

Peut-on utiliser le hasard ?

Yann OLLIVIER



CNRS & Laboratoire de recherche en informatique,
Université Paris-Sud



Marathon des sciences
2 août 2014

1 Un peu de théorie : Qu'est-ce qu'un objet aléatoire ?

2 À quoi sert le hasard ? Applications pratiques

- Sondages
- Sécurité des réseaux
- Expériences scientifiques et médicales
- Météo
- Fiabilité des systèmes
- Prise de décision efficace
- ...

Qu'est-ce qu'un objet aléatoire ?

Qu'est-ce qu'un objet aléatoire ?

Un objet aléatoire est un objet qui n'a **aucune propriété spéciale**.

Qu'est-ce qu'un objet aléatoire ?

Un objet aléatoire est un objet qui n'a aucune propriété spéciale.

Exemple : si on tire aux dés

6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6

Qu'est-ce qu'un objet aléatoire ?

Un objet aléatoire est un objet qui n'a **aucune propriété spéciale**.

Exemple : si on tire aux dés

6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 \implies les dés sont pipés...

Qu'est-ce qu'un objet aléatoire ?

Un objet aléatoire est un objet qui n'a **aucune propriété spéciale**.

Exemple : si on tire aux dés

6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 \implies les dés sont pipés...

Si on a tiré

3 – 6 – 5 – 6 – 3 – 3 – 6 – 6 – 5 – 1 – 4

Qu'est-ce qu'un objet aléatoire ?

Un objet aléatoire est un objet qui n'a **aucune propriété spéciale**.

Exemple : si on tire aux dés

6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 \implies les dés sont pipés...

Si on a tiré

3 – 6 – 5 – 6 – 3 – 3 – 6 – 6 – 5 – 1 – 4 \implies rien de spécial.

Qu'est-ce qu'une propriété spéciale ?

Qu'est-ce qu'une propriété spéciale ?

C'est, en simplifiant, une propriété qui permet de retrouver exactement l'objet avec moins de mots.

Exemple :

6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 \implies « Que des six ! »

Qu'est-ce qu'une propriété spéciale ?

C'est, en simplifiant, une propriété qui permet de retrouver exactement l'objet avec moins de mots.

Exemple :

6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 ⇒ « Que des six ! »

3 – 6 – 5 – 6 – 3 – 3 – 6 – 6 – 5 – 1 – 4 ⇒ « ... »

Qu'est-ce qu'une propriété spéciale ?

C'est, en simplifiant, une propriété **qui permet de retrouver exactement l'objet avec moins de mots.**

Exemple :

$6 - 6 - 6 - 6 - 6 - 6 - 6 - 6 - 6 - 6 - 6$ \implies « Que des six ! »

$3 - 6 - 5 - 6 - 3 - 3 - 6 - 6 - 5 - 1 - 4$ \implies « ... »

Les mathématiques et l'informatique théorique permettent de **préciser cette définition** \implies « complexité de Kolmogorov »

Qu'est-ce qu'une propriété spéciale ?

C'est, en simplifiant, une propriété **qui permet de retrouver exactement l'objet avec moins de mots.**

Exemple :

6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 – 6 \implies « Que des six ! »

3 – 6 – 5 – 6 – 3 – 3 – 6 – 6 – 5 – 1 – 4 \implies « ... »

Les mathématiques et l'informatique théorique permettent de **préciser cette définition** \implies « complexité de Kolmogorov »
+ version **quantitative**

Peut-on reconnaître si un objet est aléatoire ?

3 – 6 – 5 – 6 – 3 – 3 – 6 – 6 – 5 – 1 – 4 – 1 – 5 – 1 – 2

⇒ rien de spécial.

Peut-on reconnaître si un objet est aléatoire ?

3 – 6 – 5 – 6 – 3 – 3 – 6 – 6 – 5 – 1 – 4 – 1 – 5 – 1 – 2

⇒ rien de spécial.

Vraiment ?

Peut-on reconnaître si un objet est aléatoire ?

3 – 6 – 5 – 6 – 3 – 3 – 6 – 6 – 5 – 1 – 4 – 1 – 5 – 1 – 2

⇒ rien de spécial.

Vraiment ?

(C'est la suite des décimales de π en base 6...)

Peut-on reconnaître si un objet est aléatoire ?

