Maths 701 – Examen final

Emmanuel Beffara Nicolas Gast Benjamin Wack

8 janvier 2021

Le barème est donné à titre indicatif.

Exercise 1 Arithmétique modulaire – 3pts

1. Calculer 4^{126} mod 65.
2. 4 est-il inversible dans $\mathbb{Z}/(65\mathbb{Z})$? Si oui calculer son inverse.
3. $\mathbb{Z}/(65\mathbb{Z})$ est-il un corps ?

Exercise 2 Code correcteurs d'erreur – 6pts

Le code de Reed-Muller RM(1,3) est un code correcteur conçu pour encoder des messages de 4 bits en un mot de 8 bits. Il est construit de la façon suivante : Pour un message $u = (u_0, u_1, u_2, u_3)$ que l'on veut encoder, on défini la fonction $p_u(X_1, X_2, X_3) = u_0 + u_1X_1 + u_2X_2 + u_3X_3 \bmod 2$. Le code associé à u est le mot de huit lettres : $C(u) = (p_u(0,0,0), p_u(0,0,1), p_u(0,1,0), p_u(0,1,1), p_u(1,0,0), p_u(1,0,1), p_u(1,1,0), p_u(1,1,1))$.

1. Expliquer pourquoi $C(0,0,0,0) = (0,0,0,0,0,0,0,0)$, $C(1,0,0,0) = (1,1,1,1,1,1,1,1)$ et $C(0,1,0) = (0,0,0,0,1,1,1,1)$.
2. Exprimer $C(u)$ en fonction de $u_0, \dots, u_3$ et calculer $C(1,0,1,0)$.
3. Ce code est-il un code linéaire ? Si oui en donner une matrice génératrice.
4. Quelle est la distance minimale du code ?
5. Quelle est le rendement de ce code ? Comparer à la borne de Singleton.
6. Combien d'erreur de code peut-il détecter ? Corriger ?

Exercise 3 Probabilités : encore des tests ! – 5 pts

Un nouveau test est mis sur le marché. Si vous avez le virus, le test est positif dans 99% des cas. Si vous ne l'avez pas, il est négatif dans 90% des cas. On suppose que 5% des gens ont le virus.

1. On teste une personne au hasard.
   a) Quelle est la probabilité que le test soit positif ?
   b) Sachant que le test est positif, quelle est la probabilité que la personne ait le virus ?
   c) Sachant que le test est négatif, quelle est la probabilité que la personne n'ait pas le virus ?
2. Au sorti d'une soirée de nouvel an ayant regroupé 10000 personnes, la gendarmerie teste tout le monde et 3000 personnes ont un test positif.
   a) Pouvez vous estimer le taux de personnes réellement positives ?
   b) On teste une personne au hasard. Sachant que son test est positif, quelle est la probabilité que cette personne ait le virus ?

Exercise 4 Relations d'ordre – 6 pts

L'hydre des Alpes est une espèce de serpents à plusieurs têtes qui a une particularité : si on coupe une tête d'une hydre mais qu'il lui en reste encore au moins une, l'hydre peut se reproduire instantanément en autant d'individus qu'elle le souhaite, avec autant de têtes chacune. Par exemple, couper une tête d'une hydre à 4 têtes peut engendrer 23 hydres à 3 têtes. Si elle n'a qu'une tête et qu'on a lui coupe, elle meurt.

Hercule est chargé d'éliminer une invasion d'hydres des Alpes en coupant des têtes. On cherche à savoir s'il peut gagner ce combat. À chaque coup d'épée, il coupe une tête d'une hydre, puis celle-ci se reproduit autant de fois qu'elle le veut, si elle le peut.

On suppose d'abord qu'il n'y a que des hydres à 1 ou 2 têtes. On représente un combat comme une suite (a_n, b_n) où a_n et b_n représentent le nombre d'hydres à 1 ou 2 têtes respectivement, après n coups d'épée. La population initiale est (a_0, b_0), le combat est gagné après n coups si on $a_n = b_n = 0$, la suite s'arrête dans ce cas-là.

1. Soit n un entier tel que $(a_n, b_n) \neq (0, 0)$ (le combat n'est pas fini). Donner une relation entre (a_n, b_n) et (a_{n+1}, b_{n+1}) qui traduise les règles du combat.
2. Définir une relation $\preccurlyeq$ sur $\mathbb{N}^2$ qui soit une relation d'ordre bien fondée et pour laquelle la suite (a_n, b_n) est strictement décroissante. On justifiera bien que la relation est un ordre et qu'elle est bien fondée.
3. Montrer qu'Hercule est certain de gagner le combat.
4. Montrer qu'il n'y a pas de borne supérieure à la durée du combat (même si tous finissent).
5. Que se passe-t-il s'il y a aussi des hydres à 3 têtes ? Et s'il y a des hydres avec n'importe quel nombre de têtes ?

Rappels

La formule de Singleton est : $d_{\min}(C) \leq n(r-1)+1$ où n est la longuer d'un mot de code et r est le rendement.

Une matrice de contrôle d'un code linéaire C est une matrice telle que $x \in C$ ssi $Hx = 0$.

Règle de Bayes : $\mathrm{P(A|B) = P(B|A)P(A)/P(B)}$.

Intervales de confiance à 95% : Soit $X_1 \dots X_n$ sont des variables de Bernoulli de moyenne μ et $\bar{\mu} = \sum_{i=1}^{n} X_i/n$, alors $P(\mu \in [\bar{\mu} - 1/\sqrt{n}, \bar{\mu} + 1/\sqrt{n}]) \geq 95\%$.