Énigmes

Énigme 1. (des 100 prisonniers)

Cent prisonniers (sur une péniche), identifiés par un (unique) nombre entre 1 et 100, ont été condamnés à mort par le cruel Docteur No, qui leur offre cependant une dernière chance. Dans la timonerie, se trouvent 100 tiroirs (numérotés de 1 à 100), où il a aléatoirement mis les 100 numéros des prisonniers. Après concertation, ces derniers ont le droit d'entrer l'un après l'autre et de regarder le contenu de 50 tiroirs (qu'ils referment après leur passage). Ils auront, collectivement, la vie sauve si chacun d'entre eux trouve son numéro dans un tiroir. Malheureusement, ils ne peuvent pas communiquer entre eux et si l'un d'eux échoue, ils seront tous exécutés.

Un mathématicien, pessimiste, se trouve parmi les prisonniers. Selon lui, la probabilité de succès est de $2^{-100} \approx 8 \cdot 10^{-31}$.

Une mathématicienne, prisonnière mais aussi combinatoricienne, prétend qu'il existe une stratégie garantissant au moins 30% de chance de survie.

Qui a raison ?

Solution. La mathématicienne, dont voici la stratégie. Chaque prisonnier commence par ouvrir le tiroir correspondant à son numéro. Si son numéro n'y est pas, il ouvre le tiroir correspondant au numéro qui s'y trouve, etc., en espérant retourner à son tiroir de départ en moins de 50 essais.

En appliquant cette stratégie, les prisonniers auront la vie sauve si la permutation initiale, $\sigma : i \mapsto$ numéro dans tiroir i, choisie par le Docteur No a tous ses cycles de longueur au plus 50.

Pour $k > 50$, la probabilité que le plus long cycle soit de longueur exactement k vaut $1/k$. Par exemple parce que pour choisir une telle permutation, on a $\binom{n}{k}$ choix pour les éléments de ce long cycle, $(k-1)!$ façons de choisir l'ordre cyclique sur ces éléments, et $(n-k)!$ façons de choisir une permutation arbitraire des $n-k$ autres éléments).

La probabilité d'échec vaut donc la somme

$$\sum_{k=51}^{100} \frac{1}{k} \approx 1 - 0,3118278206.$$

Plus généralement avec $2n$ prisonniers on obtient environ $\log(2n) - \log(n) = \log(2) \approx 0,69$.

Pour une présentation plus formelle, voir par exemple l'excellent livre de Flajolet et Sedgewick qui montre que la probabilité cherchée est

$$[z^{100}] \exp\left(\frac{z}{1} + \frac{z^2}{2} + \cdots + \frac{z^{50}}{50}\right) = 1 - \sum_{k=51}^{100} \frac{1}{k} \approx 0,3118278206.$$

Pour une historique et une discussion plus complète du problème, cf. wikipédia : 100 prisoners problem

Énigme 2. (jeu de Penney)

Amaia et Beñat veulent déterminer qui fera la vaisselle après une fête. Pour faire durer le suspens, Beñat propose de lancer autant de fois que nécessaire une pièce : si le motif « FPP » [face-pile-pile] sort avant le motif, de même longueur, choisi par Amaia, il gagne. (Et ils cessent d'exécuter les lancers.)

Selon lui, tous les motifs de longueur 3 étant équiprobables, le choix de Amaia est sans importance et chacun a exactement une chance sur deux de faire la vaisselle.

Pourtant, Amaia pense qu'elle peut trouver un motif lui assurant 2 chances sur 3 de gagner.

Qui a raison ?

