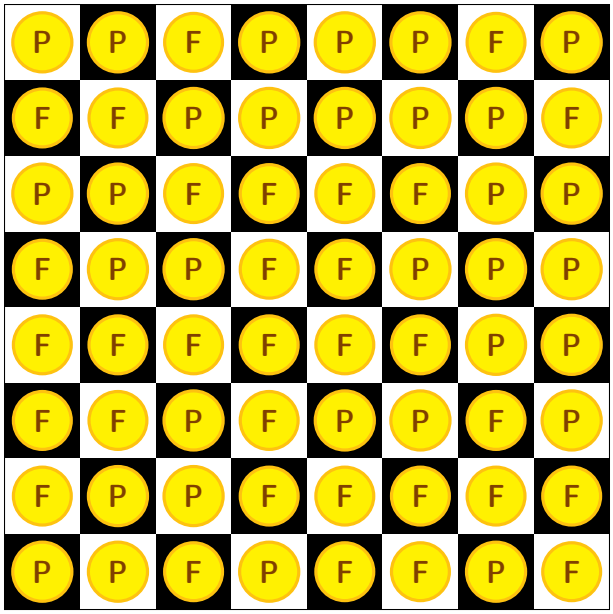
Pièces et échiquier

Question

Alice et Bob ont été capturés par Ève. Celle-ci leur propose de jouer pour leur libération. Ève va placer sur un échiquier 64 pièces de monnaie. Il y aura ainsi une pièce sur chaque case, soit sur « pile », soit sur « face ». Elle fera ensuite venir Alice, lui montrera l'échiquier, et lui désignera une des cases. Alice devra retourner une des pièces. Ève fera alors sortir Alice et entrer Bob, qui devra, en regardant l'échiquier, trouver quelle case a été désignée par Ève.



Avant le jeu, Alice et Bob ont tout le temps de mettre au point une stratégie commune, mais une fois que le jeu commence, ils ne pourront plus communiquer : la seule information transmise par Alice à Bob le sera par l'intermédiaire de l'échiquier.

Pouvez-vous trouver une stratégie qui permette à Alice et Bob d'être sûrs de gagner ?

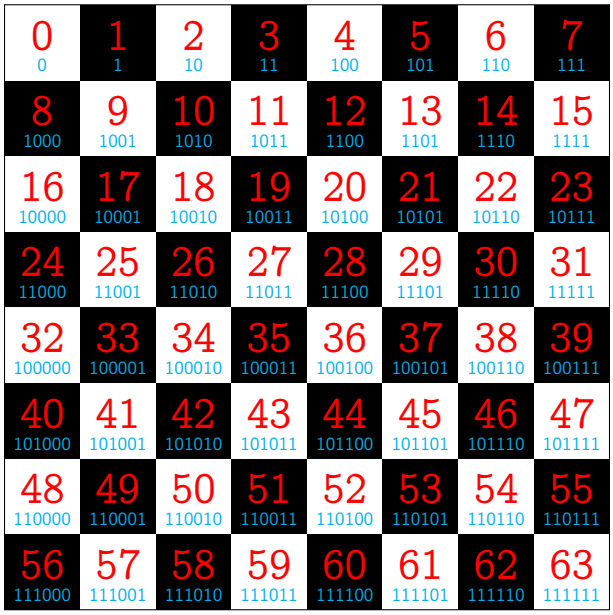
Réponse

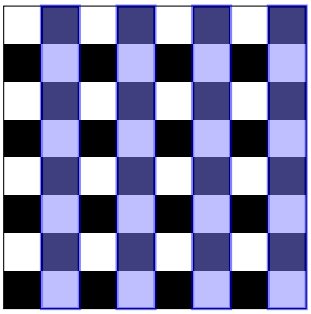
On remarque déjà qu'Alice a 64 choix d'actions, puisqu'elle doit retourner exactement une des pièces. D'un autre côté, le message qu'elle veut envoyer à Bob (la case qui a été désignée par Ève) existe également en 64 versions. Il lui faut donc trouver un moyen d'exploiter pleinement son action.

Une manière de faire est d'utiliser la numérotation binaire. Les nombres de 0 à 63 s'écrivent en binaire avec six bits (de $0 = \overline{0}$ à $63 = \overline{111111}$).

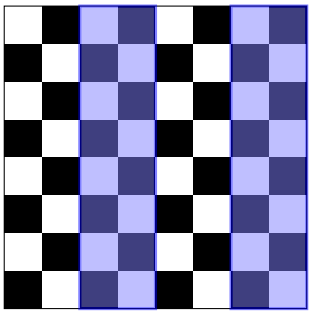
En particulier, si on numérote de 0 à 63 les cases de l'échiquier, on possède 6 groupes de 32 cases, du type

$$E_i = \{\text{case numéro } n \,|\, \text{le } i\text{-ème bit de } n \text{ est un } 1\}.$$

