Le Berlekamp's switching game

Introduction

Le "*Berlekamp's switching game*" est un jeu inventé par Elwin R. Berlekamp et David Gale, dont un exemplaire construit par Berlekamp se trouve aux Laboratoires Bell à Murray Hill. Il repose sur des codes qui en ont tiré leur nom, les "*light-bulb* codes" : en effet, son support est un tableau $m \times m$ d'ampoules contrôlé par $2m$ interrupteurs frontaux, un pour chaque ligne ou colonne. Quand un interrupteur est basculé, les ampoules qui étaient allumées dans la ligne ou la colonne correspondante sont éteintes, et celles qui étaient éteintes sont allumées. Derrière chaque ampoule se trouve un interrupteur qui permet de la commander individuellement afin de configurer un état initial du tableau. Le jeu consiste à trouver, pour un état initial donné, le nombre minimal d'ampoules allumées après manipulation à volonté des interrupteurs commandant les lignes et les colonnes, puis à maximiser ce nombre par un choix judicieux de l'état initial. On montrera les liens de ce jeu avec la théorie des codes, et on en étudiera certaines propriétés mathématiques.

Dans le cas $n = 6$, voici un exemple de partie dans laquelle on se ramène en six coups d'une configuration initiale à 18 ampoules à une configuration à 8 ampoules, qui semble optimale :

$$\begin{pmatrix} \circ & \bullet & \bullet & \bullet & \circ & \circ \\ \circ & \circ & \bullet & \bullet & \bullet & \circ \\ \circ & \circ & \circ & \bullet & \bullet & \bullet \\ \bullet & \circ & \circ & \circ & \bullet & \bullet \\ \bullet & \bullet & \circ & \circ & \circ & \bullet \\ \bullet & \bullet & \bullet & \circ & \circ & \circ \end{pmatrix} \qquad \begin{array}{c} \\ \\ \times \\ \\ \\ \\ \end{array} \begin{pmatrix} \circ & \bullet & \bullet & \bullet & \circ & \circ \\ \circ & \circ & \bullet & \bullet & \bullet & \circ \\ \bullet & \bullet & \bullet & \circ & \circ & \circ \\ \bullet & \circ & \circ & \circ & \bullet & \bullet \\ \bullet & \bullet & \circ & \circ & \circ & \bullet \\ \bullet & \bullet & \bullet & \circ & \circ & \circ \end{pmatrix}$$

$$\begin{array}{c} \\ \\ \\ \times \\ \\ \\ \end{array} \begin{pmatrix} \circ & \bullet & \bullet & \bullet & \circ & \circ \\ \circ & \circ & \bullet & \bullet & \bullet & \circ \\ \bullet & \bullet & \bullet & \circ & \circ & \circ \\ \circ & \bullet & \bullet & \bullet & \circ & \circ \\ \bullet & \bullet & \circ & \circ & \circ & \bullet \\ \bullet & \bullet & \bullet & \circ & \circ & \circ \end{pmatrix} \qquad \begin{array}{c} \begin{array}{cccccc} & \times & \times & & & \end{array} \\ \begin{pmatrix} \circ & \circ & \circ & \bullet & \circ & \circ \\ \circ & \bullet & \circ & \bullet & \bullet & \circ \\ \bullet & \circ & \circ & \circ & \circ & \circ \\ \circ & \circ & \circ & \bullet & \circ & \circ \\ \bullet & \circ & \bullet & \circ & \circ & \bullet \\ \bullet & \circ & \circ & \circ & \circ & \circ \end{pmatrix} \end{array}$$

$$\begin{array}{c} \begin{array}{cccccc} \times & & & & & \end{array} \\ \begin{pmatrix} \bullet & \circ & \circ & \bullet & \circ & \circ \\ \bullet & \bullet & \circ & \bullet & \bullet & \circ \\ \circ & \circ & \circ & \circ & \circ & \circ \\ \bullet & \circ & \circ & \bullet & \circ & \circ \\ \circ & \circ & \bullet & \circ & \circ & \bullet \\ \circ & \circ & \circ & \circ & \circ & \circ \end{pmatrix} \end{array} \qquad \begin{array}{c} \\ \times \\ \\ \\ \\ \\ \end{array} \begin{pmatrix} \bullet & \circ & \circ & \bullet & \circ & \circ \\ \circ & \circ & \bullet & \circ & \circ & \bullet \\ \circ & \circ & \circ & \circ & \circ & \circ \\ \bullet & \circ & \circ & \bullet & \circ & \circ \\ \circ & \circ & \bullet & \circ & \circ & \bullet \\ \circ & \circ & \circ & \circ & \circ & \circ \end{pmatrix}$$

1 Notions de théorie des codes

1.1 Code linéaire

Définition (Code linéaire) Un code linéaire C de longueur n est un sous-espace vectoriel de $\mathbb{F}^n$, où $\mathbb{F}$ est un corps. Les éléments de C sont appelés mots du code. La dimension k du code est sa dimension comme sous-espace vectoriel. On dit que C est un code $\mathrm{C}[n,k]$.

Le plus souvent, $\mathbb{F}$ est un corps fini, de cardinal $q = p^k$ où p est premier.

