100-prisonniers

GUETTEVILLE Nathan, LACENNE Yanis et SOAN Tony Ly

G4S12

27/11/2023

Table des matières

1 Introduction

Le problème des 100 prisonniers [1] se présente comme suit : le directeur d'une prison décide d'offrir une chance d'être libéré à 100 prisonniers condamnés à mort sous la forme d'une épreuve. Chacun d'eux porte un uniforme numéroté de 1 à 100, et dans 100 boîtes distinctes numérotées de 1 à 100 fermées, chacune contient un papier avec le numéro d'un prisonnier correspondant écrit dessus. Les papiers sont répartis aléatoirement dans les boîtes et elles sont placées dans une salle isolée.

Les prisonniers doivent y entrer tour à tour et seuls. Après le passage de chaque prisonnier, la salle est remise dans le même état qu'elle était initialement.

Lors du passage dans cette salle, chacun d'eux à le droit d'ouvrir et de regarder dans 50 boîtes au plus,

— si durant son tour un prisonnier parvient à trouver son propre numéro dans une boite, il peut alors quitter la salle.

— s'il ne parvient pas à trouver son propre numéro, alors tous les prisonniers sont exécutés.

Les prisonniers ne peuvent pas communiquer entre eux durant l'épreuve, mais il peuvent établir une stratégie avant qu'elle ne commence.

Ce problème présenté [2] par Derek Muller (alias Veritasium) est une version modifiée du problème initial [3] formulé par Peter Bro Miltersen , et de la version [4] de Philippe Flajolet et Robert Sedgewick.

2 Lien avec les mathématiques discrètes

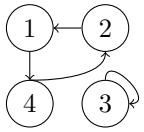
2.1 Permutations

> En mathématiques, la notion de permutation exprime l'idée de réarrangement d'objets discernables. Une permutation d'objets distincts rangés dans un certain ordre correspond à un changement de l'ordre de succession de ces objets.

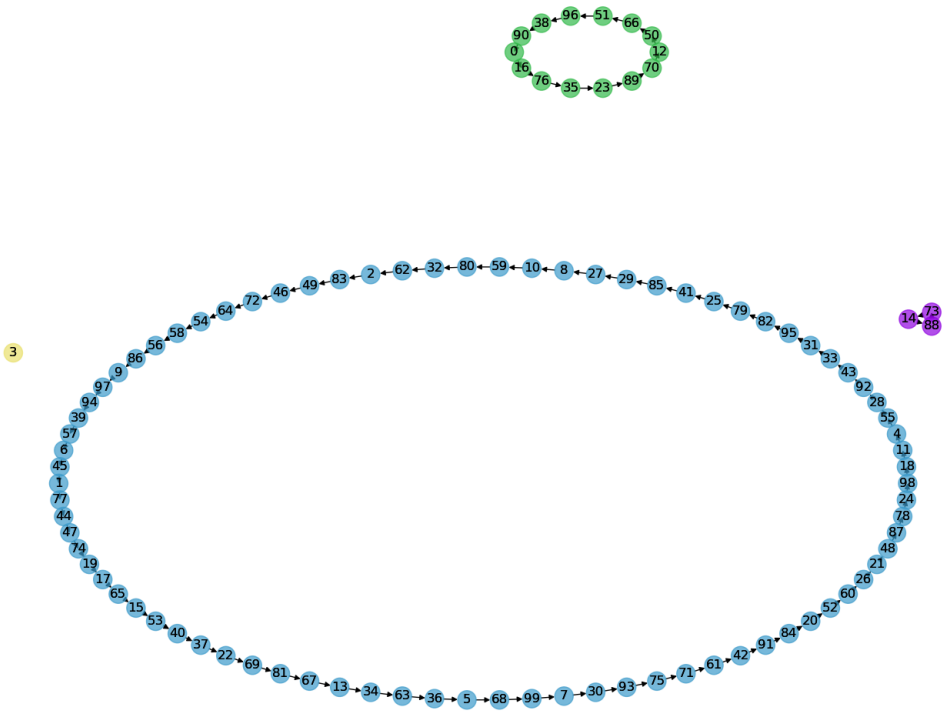
On rappelle de fait qu'il existe $n!$ moyens d'ordonner n éléments distincts. Considérons la permutation suivante qui envoie 1 vers 4, 2 vers 1, 3 vers lui-même et 4 vers 2.

$$\begin{aligned} 1 &\longrightarrow 4 \\ 2 &\longrightarrow 1 \\ 3 &\longrightarrow 3 \\ 4 &\longrightarrow 2 \end{aligned}$$

Il est tout à fait possible de représenter une permutation sous forme de graphe.



