SUJET + CORRIGÉ

OLYMPIADES DE MATHÉMATIQUES

ACADÉMIE DE BESANÇON

Classes de première S • 2018

Olympiades académiques de mathématiques

Exercices proposés par l'académie de Besançon

Mercredi 14 mars 2018

Les objets calculatrices sont autorisés, à l'exclusion de tout autre appareil électronique.

Il est conseillé aux candidats qui ne pourraient formuler une réponse complète à une question d'exposer le bilan des initiatives qu'ils ont pu prendre. Il est également important pour les candidats de bien argumenter leurs affirmations.

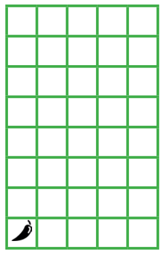
Le sujet comprend trois pages.
Les candidats traiteront les exercices 1 (Un jeu à croquer) et 2 (Clés binaires) communs à toutes les séries. Ces exercices sont indépendants.

La durée de composition est de deux heures.

Sauf cas de force majeure, aucun candidat n'est autorisé à quitter définitivement la salle de composition moins d'une heure après le début de l'épreuve. Un candidat qui quitterait la salle au bout d'une heure ou moins doit rendre sa copie et son exemplaire du sujet.

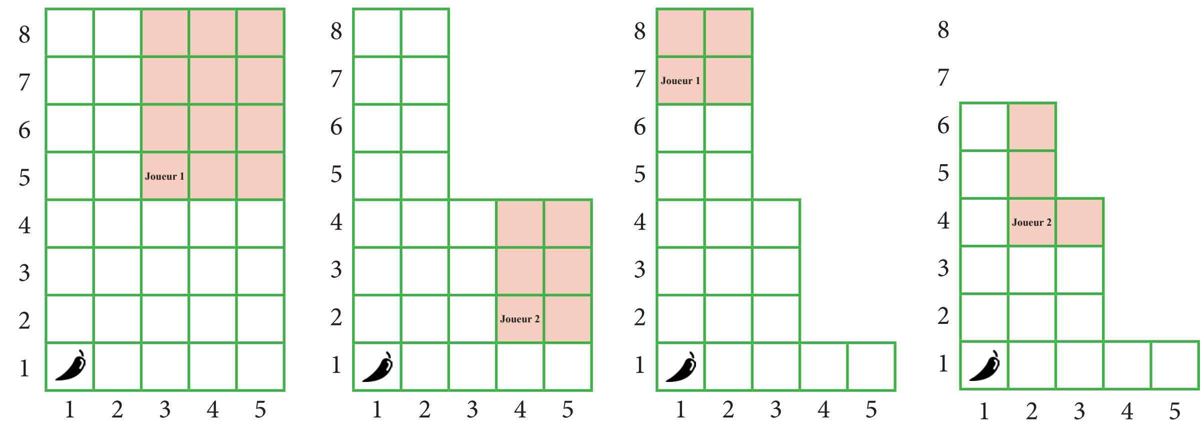
Pour les candidats composant individuellement, ils indiqueront, dans l'en-tête de leur copie, leur numéro d'anonymat figurant sur leur convocation, leur filière et l'établissement dans lequel ils sont inscrits.
Pour les candidats composant en groupe, chacun des membres du groupe indiquera dans l'en-tête de la copie son numéro d'anonymat figurant sur sa convocation, sa filière et l'établissement dans lequel il est inscrit.

Exercice 1 Un jeu à croquer



Deux personnes disposent d'une tablette de chocolat rectangulaire, divisée en carrés, dont le carré en bas à gauche contient du piment très fort. Ils se lancent un défi et décident de croquer dans la tablette de chocolat chacun leur tour selon la règle suivante : à chaque tour, un joueur choisit l'un des carrés et le mange, ainsi que tous les carrés situés au dessus et à droite de ce carré. Ils n'ont bien sûr pas le droit de faire semblant de croquer. Le joueur qui se retrouve obligé de manger le carré pimenté perd la partie.