Les caractéristiques principales d'un code linéaire sont donc sa longueur (la dimension de l'espace tout entier), sa dimension et sa distance minimale d_{C}. Celle-ci est définie, ayant muni $\mathbb{F}^n$ d'une distance d, comme la plus petite distance entre deux mots du code :

$$d_{\mathrm{C}} = min\{d(x,y)|x \in \mathrm{C}, y \in \mathrm{C}, x \neq y\}$$

On dit que C est un code $\mathrm{C}[n,k,d_{\mathrm{C}}]$.

Définition (Matrice génératrice) Une matrice génératrice G d'un code $[n,k]$ est une matrice $k \times n$ dont les lignes engendrent le code. Le codage d'un vecteur ligne u de $\mathbb{F}^k$ est ainsi la multiplication matricielle de u par G : $\theta(u) = u\mathrm{G}$.

Définition (Matrice de contrôle) Une matrice de contrôle H d'un code C $[n,k]$ est une matrice $(n-k) \times n$ telle qu'un mot c soit dans C si et seulement $\mathrm{H}\,{}^t c = 0$.

Définition (Poids d'un vecteur) Le poids d'un vecteur y est sa distance à 0. On le note $w(y)$.

1.2 Métrique de Hamming

Définition (Distance de Hamming) La distance de Hamming d(x,y) entre deux mots x et y de $\mathbb{F}^n$ est le nombre de composantes pour lesquelles ils diffèrent.

Propriété 1.1 *La distance de Hamming est une distance sur $\mathbb{F}^n$.*

Propriété 1.2 *La distance de Hamming est invariante par translation :*

$$d(y,z) = d(x+y, x+z) \text{ pour tous } x, y, z \text{ de } \mathbb{F}^n$$

La distance minimale d'un code linéaire pour la distance de Hamming est donc le plus petit poids d'un vecteur du code.

1.3 Algorithmes naïfs de décodage d'un mot

Nous appellerons décoder un mot une opération qui consiste à associer à ce mot (de l'espace $\mathbb{F}^n$ tout entier) un mot de notre code C. La façon la plus naturelle de le faire est la suivante :

Décodage au maximum de vraisemblance :

Si un mot y de $\mathbb{F}^n$ n'est pas dans le code, on le décode par le mot du code tel que l'erreur (la différence) soit de poids minimal.

Dans le cas où la distance utilisée est celle de Hamming, l'unicité n'est garantie que si le nombre d'erreurs intervenues est inférieur à l'entier $\lfloor \frac{d_{\mathrm{C}}-1}{2} \rfloor$, appelé capacité de correction du code C. (Deux mots distincts du code ne peuvent être tous deux à une distance strictement plus petite que $d_{\mathrm{C}}/2$ d'un même mot, sinon ils seraient eux-même à une distance strictement inférieure à d_{C} l'un de l'autre, ce qui contredirait la définition de d_{C}).

Définition (Syndrome) On appelle syndrome d'un élément y de $\mathbb{F}^n$, et l'on note $s(y)$, l'élément $y\,{}^t\mathrm{H}$ de $\mathbb{F}^{n-k}$, où H est une matrice de contrôle du code C.

Si $y = c + e$ où $c \in \mathrm{C}$, on a par linéarité : $s(y) = s(e)$.Un vecteur appartient donc au code si et seulement si son syndrome est nul. Le syndrome n'est pas une notion intrinsèque au code : il dépend de la matrice de contrôle choisie.

Décodage par tableau standard :

C est un sous espace de $\mathbb{F}^n$ de dimension k, c'est donc un ensemble de cardinal q^k, et l'on peut écrire $\mathrm{C} = \{c^{(1)} = 0, c^{(2)}, \cdots, c^{(q^k)}\}$.

On définit la relation $\mathcal{R}$ sur $\mathbb{F}^n$ par : $x\mathcal{R}y \Leftrightarrow x - y \in \mathrm{C}$. $\mathcal{R}$ est une relation d'équivalence, et chaque classe est de même cardinal que C, c'est-à-dire q^k. Il y a donc q^{n-k} classes d'équivalence.

On appelle chef de classe d'une classe d'équivalence pour $\mathcal{R}$ son élément de poids minimal, en prenant un élément au hasard entre les ex-aequo éventuels. On les notera $l^{(i)}, 1 \leq i \leq q^{n-k}$. Notons que l'ensemble des classes $\overline{l^{(i)}}$ forme le groupe quotient $\mathbb{F}^n/\mathrm{C}$.

Enfin, on appelle tableau standard de C le tableau de taille $q^{n-k} \times q^k$ dont l'élément (i,j) est $l^{(i)} + c^{(j)}$. La classe de chef $l^{(i)}$ se trouve ainsi sur la i-ième ligne et sur la première colonne, et l'on choisit $l^{(1)} = 0$ pour avoir les mots du code sur la première ligne.

Le décodage d'un mot consiste alors à le retrouver dans le tableau et à regarder à quelle colonne il appartient ; s'il appartient à la j-ième colonne, le mot de code le plus proche est $c^{(j)}$, par définition des chefs de classe. On lit cet élément $c^{(j)}$ sur la première ligne, dans la colonne où l'on a trouvé notre mot à décoder.