En voici un exemple plus poussé contenant 100 noeuds.



2.2 Cycles d'une permutation

On souhaite maintenant considérer les cycles contenus dans les permutations. En continuant avec notre exemple, on remarque que notre permutation contient 2 cycles. Un cycle de longueur 3 ($1 \to 4 \to 2 \to 1$) et un de longueur 1 ($3 \to 3$). Sauf que, nous pouvons également remarquer que le cycle ($1 \to 4 \to 2 \to 1$) est le même que ($4 \to 2 \to 1 \to 4$) et ($2 \to 1 \to 4 \to 2$).
Il y a $3! = 6$ manières d'écrire une permutation de 3 éléments. Toutefois, on vient de dire qu'un cycle de 3 éléments pouvait s'écrire de 3 façons différentes ; alors parmi ces 6 permutations, il n'existe que $\frac{6}{3} = 2$ cycles distincts.

$$A \to B \to C \to A \qquad A \to C \to B \to A$$
$$B \to C \to A \to B \qquad C \to B \to A \to C$$
$$C \to A \to B \to C \qquad B \to A \to C \to B$$

On peut le généraliser pour n en disant qu'il y a $\frac{n!}{n} = (n-1)!$ façons d'écrire un cycle de n éléments.

On cherche maintenant à obtenir la quantité de permutations de n contenant un cycle de longueur $0 < k \leq n$. Il y en a $\frac{n!}{k}$.

$$\binom{n}{k} * (k-1)! * (n-k)! = \frac{n!}{k! * (n-k)!} * (k-1)! * (n-k)!$$
$$= \frac{n! * (k-1)! * (n-k)!}{k * (k-1)! * (n-k)!}$$
$$= \frac{n!}{k}$$

Avec
— $\binom{n}{k}$: les éléments formant le cycle
— $(k-1)!$: le nombre de permutations des éléments formant le cycle
— $(n-k)!$: le nombre de permutations des éléments restants

3 Probabilités

3.1 Problématique

Quelle est la probabilité que les prisonniers survivent ? D'un premier instinct, si chaque prisonnier peut ouvrir la moitié des boîtes, alors la probabilité qu'un prisonnier trouve son numéro parmi les boîtes qu'il a ouvert est de $\frac{1}{2}$. Donc la probabilité que tous trouvent leur numéro respectif est de

$$\left(\frac{1}{2}\right)^{100} \approx 0.789 * 10^{-30}$$

Y a-t-il une méthode qui permettrait de considérablement augmenter ces chances ?

3.2 Probabilités de cycles

Nous avons vu dans la section précédente que le nombre de permutations de n éléments contenant un cycle de longueur $0 < k \leq n$ est de $\frac{n!}{k}$. À partir de cette information, nous sommes maintenant en mesure de calculer la probabilité d'obtenir un cycle de longueur $\frac{n}{2} < k \leq n$ dans une permutation de n éléments. Nous ne parlerons pas ici de la probabilité qu'il y ait un cycle de longueur k lorsque $0 < k \leq \frac{n}{2}$.

Soient les événements aléatoires

E_k : "Une permutation de n éléments contient un cycle de longueur k."
E'_k : "Une permutation de n éléments contient un cycle de longueur au moins k."