On donne ci-dessous le déroulement des quatre premières étapes du défi avec une tablette de taille 8 x 5 (8 lignes et 5 colonnes). Le carré pimenté est en position (1, 1). La personne qui croque en premier dans la tablette est dénommée « joueur 1 ».



Le joueur 1 choisit le carré (3 , 5). — Le joueur 2 choisit le carré (4 , 2). — Le joueur 1 choisit le carré (1 , 7). — Le joueur 2 choisit le carré (2 , 4).

On se demande si l'un des joueurs peut forcer la victoire avec une stratégie gagnante, c'est-à-dire si l'un des joueurs, avant même de commencer à croquer dans la tablette, peut être sûr de gagner quels que soient les choix de son adversaire.

Partie A – Quelques cas particuliers

1. Existe-t-il une stratégie gagnante pour le joueur 1 avec une tablette de taille 1 x 1 (tablette avec un seul carré) ?

2. Qu'en est-il pour une tablette à une seule ligne ? à une seule colonne ?

Partie B – Cas d'une tablette de chocolat carrée

On veut montrer dans cette partie que, dans le cas d'une tablette carrée, le joueur 1 peut forcer la victoire.

1. Donner une stratégie gagnante pour le joueur 1 dans le cas d'une tablette carrée 2 x 2.

2. Donner une stratégie gagnante pour le joueur 1 dans le cas d'une tablette carrée 3 x 3.

3. Élaborer une stratégie gagnante pour le joueur 1 dans le cas d'une tablette de chocolat carrée n x n où n est un nombre entier quelconque supérieur ou égal à 2.

Partie C – Cas général

On considère une tablette avec n lignes et p colonnes, n et p étant des nombres entiers supérieurs ou égaux à 2.

Montrer qu'il n'existe pas de stratégie gagnante pour le joueur 2. On pourra raisonner par l'absurde en supposant que le joueur 2 peut forcer la victoire et envisager que le joueur 1 mange le carré (p, n) au premier tour de jeu.

Exercice 2 Clés binaires

La simulation de nombres aléatoires est un enjeu fondamental de la recherche scientifique et notamment informatique. Une question importante se pose alors : étant donnée une série de nombres, comment vérifier que celle-ci est aléatoire, c'est-à-dire que chacun des nombres qui la composent a été choisi au hasard ? Un ordinateur fonctionne avec des bits qui ne peuvent prendre que deux valeurs 0 et 1. Ainsi si l'on souhaite générer un nombre aléatoire, il faut renvoyer soit 0, soit 1, chacun avec une probabilité de 0,5.

Partie A – Préliminaires

1. Combien de clés de 91 bits (c'est-à-dire de suites de 91 chiffres tous égaux à 0 ou à 1) existe-t-il ?

2. On considère l'algorithme ci-contre dans lequel la notation $cle[k]$ désigne le $k^{\text{ième}}$ élément de la liste *cle.*

Que contient la variable c à la fin de l'exécution de cet algorithme ?

```
c ← 0
Pour k allant de 1 à 91 :
  | Si cle[k] = 1 alors :
  | | c ← c + 1
  | Fin Si
Fin Pour
c ← c/91
```

Partie B – Une clé donnée est-elle aléatoire ?

Dans cette partie, on suppose qu'on dispose d'un logiciel de cryptographie capable de générer une clé de 91 bits de manière aléatoire pour protéger des données personnelles.
Aline a utilisé ce logiciel mais elle ne se rappelle plus de sa clé. Elle appelle le Service Après Vente et tombe sur Boris. Ce dernier, un brin facétieux, lui en donne quatre et lui demande de retrouver la bonne (une seule a été générée de manière aléatoire par le logiciel, les trois autres ont été inventées par Boris).

Clé 1 : 1100 1100 1100 1100 1100 1100 1100 1100 1100 1100 1100 1100 1100 1100 1100 1100 1100 1100 1100 1100 1100 1100 110

Clé 2 : 1101 1001 0111 1010 1001 0111 0101 1000 0111 1100 1110 0100 0110 0000 0000 1011 0100 0100 1010 0010 1110 0000 000

Clé 3 : 1101 1010 1001 1011 0111 0101 1100 1000 1011 0100 1011 1001 0110 0110 0010 1101 0101 0101 0010 0100 1100 1010 010

Clé 4 : 1010 0101 1101 0001 1011 1110 1111 0111 0010 1101 0000 1110 0111 1101 1100 0010 1110 0011 1111 0111 1101 1111 011

1. Aline décide de relever le défi de Boris et élimine immédiatement une des quatre clés. Selon vous laquelle et pourquoi ?