3 – 6 – 5 – 6 – 3 – 3 – 6 – 6 – 5 – 1 – 4 – 1 – 5 – 1 – 2

⇒ rien de spécial.

Vraiment ?

(C'est la suite des décimales de π en base 6...)

On **ne peut pas** être complètement sûr qu'un objet est aléatoire.

Peut-on reconnaître si un objet est aléatoire ?

3 – 6 – 5 – 6 – 3 – 3 – 6 – 6 – 5 – 1 – 4 – 1 – 5 – 1 – 2

⇒ rien de spécial.

Vraiment ?

(C'est la suite des décimales de π en base 6...)

On **ne peut pas** être complètement sûr qu'un objet est aléatoire.

Mais on **sait reconnaître** les objets **non** aléatoires. (Il suffit de leur trouver une propriété spéciale...)

Peut-on construire des objets aléatoires ?

- On **ne peut pas** construire facilement un objet complètement aléatoire.

Peut-on construire des objets aléatoires ?

- On **ne peut pas** construire facilement un objet complètement aléatoire. (Démonstration par l'absurde : donner une méthode de construction qui ne soit pas aussi compliquée que l'objet serait une propriété très spéciale \implies contradiction.)
- Pourtant,

Peut-on construire des objets aléatoires ?

- On **ne peut pas** construire facilement un objet complètement aléatoire. (Démonstration par l'absurde : donner une méthode de construction qui ne soit pas aussi compliquée que l'objet serait une propriété très spéciale \implies contradiction.)
- Pourtant, **la plupart** des objets sont aléatoires. Par exemple, la plupart des résultats de dés sont aléatoires. Ou encore : la plupart des nombres à virgule ont un développement décimal aléatoire.
- On peut construire des objets **partiellement aléatoires** qui suffisent en pratique.

Construction d'objets aléatoires

- On peut construire des objets **partiellement aléatoires** qui suffisent en pratique.

Deux sources principales :

Construction d'objets aléatoires

- On peut construire des objets **partiellement aléatoires** qui suffisent en pratique.

Deux sources principales :

- Utiliser un **processus physique complexe** (dés, mouvements...)

Construction d'objets aléatoires

- On peut construire des objets **partiellement aléatoires** qui suffisent en pratique.

Deux sources principales :

- Utiliser un **processus physique complexe** (dés, mouvements...)
⇒ mais pas de garantie

Construction d'objets aléatoires

- On peut construire des objets **partiellement aléatoires** qui suffisent en pratique.

Deux sources principales :

- Utiliser un **processus physique complexe** (dés, mouvements...)
 \implies mais pas de garantie
- Utiliser des **générateurs pseudo-aléatoires** : en enchaînant des calculs compliqués.

Construction d'objets aléatoires

- On peut construire des objets **partiellement aléatoires** qui suffisent en pratique.

Deux sources principales :

- Utiliser un **processus physique complexe** (dés, mouvements...) \implies mais pas de garantie
- Utiliser des **générateurs pseudo-aléatoires** : en enchaînant des calculs compliqués. \implies Garantis **partiellement** aléatoires.

À quoi sert le hasard ?

Un **hasard contrôlé** introduit volontairement peut aider à résoudre certains problèmes

À quoi sert le hasard ?

Un **hasard contrôlé** introduit volontairement peut aider à résoudre certains problèmes et même **éliminer d'autres sources d'incertitude**.

À quoi sert le hasard ?

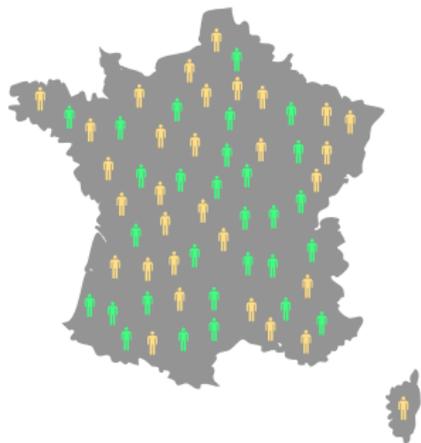
Un **hasard contrôlé** introduit volontairement peut aider à résoudre certains problèmes et même **éliminer d'autres sources d'incertitude**.

En présence de grands nombres, le hasard peut être la méthode la plus **juste et équilibrée**.

Statistiques : hasard et sondages

Sondage : parler de quelque chose en n'en ayant vu qu'une **infime partie**.

