L'échiquier du diable

Par Enigmath, le 7 janvier 2026

Énoncé

Le diable propose un défi à Alice et Bob. Il commence par convoquer Alice et lui présente un échiquier de taille 8×8 sur lequel il a disposé des pions, comme bon lui semble. Il désigne ensuite une case particulière, appelée la « case mystère ».
Alice a alors la possibilité de modifier légèrement la configuration des pions : elle peut soit retirer un pion, soit en ajouter un sur une case vide, soit ne rien faire. Après avoir effectué son action, Alice quitte la pièce.
Le diable fait ensuite entrer Bob. En observant l'échiquier tel qu'Alice l'a laissé, Bob doit identifier la case mystère.
Aucun contact n'est autorisé entre Alice et Bob une fois le défi commencé. Alice et Bob connaissent les règles du jeu à l'avance et peuvent convenir d'une stratégie commune avant le début du défi. La case mystère peut être n'importe quelle case de l'échiquier.

Questions :

1. 🌶[1.9] Trouvez une stratégie qu'Alice et Bob peuvent mettre en place pour être sûrs de trouver la case mystère. Si Alice est contrainte de modifier une case, existe-t-il une stratégie valable ?
2. 🌶[2.0] Le diable décide de retirer une case de l'échiquier (laissant ainsi $n = 63$ cases). La stratégie d'Alice et Bob reste-t-elle valable ? Si Alice est contrainte de modifier une case, existe-t-il une stratégie valable ?
3. 🌶[2.1] Trouvez une stratégie probabiliste, fixée à l'avance entre Alice et Bob (c'est-à-dire dépendant d'un tirage aléatoire partagé, mais inconnu du diable), telle que la probabilité de réussite soit strictement supérieure à $2^{1.5} - 2 \approx 0.8284$, quel que soit le nombre $n \geq 2$ de cases.
4. 🌶[1.5] Si Alice est contrainte de modifier deux cases (éventuellement la même case, ce qui revient à ne rien faire), trouvez une stratégie qu'Alice et Bob peuvent mettre en place pour être sûrs de trouver la case mystère, quel que soit le nombre $n \geq 2$ de cases.

Solution

1. Soit $n = 2^k$ le nombre de cases de l'échiquier ($k = 8$). On associe à chaque case $i \in \{1, \dots, n\}$ un vecteur binaire $V_i \in \{0,1\}^k$ distinct. Cette association est partagée entre Alice et Bob au début du défi. Soit $i^* \in \{1, \dots, n\}$ la case mystère à transmettre. Pour une configuration initiale $c \in \{0,1\}^n$, Alice calcule le vecteur binaire $W \triangleq \sum_{i=1}^{n} c_i V_i \mod 2$. Le but d'Alice est de modifier la configuration en c' de sorte que, lorsque Bob va calculer $\sum_{i=1}^{n} c'_i V_i \mod 2$, il trouve le vecteur binaire correspondant à la case mystère. Ainsi, on trouve qu'Alice doit modifier la case correspondant au vecteur binaire $V_{i^*} + W \mod 2$. En effet, une telle modification a pour effet d'ajouter $V_{i^*} + W \mod 2$ à W, et donc d'obtenir $\sum_{i=1}^{n} c'_i V_i \mod 2 = V_{i^*}$. Dans cette solution, Alice modifie systématiquement une case. Par conséquent, elle reste valable même si le diable impose à Alice de modifier une case.

2. Si $n = 2^k - 1$, la solution présentée ci-dessus reste valide. En effet, on peut utiliser la même représentation binaire pour les cases, en choisissant que la case manquante soit représentée par $0_k = (0, 0, \ldots, 0) \in \{0,1\}^k$. Ainsi, si Alice doit modifier la case manquante, c'est-à-dire ajouter le vecteur nul 0_k à W, alors, à la place, elle laisse l'échiquier inchangé.

   Cette approche ne fonctionne plus si Alice doit modifier exactement une case. Pour démontrer qu'aucune solution n'existe dans ce cas, on considère le graphe à 2^n sommets, où chaque sommet représente une configuration possible $c \in \{0,1\}^n$ du plateau. Deux sommets sont reliés si et seulement s'ils diffèrent sur une seule case, c'est-à-dire si leur distance de Hamming est égale à 1 (ce graphe est couramment appelé le n-cube, et noté Q_n). Une solution au problème revient à trouver un coloriage des sommets avec n couleurs, tel que dans le voisinage (au sens de la distance de Hamming) de chaque sommet, chaque couleur apparaisse exactement une fois. En effet, en se mettant d'accord à l'avance sur un tel coloriage, et en associant chaque couleur à une case de l'échiquier, Alice peut, à partir de n'importe quelle configuration initiale, se déplacer vers un voisin de couleur donnée, ce qui lui permet de transmettre l'information correspondant à une case quelconque (et donc la case mystère). Dans la variante contrainte où Alice doit modifier exactement une case, chaque sommet possède exactement n voisins (il n'y a pas de boucle, contrairement à la variante non-contrainte). Ainsi, chaque couleur doit apparaître une et une seule fois dans chaque voisinage. Considérons une couleur x : elle apparaît donc 2^n fois au total dans tous les voisinages. D'autre part, chaque sommet de couleur x appartient à n voisinages (un pour chacun de ses voisins). Ainsi, on a $2^n = n \times$ (nombre de sommets de couleur x), ce qui implique que n divise 2^n. Or, ceci est possible uniquement si n est une puissance de 2.