2. Ne parvenant pas, sur des critères simples et logiques, à en éliminer une autre, elle décide de faire appel à ses connaissances mathématiques pour trouver la bonne clé de manière rigoureuse.

a) Elle s'intéresse, pour chacune des trois clés restantes, au nombre de bits qui valent 1. Elle parvient alors à en éliminer une deuxième. Laquelle et pourquoi ?

b) Pour départager les deux clés restantes, Aline s'intéresse alors, pour chacune des deux clés, au nombre de bits différents du précédent. Cela lui permet d'éliminer une troisième clé (et donc de trouver celle qu'elle pense être la bonne). Laquelle et pourquoi ?

3. Après avoir crié victoire, elle réalise que la première clé qu'elle avait éliminée résiste aux deux tests de la question précédente. Elle trouve alors un troisième test permettant de l'éliminer (test réussi par la bonne clé). Quel pourrait être, à votre avis, un tel test ?

4. Proposer un algorithme qui effectue le test de la question **2. b**), c'est-à-dire qui, lorsqu'on lui rentre une clé de 91 bits, calcule le nombre de bits différents du précédent. On pourra s'inspirer, pour les instructions, de l'algorithme donné en préliminaires.

CORRECTION OLYMPIADES

EXERCICES ACADÉMIQUES

BESANÇON 2018

Exercice 1 : Un jeu à croquer

Il s'agit dans cet exercice d'étudier une variante du jeu de Chomp[1].

Partie A : Quelques cas particuliers

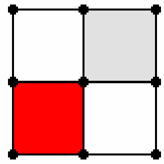
1. Si la tablette est de taille 1×1, le joueur « se retrouve obligé de manger le carré pimenté » selon les termes de l'énoncé et perd la partie. Il s'agit précisément de la situation à laquelle chaque joueur va tenter de contraindre son adversaire.

2. Dans le cas d'une tablette à une seule ligne, le joueur mange tous les carrés situés à droite du carré pimenté. Dans le cas d'une tablette à une seule colonne, le joueur mange tous les carrés situés au dessus du carré pimenté. Son adversaire se retrouve alors dans la situation de la question **1** et perd la partie.

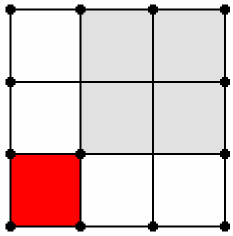
Il existe une stratégie gagnante dans le cas d'une tablette à une seule ligne ou à une seule colonne.

[1] Consulter : https://fr.wikipedia.org/wiki/Chomp_(jeu) .

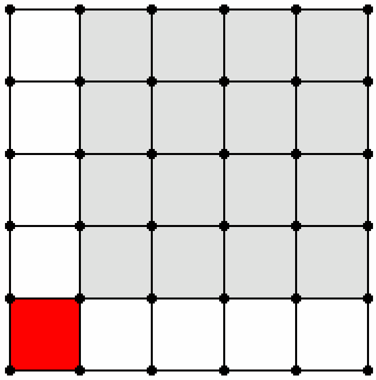
Partie B : Cas d'une tablette de chocolat carrée



1. Dans le cas d'une tablette de taille 2×2, le joueur 1 mange le carré $(2,\ 2)$, en grisé sur la figure ci-contre. La configuration « en L » obtenue est gagnante : le joueur 2 ne peut manger que l'un ou l'autre des carrés $(1,\ 2)$ ou $(2,\ 1)$, en blanc sur la figure, et le joueur 2 hérite d'une tablette à une seule ligne ou à une seule colonne, pour lesquelles une stratégie gagnante existe.



