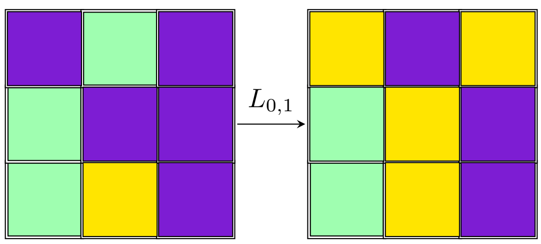


On choisit de modéliser chaque couleur par un nombre différent : Violet = 0, Jaune = 1 et Menthe = 2 On décrit alors la situation par la couleur de chaque lumière sous forme d'un vecteur :

$$\mathcal{P} = (0, 2, 0, 2, 0, 0, 2, 1, 0)$$

La lumière de la case i, j est représenté par la $i * m + j$-ème valeur.

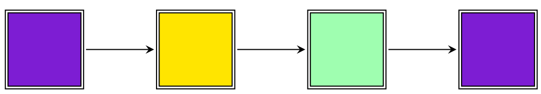
Si on appuie sur la lumière en haut au milieu :



C'est à dire :

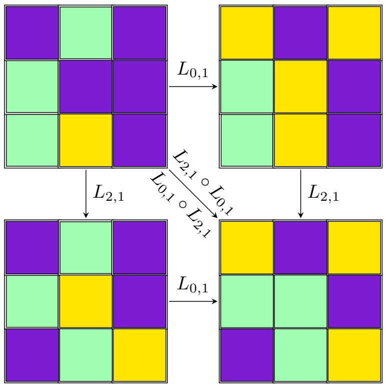
$$L_{0,1}\,(0, 2, 0, 2, 0, 0, 2, 1, 0) = (1, 0, 1, 0, 1, 1, 2, 1, 0)$$

On a plus généralement :



C'est à dire que si on agit sur une case i, j : $L_{x,y}\left(u_0, \ldots, u_{nm-1}\right) = \left(u'_0, \ldots, u'_{nm-1}\right)$ où :

$$\forall k, u'_k = \begin{cases} u_k & \text{si } im + j \text{ et } k \text{ ne sont pas adjacentes} \\ 1 & \text{si } u_k = 0 \\ 2 & \text{si } u_k = 1 \\ 0 & \text{si } u_k = 2 \end{cases}$$



Le diagramme commutatif ci-contre est valable pour toutes paires (i, j) et (k, l). C'est à dire que

$$\forall (i, j), (k, l), L_{i,j} \circ L_{k,l} = L_{k,l} \circ L_{i,j}$$

Par ailleurs, si on prend $u = (u_0, \ldots, u_{mn-1})$ et $v = (v_0, \ldots, v_{mn-1})$ deux états de jeu, on a :

$$L_{i,j}(u + v) = L_{i,j}(u) + L_{i,j}(v)$$

2 Arithmétique Modulaire

Théorème 2.1: Division Euclidienne

Soit $n, q \in \mathbb{Z}$. Il existe un unique couple (p, q) vérifiant :

$$n = pq + r \text{ et } 0 \leq r < q$$

Démonstration. **Existence** On soustrait q à n jusqu'à tomber sur $r < q$.

Unicité Si $(p, r), (p', r')$ conviennent, on a $(p - p')q = r - r'$. Mais $|r - r'| \leq q$ donc $p - p' = 0$ et par suite $r = r'$.

■

Définition 2.1: Modulo et Divisibilité

On note $a \mid b$ lorsque $r = 0$ dans la division euclidienne de a par b, i.e. $a = p \times b$.
On note $a \equiv b[n]$ lorsque a et b ont même reste dans la division euclidienne par n. On dit qu'ils sont congrus modulo n. On note $a \mod n$ ou $a[n]$ la valeur de ce reste commun.

Proposition 2.1: Sur la Relation Modulo n

Soit $a, b, n \in \mathbb{Z}$.

- $a + b \mod n = (a \mod n) + (b \mod n) \mod n$
- $ab \mod n = (a \mod n) \times (b \mod n) \mod n$
- La relation $a \mod n = b \mod n$ est une relation d'équivalence.

Démonstration. On calcule simplement les résultats à l'aide d'un tableau de congruence. ■

Définition 2.2: Anneau $\mathbb{Z}/n\mathbb{Z}$

On définit sur l'ensemble $\{0, \ldots, n-1\}$ l'addition et le produit par le passage au modulo. Formellement, il s'agit du passage au quotient de $\mathbb{Z}$ par son idéal $n\mathbb{Z}$.