3. Soit $k \triangleq \lceil \log_2 n \rceil \geq 1$ et $a \triangleq 2^k - n$. On a alors $0 \leq a \leq 2^{k-1} - 1$. Si $a < 2$, alors Alice et Bob disposent d'une stratégie gagnante comme démontré précédemment. On suppose donc désormais que $a \geq 2$, ce qui implique $k \geq 3$. Alice et Bob commencent par mélanger aléatoirement les n cases du plateau, en gardant cette permutation secrète. Ils tirent ensuite aléatoirement (et secrètement) un vecteur selon la loi uniforme sur $\{0,1\}^n$, qu'ils ajouteront (modulo 2) à la configuration du diable. Dans la suite, on omet ces tirages aléatoires préliminaires et on suppose directement que la case mystère est choisie au hasard, uniformément parmi les n cases, et que, indépendamment, la configuration du diable est aléatoire selon la loi uniforme sur $\{0,1\}^n$. À chaque case $i \in \{1, \ldots, n\}$, Alice et Bob associent un vecteur $V_i \in \{0,1\}^k \setminus \{0_k\}$, en suivant l'ordre lexicographique croissant, e.g., pour $n = 5$,

$$V_1, \ldots, V_5 = \begin{bmatrix}0\\0\\1\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix}, \begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}1\\0\\1\end{bmatrix}.$$

   Pour chaque $i \in \{1, \ldots, a\}$, on définit $V_{n+i} \in \{0,1\}^k \setminus \{V_1, \ldots, V_n\}$ comme les vecteurs restants (par construction, leur première coordonnée vaut 1, sauf 0_k). On fait alors « pointer » chaque V_{n+i} vers la même case que $V_{n+i} + (1, 0, \ldots, 0) \in \{V_1, \ldots, V_n\} \mod 2$. Cette opération garantit que tout vecteur du complément sert à désigner une case réelle. Comme précédemment, Alice calcule le vecteur binaire $W \triangleq \sum_{i=1}^n c_i V_i \mod 2$. Elle cherche alors à le modifier en ajoutant un vecteur de l'ensemble $A = \{0_k, V_1, \ldots, V_n\}$, où ajouter 0_k revient à ne rien faire, et ajouter V_i revient à modifier la case i. Son objectif est de transformer W en un vecteur pointant vers i^*, ce qui assure que Bob identifiera correctement la case mystère. Nous énumérons ci-dessous les résultats permettant de conclure notre analyse :

   Lemme. *La variable aléatoire W est uniformément distribuée sur $\{0,1\}^k$.*

   Démonstration. On exploite la structure d'espace vectoriel de $\mathbb{F}_2^k \triangleq \{0,1\}^k$. Puisque la base canonique $(V_{i_1}, \ldots, V_{i_k})$ est incluse dans l'ensemble $\{V_1, \ldots, V_n\}$, alors $\sum_{j=1}^k c_{i_j} V_{i_j}$ est uniformément distribuée dans $\mathbb{F}_2^k$, car les bits c_{i_j} sont indépendants et uniformément choisis. Toute translation indépendante dans $\mathbb{F}_2^k$ préserve la loi uniforme, ce qui assure que W est également uniforme. □

   Lemme. *Si la case mystère i^* possède deux vecteurs pointant vers elle, alors Alice est toujours capable de la transmettre.*

Démonstration. Soit A_0 l'ensemble des vecteurs dont la première coordonnée est nulle. On a $A_0 \subset A$, de taille 2^{k-1}. Parmi les deux vecteurs pointant vers i^*, exactement un seul appartient à A_0. On note ce vecteur V_0^*, et l'autre (qui commence donc par un 1) V_1^*. On distingue alors deux cas selon la première coordonnée de W :
— Si $W \in A_0$, alors $V_0^* \in A_0 = W + A_0$, donc Alice choisis $W' = V_0^*$ pour transmettre i^*.
— Si $W \notin A_0$, alors $W + V_1^* \in A_0$, donc Alice peut transmettre i^* en choisissant $W' = V_1^*$. □