Solution. Admettons qu'Amaia choisisse FFP, et soit $A(x)$ la série entière $\sum_n a_n x^n$ où a_n est le nombre de motifs de longueur n la faisant gagner. En d'autres termes, on évalue la série non commutative

$$\mathsf{FFP} + \mathsf{FFFP} + \mathsf{PFFP} + \mathsf{FFFFP} + \mathsf{FPFFP} + \mathsf{PFFFP} + \cdots$$

en $\mathsf{F} = \mathsf{P} = x$, et la probabilité qu'elle gagne au n-ième lancer (resp. à un moment quelconque) est donc $a_n/2^n$ (resp. $A(\frac{1}{2})$). De même, on peut définir la série $B(x)$ correspondant à

$$\mathsf{FPP} + \mathsf{PFPP} + \mathsf{FPFPP} + \mathsf{PPFPP} + \mathsf{PFPFPP} + \mathsf{PPPFPP} + \cdots$$

et enfin $Z(x)$ la série correspondant aux lancers/mots sans FFP ni FPP pour lesquels personne ne gagne. (On compte le mot vide de longueur 0 de sorte que $Z(x) = 1 + \cdots$.)

Il n'est pas difficile d'établir les relations suivantes : (a) $1 + Z \cdot 2x = Z + A + B$ — si l'on ajoute à un mot de type Z un F ou un P à droite, on obtient un mot type Z, A ou B et c'est une bijection, si ce n'est qu'il manque le mot vide — (b) $Z \cdot x^3 = A$ — un mot de A est obtenu en ajoutant FFP à un mot de Z —, et enfin (c) $Z \cdot x^3 = Ax + B$ — si l'on ajoute FPP à un mot de Z, on obtient un mot de type AP, si celui de Z se termine par F, ou bien un mot de type B, si celui de Z se termine par P —. En évaluant en $x = \frac{1}{2}$, on trouve, avec les deux dernières relations,

$$A(\tfrac{1}{2}) = \tfrac{1}{2}A(\tfrac{1}{2}) + B(\tfrac{1}{2}),$$

d'où

$$A(\tfrac{1}{2}) = 2B(\tfrac{1}{2}).$$

(On a aussi $A(\frac{1}{2}) + B(\frac{1}{2}) = 1$, d'où $A(\frac{1}{2}) = \frac{2}{3}$.)

On trouve $1 + 2xZ = Z(1 + x^3 + x^3(1 - x))$ d'où, en factorisant, que a_n est le coefficient de z^n dans la série $\frac{z^3}{(1-z)^3(1+z)}$. Comme

$$\frac{1}{(1-z)^3(1+z)} = \frac{\frac{1}{8}}{1+z} + \frac{\frac{7}{8} - \frac{1}{2}z + \frac{1}{8}z^2}{(1-z)^3},$$

et que $[z^n]\frac{1}{(1-z)^3} = \frac{1}{2}(n+1)(n+2)$, on trouve que

$$[z^{n+1}]\frac{z^3}{(1-z)^3(1+z)} = \tfrac{1}{4}n^2 - \tfrac{1}{8}(1 - (-1)^n) = \text{entier le plus proche de } n^2/4.$$

La probabilité demandée est donc équivalente à $n^2/2^{n+2}$. (On trouve bien $\frac{1}{8}$ pour $n = 3$ et $n = 4$.)

On peut montrer que, quelque soit le choix de Beñat, Amaia a toujours une probabilité de gagner $> \frac{1}{2}$ et on peut déterminer un choix optimal : voir la section 5.1 du survol Enumeration of strings d'Odlyzko.

Énigme 3. Le cruel Docteur No a capturé deux mathématiciens, que nous appellerons Alice et Bob. Après avoir permis à ceux-ci de se concerter sur leur stratégie, il va les soumettre à son épreuve dont il leur communique les termes : chacun des deux pourra observer une suite binaire infinie aléatoire uniformément distribuée (c'est-à-dire une suite de 0 et 1 dont chaque terme vaut 0 ou 1 avec probabilité $\frac{1}{2}$, indépendamment les uns des autres ; on peut imaginer une suite de résultats de tirages de pile ou face), les deux suites (celle qu'Alice observe et celle que Bob observe) étant indépendantes. Pour fixer les idées, mettons que les termes de chaque suite sont numérotés par les entiers naturels $(0, 1, 2, 3, \ldots)$: appelons (A_n) la suite observée par Alice et (B_n) la suite observée par Bob. Alice et Bob ne peuvent pas communiquer entre eux (une fois finie la concertation initiale sur leur stratégie commune, mais celle-ci est antérieure à l'observation des suites). Alice, après avoir observé sa suite choisit un entier naturel a qui sera le numéro d'un terme dans la suite de Bob ; de même, Bob, après avoir observé sa suite, choisit un entier naturel b qui sera le numéro d'un terme dans la suite d'Alice. Alice et Bob gagnent (un gentil petit cadeau de la part du Docteur No) si chacun a choisi un terme valant 1 dans la suite de l'autre, c'est-à-dire, si la valeur A_b du terme de la suite d'Alice numéroté par l'entier b choisi par Bob et la valeur B_a du terme de la suite de Bob numéroté par l'entier a choisi par Alice valent tous les deux 1.