Ce décodage implique toutefois une complexité de calculs en $\mathrm{O}(nq^n)$, car il faut parcourir le tableau dans son ensemble. Un décodage utilisant le syndrome permet lui d'avoir une complexité en $\mathrm{O}(nq^{n-k})$, en construisant un tableau associant chaque chef de classe à son syndrome. En effet, les classes sont en bijection avec les syndromes car, par linéarité, deux mots ont même syndrome si et seulement si ils diffèrent par un mot du code.

Ces algorithmes de décodage ne sont pas beaucoup utilisés du fait de leur complexité ; on peut en effet décoder un mot en le comparant à tous les mots du code, soit une complexité *a priori* moindre, en $\mathrm{O}(nq^k)$. (sauf si $n - k < k$)

1.4 Rayon de recouvrement

Définition (Rayon de recouvrement) On appelle rayon de recouvrement d'un code C, et l'on note $\rho(\mathrm{C})$, la plus grande distance possible entre un vecteur de $\mathbb{F}^n$ et un mot de C :

$$\rho(\mathrm{C}) = \max\{\min\{d(x,c) \mid c \in \mathrm{C}\} \mid x \in \mathbb{F}^n\} = \max_x d(x, \mathrm{C})$$

En d'autres termes, le rayon de recouvrement est le poids maximum d'un chef de classe. Un algorithme assez naïf pour le calculer consiste donc à parcourir la première colonne du tableau standard, mais la complexité est en $\mathrm{O}(nq^{n-k})$, et ce une fois le tableau construit.

2 Berlekamp's switching game

2.1 Principe du problème

Le principe exposé dans l'introduction s'étend à un tableau de taille $l \times m$. Pour une configuration initiale S d'ampoules allumées, on note $f(\mathrm{S})$ le nombre minimum d'ampoules restant allumées après manipulation illimitée des interrupteurs frontaux. Le problème consiste à trouver une configuration initiale S maximisant $f(\mathrm{S})$. Ce maximum est noté $g(l,m)$. Le cas des tableaux carrés a été plus spécialement étudié, et on notera $g(n,n) = f(n)$. L'exemplaire construit par Berlekamp est lui de taille 10×10. Les valeurs de $f(m)$ ne sont connues que pour $m \in [\![1,10]\!]$. Ces valeurs et les configurations associées peuvent être utilisées dans le cas d'un jeu à deux joueurs, où le premier joueur doit proposer une configuration empêchant l'autre joueur, chargé de la décoder, de faire un trop bon score.

2.2 Solutions pour $n \in [\![1,10]\!]$

Voici pour les valeurs de 1 à 10 les valeurs de $f(n)$, ainsi que des configurations associées. Pour les valeurs de n suffisamment grandes, ces résultats sont bien sûr obtenus grâce à un programme.

$$f(1) = 0 \begin{pmatrix} \circ \end{pmatrix} \quad f(2) = 1 \begin{pmatrix} \bullet & \circ \\ \circ & \circ \end{pmatrix} \quad f(3) = 2 \begin{pmatrix} \bullet & \circ & \circ \\ \circ & \bullet & \circ \\ \circ & \circ & \circ \end{pmatrix}$$

$$f(4) = 4 \begin{pmatrix} \bullet & \circ & \circ & \circ \\ \circ & \bullet & \circ & \circ \\ \circ & \circ & \bullet & \circ \\ \circ & \circ & \circ & \bullet \end{pmatrix} \quad f(5) = 7 \begin{pmatrix} \bullet & \bullet & \circ & \circ & \circ \\ \bullet & \circ & \bullet & \circ & \circ \\ \circ & \bullet & \circ & \circ & \circ \\ \circ & \circ & \bullet & \circ & \circ \\ \circ & \circ & \circ & \bullet & \circ \end{pmatrix}$$

$$f(6) = 11 \begin{pmatrix} \circ & \bullet & \circ & \circ & \circ & \circ \\ \circ & \circ & \bullet & \circ & \bullet & \circ \\ \circ & \circ & \bullet & \circ & \bullet & \bullet \\ \circ & \circ & \circ & \bullet & \bullet & \circ \\ \circ & \circ & \circ & \bullet & \circ & \circ \\ \circ & \circ & \circ & \circ & \circ & \bullet \end{pmatrix}$$

Pour $n = 7$, on a bien $f(7) = 16$, mais la configuration que l'on trouve dans la littérature, donnée à l'origine par Sloane et Fishburn, est en fait fausse : on peut en effet faire descendre le nombre d'ampoules de 16 à 14 en basculant quatre interrupteurs (ceux indiqués par des croix) comme suit :

