Multiplication binaire et factorisation

Position du problème

On cherche un système dynamique discret qui, étant donné un entier non-premier, trouve un de ses diviseurs non-triviaux. On se base sur la multiplication binaire. En effet, on observe qu'une matrice à coefficients dans $\{0, 1\}$ peut s'interpréter comme une multiplication binaire si ses lignes non-nulles sont égales entre elles, comme illustré dans la figure 1. Les colonnes non-nulles sont alors aussi égales entre elles, et les deux facteurs de la multiplication sont alors lisibles, en base 2, sur les lignes non-nulles pour l'un, et de bas en haut sur les colonnes non-nulles pour l'autre. Si on pose leur multiplication, toujours en base 2, on retrouve en effet la matrice de départ, décalée par les retenues (cf. Figure 1).

1	0	1	1
0	0	0	0
1	0	1	1
1	0	1	1

					1	0	1	1	×
					1	0	1	1	1
+				0	0	0	0	.	0
+			1	0	1	1	.	.	1
+		1	0	1	1	.	.	.	1
	1	0	0	0	1	1	1	1	

FIGURE 1 – La matrice de gauche s'interprète comme la multiplication de 11 (1011 horizontalement) par 13 (1101 verticalement, de haut en bas).

Par ailleurs, étant donné une matrice M à coefficients dans $\{0, 1\}$, on pose $\sigma(M)$ l'entier obtenu en sommant ses lignes décalées par des retenues (cf. Figure 2). Si M représente une multiplication, σ est par construction le produit.
L'idée est donc de partir d'une matrice à coefficients dans $\{0, 1\}$ pour laquelle σ vaut le nombre qu'on cherche à factoriser, et de lui appliquer des transformations qui conservent σ jusqu'à atteindre une matrice qui représente une multiplication.

$$M = \begin{matrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{matrix} \qquad \sigma(M) = \begin{array}{cccccccc} & & & & 1 & 1 & 0 & 1 \\ + & & & 0 & 0 & 1 & 1 & . \\ + & & 1 & 0 & 0 & 1 & . & . \\ \hline & & 1 & 1 & 0 & 1 & 1 & 1 \end{array} = 55$$

FIGURE 2 – Exemple de calcul de σ.

$$\mathbf{1} \quad \underset{\text{R2}}{\overset{\text{R1}}{\rightleftarrows}} \quad \mathbf{0} \qquad 0 \quad \underset{\text{R2}}{\overset{\text{R1}}{\rightleftarrows}} \quad 1$$

$$0 \quad \underset{\text{R4}}{\overset{\text{R3}}{\rightleftarrows}} \quad 1 \qquad \mathbf{1}\ 0 \quad \underset{\text{R4}}{\overset{\text{R3}}{\rightleftarrows}} \quad \mathbf{0}\ 1$$

$$\mathbf{1}\ 0 \quad \underset{\text{R6}}{\overset{\text{R5}}{\rightleftarrows}} \quad \mathbf{0}\ 1 \qquad 0 \quad \underset{\text{R6}}{\overset{\text{R5}}{\rightleftarrows}} \quad 1$$

FIGURE 3 – Transformations locales préservant σ.

Un algorithme

Soit n le nombre de chiffres en base 2 du nombre composé N dont on cherche un diviseur non-trivial. On se donne une matrice M de taille $n-1 \times \lceil \frac{n}{2} \rceil$ telle que $\sigma(M) = N$. Pour tous a et b différents de 1 et N, et tels que $N = ab$, a ou b est de taille inférieure à $\lceil \frac{n}{2} \rceil$ et l'autre est de taille inférieure à $n-1$, on peut donc représenter leur multiplication sur une matrice de la taille de M.

Formellement, on pose $\mathcal{L} = [\![1, n-1]\!] \times [\![1, \lceil \frac{n}{2} \rceil]\!]$ l'ensemble des cases de la matrice, et $\mathcal{E} = \{0,1\}^{\mathcal{L}}$ l'ensemble des configurations. Pour tout $x \in \mathcal{E}$, $(i,j) \in \mathcal{L}$, on note $x_{i,j}$ le coefficient (i,j) de la matrice x.

On se donne également un ensemble $\Gamma \subset \mathcal{E}^{\mathcal{E} \times \mathcal{L}}$ de transformations locales qui conservent σ. Elles sont représentées sur la figure 3.

Une formulation équivalente de l'égalité des lignes non-nulles est qu'un coefficient situé sur la même ligne qu'un 1 et sur la même colonne qu'un 1 vaut nécessairement 1 dans une matrice qui représente une multiplication. On va donc appliquer aléatoirement des règles conservant σ, en privilégiant les mouvements qui retirent les zéros de telles cases. Dans la suite, on dira qu'une case est *sûre* s'il n'y a pas de 1 sur la même ligne ou s'il n'y en a pas

0	1	0	0	1	1	0	[0]
0	[0]	0	0	1	1	0	1
0	[0]	0	0	1	1	0	1
0	0	0	0	0	0	0	0
0	[0]	0	0	1	1	0	1

FIGURE 4 – Exemple de situation bloquée si on interdit les mouvements ne déplaçant pas les zéros menacés (encadrés) : aucune des règles de la Figure 3 ne s'applique à eux.

sur la même colonne, et *dangereuse* s'il y a à la fois un 1 sur la même ligne et un sur la même colonne.
Pour diriger les zéros vers les cases sûres, on voudrait n'effectuer que des mouvements qui sortent un zéro d'une case dangereuse, mais cette restriction est trop forte : il existe alors des situations bloquées, la figure 4 en donne un exemple. Il est donc nécessaire d'autoriser au moins certains mouvements qui ne sont pas directement utiles en ce sens, pour permettre d'autres mouvements par la suite. De même, on pourrait vouloir restreindre les mouvements des zéros vers des cases dangereuses, de la même façon que pour le problème des n reines. Cependant, il se forme alors des blocs stables de 1 : les zéros qui viennent remplacer un 1 du bord du bloc en sont rapidement éjectés (les seules cases sûres proches sont à l'extérieur du bloc).
On prend donc le parti de ne pas restreindre les mouvements des zéros vers des cases dangereuses, et on se donne une probabilité d'agitation p : un mouvement valide mais qui ne sort pas un zéro d'une case dangereuse est effectué avec une probabilité p, alors qu'un mouvement valide qui sort un zéro d'une case dangereuse est toujours effectué.