Lemme. *La probabilité totale d'échec est*

$$\mathbb{P}(\textit{échec}) = \frac{a-1}{2^k} \cdot \frac{2^k - 2a}{2^k - a}.$$

Démonstration. C'est la probabilité que Alice ne puisse pas transmettre la case i^*. Cela se produit lorsque deux conditions sont réunies :
— La case i^* ne possède qu'un seul vecteur représentant (c'est-à-dire uniquement V_{i^*}) ;
— Ce vecteur V_{i^*} ne se trouve pas dans l'ensemble $W + A$, autrement dit $W \notin A + V_{i^*}$.
La première probabilité vaut $\frac{n-a}{n}$, puisque parmi les n cases, seules $n - a$ ont un unique représentant. La seconde probabilité, conditionnellement à un vecteur fixé V_{i^*}, vaut $\frac{a-1}{2^k}$. En effet, W est indépendant de V_{i^*} et uniformément distribué sur $\{0,1\}^k$, tandis que $A + V_{i^*}$ est un ensemble de taille $n + 1$. Ainsi, la probabilité que $W \notin A + V_{i^*}$ est donnée par :

$$\frac{2^k - (n+1)}{2^k} = \frac{a-1}{n+a}.$$

La probabilité totale d'échec est donc le produit des deux probabilités. □

Lemme.

$$f(a) \triangleq \frac{a-1}{2^k} \cdot \frac{2^k - 2a}{2^k - a} < 3 - 2^{1.5}.$$

Démonstration. La fonction f est concave :

$$f'(a) = \frac{-a(2^{k+2} - 2a) + 2^k + 4^k}{2^k(2^k - a)^2}.$$
$$f''(a) = -\frac{2^{k+1} - 2}{(2^k - a)^3}.$$

La solution de $f'(a) = 0$ est $a = 2^{k-1}\left(2 - \sqrt{2 - 2^{1-k}}\right)$. En réinjectant dans f, on trouve

$$f(a) \leq 3 - 2^{-k}\left(2 + 2^{\frac{3+k}{2}}\sqrt{2^k - 1}\right) < 3 - 2^{1.5}.$$

□

4. Soit $k \triangleq \lceil \log_2 n \rceil \geq 1$ (on a alors $2^k \geq n > 2^{k-1}$). À chaque case $i \in \{1, \ldots, n\}$, Alice et Bob associent un vecteur $V_i \in \{0,1\}^k$, en suivant l'ordre lexicographique croissant, e.g., pour $n = 5$,

$$V_1, \ldots, V_5 = \begin{bmatrix}0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix}, \begin{bmatrix}1\\0\\0\end{bmatrix}.$$

Par construction, $(1, 0, \ldots, 0)$ et les vecteurs dont la première coordonnée vaut 0 appartiennent à l'ensemble $\{V_1, \ldots, V_n\}$. Comme précédemment, Alice calcule le vecteur binaire $W \triangleq \sum_{i=1}^n c_i V_i \mod 2$, et souhaite transmettre la case mystère en ajoutant le vecteur $V_{i^*} + W \mod 2$.
— Si la première coordonnée de $V_{i^*} + W \mod 2$ est égale à 0, alors Alice modifie la case correspondante (ainsi que la case associée à 0_k, pour respecter la contrainte de deux modifications).
— Sinon, Alice commence par modifier la case correspondant au vecteur $(1, 0, \ldots, 0)$, ce qui lui permet de se ramener au cas précédent pour la seconde modification.

Notes et références

L'énigme de l'échiquier du diable est présenté sous le nom *Chessboard Guess* dans [1] (chapitre 17). Une version simplifié est également présenté comme un tour de magie par Andy Liu [2].
L'énigme est lié à la théorie des codes correcteurs d'erreurs, en particulier au code de Hamming. Dans un code de Hamming classique, on encode un message avec redondance afin de détecter et corriger les erreurs. L'objectif est qu'une erreur (changement d'un bit) ne modifie pas le message décodé. Dans l'énigme, la logique est inversée : on veut qu'une seule erreur (modification d'une case) permette de transmettre une information parmi n possibilités (la case mystère). Le code n'est plus conçu pour être robuste aux erreurs, mais pour exprimer une information à travers une erreur contrôlée.
Un concept connexe est le *nombre domatique* $d(G)$ d'un graphe G [3]. Dans notre contexte, si l'on prend $G = Q_n$, le n-cube (dont les sommets sont les éléments de $\{0,1\}^n$ reliés par une arête lorsqu'ils diffèrent d'un seul bit), alors $d(Q_n)$ correspond au nombre maximal de « couleurs » qu'Alice peut transmettre. Comme Q_n est régulier de degré n, on a : $d(Q_n) \leq n+1$. Similairement à ce que nous avons démontré, on a que l'égalité $d(Q_n) = n+1$ est atteinte si et seulement si $n = 2^p - 1$ pour un certain entier p. On a également $d(Q_{2^p-1}) = d(Q_{2^p}) = 2^p$. Par exemple, pour $n = 1$, on a $d(Q_1) = 2$. En effet, Alice observe une unique case, et peut choisir de la laisser telle quelle ou de la modifier. Cela lui permet de transmettre deux « couleurs » possibles à Bob.

Sources

[1] Peter Winkler. *Mathematical puzzles : a connoisseur's collection*. CRC Press, 2003.

[2] Andy Liu. Two applications of a hamming code. *The College Mathematics Journal*, 40(1):2–5, 2009.

[3] Jean-Marie Laborde. Sur le nombre domatique du n-cube et une conjecture de zelinka. *European Journal of Combinatorics*, 8(2):175–177, 1987.