$$\begin{pmatrix} \bullet & \circ & \circ & \circ & \circ & \circ & \circ \\ \circ & \bullet & \circ & \circ & \bullet & \bullet & \circ \\ \circ & \bullet & \circ & \circ & \circ & \circ & \bullet \\ \circ & \circ & \bullet & \circ & \bullet & \circ & \bullet \\ \circ & \circ & \bullet & \circ & \circ & \bullet & \circ \\ \circ & \circ & \circ & \bullet & \circ & \bullet & \circ \\ \circ & \circ & \circ & \bullet & \bullet & \circ & \bullet \end{pmatrix} \Longrightarrow \begin{array}{cc} & \begin{matrix} & \times & & & & \times & \end{matrix} \\ \begin{matrix} \\ \\ \\ \times \\ \\ \\ \times \end{matrix} & \begin{pmatrix} \bullet & \bullet & \circ & \circ & \circ & \bullet & \circ \\ \circ & \circ & \circ & \circ & \bullet & \circ & \circ \\ \circ & \circ & \circ & \circ & \circ & \bullet & \bullet \\ \bullet & \circ & \circ & \bullet & \circ & \circ & \circ \\ \circ & \bullet & \bullet & \circ & \circ & \circ & \circ \\ \circ & \bullet & \circ & \bullet & \circ & \circ & \circ \\ \bullet & \circ & \bullet & \circ & \circ & \circ & \circ \end{pmatrix} \end{array}$$

$$f(7) = 16 \begin{pmatrix} \circ & \circ & \circ & \bullet & \circ & \circ & \bullet \\ \circ & \circ & \circ & \circ & \bullet & \circ & \circ \\ \circ & \circ & \bullet & \circ & \circ & \bullet & \circ \\ \circ & \bullet & \bullet & \bullet & \circ & \circ & \circ \\ \bullet & \bullet & \circ & \circ & \circ & \circ & \circ \\ \bullet & \circ & \circ & \bullet & \circ & \bullet & \circ \\ \bullet & \circ & \bullet & \circ & \circ & \circ & \bullet \end{pmatrix}$$

$$f(8) = 22 \begin{pmatrix} \bullet & \bullet & \circ & \bullet & \circ & \circ & \circ & \circ \\ \circ & \bullet & \bullet & \circ & \bullet & \circ & \circ & \circ \\ \circ & \circ & \bullet & \bullet & \circ & \bullet & \circ & \circ \\ \circ & \circ & \circ & \bullet & \bullet & \circ & \bullet & \circ \\ \bullet & \circ & \circ & \circ & \bullet & \bullet & \circ & \circ \\ \circ & \bullet & \circ & \circ & \circ & \bullet & \bullet & \circ \\ \bullet & \circ & \bullet & \circ & \circ & \circ & \bullet & \circ \\ \circ & \circ & \circ & \circ & \circ & \circ & \circ & \bullet \end{pmatrix}$$

$$f(9) = 27 \begin{pmatrix} \bullet & \circ & \circ & \bullet & \circ & \circ & \bullet & \circ & \circ \\ \bullet & \circ & \circ & \circ & \bullet & \circ & \circ & \bullet & \circ \\ \bullet & \circ & \circ & \circ & \circ & \bullet & \circ & \circ & \bullet \\ \circ & \bullet & \circ & \bullet & \circ & \circ & \circ & \circ & \bullet \\ \circ & \bullet & \circ & \circ & \bullet & \circ & \bullet & \circ & \circ \\ \circ & \bullet & \circ & \circ & \circ & \bullet & \circ & \bullet & \circ \\ \circ & \circ & \bullet & \bullet & \circ & \circ & \circ & \bullet & \circ \\ \circ & \circ & \bullet & \circ & \bullet & \circ & \circ & \circ & \bullet \\ \circ & \circ & \bullet & \circ & \circ & \bullet & \bullet & \circ & \circ \end{pmatrix}$$

$$f(10) = 34 \begin{pmatrix} \bullet & \circ & \circ & \bullet & \circ & \circ & \bullet & \circ & \circ & \bullet \\ \bullet & \circ & \circ & \circ & \bullet & \circ & \circ & \bullet & \circ & \circ \\ \bullet & \circ & \circ & \circ & \circ & \bullet & \circ & \circ & \bullet & \circ \\ \circ & \bullet & \circ & \bullet & \circ & \circ & \circ & \circ & \bullet & \circ \\ \circ & \bullet & \circ & \circ & \bullet & \circ & \bullet & \circ & \circ & \circ \\ \circ & \bullet & \circ & \circ & \circ & \bullet & \circ & \bullet & \circ & \bullet \\ \circ & \circ & \bullet & \bullet & \circ & \circ & \circ & \bullet & \circ & \circ \\ \circ & \circ & \bullet & \circ & \bullet & \circ & \circ & \circ & \bullet & \bullet \\ \circ & \circ & \bullet & \circ & \circ & \bullet & \bullet & \circ & \circ & \circ \\ \circ & \circ & \circ & \circ & \circ & \circ & \bullet & \bullet & \bullet & \bullet \end{pmatrix}$$

2.3 Approche théorique

2.3.1 Lien avec la théorie des codes

Soit $\mathcal{M}(m,n)$ l'ensemble des matrices binaires $m \times n$. Soit E le sous-ensemble des matrices ayant exactement une ligne ou une colonne de 1. On considère le sous-espace vectoriel $\mathrm{C}_{m,n}$ engendré par les éléments de E comme un code de longueur mn. Les ampoules allumées sont symbolisées par des 1, les ampoules éteintes par des 0. Basculer un interrupteur revient ici à ajouter la matrice avec des 1 dans la ligne ou la colonne correspondante. Donc l'ensemble des configurations accessibles à partir d'une configuration initiale S est $\mathrm{S} + \mathrm{C}_{m,n}$.

