I 23. Mathématiques pour l'informatique — Examen

Lundi 16 mai 2010 [W'210, 09h00 - 11h30]

Les documents sont interdits. La calculatrice est autorisée. Le barème est basé sur la résolution de 5 des 6 exercices (1/2 heure par exercice environ) notés sur 4 points chacun approximativement. Toutes les réponses doivent être *justifiées* ! Durée : 2h30.

Exercice 1. [4pts] Les fonctions $f : E \to F$ suivantes sont-elles : injectives, surjectives, bijectives ?

(1) E est l'ensemble des français, $F := \{bleu, marron, vert, noir\}$ et f est l'application qui, à un français, associe la couleur de ses yeux ;

(2) $E := \mathbf{Z}$, $F := \mathbf{N}$ et $f(x) := |x|$;

(3) $E := \mathbf{R}_+ \setminus \{0\}$, $F := \mathbf{R}_+ \setminus \{0\}$ et $f(x) := 1/x$;

(4) E est un ensemble quelconque de cardinal n et F de cardinal m avec $n < m$.

(5) E est un ensemble quelconque et $F := \mathcal{P}(E)$ avec $f(x) := \{x\}$.

Exercice 2. [4pts] Un mot de passe est constitué de 6 caractères exactement. 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. [4pts] On définit une relation binaire $\mathcal{R}$ sur l'ensemble $E^{\mathbf{N}}$ des suites d'éléments d'un ensemble E :

$$(u_n) \quad R\,(v_n) \iff \exists M \in \mathbf{N},\ \forall n \geq M,\ u_n = v_n.$$

Autrement dit, deux suites sont en relation si leurs termes sont égaux à partir d'un certain rang M. Démontrez qu'il s'agit d'une relation d'équivalence.

Soit $E := \{a, b, c\}$. On rappelle que la relation d'inclusion sur l'ensemble $\mathcal{P}(E) \setminus \{\varnothing\}$ est une relation d'ordre. Ecrivez la matrice binaire de cette relation. Montrez qu'il s'agit d'une relation d'ordre partiel. Quels sont les éléments minimaux pour cette relation ? Comment se traduit le fait qu'il s'agit d'une relation d'ordre partiel dans la matrice ?

Exercice 4. [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^{2011}.

Exercice 5. [4pts] Calculez les carrés de chacun des éléments de $\mathbf{Z}/8\mathbf{Z}$. En déduire l'ensemble des solutions dans $\mathbf{Z}/8\mathbf{Z}$ des équations suivantes :

$$X^2 - 3 = 0$$

$$X^2 - 1 = 0.$$

Trouvez toutes les solutions entières de l'équation diophantienne

$$62u + 105v = 1.$$

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

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

Déterminez la matrice génératrice G de ce code. 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. Calculez la capacité de correction de ce code.