

Dans notre histoire des 50 prisonniers, si tous utilisent la stratégie *Suivre*, alors ils gagnent quand il n'y a aucun cycle de longueur supérieure à 25. S'il existe un cycle de longueur 50, ils perdent tous. Dans les autres cas, par exemple si on a un cycle de longueur 30 et d'autres cycles (nécessairement de longueur inférieure à $20 = 50 - 30$), il y aura autant de prisonniers perdants que d'éléments du plus grand cycle, et les prisonniers perdront collectivement (voir l'encadré page 79, qui détaille le cas de 4 prisonniers). Le problème se ramène donc à calculer combien de permutations de l'ensemble à 50 éléments ont un cycle de longueur supérieure à 25.

La probabilité de gagner des 50 prisonniers

Nous allons montrer que la probabilité qu'une permutation des entiers $\{1, 2, 3, \dots, 2n\}$ ne contienne pas de cycle de longueur supérieure à n est supérieure à $1 - \ln(2)$ (où $\ln$ désigne le logarithme népérien), soit 0,306852... Cela montrera que la probabilité que les prisonniers gagnent est supérieure à 30 %.

Soit k un entier tel que $n < k \leq 2n$. Évaluons le nombre de permutations ayant un cycle d'ordre k parmi les $(2n)!$ permutations possibles de l'ensemble $\{1, 2, 3, \dots, 2n\}$. Il y a $C(2n, k) = \frac{(2n)!}{k!(2n-k)!}$ façons de choisir les entiers du cycle. Le nombre $C(2n, k)$ est le nombre de combinaisons de k éléments pris parmi $2n$. Il y a $(k-1)!$ façons d'ordonner les k entiers choisis en un cycle, et il y a $(2n-k)!$ façons de classer les autres entiers pour déterminer la permutation. Le nombre total de permutations de $\{1, 2, 3, \dots, 2n\}$ ayant un cycle d'ordre k supérieur à n est donc : $\left[\frac{(2n)!}{k!(2n-k)!} \right] \times (k-1)! \times (2n-k)! = \frac{(2n)!}{k}$. Il s'ensuit que la probabilité de tomber sur une permutation ayant un cycle d'ordre k est $1/k$.

Par conséquent, la probabilité qu'il n'y ait aucun cycle d'ordre k supérieur à n est $1 - \left[\frac{1}{n+1} + \frac{1}{n+2} + \dots + \frac{1}{2n} \right] = 1 - H(2n) + H(n)$, où $H(i) = 1 + \frac{1}{2} + \dots + \frac{1}{i}$. On sait que $H(i)$ vaut à peu de chose près $\ln(i)$. La probabilité recherchée vaut donc approximativement $1 - \ln(2n) + \ln(n) = 1 - \ln(2) = 0,306852...$

Démonstration d'optimalité

La magnifique démonstration qui suit est due à Eugene Curtin et Max Warshauer.

Elle prouve qu'il est impossible de faire mieux que la stratégie *Suivre*. Nous

considérons une variante du jeu où les prisonniers procèdent comme pour le jeu initial, mais s'arrêtent d'ouvrir des boîtes quand ils ont trouvé leur numéro (cela ne les désavantage pas), et, surtout, ne referment pas les boîtes ouvertes.

Le prisonnier p bénéficie donc des informations données par les boîtes ouvertes par les prisonniers $1, 2, \dots, p-1$. Cette variante rend le jeu plus facile, et donc la meilleure stratégie de jeu pour cette variante conduira à une probabilité de gagner supérieure ou égale à celle de la meilleure façon de jouer pour le jeu initial.

Jouer à cette variante équivaut à ne considérer qu'un prisonnier qui ouvre les $2n$ boîtes dans un certain ordre et qui s'arrête une première fois au bout de a_1 boîtes quand il a trouvé la boîte contenant le carton 1, puis une seconde fois après avoir ouvert a_2 boîtes quand il a trouvé le carton 2, etc. Le prisonnier a gagné si aucun des nombres a_i n'est supérieur à n .

Comme les contenus des boîtes ont été choisis au hasard par les gardiens, l'ordre d'ouverture qu'utilise le prisonnier de la variante est sans importance : toutes les façons d'ouvrir les boîtes donnent la même probabilité générale de gagner. On peut donc supposer que le prisonnier de la variante ouvre simplement les boîtes dans l'ordre où elles se présentent sur la table. Calculer sa probabilité de gagner sous cette hypothèse donnera la probabilité la meilleure de gagner pour la variante.

Prenons le cas $n=3$, $2n=6$. Les boîtes contiennent les cartons 6-1-2-4-3-5, dans cet ordre. Le prisonnier ouvre d'abord les boîtes contenant le 6 et le 1 (il cherche le 1). Donc $a_1=2$. Puis la boîte contenant le 2 (il cherche le 2) : $a_2=1$. Puis les boîtes contenant le 4 et le 3 (il cherche le 3) : $a_3=2$. Pour le 4, il n'ouvre aucune nouvelle boîte, puisque le carton 4 est déjà trouvé : $a_4=0$. Il ouvre ensuite les boîtes contenant le 5 (il cherche le 5) : $a_5=1$. Pour le 6, il n'ouvre aucune boîte nouvelle : $a_6=0$. Le prisonnier gagne, car à aucun moment il n'a eu plus de

3 boîtes à ouvrir pour trouver le carton suivant (chaque a_i est inférieur à 3).

Nous noterons $[6, 1][2][4, 3][5]$ cette séquence d'ouverture des boîtes. Une séquence de jeu perdante serait par exemple $[1][3, 4, 5, 2][6]$: la deuxième recherche oblige le joueur à ouvrir 4 boîtes.

La notation adoptée pour représenter les séquences possibles pourrait être utilisée pour représenter la décomposition en cycles d'une permutation. La séquence $[6, 1][2][4, 3][5]$ représenterait ainsi la permutation qui envoie 1 sur 6 et 6 sur 1, envoie 2 sur 2, envoie 4 sur 3 et 3 sur 4, et envoie 5 sur 5 (cette notation est la « forme canonique » de la permutation, voir <https://fr.wikipedia.org/wiki/Permutation>).

À chaque séquence de jeu de la variante correspond exactement une permutation en forme canonique et réciproquement. Il y a donc exactement autant de séquences de jeux gagnantes que de permutations dépourvues de cycles d'ordre strictement supérieur à n , c'est-à-dire $1 - H(2n) + H(n)$, où $H(i) = 1 + \frac{1}{2} + \dots + \frac{1}{i}$ (voir le calcul effectué dans le texte ci contre). La meilleure façon de jouer à la variante du jeu, plus facile que le jeu initial, gagne donc avec une probabilité égale à celle de gagner pour les prisonniers du jeu initial appliquant la stratégie *Suivre*. La meilleure façon de jouer au jeu initial ne peut donc pas dépasser ce nombre. La stratégie *Suivre* obtient ainsi une probabilité de succès impossible à améliorer.