$$(\ell_1, \ldots, \ell_m, c_1, \ldots, c_n) \in \mathbb{F}_2^{m+n} \mapsto \begin{pmatrix} \ell_1 + c_1 & \ell_1 + c_2 & \cdots & \ell_1 + c_n \\ \ell_2 + c_1 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \ell_m + c_1 & \cdots & \cdots & \ell_m + c_n \end{pmatrix},$$

en considérant les matrices $m \times n$ comme des mots de $\mathbb{F}_2^{mn}$. ($\mathbb{F}_2$ est le corps à deux éléments, 0 et 1)

Théorème 2.1 *$g(m,n)$ est le rayon de recouvrement du code $\mathrm{C}_{m,n}$.*

Démonstration Soit S une configuration initiale, considérée comme un mot de $\mathbb{F}_2^{mn}$. Soit c_S le mot de code le plus proche. Si u est un mot de $\mathbb{F}_2^{mn}$, le poids $w(u)$

du mot est égal au nombre d'ampoules allumées de la configuration associée. Par construction, c_S minimise $\{w(S-c) \mid c \in C_{m,n}\}$.

Donc $$f(S) = w(S - c_S) = d(S, C_{m,n})$$

Ainsi, $$\max_S f(S) = \max_S d(S, C_{m,n}) = \rho(C_{m,n})$$ □

On peut donc résoudre le problème de Berlekamp en utilisant le tableau standard, ou en utilisant le décodage par syndrome. La théorie du codage permet bien d'apporter une réponse au problème. Toutefois, cette réponse n'est accessible en des temps de calcul raisonnables que pour de petites valeurs de m et n.

2.3.2 Etude du code $C_{m,m}$

Théorème 2.2 $C_{m,m}$ *est un code* $[m^2, 2m-1, m]$.

Démonstration En notant C_i la matrice avec des 1 sur la i-ième colonne, et L_i la matrice avec des 1 sur la i-ième ligne, on vérifie que la famille

$$(C_1, \dots, C_m, L_1, \dots, L_{m-1})$$

est libre et génératrice. Donc $\dim C_{m,m} = 2m - 1$.

$w(L_1) = m$ donc $d_{C_{m,m}} \leq m$.

Soit $T \in C_{m,m}$ tel que $w(T) < m$. On pose $T = \sum_{i=1}^{n} (\alpha_i C_i + \beta_i L_i)$. T a moins de m coefficients non nuls, donc au moins une colonne nulle, par exemple la j-ième.

On a donc $$\forall i \in [\![1, m]\!], \alpha_j + \beta_i = 0$$

- Si $\alpha_j = 1$, alors $\beta_i = 1$ pour tout i et donc $T = J + \sum_i \alpha_i C_i$, où J désigne la matrice avec des 1 partout.
- Si $\alpha_j = 0$ alors $\beta_i = 0$ pour tout i, et $T = \sum_i \alpha_i C_i$.

Dans les deux cas, $w(T)$ est un multiple de m, donc $w(T) = 0$, soit $T = 0$. Ainsi $d_{C_{m,m}} = m$.

□

La complexité du calcul naïf de $f(n)$ est donc en $O(n^2 2^{(n-1)^2})$, une fois le tableau construit. C'est énorme, donc très couteux, pour des valeurs de n assez faible : $10^2 2^{9^2} \simeq 2.4 10^{26}$!

2.3.3 Exemple : cas n=3

Pour $n = 3$, le code $C_{3,3}$ est un code $[9, 5, 3]$, de matrice de contrôle :

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

(Les matrices 3×3 étant considérées comme des vecteurs, donc représentées par des vecteurs ligne de longueur 9).

Notre matrice de contrôle est obtenue en recherchant une base de l'espace vectoriel des mots x de $\mathbb{F}^n$ tels que $\forall y \in \mathrm{C}, < x, y >= \sum_{i=1}^{n} x_i y_i = 0$.

Les mots de poids 1, correspondant aux 9 matrices ayant un seul 1, ont pour syndromes respectifs les transposés des vecteurs colonnes de la matrice précédente, ces syndromes sont donc deux à deux distincts, et donc ces mots sont des chefs de classe. On a ainsi déjà 10 chefs de classe (avec le mot nul) sur $2^{9-5} = 16$ à trouver.

On cherche ensuite des mots de poids 2 ayant des syndromes distincts de ceux déjà trouvés. Ces syndromes sont les sommes, réduites modulo 2, de deux des syndromes déjà trouvés. On trouve 6 mots de poids 2 qui conviennent, par exemple ceux-ci, donnés sous forme matricielle :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Comme on a 16 chefs de classe de poids au plus 2, on a montré que $f(3) = 2$. Dans le jeux de taille 3×3, on peut donc toujours se ramener à l'une des six situations précédentes ou à une seule ampoule allumée (voire aucune).

