I 23. Mathématiques discrètes — Examen

Vendredi 25 juin 2010 [S111, 13 :30 - 15 :30]

Les documents sont interdits. La calculatrice est autorisée. Le barème est approximatif et il est donné à titre indicatif. Durée : 2h00.

Exercice 1. [4pts] On définit une relation binaire de divisibilité notée | sur l'ensemble $\mathbf{Z}$ des entiers relatifs par $a|b$ si et seulement s'il existe un entier $c \in \mathbf{Z}$ tel que

$$ac = b.$$

Démontrez qu'il s'agit d'une relation d'ordre. Montrez qu'il s'agit d'une relation d'ordre partiel. Quelle est le plus grand élément (s'il existe) pour cette relation ?

Exercice 2. [6pts] Un mot de passe est constitué de 6 caractères. Ces caractères sont à choisir parmi les 26 lettres $\{a, b, \ldots, z\}$ (on ne fait pas le distingo entre minuscules et majuscules) et les 10 chiffres $\{0, 1, \ldots, 9\}$. Combien de mots de passe peut-on constituer :

(1) si le choix des caractères est totalement arbitraire ?

(2) si tous les caractères sont des lettres ?

(3) s'il faut au moins une lettre ?

(4) s'il faut au moins une lettre et un chiffre ?

Sachant qu'un ordinateur est capable de tenter 3.2×10^9 mots de passe par seconde pour faire intrusion dans un système protégé, combien de temps faudrait-il dans le pire des cas pour trouver le bon ? Quelle longueur devrait faire un mot de passe pour protéger efficacement le système ? Expliquez.

Exercice 3. [2pts] Dressez les tables d'addition et de multiplication de $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$. On considère un circuit logique binaire qui comporte 8 entrées et une seule sortie, autrement dit une application f de $\mathbf{F}_2^8$ dans $\mathbf{F}_2$. Quel est le cardinal de $\mathbf{F}_2^8$? Combien de circuits (applications) distincts peut-on imaginer ? Est-il envisageable de concevoir réellement tous ces circuits ? Justifiez.

Exercice 4. [3pts] Montrez que l'application $f : \mathbf{N} \to \mathbf{Z}$ définie par

$$f(n) := \begin{cases} k & \text{si } n \text{ est pair, i.e. } \exists k \in \mathbf{N} \mid n = 2k. \\ -(k+1) & \text{si } n \text{ est impair, i.e. } \exists k \in \mathbf{N} \mid n = 2k+1. \end{cases}$$

est une bijection. Pour cela montrez qu'elle est injective puis surjective.

Exercice 5. [4pts] Considérons la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 7 & 10 & 2 & 9 & 5 & 4 & 6 & 8 & 1 \end{pmatrix}$$

comme élément du groupe symétrique $\mathfrak{S}_{10}$. Décomposer la permutation σ en produit de cycles à supports disjoints. Déterminer l'ordre et la signature de σ puis déterminer σ^8.

Exercice 6. [4pts] On considère la matrice de contrôle H d'un code linéaire C de longueur 4 sur $\mathbf{F}_3$.

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

En notant $u = (x, y, z, t)$ un vecteur de $\mathbf{F}_3^4$, écrivez les deux équations que doivent satisfaire x, y, z et t pour que u appartienne au code C (i.e. $H({}^t u) = \binom{0}{0}$, où ${}^t u$ désigne le vecteur u en colonne). Enumérez tous les quadruplets de $\mathbf{F}_3^4$ qui satisfont ces deux équations.