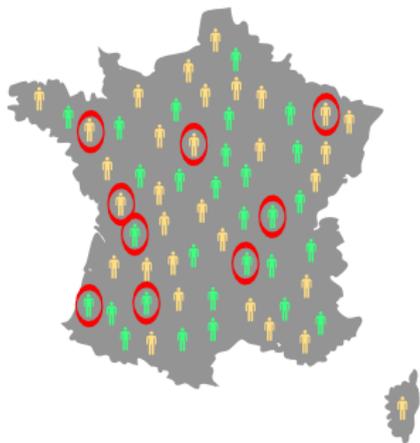
Méthode efficace : prendre un échantillon **au hasard**.



Statistiques : hasard et sondages

Sondage : parler de quelque chose en n'en ayant vu qu'une **infime partie**.

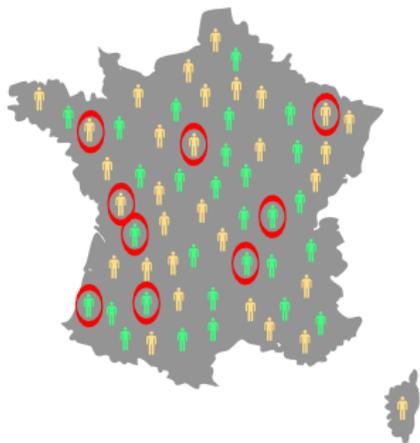
Méthode efficace : prendre un échantillon **au hasard**.



Statistiques : hasard et sondages

Sondage : parler de quelque chose en n'en ayant vu qu'une **infime partie**.

Méthode efficace : prendre un échantillon **au hasard**.



⇒ Le hasard est **introduit par le statisticien**.

Statistiques : expériences « randomisées »

Application la plus importante du hasard : expériences randomisées.

La **randomisation** (assignation aléatoire) élimine beaucoup de biais et de corrélations cachées.

Hasard et structures optimales

Le hasard est parfois la **meilleure méthode** pour construire des objets ayant de **bonnes propriétés de robustesse**.

Exemples : réseaux de communication, cryptographie et sécurité.

Hasard et structures optimales

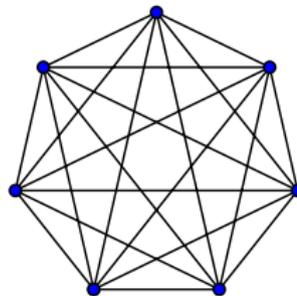
Le hasard est parfois la **meilleure méthode** pour construire des objets ayant de **bonnes propriétés de robustesse**.

Exemples : réseaux de communication, cryptographie et sécurité.

Réseau facile à casser



Réseau difficile à casser



Hasard et fiabilité

Introduction de hasard : permet de tester comment un système ou une prévision résiste à des **imprévus** ou à de **petites variations**.

Hasard et fiabilité

Introduction de hasard : permet de tester comment un système ou une prévision résiste à des **imprévus** ou à de **petites variations**.

Presque toutes les **simulations** utilisent du hasard à certains endroits pour imiter des situations difficiles.

Hasard et fiabilité

Introduction de hasard : permet de tester comment un système ou une prévision résiste à des **imprévus** ou à de **petites variations**.

Presque toutes les **simulations** utilisent du hasard à certains endroits pour imiter des situations difficiles.

Météo : introduire un peu de hasard est indispensable pour évaluer la **fiabilité de la prévision**

Hasard et fiabilité

Introduction de hasard : permet de tester comment un système ou une prévision résiste à des **imprévus** ou à de **petites variations**.

Presque toutes les **simulations** utilisent du hasard à certains endroits pour imiter des situations difficiles.

Météo : introduire un peu de hasard est indispensable pour évaluer la **fiabilité de la prévision** (probabilité de pluie...)

Hasard et décisions

Sur des **grands nombres**, le hasard peut être la méthode la plus juste.

Même sur des petits nombres, pour des **décisions peu importantes**, le hasard peut être la méthode la plus efficace.

Hasard et décisions

Sur des **grands nombres**, le hasard peut être la méthode la plus juste.

Même sur des petits nombres, pour des **décisions peu importantes**, le hasard peut être la méthode la plus efficace.

⇒ **Hasard indispensable** dans des situations bloquées (âne de Buridan...)