IFT6170 Devoir 5

à rendre avant la tombée de la nuit le vendredi 19 décembre 1997

Codes BCH sont Alternants [8 points]

Montrez de façon générale que les codes BCH sont des codes alternants. C'est-à-dire que les mots de codes peuvent être obtenus par la restriction sur $\mathcal{F}_q$ des mots d'un code $\mathrm{RSG}(\alpha, v)$ sur $\mathcal{F}_{q^m}$.

Prenez le code BCH binaire de longueur 23 et de distance de design 3. Un polynôme générateur de ce code est $M^{(1)}(x)$. La dimension de ce code est de 12 et sa distance minimale réelle est de 7. En utilisant votre construction générale donnez le code $\mathrm{RSG}(\alpha, v)$ dont ce code BCH est la restriction sur $\mathcal{F}_2$.

Calculez le syndrome S du patron d'erreur (01000000000000000000000). Trouvez les polynômes σ et ω associés à ce patron. Vérifiez que $\omega(x) \equiv \sigma(x)S(x) \pmod{x^r}$.

Codes Intersectants [8 points]

1. Si on étend la définition de codes intersectants à tous les corps $\mathcal{F}_q$ il est possible sur certains corps de construire explicitement de tels codes. Montrez que pour des $q > 2$ assez grand certains codes Reed-Solomon sont intersectants sur $\mathcal{F}_q$.
   suggestion: Tout code $[n, k, d]$ pour d assez grand est intersectant.
2. Pourquoi est-ce que la **suggestion** du point 1 ne nous aide pas à montrer directement qu'il existe une bonne famille de codes intersectants sur $\mathcal{F}_2$.
3. Montrez que la concaténation de deux codes intersectants est également un code intersectant.
4. Expliquez comment combiner les points précédents et ce que l'on connais déja sur les codes intersectants pour obtenir une construction efficace probabiliste d'une bonne famille de codes binaires (vérifiablement) intersectants. Donnez de façon explicite le lien entre k et n des codes binaires ainsi obtenus.