Quelle stratégie Alice et Bob peuvent-ils employer pour maximiser leur chance de gain ?

Solution. [1]

Raisonnement incorrect : Alice et Bob ne peuvent pas communiquer, n'ont aucune information sur la suite de l'autre, et leurs deux suites sont indépendantes, donc il est impossible que l'observation de sa propre suite puisse aider Alice à faire quoi que ce soit d'utile sur la suite de Bob. Donc il n'y a rien de mieux à faire que de choisir des a et b constants (dont la valeur n'a pas d'importance).

Et pourtant, c'est faux ‼

Il n'est pas très compliqué de faire mieux que $1/4$. Voici une stratégie simple — sauf erreur due à Guillaume Aubrun — qui donne une probabilité $1/3$ de succès à Alice et Bob : Alice choisit pour a l'indice du premier 1 dans sa propre suite, et Bob choisit de même pour b l'indice du premier 1 dans la sienne. La probabilité d'avoir $a = b$ est la somme de $1/4$ (probabilité d'avoir $a = b = 0$) plus $1/4^2$ (probabilité d'avoir $a = b = 1$) plus $1/4^3$ (probabilité d'avoir $a = b = 2$), etc., c'est-à-dire la somme des $1/4^k$, qui vaut $1/3$; et lorsque c'est le cas, par construction, $A_b = B_a = 1$; par ailleurs, si $a \neq b$, alors Alice et Bob perdent (par exemple, si $a < b$, on a $B_a = 0$ puisque b est l'indice du premier 1 dans la suite B). Donc la probabilité de succès de cette stratégie est exactement $1/3$.

Cette stratégie n'est *pas* optimale : on peut obtenir $7/20$ (c'est-à-dire 35%), mais — bien que cela soit conjecturé — on ne sait pas si c'est optimum. (Voir l'article 1407.4711 sur arXiv.)

Par contre, comme l'a observé Édouard Maurel-Segala (cf. discussion « guessing-each-others-coins » sur MO, on peut montrer que la probabilité optimale de succès est majorée par $\frac{3}{8}$. Si on note a l'entier choisi par Alice et a' l'entier qu'elle choisirait avec la même stratégie si elle observait la suite $(1 - A_n)$ au lieu de (A_n) (i.e., si on échange les 0 et 1 dans ce qu'Alice observe), et de même b et b' pour Bob, alors on peut remarquer que l'espérance $\mathbb{E}(A_b\, B_a)$ de $A_b\, B_a$ (qui est la probabilité de succès p qu'on cherche à maximiser) est aussi égale à l'espérance de $(1-A_{b'})\, B_a$ (puisque $1-A$ est une variable distribuée comme A et toujours indépendante de B) ou de $A_b\,(1-B_{a'})$ ou encore de $(1-A_{b'})\,(1-B_{a'})$. La somme de ces quatre espérances (qui est $4p$) est donc l'espérance de $(A_b + 1 - A_{b'})\,(B_a + 1 - B_{a'})$, soit

$$4p \leq \mathbb{E}((A_b + 1 - A_{b'})\,(B_a + 1 - B_{a'})) = 1 + \mathbb{E}(A_b - A_{b'}) + \mathbb{E}(B_a - B_{a'}) + \mathbb{E}((A_b - A_{b'})\,(B_a - B_{a'}))$$

