QuiProCo

QUI est-ce, ré**P**onse **R**and**O**misée, **CO**nfidentialité différentielle

Suite au développement d'internet et des outils de stockage d'information, il est aujourd'hui possible d'accumuler de gigantesques masses de données personnelles. Cette accumulation de données est à la fois une chance et un danger. D'une part, la collecte de données permet d'acquérir des informations sur la population et de mener des enquêtes. On peut ainsi traquer l'évolution d'une maladie, mesurer le niveau de pauvreté, optimiser les moyens de transports, etc. D'un autre coté, la collecte et le stockage de ces informations attentent à la vie privée des personnes concernées qui doivent révéler des informations personnelles et parfois sensibles, comme par exemple leur maladie ou leur niveau de richesse.

La confidentialité différentielle permet de rendre possible des enquêtes globales, tout en limitant les informations que l'on peut obtenir d'une personne particulière.

Le but de cette activité, basée sur le jeu *Qui est-ce ?*, est d'illustrer une technique de confidentialité différentielle : la réponse randomisée. Le principe est simple : lorsqu'une question est posée à une personne, cette dernière choisit aléatoirement de mentir ou de dire la vérité. Selon la probabilité de mentir, les résultats globaux de l'enquête seront plus ou moins influencés mais il sera difficile de connaître les réponses d'un individu particulier.

Matériel

- 24 cartes personnages, avec 3 caractéristiques variables
- 1 dé, ou autre source d'aléas
- 4 cartes objectifs globaux
- 4 cartes objectifs personnels

Déroulement de l'activité

Tout d'abord, une personne est désignée dans le groupe et sera « l'enquêteur ». C'est elle qui posera les questions aux autres joueurs, qui seront les « répondants ».

L'enquêteur tire une carte « objectif global » et une carte « objectif personnel ». L'objectif global est correspond au résultat d'une enquête sur l'ensemble des répondants, l'objectif personnel est une information privée que l'enquêteur doit trouver sur un répondant en particulier.

Chaque répondant va ensuite choisir secrètement un nombre dans sa tête et le marquer sur un bout de papier. Il ne dit ni ne montre ce nombre à personne.

L'activité se déroule en deux phases durant lesquels l'enquêteur a droit à un nombre limité de questions (en fonction du temps disponible) pour réaliser ses deux objectifs.

Lors de la première phase, un dé est lancé à chaque question. Si le dé correspond au nombre qu'il a choisi, le répondant ment. Sinon il dit la vérité.

Lors de la deuxième phase, tout le monde dit la vérité.

Objectif pédagogique et complément scientifique

Le but de cette activité est d'illustrer une technique de protection de la vie privée. Normalement l'objectif global devrait être rempli tandis que l'objectif personnel devrait échouer. Il s'agit de sensibiliser au fait qu'il est possible de collecter des données utiles tout en limitant l'impact sur la vie privée.

Réponse randomisée

Le mécanisme de réponse randomisée a été introduit par le sociologue Stanley Warner en 1965 [5] afin de mener des enquêtes sur des sujets sensibles, par exemple estimer la proportion de tricheurs parmi les étudiants [4], ou de recours à l'avortement [1].

Une description de ce mécanisme se résume par la suite d'étapes ci-dessous :

- L'enquêteur pose une question fermée (dont la réponse est oui ou non) au participant
- Le ou la participant.e répond la vérité avec une certaine probabilité p connue de l'enquêteur, et ment sinon (par exemple, il peut jeter un dé, et mentir si le résultat est 1 et dire la vérité sinon ; on aura alors $p = \frac{5}{6}$)
- L'enquêteur récupère la réponse sans savoir si elle est vraie (le ou la participant.e peut toujours nier sa réponse du fait du protocole)
- Avec un nombre suffisant de réponses, des statistiques fiables peuvent quand même être établies

Confidentialité différentielle

La confidentialité différentielle est un formalisme récent de la notion de vie privée, proposé puis complété par Cynthia Dwork depuis 2007 [3, 2]. Cette notion constitue l'état de l'art actuel en matière de confidentialité et de protection de la vie privée.

L'idée générale est que la réponse à une question sur un ensemble d'individus n'est que très faiblement liée à la présence ou à l'absence d'un individu spécifique. En particulier, la réponse randomisée répond à cette définition.

Description du prototype fourni

Cartes personnages

Un jeu de 24 cartes avec 3 caractéristiques

- La couleur du chat (marron, roux, blanche)
- La forme des yeux (petit, allongé, grand)
- Un accessoire (le chapeau, walkman, bandana, noeud papillon)

Objectifs globaux

Quelques objectifs statistiques pouvant être réalisés avec ces personnages

- Quel est le nombre de chats roux écoutant de la musique ?
- Est-ce que les chats blancs ont plus de chance d'avoir des petits yeux que les autres ?
- Y a-t-il plus de chats marrons portant un nœud papillon ou de chats roux avec les yeux allongés ?
- Quelle est la couleur la plus représentée parmi les chats qui portent un bandana ?

Objectifs personnels

Quelques objectifs personnels pouvant être réalisés avec ces personnages

- Quel joueur a le chat roux aux grand yeux et écoutant de la musique ?
- Quel joueur a le chat blanc aux petits yeux et portant un bandana ?
- Choisissez un joueur. Quelles sont les caractéristiques du chat de ce joueur ?
- Identifiez les chats marrons à gros yeux et n'ayant pas de chapeau.

Références

[1] James R Abernathy, Bernard G Greenberg, and Daniel G Horvitz. Estimates of induced abortion in urban north carolina. *Demography*, 7(1) :19–29, 1970.

[2] Cynthia Dwork. Differential privacy. In *33rd International Colloquium on Automata, Languages and Programming, part II (ICALP 2006)*, volume 4052, pages 1–12, Venice, Italy, July 2006. Springer Verlag.

[3] Cynthia Dwork and Aaron Roth. The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, 9 :211–407, 2014.

[4] NJ Scheers and C Mitchell Dayton. Improved estimation of academic cheating behavior using the randomized response technique. *Research in Higher Education*, 26(1) :61–69, 1987.

[5] Stanley L. Warner. Randomized response : A survey technique for eliminating evasive answer bias. *Journal of the American Statistical Association*, 60(309) :63–69, 1965.

Cartes personnages à découper

Images : https ://github.com/NoahDragon/cat-generator-avatars.

Cartes objectifs globaux à découper

Quel est le nombre de chats roux écoutant de la musique ?	Est-ce que les chats blancs ont plus de chance d'avoir des petits yeux que les autres ?
Y a-t-il plus de chats marrons portant un nœud papillon ou de chats roux avec les yeux allongés ?	Quelle est la couleur la plus présente parmi les chats qui portent un bandana ?

Cartes objectifs personnels à découper

Quel joueur a le chat roux aux grand yeux et écoutant de la musique ?	Quel joueur a le chat blanc aux petits yeux et portant un bandana ?
Choisissez un joueur. Quelles sont les caractéristiques du chat de ce joueur ?	Identifiez les chats marrons à gros yeux et n'ayant pas de chapeau.