Muni de la loi uniforme discrète, on sait que $P(X \in B) = \frac{\#(A \cap B)}{\#A}$, de fait :

$$P(E_k) = \frac{\frac{n!}{k}}{n!} = \frac{1}{k} \tag{1}$$

À partir de $P(E_k)$, on peut désormais aisément calculer $P(E'_k)$:

$$P(E'_k) = \sum_{i=k}^{n} P(E_i) = \sum_{i=k}^{n} \frac{1}{i} \tag{2}$$

On reconnaît ici une forme de série harmonique. En prenant $k = \frac{n}{2}$, on obtient

$$P(E'_{\frac{n}{2}}) = \frac{1}{\frac{n}{2}} + \ldots + \frac{1}{n-1} + \frac{1}{n} \tag{3}$$

Il est possible de développer en utilisant la série Harmonique.

$$\begin{aligned} P(E'_{\frac{n}{2}}) &= H(n) - H(\lfloor \frac{n}{2} \rfloor) \\ &\approx \ln n - \ln \frac{n}{2} \\ &\approx \ln \frac{n}{\frac{n}{2}} = \ln 2 \\ &\approx 0.693147181 \end{aligned}$$

En conclusion, il y a environ 70% de chances qu'une permutation de n éléments contiennent un cycle d'au moins $\frac{n}{2}$.

3.3 Interpretation

Nous savons que les prisonniers ne peuvent s'en sortir que si le cycle maximal est de $\frac{n}{2}$. Ce qui leur laisse environ 30% de chance de survie.

4 Baby-Step Giant-Step

La méthode utilisée pour la recherche de cycles dans l'énigme des 100 prisonniers peut être appliquée dans le domaine de la cryptographie.

> Un groupe G est cyclique s'il existe $x \in G$ tel que tout élément de G est un multiple de x. On dit alors que x est un générateur de G

Algorithm 1: Algorithme Baby-Step Giant-Step

Entrée: g un groupe cyclique, α générateur de g, β élément de g
Sortie : une valeur x telle que $g^x \equiv \alpha \pmod{\beta}$

1. Calculer $m = \sqrt{\beta} + 1$.
2. Baby-Step :
   pour $i = 0$ à $m - 1$: stocker à l'indice i d'une liste $babyStep$: α^i
3. Soit $\gamma = \beta$
4. Giant-Step : pour $i = 0$ à $m - 1$: si γ est égal à $babyStep[i]$
   alors retourner $i \cdot m + j$
   sinon $\gamma = \gamma \cdot \alpha^{-m}$

Cet algorithme permet de trouver le logarithme discret d'un groupe cyclique G, c'est-à-dire le plus petit entier naturel k tel que $x = b^k$ avec b générateur de G et x élément quelconque de G.

Couplé à l'exponentiation rapide, le logarithme discret sert à la cryptographie à clé publique, la combinaison des deux objets produisant l'asymétrie recherchée dans le contexte de l'échange de clés.

Si on applique le même type de recherche des cycles (cf Annexe) que pour le problème des 100 prisonniers, puis que l'on applique l'algorithme Baby-Step Giant-Step sur les cycles optimaux trouvés, on obtient alors leurs logarithmes discrets respectifs.

5 Conclusion

Nous avons étudié un problème pour lequel la première solution qui nous parvenait était toute sauf optimale. Nous avons vu qu'il est possible d'appliquer des concepts de mathématiques discrètes à des problèmes concrets afin d'en obtenir des solutions plus efficaces. Nous avons également vu qu'une fois appliquée à de simples problèmes, il est possible de généraliser la solution trouvée à une échelle complètement différente, ce qui nous a permis dans notre cas d'utiliser la présence de cycles dans les graphes pour expliquer l'algorithme 'Baby-Step Giant-Step'.

6 Annexe

— Annexe numérique : `https://github.com/YanisLcn/100-prisoners/blob/master/`

7 Références

[1] "100 prisoners problem," *Wikipedia*, Nov. 2023. [Online]. Available : https://en.wikipedia.org/w/index.php?title=100_prisoners_problem&oldid=1183839528

[2] Veritasium, "The Riddle That Seems Impossible Even If You Know The Answer," Jun. 2022. [Online]. Available : https://www.youtube.com/watch?v=iSNsgj1OCLA

[3] P. B. Miltersen and A. Gal, "The Cell Probe Complexity of Succinct Data Structures," *Theoretical Computer Science*, vol. 379, no. 3, pp. 405–417, 2007.

[4] P. Flajolet and R. Sedgewick, *Analytic Combinatorics*. Cambridge ; New York : Cambridge University Press, 2009.