IFT6170 Devoir 1

à rendre au début du cours le mercredi 1 octobre 1997

Polynôme Irréductible [4 points]

Considérez l'ensemble des nombres modulo 17 étiquetés ainsi:

$$\{\mathbf{0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F,G}\},$$

les symboles "**A,B,C,D,E,F,G**" repésentant les nombres 10,11,12,13,14,15,16. On utilise sur ces nombres les opérations d'addition, soustraction et multiplication modulo 17. Par exemple $F + 1 \equiv G \pmod{17}$ et $3 * A \equiv D \pmod{17}$. On considère les polynômes sur $\mathcal{F}_{17}$ comme une suite finie de symboles parmis l'ensemble ci-haut. Par exemple ($1\ 0\ 1\ 0\ 0\ 0\ A\ B\ C\ D\ E\ F\ G$) correspond à

$$1x^{12} + 1x^{10} + Ax^6 + Bx^5 + Cx^4 + Dx^3 + Ex^2 + Fx + G.$$

Donnez un polynôme **irréductible** sur $\mathcal{F}_{17}$ de **degré 23** contenant votre date de naissance de façon consécutive dans sa représentation ainsi qu'une preuve de ce fait. Par exemple pour 17-02-62

$$(1\ 7\ 0\ 2\ 6\ 2\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ A\ 5\ 4\ 2\ 1\ F\ 7)$$

pourrait être un tel polynôme contenant ma date de naissance. (Je n'ai pas vérifié s'il est irréductible.)

Donnez également un élément primitif du corps fini engendré par votre polynôme. Pour vous aider, sachez que $17^{23} - 1 = 2^4 * 47 * 2655261821922809016297748\,1$. Vous pouvez utiliser les moyens (ordinateurs, logiciels, etc) que vous voudrez pour obtenir votre réponse.

Dual des codes de Hamming [4 points]

Les codes de Hamming forment une famille infinie $\{\mathcal{H}_m\}_{m>0}$ de codes linéaires binaires ayant les paramètres $[2^m - 1, 2^m - m - 1, 3]$. Donnez les paramètres $[n_m, k_m, d_m]$ des codes $\{\mathcal{H}_m^\top\}_{m>0}$ duaux des codes de Hamming en fonction de m. Ces codes sont-ils parfaits? Prouvez vos réponses.

Codes ISBN [4+1 points]

Le code ISBN que l'on trouve sur les livres est un code linéaire sur $\mathcal{F}_{11}$ où l'on utilise l'alphabet

$$\{\mathbf{0,1,2,3,4,5,6,7,8,9,X}\},$$

le symbole "**X**" repésentant le nombre 10. Les paramètres de ce code sont $[10, k, d]$. Utilisez un certain nombre de livres (donnez les titres et numéro ISBN des livres utilisés) afin de déterminer une matrice génératrice pour ce code, sous forme systématique. Donnez les valeurs de k et d pour ce code. Démontrez finalement que ce code a la propriété supplémentaire que si l'on permute deux symboles différents d'un mot de code, le mot résultant n'est plus un mot de code. Justifiez vos réponses.

Un point supplémentaire à celui ou celle qui trouvera un plus petit ensemble de livres (je veux les titres et les codes ISBN) dont les codes ISBN sont linéairement dépendants...

Canaux de transmission [total 4 points]

–canal majorité [1.5 points]

Considérez le canal suivant:

$$MAJ_\epsilon^k(x) = \text{maj}\ \{\overbrace{BS_\epsilon(x), BS_\epsilon(x), ..., BS_\epsilon(x)}^{2k-1}\}.$$

C'est-à-dire que $MAJ_\epsilon^k(x)$ retourne le bit majoritaire parmis $2k - 1$ exécutions indépendantes de $BS_\epsilon(x)$. Trouvez un ϵ_k tel que

$$MAJ_\epsilon^k(x) = BS_{\epsilon_k}(x).$$

Montrez que

$$\lim_{k\to\infty} \epsilon_k = 0.$$

–canal xor [1.5 points]

Considérez le canal suivant:

$$XOR_\epsilon^k(x) = \overbrace{BS_\epsilon(x) \oplus BS_\epsilon(x) \oplus ... \oplus BS_\epsilon(x)}^{2k-1}.$$

C'est-à-dire que $XOR_\epsilon^k(x)$ retourne le ou–exclusif de $2k-1$ exécutions indépendantes de $BS_\epsilon(x)$. Trouvez un ϵ_k tel que

$$XOR_\epsilon^k(x) = BS_{\epsilon_k}(x).$$

Montrez que

$$\lim_{k \to \infty} \epsilon_k = 1/2.$$

–canal mixte [1 point]

Soient $U = BS_\epsilon(x)$ et $V = BS_\epsilon(x)$ deux échantillons indépendants obtenus à travers un canal bruyant de probabilité d'erreur ϵ. Considérez le canal suivant:

$$MIX_\epsilon(x) = \begin{cases} b & \text{si } U = V = b \\ \varepsilon & \text{si } U \neq V \end{cases}.$$

C'est-à-dire que $MIX_\epsilon(x)$ retourne le bit commun obtenu de deux exécutions indépendantes de $BS_\epsilon(x)$, mais la chaîne nulle si ces deux exécutions ne donne pas la même réponse. Trouvez des α, β tels que

$$MIX_\epsilon(x) = EF_\alpha(BS_\beta(x)).$$