Proposition 2.2: Corps Primaux

L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps (i.e. il y a des inverses multiplicatifs) si et seulement si il est intègre si et seulement si $p \in \mathcal{P}$.

Si nos lampes peuvent avoir p couleurs différentes, on va donc modéliser l'état de chacune de nos lampes comme un nombre sur $\mathbb{Z}/p\mathbb{Z}$. On a alors bien :

$$\begin{aligned} 0+1&=1\\ 1+1&=2\\ &\vdots\\ p-1+1&=0 \end{aligned}$$

et on modélise correctement le cycle des couleurs.

3 Algèbre Linéaire

Définition 3.1: Espace Vectoriel

Étant donné un corps $\mathbb{K}$, on appelle espace vectoriel sur $\mathbb{K}$ ou $\mathbb{K}$-espace vectoriel un ensemble E muni d'une addition commutative $+$ et d'un produit externe $\times$ distributif sur l'addition.

Proposition 3.1: Quelques Exemples

- $\mathbb{R}$, $\mathbb{R}^{\mathbb{R}}$, $\mathbb{R}^{\mathbb{N}}$ ou $\mathbb{R}[X]$ sont des $\mathbb{R}$-ev.
- $\mathbb{Z}/p\mathbb{Z}$ est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel.

Définition 3.2: Application Linéaire

Soient E, F deux $\mathbb{K}$-espaces vectoriels. Une application $f : E \to F$ est dite linéaire si :

- $\forall x, y \in E,\ f(x+y) = f(x) + f(y)$
- $\forall x \in E, \lambda \in \mathbb{K}, f(\lambda x) = \lambda f(x)$

Proposition 3.2: Exemples

- $ev_x : P \in \mathbb{R}[X] \mapsto P(x) \in \mathbb{R}$ est linéaire.
- $\Delta : P \in \mathbb{R}[X] \mapsto P' \in \mathbb{R}[X]$ est linéaire.
- $L_a : x \in \mathbb{Z}/p\mathbb{Z} \mapsto a \times x \in \mathbb{Z}/p\mathbb{Z}$ est linéaire.

Définition 3.3: Espace Engendré

Soit $e = e_1, \ldots, e_n \in E$. On appelle Espace Vectoriel Engendré par $e_1, \ldots, e_n$ le plus petit sous-espace vectoriel de E comprenant chacun des e_i i.e.

$$\mathrm{Vect}(e) = \mathrm{Vect}(e_1, \ldots, e_n) = \left\{ \sum_{i=1}^{n} \lambda_i e_i \mid (\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n \right\}$$

Par exemple :

$$\mathrm{Vect}(1, X, \ldots, X^n, \ldots) = \mathbb{R}[X]$$

Définition 3.4: Famille Génératrice, Libre, Base

On dit que :

- e est une base si $\mathrm{Vect}\,(e \setminus \{e_i\}) \subsetneq \mathrm{Vect}(e)$ pour tout i
- e est génératrice si $\mathrm{Vect}(e) = E$
- e est une base si e est génératrice et libre

E est de dimension finie s'il existe une famille génératrice finie.
En dimension finie $(\mathbb{K}^n, \mathbb{K}_n[X], L(\mathbb{K}, \mathbb{K}))$, ces trois propositions sont équivalentes.

Proposition 3.3: Image d'une Base

L'image par une application linéaire est une famille génératrice de l'image de l'application linéaire.

Démonstration. Si $x = \sum_i \lambda_i e_i$, $f(x) = \sum_i \lambda_i f(e_i)$. ∎

On n'a donc besoin que de l'image d'une base pour caractériser une application linéaire. On n'a par ailleurs besoin que d'une base pour caractériser un espace.

Définition 3.5: Matrice d'une Application Linéaire

Soit $e = e_1, \dots, e_n$ une base d'un $\mathbb{K}$-espace E, $f = f_1, \dots, f_m$ une base d'un $\mathbb{K}$-espace F. Soit $u : E \to F$ linéaire. Si on a, pour tout $i \in [\![1, m]\!]$: $u(e_i) = \sum_{j=1}^{n} a_{i,j} f_j$ la matrice de u relativement à e et f est :

$$Mat_{e,f}(u) = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix}$$

Elle est de taille m, n. On note $\mathcal{M}_{m,n}(\mathbb{K})$ l'ensemble des telles matrices.