3 Bornes sur le rayon de recouvrement

3.1 Bornes naïves

Théorème 3.1 *Soit m un entier. Alors $f(m)$ vérifie :*

$$f(m) \leq \frac{m^2}{2} \quad et \quad \sum_{i=0}^{f(m)} \mathrm{C}_{m^2}^{i} \geq 2^{(m-1)^2}$$

Démonstration La matrice J avec des 1 partout et la matrice nulle appartiennent à $\mathrm{C}_{m,m}$. Soit $\mathrm{M} \in \mathcal{M}(m, m)$. On a $w(\mathrm{M}) \in [\![0, m^2]\!]$.

- Si $w(\mathrm{M}) \geq \frac{m^2}{2}$, alors $w(\mathrm{M} - \mathrm{J}) \leq \frac{m^2}{2}$;
- sinon $w(\mathrm{M}) \leq \frac{m^2}{2}$.

Dans tous les cas : $$d(\mathrm{M}, \mathrm{C}_{m,m}) \leq \frac{m^2}{2}$$

La seconde formule s'obtient en remarquant que les boules centrées sur les mots de $\mathrm{C}_{m,m}$ et de rayon $f(m)$ recouvrent $\mathcal{M}(m, m)$. (Tout mot est à distance au plus $f(m)$ d'un mot du code, d'après le théorème 2.1).

Or le cardinal d'une boule de rayon R dans $\mathbb{F}_2^n$ est $\sum_{i=0}^{\mathrm{R}} \mathrm{C}_n^i$ (l'indice i correspond au nombre de composante que l'on change, et une fois i fixé, il reste à choisir i composantes à changer parmis n).

Donc $$|\mathrm{C}_{m,m}| \times \sum_{i=0}^{f(m)} \mathrm{C}_{m^2}^{i} \geq |\mathcal{M}(m, m)|$$

Or $$|\mathrm{C}_{m,m}| = 2^{2m-1}, \quad \text{et} \quad |\mathcal{M}(m, m)| = 2^{m^2}$$

D'où $$\sum_{i=0}^{f(m)} \mathrm{C}_{m^2}^{i} \geq 2^{m^2-2m+1} = 2^{(m-1)^2}$$ □

On en déduit de premiers encadrements pour les valeurs de $f(m)$ $(m \leq 15)$:

$$\begin{array}{ccc}
f(1)=0 & 8 \leq f(6) \leq 18 & 34 \leq f(11) \leq 60 \\
1 \leq f(2) \leq 2 & 12 \leq f(7) \leq 24 & 41 \leq f(12) \leq 72 \\
2 \leq f(3) \leq 4 & 16 \leq f(8) \leq 32 & 50 \leq f(13) \leq 84 \\
3 \leq f(4) \leq 8 & 21 \leq f(9) \leq 40 & 59 \leq f(14) \leq 98 \\
5 \leq f(5) \leq 12 & 27 \leq f(10) \leq 50 & 69 \leq f(15) \leq 112
\end{array}$$

3.2 Encadrement asymptotique des valeurs de f

Pour de grandes valeurs de n, le calcul de $f(n)$ demanderais une bien trop grande puissance de calcul. D'autre part, les bornes données par le théorème 3.1 sont vite assez mauvaises. On a alors des résultats bien plus précis, à savoir :

Théorème 3.2

$$f(n) \leq \frac{n^2}{2} - \frac{n^{\frac{3}{2}}}{\sqrt{2\pi}} + o(n^{\frac{3}{2}}).$$

Démonstration On considère désormais les tableaux d'ampoules comme des matrices de $+1$ et -1($+1$: ampoule allumée ; -1 : ampoule éteinte). Basculer un interrupteur revient donc ici à multiplier la ligne ou la colonne correspondante par -1, c'est-à-dire à multiplier à gauche ou à droite la matrice par une matrice diagonale (avec un coefficient égal à -1 et des 1 ailleurs). On note $\mathcal{C}(m,n)$ l'ensemble des matrices à coefficients ± 1. Pour A, B éléments de $\mathcal{C}(m,n)$, on définit la relation $\cong$ par : $\mathrm{A} \cong \mathrm{B} \Leftrightarrow \mathrm{B} = \mathrm{D}_m \mathrm{A} \mathrm{D}_n$, où $\mathrm{D}_m, \mathrm{D}_n$ sont des matrices diagonales d'ordre m, n à coefficients ± 1. La relation $\cong$ est clairement une relation d'équivalence. Soit $\{\mathrm{A}\}$ la classe de A. On pose :

$$d(\mathrm{A}) = \sum_{i,j} a_{ij},$$

et $\qquad l(\mathrm{A}) = \frac{1}{2}[d(\mathrm{A}) + mn] \quad$ (nombre de coefficients égaux à $+1$)

Alors $\qquad g(m,n) = \max_{\mathrm{A} \in \mathcal{C}(m,n)} \{ \min_{\mathrm{B} \in \{\mathrm{A}\}} \{l(\mathrm{B})\}\} \quad \text{et} \quad f(n) = g(n,n)$

On définit également : $r_i(\mathrm{A}) = \sum_j a_{ij}, \quad s_i(\mathrm{A}) = |r_i(\mathrm{A})|$,
et $l_i(\mathrm{A}) = \frac{1}{2}[r_i(\mathrm{A}) + n]$ (nombre de coefficients $+1$ sur la i-ième ligne).