Dans le cas d'une tablette de taille 3×3, le joueur 1 mange encore le carré $(2,\ 2)$, en grisé sur la figure ci-contre. Le joueur 2 ne peut manger deux carrés blancs, sinon il laisserait à son adversaire une tablette à une ligne ou à une colonne. Donc, il n'en mange qu'un, $(3,\ 1)$ ou $(1,\ 3)$. Le joueur 1 mange alors celui des deux carrés restants, et la configuration laissée à son adversaire est celle, perdante, du cas précédent.



Dans le cas général, le joueur 1 mange toujours le carré $(2,\ 2)$, en grisé sur la figure ci-contre. Le joueur 2 ne peut manger tous les carrés blancs de la ligne 1 ou de la colonne 1, sous peine de laisser à son adversaire une tablette à une seule ligne ou à une seule colonne. Ce joueur va donc manger un certain nombre de carrés, mais pas tous, soit sur la ligne 1 soit sur la colonne 1. Le joueur 1 mange le même nombre de carrés, respectivement soit sur la colonne 1, soit sur la ligne 1, de façon à rétablir une symétrie par rapport à la première diagonale du carré. Au bout d'un nombre fini de coups, la situation dévolue au joueur 2 par le joueur 1 sera identique à celle « en L » de la question **1**, gagnante pour le joueur 1.

Partie C : Cas général

Supposons qu'il existe une stratégie gagnante pour le joueur 2. Le joueur 1 mange le carré $(p,\ n)$, c'est-à-dire le dernier carré le plus haut et le plus à droite.

Le joueur 2 enclenche sa stratégie gagnante en mangeant le carré $(x,\ y)$ qui lui convient.

Mais dans ce cas, le joueur 1 pourrait manger lui-même dès son premier coup ce carré $(x,\ y)$ et usurper la stratégie gagnante du joueur 2, qui, de ce fait, perdrait la partie.

Le deuxième joueur ne peut pas posséder de stratégie gagnante.

Exercice 2 : Clés binaires

Partie A : Préliminaires

1. Il existe 2^{91} clés différentes, soit un nombre compris entre $2{,}4\times 10^{27}$ et $2{,}5\times 10^{27}$

2. La variable c contient la proportion de « 1 » parmi la suite des 91 chiffres de la clé.

Partie B : Une clé donnée est-elle aléatoire ?

1. Aline élimine d'emblée la clé 1. La clé 1 est une suite de chiffres périodique de période 4. Or, un phénomène aléatoire, imprévisible, n'a pas de période.

2.a. En cas de clé aléatoire, le nombre d'occurrences d'un « 1 » dans la clé est une variable aléatoire qui suit la loi binomiale $B\left(91\ ;\ \frac{1}{2}\right)$.

Utilisons un outil d'analyse d'un résultat d'échantillonnage en construisant un intervalle de fluctuation au seuil 0,95 dans lequel devrait se trouver la fréquence observée des occurrences du « 1 ».

Nous proposons ci-dessous deux méthodes.

> ***Première méthode : l'outil d'échantillonnage vu en classe de Seconde***
>
> *« Pour des échantillons de taille $n > 25$ et des proportions p du caractère comprises entre 0,2 et 0,8 : si f désigne la fréquence du caractère dans l'échantillon , f appartient à l'intervalle $\left[p-\frac{1}{\sqrt{n}}\ ;\ p+\frac{1}{\sqrt{n}}\right]$ avec une probabilité d'au moins 0,95. »*

Selon cet outil, un intervalle de fluctuation de la fréquence autour de la valeur $\frac{1}{2}$ est ici l'intervalle $\left[0{,}5-\frac{1}{\sqrt{91}}\ ;\ 0{,}5+\frac{1}{\sqrt{91}}\right]$, inclus dans l'intervalle $[0{,}395\ ;\ 0{,}605]$

Le nombre d'occurrences du « 1 » dans les clés 2, 3 et 4 est, respectivement, 40, 46 et 58.
La proportion de « 1 » dans chaque échantillon de 91 chiffres est, respectivement, égale à 0,44 ; 0,51 et 0,64 à 0,01 près. La proportion de « 1 » de la clé numéro 4 est en dehors de cet intervalle de fluctuation. On peut, pour cette raison, éliminer cette clé.