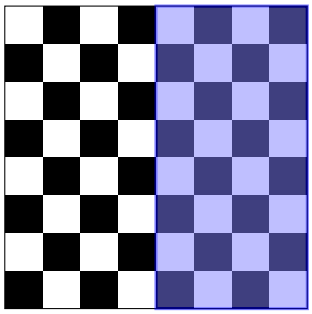




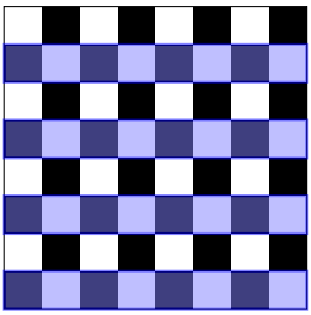
E_0



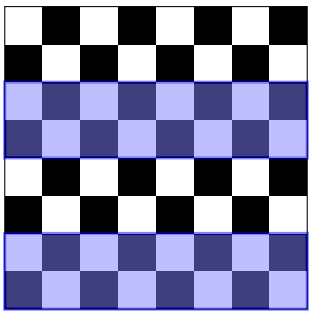
E_1



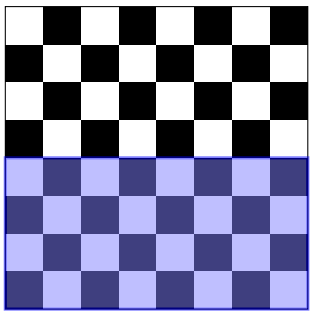
E_2



E_3



E_4



E_5

Par construction, cette famille $(E_i)_{i=0}^5$ a la propriété remarquable [1] que quel que soit l'ensemble $I \subseteq \{0, 1, \ldots, 5\}$, il existe une unique case sur l'échiquier appartenant aux E_i pour $i \in I$ et n'appartenant pas aux E_j pour $j \notin I$. En effet, si l'on cherche la case appartenant à E_2, E_3 et E_5 et à aucun autre E_i, par exemple, il s'agit nécessairement de la case dont le numéro possède un 1 aux bits numéro 2, 3 et 5 et un 0 aux autres bits, c'est-à-dire à la case numéro $\overline{101100} = 44$.

Ces ensembles permettent d'associer à chaque configuration de pièces sur l'échiquier un nombre entre 0 et 63 que l'on appellera son *résultat* (et donc une case de l'échiquier). Pour

1. En fait, cette propriété est essentiellement équivalente au fait que si on regarde l'univers $\Omega = \{0, 1, \ldots, 63\}$ muni de la probabilité uniforme, les ensembles $E_0, \ldots, E_5$ sont des événements de probabilité $1/2$ deux à deux indépendants. N'importe quelle famille (E_i) vérifiant ces propriétés permettrait d'ailleurs à Alice et Bob d'appliquer leur stratégie.

chaque $i \in \{0, 1, \ldots, 5\}$, on compte le nombre de « face » dans E_i, si celui-ci est pair, on pose $b_i = 0$; dans le cas contraire, $b_i = 1$. Le résultat de l'échiquier est alors le nombre dont la décomposition en base 2 est $\overline{b_5 b_4 b_3 b_2 b_1 b_0}$, c'est-à-dire $R = \sum_{i=0}^{5} b_i 2^i$.

Par exemple, dans le cas de l'échiquier de l'énoncé, il y a :

— 15 « face » dans E_0, donc $b_0 = 1$;
— 15 « face » dans E_1, donc $b_1 = 1$;
— 15 « face » dans E_2, donc $b_2 = 1$;
— 14 « face » dans E_3, donc $b_3 = 0$;
— 17 « face » dans E_4, donc $b_4 = 1$;
— 20 « face » dans E_5, donc $b_5 = 0$;

ainsi, $R = \overline{010111} = 23$.

La stratégie d'Alice va donc être de retourner une pièce de telle sorte que le résultat de la nouvelle configuration soit le numéro de la case désignée par Ève. Bob n'aura plus donc qu'à calculer le résultat et montrer (fièrement) la case correspondante, leur assurant la liberté.

Pour vérifier que cette stratégie fonctionne, il faut donc s'assurer qu'Alice peut, en retournant une pièce, faire apparaître n'importe quel résultat, et ce quelle que soit la configuration initiale.

C'est en fait étonnamment facile : pour chacun des E_i, il y a deux possibilités. Soit le nombre de « face » est déjà de la bonne parité (c'est-à-dire que le b_i correspondant est bien le i-ème bit du nombre qu'Alice souhaite obtenir), soit il ne l'est pas. Notons I l'ensemble des i tels que b_i ne soit pas le bon. D'après la propriété cruciale des (E_i), il existe une unique case appartenant à tous les E_i pour $i \in I$ et à aucun autre. Si Alice retourne cette case, elle change le nombre de « face » appartenant à ces E_i d'une unité, et elle change donc les b_i correspondant. En revanche, comme la pièce qu'elle retourne n'appartient pas aux E_j, $j \notin I$, les b_j « déjà corrects » restent inchangés. Alice peut donc obtenir n'importe quel résultat, et elle peut donc envoyer le bon message à Bob.

Par exemple, dans la situation de l'énoncé, si Ève avait désigné la case $18 = \overline{01010}$, Alice veut changer les valeurs de b_0 et b_2, donc il lui faut retourner la case $\overline{000101} = 5$. Pour donner [2] un autre exemple, dans le cas où la configuration donnée par Ève fournit déjà le bon résultat, Alice doit retourner la pièce située sur la case 0.

2. En fait, si le résultat de la configuration initiale est R_0 et que le résultat voulu est R_1, Alice doit retourner la case de numéro $R_0 \oplus R_1$, où $\oplus$ désigne le ou exclusif bit à bit. Mais cela n'est qu'une manière légèrement plus savante de dire la même chose.