Soit $\mathrm{A} \in \mathcal{C}(n,n)$. Si σ parcourt l'ensemble des 2^n façons de multiplier par -1 certaines colonnes, la i-ième ligne de A parcourt l'ensemble des 2^n valeurs possibles. On peut considérer $r_i(\mathrm{A})$ comme l'abscisse X d'un point après une marche aléatoire symétrique de n pas de ± 1, et $s_i(\mathrm{A})$ comme sa distance à l'origine. Donc, si E(X) désigne l'espérance mathématique de la variable X, en considérant toutes les possibilités σ comme équiprobables, on a :

$$\mathrm{E}_\sigma(s_i(\mathrm{A}^\sigma)) = \mathrm{E}(\mathrm{X})$$

et par sommation : $\qquad \mathrm{E}_\sigma(\sum_{i=1}^n s_i(\mathrm{A}^\sigma)) = n\mathrm{E}(\mathrm{X})$

D'où $\qquad \exists \sigma, \quad \sum_{i=1}^n s_i(\mathrm{A}^\sigma) \geq n\mathrm{E}(\mathrm{X})$

On obtient un élément $A^{\sigma\tau}$ en multipliant au besoin par -1 certaines lignes pour minimiser le nombre de $+1$, l'élément $A^{\sigma\tau}$ vérifiant :

$$\forall i, \quad l_i(A^{\sigma\tau}) = \tfrac{1}{2}[n - s_i(A^\sigma)]$$

(En effet, en multipliant au besoin la i-ème ligne par -1 pour minimiser le nombre de $+1$ sur cette ligne, on obtient nécessairement plus de -1 que de $+1$ sur cette ligne, donc $r_i\left(A^{\sigma\tau}\right) < 0$).

Et donc $\; l(A^{\sigma\tau}) = \sum_{i=1}^n l_i(A^{\sigma\tau}) = \sum_{i=1}^n \frac{1}{2}[n - s_i(A^\sigma)] \leq \frac{n^2}{2} - \frac{n}{2}E(X)$

On a donc montré $\quad \forall A, \exists \sigma, \tau, l(A^{\sigma\tau}) \leq \frac{n^2}{2} - \frac{n}{2}E(X)$

soit
$$f(n) \leq \tfrac{n^2}{2} - \tfrac{n}{2}E(X) \tag{1}$$

Or, pour n pair,
$$E(X) = 2^{-n} \textstyle\sum_{k=0}^{n/2} 2k C_n^{k+\frac{n}{2}} \tag{2}$$

et pour n impair,
$$E(X) = 2^{-n} \textstyle\sum_{k=0}^{\frac{n-1}{2}} (2k+1) C_n^{k+\frac{n+1}{2}} \tag{3}$$

En utilisant la formule de Stirling, on a $E(X) = \sqrt{n}\sqrt{\frac{2}{\pi}} + o(n^{1/2})$, et donc :

$$f(n) \leq \frac{n^2}{2} - \frac{n^{\frac{3}{2}}}{\sqrt{2\pi}} + o\left(n^{\frac{3}{2}}\right) \qquad \square$$

Pour de petites valeurs de m ($m \leq 15$), les formules **(2)** et **(3)** nous permettent de calculer $E(X)$ et d'obtenir ainsi une majoration assez précise de $f(m)$. Ainsi :

$f(1) = 0$	$f(6) \leq 12$	$f(11) \leq 45$
$f(2) = 1$	$f(7) \leq 16$	$f(12) \leq 55$
$f(3) = 2$	$f(8) \leq 23$	$f(13) \leq 65$
$f(4) \leq 5$	$f(9) \leq 29$	$f(14) \leq 77$
$f(5) \leq 7$	$f(10) \leq 37$	$f(15) \leq 88$

On peut également minorer asymptotiquement $f(n)$ par une expression de la forme :

$$\tfrac{n^2}{2} - \tfrac{n^{\frac{3}{2}}}{2} + o(n^{\frac{3}{2}})$$

Théorème 3.3 *Soit n un nombre d'Hadamard. Alors*

$$\frac{n^2}{2} - \frac{n^{\frac{3}{2}}}{2} \leq f(n)$$

Un nombre d'Hadamard n est un nombre tel qu'il existe une matrice d'Hadamard de taille $n \times n$, c'est-à-dire une matrice à coefficients ± 1 vérifiant $H\,{}^t H = nI$, où I est la matrice identité.

Démonstration Soit H une matrice d'Hadamard de taille $n \times n$.

On considère les lignes de H comme des vecteurs $\vec{u_1}, \ldots, \vec{u_n} \in \mathbb{R}^n$. Ils sont deux à deux orthogonaux, et de norme $\sqrt{n}$. Soit $\vec{v}$ le vecteur de $\mathbb{R}^n$ de coordonnées $(1, \ldots, 1)$. On a ainsi : $d(H) = \sum_{i=1}^n \vec{v} \cdot \vec{u_i}$.