> ***Deuxième méthode : l'outil d'échantillonnage vu en classe de Première S***
>
> *« Exploiter l'intervalle de fluctuation à un seuil donné, déterminé à l'aide de la loi binomiale, pour rejeter ou non une hypothèse sur une proportion. (...)*
>
> *L'intervalle de fluctuation peut être déterminé à l'aide d'un tableur ou d'un algorithme.»*

Construisons, à l'aide d'un tableur, la loi de probabilité d'une variable aléatoire X qui suit la loi $B\left(91\ ;\ \dfrac{1}{2}\right)$. Pour tout entier k tel que $0 \le k \le 91$, $P(X=k) = \dbinom{91}{k} \times \left(\dfrac{1}{2}\right)^{91}$.

Ces probabilités sont listées en colonne **probas**.

La colonne **cumul** est la liste des probabilités cumulées. Elle donne, pour tout entier k, la probabilité $P(X \le k)$.

Repérons la valeur pour laquelle le seuil 0,025 est atteint. Il s'agit de la valeur 36.

Repérons de même la valeur pour laquelle le seuil 0,975 est atteint. Il s'agit de la valeur 55.

La probabilité que le nombre d'occurrences du « 1 » prenne une valeur comprise au sens large entre 36 et 55 est au moins égale à 0,95.

Le nombre d'occurrences du « 1 » dans la clé 4 est en dehors de cette fourchette. On peut, pour cette raison, éliminer cette clé.

En termes de fréquences, la probabilité que la fréquence des occurrences du « 1 » soit entre $\dfrac{36}{91}$ et $\dfrac{55}{91}$ est au moins égale à 0,95.

L'intervalle de fluctuation construit par cette méthode est $\left[\dfrac{36}{91}\ ;\ \dfrac{55}{91}\right]$, inclus dans $[0{,}396\ ;\ 0{,}605]$. Il n'y a pas de différence significative avec l'intervalle de fluctuation obtenu par la méthode de la classe de Seconde.

2.b et 4. Le nombre de bits différents du précédent suit la loi binomiale $B\left(90\ ;\ \dfrac{1}{2}\right)$. Un intervalle de fluctuation de la fréquence autour de la valeur $\dfrac{1}{2}$ est ici l'intervalle $\left[0{,}5-\dfrac{1}{\sqrt{90}}\ ;\ 0{,}5+\dfrac{1}{\sqrt{90}}\right]$, inclus dans l'intervalle $[0{,}395\ ;\ 0{,}606]$.

Les listes **aa**, **bb**, **cc** représentent ci-contre, respectivement, les clés 2, 3 et 4.

La fréquence du changement de chiffre dans la clé numéro 3 (liste **bb**) est à l'extérieur de cet intervalle. On peut, pour cette raison, éliminer cette clé.

	A valeurs	B probas	C cumul	D
=	=seq(n,n,0,91)	=seq(ncr(91,k)/2^91,k,0,91)	=cumulativesum(probas)	
30	29.	0.000196	0.000353	
31	30.	0.000406	0.000758	
32	31.	0.000798	0.001556	
33	32.	0.001496	0.003053	
34	33.	0.002675	0.005728	
35	34.	0.004564	0.010292	
36	35.	0.007433	0.017725	
37	36.	0.011562	0.029287	
38	37.	0.017187	0.046473	
39	38.	0.024423	0.070897	
40	39.	0.033191	0.104087	

37

	A valeurs	B probas	C cumul	D
=	=seq(n,n,0,91)	=seq(ncr(91,k)/2^91,k,0,91)	=cumulativesum(probas)	
49	48.	0.07281	0.735199	
50	49.	0.063895	0.799094	
51	50.	0.053672	0.852765	
52	51.	0.043148	0.895913	
53	52.	0.033191	0.929103	
54	53.	0.024423	0.953527	
55	54.	0.017187	0.970713	
56	55.	0.011562	0.982275	
57	56.	0.007433	0.989708	
58	57.	0.004564	0.994272	
59	58.	0.002675	0.996947	