Définition 3.6: Anneau Matriciel

- Si $P, Q \in \mathcal{M}_{p,q}(\mathbb{K})$ sont les matrices de u et v dans certaines bases, $P + Q$ est la matrice de $u + v$ dans ces bases.
- Si $P \in \mathcal{M}_{p,q}(\mathbb{K})$ est la matrice de $u : F \to G$ et si $Q \in \mathcal{M}_{q,r}(\mathbb{K})$ est la matrice de $v : E \to F$ alors $PQ \in \mathcal{M}_{p,r}(\mathbb{K})$ est la matrice de $u \circ v : E \to G$.

Proposition 3.4: Propriétés des Matrices

- La matrice d'une application la caractérise entièrement.
- $P + Q$ est la matrice somme des coefficients :

$$\boxed{(P + Q)_{i,j} = P_{i,j} + Q_{i,j}}$$

- $P \times Q$ se calcule comme suit :

$$\boxed{(P \times Q)_{i,j} = \sum_{k=1}^{q} p_{i,k} q_{k,j}}$$

On peut voir une transition de jeu comme une application linéaire de $\mathbb{Z}/p\mathbb{Z}^{mn}$ vers $\mathbb{Z}/p\mathbb{Z}^{mn}$.

En 3×3 :

$$\mathcal{L}(3,3) = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

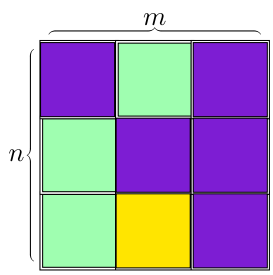
4 Résolution du Jeu

On peut finalement voir `Lights Out` comme un système linéaire :

$$\mathcal{L}(3,3) \times a = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \times a = b$$

où b est la situation initiale et où on cherche a

Dans notre cas :



$$b = \begin{pmatrix} 0 \\ 2 \\ 0 \\ 2 \\ 0 \\ 0 \\ 2 \\ 1 \\ 0 \end{pmatrix} \qquad a = \begin{pmatrix} 2 \\ 0 \\ 2 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 2 \end{pmatrix}$$

Pour résoudre le problème, on a calculé la matrice inverse de $\mathcal{L}(3,3)$ notée $\mathcal{L}(3,3)^{-1}$.

Définition 4.1: Déterminant d'une Matrice

Si $A = (a_{i,j}) \in M_{n,n}(\mathbb{K})$, on appelle déterminant de A le nombre :

$$\det A = \begin{vmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{vmatrix} = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$$

Proposition 4.1: Inversibilité et Déterminant

A est inversible, i.e. A^{-1} existe si et seulement si $\det A \neq 0$.

Proposition 4.2: Déterminant Sur $\mathbb{Z}/p\mathbb{Z}$

On a, si $A \in \mathcal{M}_n(\mathbb{Z}/p\mathbb{Z})$:

$$\det_{\mathbb{Z}/p\mathbb{Z}} A = \det_{\mathbb{R}} A \bmod p$$

$p \backslash n$	2	3	4	5	6	7	8	9
2	$\top$	$\top$	$\bot$	$\bot$	$\top$	$\top$	$\top$	$\bot$
3	$\bot$	$\top$	$\bot$	$\bot$	$\top$	$\top$	$\bot$	$\bot$
4	$\top$	$\top$	$\bot$	$\bot$	$\top$	$\top$	$\top$	$\bot$
5	$\top$	$\top$	$\bot$	$\bot$	$\top$	$\top$	$\top$	$\bot$

Pour calculer A^{-1} on dispose de l'algorithme de Gauss-Jordan :

Algorithme 1 Algorithme de Gauss-Jordan

```
r ← 0
for j = 1 à m do
    k ← arg max_{r+1≤i≤n} |A_{i,j}|
    if A_{k,j} ≠ 0 then
        r ← r + 1
        Diviser la ligne k par A_{k,j}
        if k ≠ r then
            Échanger les lignes k et r
        end if
        for i = 1 à n do
            if i ≠ r then
                Soustraire à la ligne i la ligne r multipliée par A[i, j]
            end if
        end for
    end if
end for
```

Celui-ci n'est pas très efficace et, en pratique, on pourrait juste calculer directement a par la méthode employée ici pour avoir un résultat plus précis plus rapidement.