Les $\frac{1}{\sqrt{n}}\vec{u_i}$ forment une base orthonormée de $\mathbb{R}^n$. Par un changement de bases orthonormées, on envoie ces vecteurs sur la base canonique de $\mathbb{R}^n$, notée $(\epsilon_1, \ldots, \epsilon_n)$. Le vecteur $\frac{1}{\sqrt{n}}\vec{v}$, de norme 1, est envoyé sur un vecteur noté $\vec{v*} = (v_1, \ldots, v_n)$ de norme 1 également. Et l'on a $d(\mathrm{H}) = n \sum_{i=1}^{n} \vec{v*} \cdot \vec{\epsilon_i} = n \sum_i v_i$. Cette quantité est minimale lorsque $v_i = -\frac{1}{\sqrt{n}}$ pour tout i, grâce au principe des extrema liés. Donc $d(\mathrm{H}) \geq -n^{3/2}$, et comme $l(\mathrm{H}) = 1/2\left(d(\mathrm{H}) + n^2\right)$, on obtient :

$$f(n) \geq l(\mathrm{H}) \geq n^2/2 - n^{3/2}/2 \qquad \square$$

Le problème est que les matrices d'Hadamard n'existent pas à tous ordres. L'ensemble des nombres d'Hadamard (tels qu'il existe une matrice d'Hadamard à cet ordre) est stable par multiplication, le produit de Kronecker de deux matrices d'Hadamard étant encore une matrice d'Hadamard. On peut montrer que les nombres d'Hadamard sont $1, 2$ ou multiples de 4. Le fait que tous les multiples de 4 soient des nombres d'Hadamard est encore une conjecture. Actuellement, le premier multiple de 4 pour lequel il y a un doute est 468.

Pour d'autres ordres, on prend m le plus grand nombre d'Hadamard inférieur à n et on considère la matrice d'Hadamard associée dans le bloc supérieur gauche d'une matrice $n \times n$, la minoration obtenue est alors

$$f(n) \geq m^2/2 - m^{3/2}/2$$

Si tout multiple de 4 est un nombre d'Hadamard, on a $m > n - 4$ et ceci nous permet de conclure qu'asymptotiquement, on a bien une minoration de $f(n)$ par un terme de développement $\frac{n^2}{2} - \frac{n^{\frac{3}{2}}}{2}$.

Mais ceci est une conjecture. En fait, on arrive à ce résultat en utilisant les nombres de la forme $2^i 12^j$, qui sont tout des nombres d'Hadamard, puisque 12 et 2 le sont. On a en effet une propriété de “densité” de ces nombres, de la forme :

$$\forall \epsilon \exists n_0 \forall n \geq n_0, \quad \exists i, j \geq 0, \quad n(1-\epsilon) \leq 2^i 12^j \leq n$$

Aussi, si m désigne le plus grand nombre d'Hadamard inférieur à n, la minoration $f(n) \geq m^2/2 - m^{3/2}/2$ nous donne bien une minoration de la forme voulue.

Pour des petites valeurs de m, on peut utiliser ce qui précède, en remarquant également que, si l'on découpe la matrice en blocs, la juxtaposition de configurations minimales est encore minimale. On admet de plus les formules $g(2\mathrm{K}, 2) = g(2\mathrm{K}+1, 2) = \mathrm{K}, g(4\mathrm{K}, 3) = g(4\mathrm{K}+1, 3) = 3\mathrm{K}, g(4\mathrm{K}+2, 3) = 3\mathrm{K}+1$, et $g(4\mathrm{K}+3, 3) = 3\mathrm{K}+2$.

On en déduit les bornes suivantes :

$$\begin{array}{ccc}
f(1) = 0 & 9 \leq f(6) \leq 12 & 35 \leq f(11) \leq 45 \\
f(2) = 1 & 12 \leq f(7) \leq 16 & 52 \leq f(12) \leq 55 \\
f(3) = 2 & 21 \leq f(8) \leq 23 & 53 \leq f(13) \leq 65 \\
4 \leq f(4) \leq 5 & 22 \leq f(9) \leq 29 & 65 \leq f(14) \leq 77 \\
5 \leq f(5) \leq 7 & 30 \leq f(10) \leq 37 & 72 \leq f(15) \leq 88
\end{array}$$

L'approximation est excellente pour les nombres d'Hadamard $(1, 2, 4, 8$ et $12)$.

Conclusion

Le jeu étudié ici n'est pas le seul à utiliser le tableau d'ampoules. On peut aussi choisir de minimiser la différence entre le nombre d'ampoules allumées et le nombre d'ampoules éteintes. Il est en fait toujours possible de se ramener à 1 si n est impair, à 0 ou 2 si n est pair.

Enfin, le principe du "*Berlekamp's switching game*" a été étendu, le calcul de $g(n,m)$ correspondant au calcul pour $p=1$ de

$$\mathrm{B}_p(n,m) = \min_{\varepsilon_{ij}=\pm 1} \max_{\theta_i=\pm 1} \left(\sum_{j=1}^{m} \left| \sum_{i=1}^{n} \theta_i \varepsilon_{ij} \right|^p \right)^{1/p}.$$

Cette extension a permis en particulier d'améliorer la borne supérieure :

$$f(n) \leq \frac{n^2}{2} - \frac{n^{\frac{3}{2}}}{\sqrt{2\pi}} + o(\sqrt{n}).$$