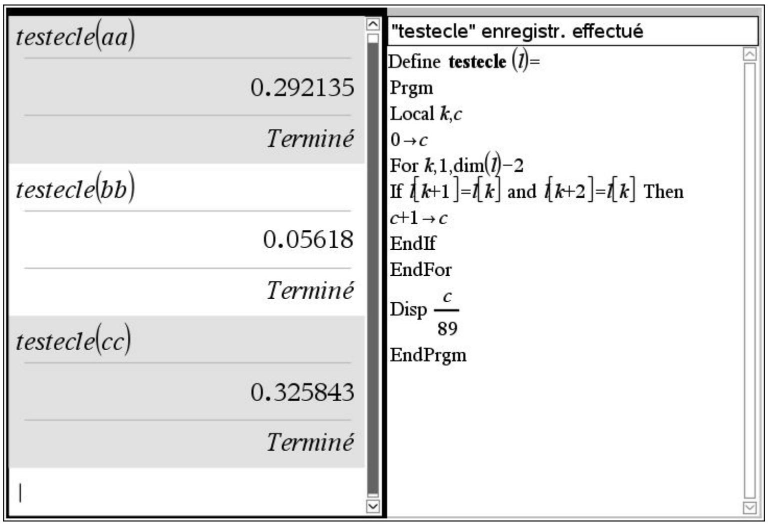
56

```
testecle(aa)
                0.477778
                Terminé
testecle(bb)
                0.677778
                Terminé
testecle(cc)
                0.444444
                Terminé
```

```
testecle                                 4/8
Define testecle(l)=
Prgm
Local k,c
0→c
For k,1,dim(l)−1
If l[k+1]≠l[k] Then
c+1→c
EndIf
EndFor
Disp c/90
EndPrgm
```

3. Une possibilité de test qui éliminerait la clé 1 serait par exemple de déterminer la fréquence des séquences de trois chiffres consécutifs identiques 000 ou 111.

Le programme précédent a été modifié en conséquence.



La probabilité d'obtenir trois chiffres consécutifs identiques est égale à $\frac{1}{4}$ (il faut, dans une séquence de trois chiffres, que les deuxième et troisième chiffres soient égaux au premier).

La fréquence des occurrences dans un échantillon de 89 séquences aléatoires de trois chiffres devrait donc se situer dans l'intervalle $\left[0{,}25-\frac{1}{\sqrt{89}}\ ;\ 0{,}25+\frac{1}{\sqrt{89}}\right]$.

Les clés 2 et 4 réussissent ce test, mais pas la clé 3 (liste **bb**).

La clé 1 ne réussit pas non plus ce test car on n'y observe jamais trois chiffres consécutifs identiques.

En conclusion, seule la clé 2 résiste aux trois tests. On note qu'un test donné permet d'éliminer une clé, mais ne garantit en aucune manière qu'une clé résistante est bien une clé aléatoire. Un tel test permet d'éliminer mais non de sélectionner.

Commentaire

Pourquoi le choix d'une « clé de 91 bits » dans cet exercice ? Consultons à ce sujet le site :
https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/

Voici ce qu'il nous dit :

> *« La force d'un mot de passe peut être estimée par comparaison avec les techniques cryptographiques. Une taille de clé cryptographique de 64 bits est aujourd'hui considérée comme non sûre car les capacités de calcul modernes permettent de retrouver cette clé en énumérant toutes les clés possibles. Or une telle clé peut être vue comme un mot de passe de 64 caractères où les seuls caractères possibles sont 0 et 1. La « force » d'un tel mot de passe est donc 2^{64}.*
>
> *Les règles édictées par l'ANSSI en matière de mécanismes cryptographiques imposent par exemple une taille de clé minimale de 100 bits. Il est même recommandé une taille de clé de 128 bits pour des clés dont l'usage présumé est de longue durée. Il est par ailleurs communément admis que des tailles de clé de 80 bits sont désormais exposées à des attaques utilisant des moyens techniques conséquents. »*

Une clé de 91 bits est donc une clé de force « à peine moyenne ».