soit encore $1 + \mathbb{E}((A_b - A_{b'})\,(B_a - B_{a'}))$ puisque $\mathbb{E}(A_b) = \mathbb{E}(A_{b'})$ et $\mathbb{E}(B_a) = \mathbb{E}(B_{a'})$ (en fait, chacune de ces quatre espérances vaut $\frac{1}{2}$). Enfin, comme $A_b - A_{b'}$ vaut ± 1, l'espérance $\mathbb{E}((A_b - A_{b'})\,(B_a - B_{a'}))$ est majorée par $\mathbb{E}(|B_a - B_{a'}|)$, elle-même majorée par $\frac{1}{2}$ (si $i \neq j$ alors $\mathbb{E}(|B_i - B_j|) = \frac{1}{2}$). Au final, on a prouvé $4p \leq 1 + \frac{1}{2}$, soit $p \leq 3/8$ comme annoncé.

[1] J'ai appris ce problème de David Madore, dont j'ai repris la formulation et la discussion.

Énigme 4. (connaissance commune)

Lors d'une fête rassemblant 100 personnes sur une péniche, ces dernières peuvent notamment tremper des bâtons de carottes dans un pot de mayonnaise. Certaines d'entre elles, trente en l'occurrence (mais personne ne le sait), s'en mettent sur le bout du nez mais (1) personne n'ose leur dire (2) elles ne peuvent le voir (pas de miroir) (3) elles préfèrent s'abstenir, dans le doute, de s'essuyer le nez.

Toute personne sachant avoir de la mayonnaise sur le nez irait, (exactement) une minute plus tard — pour ne pas donner l'impression d'agir précipitamment —, aux toilettes de la péniche.

L'organisatrice de cette fête, qui arrive à l'heure du dessert, commence un petit discours en plaisantant sur le fait qu'elle observe certains collègues ayant de la mayonnaise sur le visage.

Quelle conséquence cela a-t-il ?

On fait l'hypothèse que les 100 *fêtards sont parfaitement logiques, savent que leurs collègues le sont, savent que leurs collègues savent que...*

Solution. (Pour une formulation plus précise du problème, voir le blog de Tao (blue-eyed islanders).)

Au bout d'exactement 30 minutes, les 30 maladroits se dirigent vers les toilettes. Commencer par comprendre les cas où seules une ou deux personnes ont de la mayonnaise puis procéder par récurrence. On trouve des discussions détaillées sur internet, par exemple dans le blog de Robert Heaton, ainsi que dans un recueil de quelques énigmes de Peter Winkler. Pour une démonstration rigoureuse, voir une autre entrée du blog de Tao : epistemic-logic...-puzzle-lower-bound.

Pour une discussion plus générale de questions de « connaissances communes », voir par exemple la page wikipédia (Common knowledge) ou celle, sur le même sujet, de la Stanford Encyclopedia of Philosophy (§1.2).

Énigme 5. (axiome du choix)

Un méchant rassemble une infinité dénombrable de nains en file indienne. Ils sont indexés par $\mathbb{N}$. Le nain 0 voit tous les dos des nains $1, 2, \ldots$; le nain 1 voit les dos de $2, 3, \ldots$, etc.

Il accroche sur le dos de chacun un nombre *réel* et demande ensuite à chaque nain de deviner le nombre réel qui est écrit sur son propre dos (qu'il ne voit pas).

Les nains gagnent si seulement un nombre fini d'entre eux se trompe. (Sinon, puisqu'il est méchant, il les tue tous.)

Ils ont le droit de se concerter avant l'affichage des nombres, mais pas après et communiquent tous leur réponse en même temps au méchant.

(On suppose que les nains ont une mémoire infinie, la capacité de lire instantanément tous les nombres réels devant eux, etc. : il s'agit de mathématique et on idéalise le problème…)

Solution. [2] On pose sur l'ensemble des suites la relation d'équivalence être égales à partir d'un certain rang. Les nains retiennent pour chaque classe d'équivalence un représentant.

Chaque nain (numéro n) voit la fin de la suite qui aura été choisie par le méchant. Il se souvient du représentant de sa classe d'équivalence (noté u) et donne comme réponse la valeur de u_n. Comme u est dans la classe d'équivalence de la suite choisie par le méchant, il n'y a qu'un nombre fini d'erreurs.

[2] Ce problème m'a été communiqué par Saïd Ladjal.